Installazione pulita di un PC infetto Windows 7

Il vostro computer è stato infettato dal malware. Non sapete come eseguire una nuova installazione pulita del sistema nel modo giusto? Le istruzioni seguenti vi mostrano passo dopo passo come rimettere in sesto il PC limitando al contempo il rischio di una nuova infezione.

Abbiamo cercato di creare le linee guida più generali possibili per gli utenti privati. Naturalmente in alcuni casi specifici le operazioni necessarie potrebbero essere diverse.

Queste istruzioni si basano su un sistema con Windows 7 Professional 32 bit, ma valgono anche per i sistemi a 64 bit.

Per reinstallare correttamente il vostro sistema operativo seguendo queste istruzioni, avrete bisogno del CD di installazione di Windows 7 e di un supporto di memorizzazione esterno per il backup dei dati.

Fase 1: scollegare il PC dalla rete

- Se il vostro PC è collegato alla rete tramite cavo, è sufficiente scollegare il cavo di rete.
- Se siete connessi a una rete senza fili (WLAN), è necessario disabilitare la scheda di rete in Gestione dispositivi (clic su *Start* → clic destro su *Computer* → clic su *Proprietà* → clic su *Gestione dispositivi*).

Fase 2: salvataggio dei dati personali

- Collegate un supporto di memorizzazione esterno tenendo premuto il tasto «Maiusc» e salvate i vostri dati personali. Non utilizzate il vostro supporto di backup «solito», ma se possibile procuratevene uno nuovo, completamente vuoto.

  NOTA: il malware presente sul PC potrebbe infettare anche il supporto di memorizzazione esterno e i dati archiviati su di esso. In particolare i malware sfruttano la funzione di esecuzione automatica per diffondersi sui supporti di memorizzazione esterni (chiavette USB, ecc.). Disattivare temporaneamente la funzione di esecuzione automatica è relativamente semplice: è sufficiente premere e tenere premuto il tasto «Maiusc» della tastiera, collegare al PC il supporto di memorizzazione esterno e lasciare il tasto «Maiusc» solo dopo alcuni secondi. In questo modo si impedisce che Windows esegua automaticamente i programmi e i file contenuti sul supporto esterno.

Fase 3: pulizia del Master Boot Record (MBR)

Alcuni virus informatici si insediano nel cosiddetto Master Boot Record (MBR) del computer. Per questo motivo è consigliabile sovrascriverlo e quindi ripulirlo. Per farlo utilizzate l'utilità «Bootrec.exe» dell'Ambiente ripristino Windows.

- Inserite nell'unità ottica il CD di installazione di Windows 7 e riavviate il PC.
- Se il PC non si avvia dal CD inserito, impostate l'unità CD come prima periferica nel BIOS (la procedura è descritta nel manuale della scheda madre). In alternativa, subito dopo aver avviato il PC si può premere il tasto funzione «F8». Si aprirà il Boot Manager, che consente di selezionare l'unità CD.
- Premete un tasto quando viene chiesto di farlo.
- Selezionate una lingua, un formato ora e valuta, un layout di tastiera o metodo di input, e fate clic su *Avanti*.
- Fate clic su *Ripristina il computer*.
- Fate clic sul sistema operativo e quindi su *Avanti*.

- Nella finestra di dialogo Opzioni ripristino di sistema fate clic su *Prompt dei comandi*.
- Digitate «`bootrec.exe /fixmbr`» e premete il tasto Invio (*Enter*). In questo modo viene ripristinato l'MBR (disattivando così la funzionalità MBR Rootkit di un eventuale malware).
- Chiudete il prompt dei comandi e spegnete il PC mediante *Arresta il sistema*. Lasciate il CD di installazione di Windows 7 nell'unità ottica.

