Cadmo

Sistema Informativo e Rete Locale

PRECAUZIONI APERTURA ALLEGATI MAIL E UTILIZZO CHIAVETTE USB

Attenzione!

Negli ultimi anni stanno continuando a girare svariate email contenenti un virus molto pericolosi, nuove versioni del Cryptolocker, che, una volta infettato il PC, cripta tutti i documenti presenti chiedendo poi un riscatto economico per poterli sbloccare.

Le email potrebbero presentarsi in varie versioni ma sono caratterizzate dalla presenza di un allegato solitamente in formato ZIP che contiene il virus.
Altre forme del virus tendono ad infettare le chiavette USB nascondendone il contenuto.

Per i file criptati **non esiste alcun modo per recuperare i dati compromessi** presenti su un computer infetto se non partendo da un backup recente. Inoltre in ambiente di rete vengono infettati anche tutti i file presenti sulle cartelle condivise.

Per evitare i virus NON aprire i file allegati ai messaggi mail!

Ricordiamo, in via generale, di evitare l'apertura di qualsiasi allegato non proveniente da fonte sicura, e soprattutto se:

- è in formato sconosciuto (.pif, .cab, .exe ecc.)
- non è in formato .pdf
- presenta una doppia estensione (per esempio .pdf.exe o .pdf.zip)

Se il documento proviene da fonte sicura ma è all'interno di un file compresso (.zip, .rar, .7z) è consigliato chiedere sempre al mittente una conferma dell'effettiva spedizione e affidabilità del file, perché il mittente potrebbe essere stato infettato a sua volta e aver inviato il virus senza saperlo.

Inoltre sempre per evitare i virus e il furto delle proprie credenziali NON fare mai clic sui link contenuti nei messaggi mail se non siete sicuri della provenienza del messaggio!!

Si raccomanda inoltre di limitare al minimo indispensabile l'utilizzo delle chiavette USB che possono essere ulteriore veicolo di infezione fra un computer e l'altro.
Si sconsiglia l'utilizzo chiavette USB "personali" che hanno elevata probabilità di venire in contatto con molti computer, non vengono controllate periodicamente e sono quindi a forte rischio di infezione.
Nel caso si ritenga comunque necessario l'utilizzo di chiavette USB, si suggerisce

che l'Ente si doti di un numero limitato di chiavette, controllate periodicamente e le attribuisca singolarmente ai soli operatori che ne hanno stretta necessità, dopo aver fornito le informazioni sulle precauzioni da adottare e le procedure da seguire mediante appositi corsi di addestramento e formazione.

Si ricorda infine che il mittente dei messaggi email può facilmente essere falsificato e che gli *spammers* spesso usano indirizzi sottratti da rubriche di computer infetti per mandare in seguito messaggi ingannevoli o contenenti malware alla cerchia di conoscenze ricostruibili dal contenuto della rubrica stessa, inducendo in questo modo i destinatari a fidarsi del mittente.

Si consiglia quindi di prestare sempre attenzione al contenuto delle email che si ricevono, anche se apparentemente provenienti da persone conosciute e di diffidare sempre di mail non attese o richieste, o che abbiano allegati compressi o che richiedano di fare clic su un determinato link.