

INTRODUCCIÓ A LA SEGURETAT

Àlex Arjona López
1r ASIXC
Institut Carles Vallbona
Hector Pascual Comín

ÍNDEX

| | |
|---|----------|
| 1. DIFERÈNCIES ENTRE ANTIVIRUS, FIREWALL I SPYWARE..... | 2 |
| 1.1: Què és un antivirus?..... | 2 |
| 1.2: Què es un firewall?..... | 2 |
| 1.3: Què és un spyware?..... | 2 |
| 1.4: Diferències:..... | 2 |
| 2. CÒPIES DE SEURETAT:..... | 3 |
| 2.1: Què és una còpia de seguretat?..... | 3 |
| 2.2: Tipus de còpies de seguretat:..... | 3 |
| 2.3: Còpia de seguretat completa:..... | 3 |
| 2.4: Avantatges de les còpies de seguretat completes:..... | 3 |
| 2.5: Desavantatges de les còpies de seguretat completes:..... | 3 |
| 2.6: Còpia de seguretat incremental:..... | 4 |
| 2.7: Avantatges de les còpies de seguretat incrementals:..... | 4 |
| 2.8: Desavantatges de les còpies de seguretat incrementals:..... | 4 |
| 2.9: Còpia de seguretat diferencial:..... | 4 |
| 2.9.1: Avantatges de les còpies de seguretat diferencials:..... | 4 |
| 2.9.2: Desavantatges de les còpies de seguretat diferencials:..... | 5 |
| 2.9.3: Diferències clau:..... | 5 |
| 3. GESTIÓ DE DISCOS..... | 6 |
| 3.1: Què és una partició?..... | 6 |
| 3.2: Què son les particions primàries i les particions lògiques?..... | 6 |
| 4. PRINCIPALS SISTEMES D'ARXIU..... | 6 |
| 5. EINES DE GESTIÓ DE DISCS:..... | 7 |
| 6. CONCLUSIÓ..... | 7 |

1. DIFERÈNCIES ENTRE ANTIVIRUS, FIREWALL I SPYWARE

1.1: Què és un antivirus?

Un antivirus és un programa que s'utilitza per poder prevenir, detectar i eliminar virus informàtics que son maliciosos. Aquest actua escanejant els arxius de l'ordinador, a més de les aplicacions per tal de detectar intrusions no autoritzades, que en aquest cas, serien els virus diferents que existeixen.

1.2: Què es un firewall?

Un firewall és un programari de seguretat en la qual filtra i controla el trànsit de la xarxa entrant i sortint entre una xarxa privada i l'internet.

1.3: Què és un spyware?

Un spyware és un tipus de virus en la qual s'estableix en un dispositiu (ja sigui un PC, una tauleta, un mòbil... etc) sense que l'usuari es dongui compte que està infectat per un spyware. A més, al ser un tipus de virus que no es detecta amb facilitat, pot recollir dades de l'usuari com: contrasenyes, informació bancària... etc i aquests es poden fer servir per tal de vendre aquesta informació o intimidar a la persona afectada per l'spyware.

1.4: Diferències:

Les diferències que podem trobar en cada programa, observem que hi han diferències, com per exemple, l'antivirus el que fa és detectar, prevenir i eliminar programes maliciosos, com els virus o malware.

També, podem observar que el firewall actua com una barrera que controla i filtra el trànsit de la xarxa i aquesta permet o bloqueja connexions. Per últim, l' spyware, és un tipus de malware en la qual espia les activitats de l'usuari. Bàsicament, és una amenaça en la qual no és un sistema de protecció.

2. CÒPIES DE SEURETAT:

2.1: Què és una còpia de seguretat?

Les còpies de seguretat en els nostres sistemes operatius són essencials per tal de protegir la nostra informació davant de les possibles pèrdues de dades que poden ser causades o bé per errors de maquinari, atacs informàtics o errors que podem cometre nosaltres mateixos.

El fet de mantenir còpies de seguretat ens garanteix a nosaltres la continuïtat de la nostra activitat, ja que ens permet recuperar les dades originals en cas de que ens falli el nostre sistema operatiu.