Fase 4: reinstallazione di Windows 7

- Avviate nuovamente il PC.
- Se il PC non si avvia dal CD inserito, impostate l'unità ottica come prima periferica nel BIOS (la procedura è descritta nel manuale della scheda madre). In alternativa, subito dopo aver avviato il PC si può premere il tasto funzione «F8». Si aprirà il Boot Manager, che consente di selezionare l'unità CD.
- Premete un tasto quando viene chiesto di farlo.
- Selezionate una lingua, un formato ora e valuta, un layout di tastiera o metodo di input, e fate poi clic su *Avanti*.
- Ora è sufficiente un clic su *Installa ora*.
- Selezionate quindi le opzioni di gestione dei vari dischi, che vi consentono di eliminare, creare e formattare le partizioni.

  ATTENZIONE: con l'eliminazione o la formattazione di una partizione si perdono tutti i dati salvati su quella partizione!

  NOTA: per essere certi che sul PC non ci sia più nessun malware, le partizioni presenti vanno eliminate e ricreate da zero. Le nuove partizioni andranno poi formattate. Tenete presente anche che potrebbe esserci una partizione di ripristino («Recovery») del produttore. Questa partizione non va né eliminata né formattata.
- Completate l'installazione di Windows 7 con le impostazioni consigliate.
- Collegate quindi il PC a Internet (reinserite il cavo di rete).
- Aggiornate il sistema operativo tramite Windows Update (clic su *Start* → *Pannello di controllo* → *Windows Update*).

Fase 5: installazione di un programma antivirus

- Installate un programma antivirus ottenuto da una fonte affidabile e aggiornatelo con l'apposita funzione integrata.

  NOTA: un elenco di programmi antivirus raccomandati è disponibile su www.ebas.ch/5steps_step2.

Fase 6: installazione e aggiornamento dei programmi

- Installate i programmi desiderati. Aggiornate tutti i programmi e dove possibile attivate la funzione di aggiornamento automatico.

  NOTA: prestate attenzione a installare soltanto programmi provenienti da fonti affidabili (come le pagine di Download dei produttori o archivi software come PCtipp, Heise, ecc.).

Fase 7: analisi dei dati

- Tenete premuto il tasto «Maiusc» e collegate al PC il supporto di memorizzazione esterno contenente i dati salvati in precedenza.

  NOTA: se durante il backup dei dati è stato copiato sul supporto di memorizzazione esterno del malware, il PC potrebbe infettarsi di nuovo! Per prevenire questo problema, è indispensabile tenere premuto il tasto «Maiusc» quando si collega il supporto di memorizzazione esterno (vd. nota alla fase 2).

- Eseguite un'analisi dell'intero sistema e del supporto di memorizzazione esterno con il programma antivirus appena installato. Se vengono individuati dei file infetti, occorre pulirli o eliminarli!

  NOTA: un'alternativa migliore ma più impegnativa rispetto all'analisi del sistema appena installato sarebbe quella di controllare il supporto di memorizzazione esterno con un Live-CD avviabile o un sistema operativo diverso (per es. Linux, macOS).

Fase 8: ripristino dei dati

- Copiate i dati del vostro backup dal supporto di memorizzazione esterno al PC.

Fase 9: che cosa rimane da fare!

- Poiché oggigiorno il malware si impossessa molto frequentemente di nomi utente e password, è assolutamente necessario modificare tutte le password del sistema stesso, come pure tutte le password dei siti Internet (per es. e-banking, accesso all'e-mail, Facebook, ecc.).
- Oltre a questo, controllate attentamente i vostri estratti conto dell'e-banking e delle carte di credito.

Queste istruzioni sono state preparate da «eBanking – ma sicuro!» in collaborazione con SWITCH

eBanking ma sicuro!

Sul sito Internet gratuito **www.ebankingmasicuro.ch** si trovano ulteriori informazioni sui provvedimenti necessari e le regole di comportamento per un uso sicuro delle applicazioni di e-banking.

SWITCH

SWITCH offre esclusivi servizi Internet innovativi e pratici per le scuole universitarie e gli utenti Internet della Svizzera.