Autorità per l'Informatica nella Pubblica Amministrazione

LINEE GUIDA PER LA DEFINIZIONE DI UN PIANO PER LA SICUREZZA DEI SISTEMI INFORMATIVI AUTOMATIZZATI NELLA PUBBLICA AMMINISTRAZIONE

Gruppo di Lavoro AIPA-ANASIN-ASSINFORM-ASSINTEL

ALLEGATO 2 - VIRUS INFORMATICI

fattori di incremento del rischio e comportamenti da evitare

1. I seguenti comportamenti, comportano un incremento dei livelli di rischio informatico
   a) riutilizzo di dischetti già adoperati in precedenza
   b) uso di software gratuito (o shareware) prelevato da siti internet o in allegato a riviste o libri
   c) uso di dischetti preformattati
   d) collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido
   e) collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del server
   f) uso di modem per la posta elettronica e prelievo di file da BBS o da servizi commerciali in linea o da banche dati
   g) ricezione di applicazioni e dati dall'esterno, Amministrazioni, fornitori, ecc.
   h) utilizzo dello stesso computer da parte di più persone
   i) collegamento in Internet con download di file eseguibili o documenti di testo da siti WEB o da siti FTP
   l) collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi
   m) file attached di posta elettronica

norme basilari di comportamento

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate almeno le seguenti prescrizioni:

a) i floppy disk, sia quando vengono forniti sia quando vengono ricevuti, devono essere sottoposti a scansione da parte del programma antivirus
b) è obbligatorio sottoporre a controllo tutti i floppy disk di provenienza incerta prima di eseguire o caricare uno qualsiasi dei files in esso contenuti.
c) non si deve utilizzare il proprio "disco sistema" su di un altro computer se non in condizione di "protezione in scrittura".
d) proteggere in "scrittura" tutti i propri floppy disk di sistema o contenenti programmi eseguibili.
e) se si utilizza un computer che necessita di un "bootstrap" da floppy, usare un floppy disk protetto in scrittura.
f) non attivare mai da floppy un sistema basato su hard disk a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto.
g) limitare la trasmissione di files eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computers in rete.
h) non utilizzare i server di rete come stazioni di lavoro.
i) non aggiungere mai dati o files ai floppy disk contenenti programmi originali.

regole operative

1. Tutti i computer dell'Amministrazione devono essere dotati di programmi antivirus
2. L'Amministrazione deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus
3. Il personale delle ditte addette alla manutenzione dei supporti informatici devono usare solo dischetti preventivamente controllati e certificati singolarmente ogni volta
4. Ogni P.C. deve essere costantemente sottoposto a controllo anti-virus .
5. I dischetti provenienti dall' esterno devono essere sottoposti a verifica da attuare con un P.C. non collegato in rete (macchina da quarantena), ed inoltre devono essere individuate le aree dell'Amministrazione che, in relazione alla loro particolare attività, sono da considerare a più alto rischio nei riguardi dell'infezione da virus.
6. All'atto della individuazione di una infezione il virus deve essere immediatamente rimosso.
7. Tutti gli utenti del sistema informatico devono sapere a chi rivolgersi per la disinfezione e l'informazione dell'infezione deve essere mantenuta riservata.
8. Il personale deve essere a conoscenza che la diffusione dei virus è punita dall'art. 615 quinquies del Codice Penale.
9. Il software acquisito deve essere sempre controllato contro i virus e verificato perchè sia di uso sicuro prima che sia installato .

Caratteristiche di base del software antivirus

1. Il software antivirus deve essere sottoposto a costante e frequente aggiornamento (almeno due volte al mese) ed in particolare
   a) gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite BBS o Internet
   b) deve essere particolarmente efficace contro i virus della nostra area geografica
   c) deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma
   d) deve poter effettuare una scansione automatica del floppy disk
   e) deve accorgersi del tentativo di modificare le aree di sistema
   f) deve essere in grado di effettuare scansioni a intervalli regolari e programmati
   g) deve essere in grado di effettuare la scansione all'interno dei file compressi
   h) deve mantenere il livello di protezione in tempo-reale
   i) deve eseguire la scansione in tempo-reale
   l) deve poter eseguire la rimozione del codice virale in automatico
   m) in caso di impossibilità di rimozione i file non pulibili devono essere spostati una subdirectory predefinita,
   n) deve essere attivo nella protezione per Applet di ActiveX e Java contenenti codice malizioso

o) deve essere in grado di effettuare la rilevazione/pulizia dei virus da Macro sconosciuti
p) deve essere in condizione di rilevare e rimuovere i virus da macro senza file pattern con un grado di riconoscimento superiore al 97 %
q) deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo

Considerato che in sistemi basati su reti locali o su reti geografiche, aumenta il pericolo di diffusione dei virus, ove possibile il sistema antivirus deve essere centralizzato e predisposto a svolgere almeno le funzioni di:

1. distribuzione degli aggiornamenti sia dei motori di scansione che degli eventuali file "pattern"
2. controllo e monitoraggio degli eventi virali
3. automatico spostamento in directory di "quarantena" di virus informatici risultati non pulibili
4. avviso all'amministratore di sistema di rilevazione di virus e indicazione del file "infetto"