Ufficio Scolastico
Regionale
per la Lombardia

Virus informatici

Prevenzione delle infezioni e riduzione del rischio

Introduzione

Prevenzione

L'Ufficio Scolastico Regionale per la Lombardia ha ricevuto diverse segnalazioni da Dirigenti Scolastici relative al verificarsi di **infezioni** causate da **virus informatici**.

Al fine di fornire utili elementi conoscitivi per affrontare il preoccupante fenomeno, si rappresentano di seguito alcune buone pratiche volte a **prevenire** eventuali, gravi danni ai computer delle scuole.

La categoria di virus che maggiormente ha colpito i sistemi informatici nel corso degli ultimi due anni, tuttora in grado di danneggiare i sistemi che riesce a raggiungere, si chiama "**ransomware**" (da ransom=riscatto).

Pur non essendo l'unica, i software malevoli appartenenti a questo gruppo sono particolarmente insidiosi perché il meccanismo d'azione consiste nel rendere illeggibili tutti, o comunque molti, dei file del sistema infettato, e propagare rapidamente l'infezione attraverso la rete cui è connessa la macchina colpita.

Su quest'ultima compare poi un messaggio col quale l'autore del virus chiede il pagamento di una somma per fornire la chiave che renderà nuovamente leggibili i file secretati.

Nel particolare caso di infezione da ransomware occorre procedere immediatamente con le seguenti azioni:

- disconnettere il cavo di rete del sistema infettato. Per i sistemi non connessi mediante cavo (wireless) chiudere la connessione di rete;
- se possibile, prima di qualsiasi ulteriore azione, creare una copia dei file alterati su un dispositivo esterno alla macchina infettata. In questo modo sarà possibile un'analisi a posteriori utile a capire meccanismo di azione e strategia di recupero dei file danneggiati;
- ripristinare il proprio sistema da una copia di backup;
- in un secondo tempo rivolgersi ad un esperto per identificare la variante del virus infettante e determinare, se esistente, il relativo software antidoto.

L'attacco da ransomware ha immediata evidenza e per questo chi viene colpito è messo al corrente dell'accaduto in tempo reale.

Esistono altre **infezioni da virus informatici**, molte delle quali avvengono del tutto sotto traccia: in questi casi il software (cosiddetto zombie) si insinua nel sistema sotto attacco **senza manifestarsi all'utente**, pronto ad essere risvegliato dai suoi autori attraverso la rete Internet.

Prevenzione

Non esiste antivirus con efficacia nel 100% dei casi, i virus informatici vengono continuamente modificati dagli autori in modo da sfuggire alla rilevazione.

Occorre quindi, oltre che dotarsi di un buon antivirus da aggiornare con continuità, affinché rimanga al corrente delle più recenti mutazioni, adottare alcune condotte virtuose: la **consapevolezza** è senz'altro lo strumento più efficace.

L'**incipit** dell'infezione di un virus informatico avviene quasi sempre nei modi seguenti:

- eseguendo file infetti scaricati dalla rete Internet;
- aprendo file che hanno sembianza di documenti innocui, allegati a mail, in genere provenienti da mittenti conosciuti;
- utilizzando pen drive (comunemente chiamate "chiavette") a loro volta contenenti file infetti.

Le relative **contromisure** di prevenzione più comuni richiedono di:

- utilizzare il computer con un'utenza ad autorizzazioni limitate;
- non lasciare il computer incustodito con tastiera non bloccata;
- evitare l'uso di chiavette. Per la memorizzazione di file utilizzare in alternativa gli strumenti cloud (Google drive, dropbox etc), molti dei quali disponibili gratuitamente;
- disabilitare l'anteprima dei messaggi mail (se si usa Outlook);
- aprire gli allegati di una mail solo se si conosce il mittente e si è a conoscenza dell'effettiva volontà di quest'ultimo di inviare un particolare allegato. L'oggetto delle mail malevole è spesso del tipo "Fattura non pagata", "Hai vinto un premio", "Documento urgente"… Nel dubbio prima informarsi chiamando telefonicamente il mittente, se conosciuto;
- non cliccare su eventuali link presenti nelle mail dello stesso tipo descritto al punto precedente. Il software malevolo potrebbe essere sulla pagina raggiungibile dal link.

Nel caso di utilizzo della rete Internet, in particolare durante la consultazione di portali di informazione dove oltre agli articoli tematici si possono trovare inserti pubblicitari:

- non cliccare su aree della pagina web che hanno le sembianze di elementi con domanda "civetta" e pulsante di "ok", se non si è certi dell'effetto.

Per ultimo, non per importanza, e come regola generale che travalica lo scopo preventivo di questo approfondimento, occorre effettuare con regolarità il salvataggio (**backup**) dei dati importanti, usando un **dispositivo dedicato** da conservare in **luogo sicuro**.

Prof. Emanuele Alberto Vecchi
Ufficio scolastico regionale per la Lombardia
Via Pola, 11 - 20124 Milano
Gruppo di lavoro Didattica dei media
email: emanuelealberto.vecchi1@istruzione.it