aquest document queda immediatament infectat. Això ens porta a dues conclusions:

• Cal desconfiar dels annexos del correu.

• Intentem fer servir formats que no siguin habituals (si volem escriure una carta, fem-ho amb el Bloc de Notes, per exemple), i així no serem portadors de virus.

A més, a Internet ens trobem un altre tipus de virus, anomenats virus-broma. Rebem una carta amb un text que ens alerta d'una situació i ens diu que el reenviem als nostres coneguts dintre d'Internet. Aquests missatges són capaços de capturar altres adreces, per tant no s'han de reenviar. El seu únic objectiu és capturar el major nombre possible d'adreces.

És fàcil construir virus?

Actualment al mercat hi ha programes que generen virus encara que l'usuari no tingui ni idea de programació. Només cal seguir les instruccions que surten per pantalla i tindrem generat un nou virus. Hi ha adreces d'Internet on podem trobar aquests programes i baixar-los via FTP. Són capaços fins i tot de generar virus polimòrfics, o sigui, virus que van canviant la seva forma i ubicació; això fa molt més difícil per al programa antivirus la seva detecció i eliminació. El cert és que quan es detecta un nou virus, el seu antídot està en el mercat a disposició de l'usuari en un termini màxim de 48 hores.

Conseqüències dels virus

• Missatges i bromes

• Negació d'accés a serveis o arxius.

• Revelació de dades: quan connectem a Internet el virus envia dades del nostre ordinador a una adreça concreta.

• Corrupció de dades: esborra o canvia dades dels fitxers.

• Destrucció de dades: tots els fitxers que s'obren s'esborren en una data en concret.

• A vegades espatllen la *bios* de l'ordinador; a causa d'això en alguns casos s'ha hagut de canviar.

Estratègies preventives

1. Preparació: realitzar còpies de seguretat periòdiques per poder recuperar informació si és necessari. Assegurar que aquestes còpies estiguin lliures de virus. Convé també tenir discos d'arrancada per destruir els virus que estan en el sector d'arrancada i poder així obrir l'ordinador sense cap virus en memòria.

2. Prevenció: conscienciació dels usuaris, o sigui, no obrir annexos d'Internet, desconfiar de programari dubtós, etc.

3. Detecció: tenir un antivirus actualitzat que avisi abans que entri el virus.

4. Contenció: si estem parlant d'un sistema en xarxa, és necessari aïllar-ne l'usuari infectat (la millor forma és treure el cable de la xarxa d'aquest ordinador). Després s'ha de mirar si aquest usuari ha treballat amb algun disquet i, en cas afirmatiu, netejar els disquets. Una bona manera que un virus no entri en un disquet és tenir-lo protegit contra escriptura.

5. Recuperació: si un usuari s'ha infectat s'ha de netejar tot el disc i tornar-lo a deixar com estava abans mitjançant les còpies fetes.

Conclusió final

Tot el que es pot fer amb programari es pot fer amb programari infectat. Per tant, cal prevenir.

FRANCESC MIQUEL CLARET PONS

Racó Poètic

La fatxada

Veus una fatxada, l'observes amb deteniment
i sens més la jutges.
Als teus ulls els ha causat una bona impressió,
i dius que és eixerida.
Però ho fas cegament
perquè no saps com és el seu interior.
No saps si serà freda o càlida,
si t'hi sentiràs còmoda o no;
però els teus ulls han dit: –És eixerida.
Els teus ulls color mel han guaitat una fatxada diferent a la resta,
i la rebutgen sens més.
Tan sols ha estat jutjada iniquament
perquè no feia goig.
Però aquesta fatxada tal vegada et pot donar molt més
que aquella que t'havia enlluernat.
Aquesta a simple vista és més opaca,
però dins seu hi brilla la més gran resplendor.
Però ja l'has descartat,
sols perquè als teus ulls no els ha agradat.
Així que et quedes amb la fatxada eixerida i freda,
i et passes la vida pintant-la de colors càlids
perquè creus que així t'hi sentiràs millor.
I aquella fatxada iniqua però càlida
segueix allà al pas del temps.
Ningú l'ha tocat,
car temen el desconegut.
Però allà segueix,
lluent i resplendent com el primer dia.

MONTSE CARRERAS OLIVER