2.2: Tipus de còpies de seguretat:

2.3: Còpia de seguretat completa:

Aquest tipus de còpies de seguretat, fan còpies de tots els fitxers i les dades del sistema (o també d'una ubicació) específica, independentment de si aquestes han canviat o no. A més, cada còpia completa és una còpia independent que conté totes les nostres dades.

2.4: Avantatges de les còpies de seguretat completes:

- **Restauració ràpida i senzilla:** Al ser una còpia completa de totes les nostres dades, podem restaurar aquelles dades que necessitem sense tenir que restaurar totes les dades d'altres còpies.
- **Simplicitat:** A més, és el tipus de còpia de seguretat més senzilla de gestionar, ja que no es depèn entre cap còpia.

2.5: Desavantatges de les còpies de seguretat completes:

- **Espai d'emmagatzematge:** Aquest tipus de còpies ocupen molt més espai que altres tipus de còpies, ja que es copien tots els nostres fitxers cada vegada que fem una còpia, independentment si les dades d'aquestes carpetes han canviat o no.

2.6: Còpia de seguretat incremental:

Aquest tipus de còpies fa una còpia només d'aquells fitxers que nosaltres ja hem modificat o aquells que hem creat des de l'última còpia de seguretat (ja sigui completa o incremental). Bàsicament, vol dir que cada còpia només inclou els canvis ja fets des de l'última còpia que vam generar, independentment sigui el tipus de còpia que hem realitzat anteriorment.

2.7: Avantatges de les còpies de seguretat incrementals:

- **Estalvi d'espai:** Aquest tipus de còpies, cada còpia que generem, ocupa menys espai ja que només s'inclouran en la còpia que generem aquells fitxers que hem creat o que hem modificat des de l'última còpia que vam generar.
- **Estalvi de temps:** A més, aquest tipus de còpies, és molt més ràpida que en comparació amb altres tipus de còpies, ja que aquesta s'executa només sobre aquells fitxers que hagin sigut canviats.

2.8: Desavantatges de les còpies de seguretat incrementals:

- **La restauració és molt lenta:** Per poder restaurar el nostre sistema operatiu, es requereix la còpia completa original i totes les còpies incrementals fins a l'últim punt de la restauració. En conclusió, aquests processos fan que el procés de restauració sigui més complex i llarg.

2.9: Còpia de seguretat diferencial:

Aquest tipus de còpia de seguretat realitza una còpia dels nostres fitxers que ja hem modificat anteriorment o aquells fitxers que s'han creat de nous des de l'última còpia completa més recent.

2.9.1: Avantatges de les còpies de seguretat diferencials:

- **La restauració dels arxius és més ràpid.** Nosaltres, al restaurar el sistema operatiu, necessitarem la còpia completa original dels arxius, a més de l'última còpia diferencial, fent que aquest procés resulta ser molt més senzill i molt més ràpid que amb les còpies incrementals.

2.9.2: Desavantatges de les còpies de seguretat diferencials:

- **Es requereix més espai d'emmagatzematge:** A mesura del temps que realitzem diverses còpies diferencials, aquestes còpies creixen el seu volum d'emmagatzematge ja que acumulen tots els nostres canvis des de l'última còpia completa que hem realitzat, resultant que ocupa molt més espai que les còpies incrementals.
- **La còpia dels arxius és més lenta:** A més, amb el pas del temps des de l'última còpia completa, les còpies diferencials es tornen més pesades, resultant que trigarà més temps a completar-se la còpia.

2.9.3: Diferències clau:

1. **Còpia completa:** Les còpies completes, cada còpia inclouen els nostres fitxers. Això fa que sigui més senzilla i molt més ràpid a l'hora de restaurar, però l'inconvenient és que consumeix molt espai, a més de trigar bastant temps en realitzar-se.
2. **Còpia Incremental:** Les còpies incrementals solament inclouen els fitxers que hem generat de nous o els que hem modificat anteriorment des de l'última còpia que hem realitzat, sigui el tipus de còpia que sigui. A més, és la més eficient en terminis d'espai i també en temps de còpia, però malauradament la restauració de la còpia és més complexa, ja que es requereix la còpia completa original i totes les còpies incrementals.
3. **Còpia Diferencial:** Les còpies diferencials inclouen aquells fitxers que siguin creats de nous o aquells que hagin sigut modificats per nosaltres. A més de consumir més espai que la còpia incremental, amb la diferència de que el procés de restauració és més senzill, ja que solament requerim de la nostra còpia completa i l'última còpia diferencial.

3. GESTIÓ DE DISCOS

3.1: Què és una partició?

Una partició és dividir el disc dur en vàries parts, en la qual podem assignar diferents tipus de sistemes d'arxius i assignar els espais d'emmagatzematge d'aquestes particions que ens sigui necessari, sempre i quan no ens passem de la capacitat màxima del disc dur.

Per exemple, podem tenir una partició per guardar les nostres dades més sensibles amb diferents mesures de seguretat.

3.2: Què son les particions primàries i les particions lògiques?

Les particions primàries són les divisions primàries del disc dur que depenen d'una taula de particions i són aquestes les que detecten l'ordinador a l'hora d'iniciar-lo per poder arrencar el sistema operatiu.

Les particions lògiques son aquelles particions que es fan dins d'una partició extesa, és a dir, son particions que no es poden instal·lar sistemes operatius com si es pot amb les particions primàries, però el que si es pot fer és assignar-li un sistema de fitxers (com per exemple, ext2, FAT32 o NTFS) i ja es pot utilitzar sense problema.

4. PRINCIPALS SISTEMES D'ARXIUS

Existeixen diferents sistemes d'arxius, com per exemple:

- **FAT32:** És un sistema de fitxers compatible amb la majoria de sistemes operatius, amb la diferència de que es troba limitat de fins una capacitat menor de 4GB.
- **NTFS:** És el sistema d'arxius que disposa per defecte Windows en la qual suporta fitxers de gran tamany, a més de permetre la gestió dels permisos dels fitxers i la compressió de les dades.
- **ext4:** És el sistema d'arxius que es troba a les diferents distribucions de Linux, en la qual aquesta proporciona una millor gestió de grans quantitats de dades i proporciona una major velocitat en comparació amb ext3, per exemple.
- **exFAT:** És un sistema d'arxius compatible amb els diferents tipus de memòries externes, com per exemple els USB que ens permeten poder emmagatzemar fitxers de qualsevol tamany, a més de ser compatible amb Windows i algunes distribucions de Linux.

5. EINES DE GESTIÓ DE DISCS:

Per a Windows, podem utilitzar disk manager que es un programari ja integrat a Windows per poder gestionar les nostres particions també podem formatar els discos. A més, ens permet crear particions, eliminar-les i canviar les lletres de l'unitat per ordenar-les com nosaltres volguem.

Per a sistemes Linux, podem utilitzar Gparted, una eina àmpliament utilitzada en els sistemes Linux, cosa que també es troba disponible en format live CD/USB. Aquesta eina també ens permet crear les particions, moure-les de lloc, eliminar-les i per últim podem redimensionar les particions.

6. CONCLUSIÓ

Com a conclusió final d'aquesta pràctica, hem de tenir molt en cura que és el que fem amb els nostres dispositius, ja que cada vegada és més senzill que podem ser infectats, inclòs poden arribar a ficar un malware dins d'un fitxer escrit, com aquest, per exemple. A més, de les còpies de seguretat, que en cas de ser infectats i no poder recuperar les nostres dades (per exemple, que l'atacant hagi encriptat el nostre ordinador) i nosaltres al tenir còpies de seguretat (cosa que aquestes còpies han d'estar emmagatzemades fora del PC, si no, no podrem recuperar res), no hi hauria cap problema. També és molt útil saber que no tots els sistemes de fitxers són compatibles entre ells, ja que cada sistema operatiu té el seu propi sistema, ja que a vegades ens podem confondre i no fer una versió dels arxius a una versió que fos compatible amb els diferents sistemes operatius en el qual estem treballant.