

Sistemi operativi Windows e partizioni Gpt

Su un computer HP Pro 3520 sono alle prese con il ritorno a Windows 7. Dal sito di Microsoft ho appreso che l'operazione richiede un codice d'attivazione anche già usato: verrà accettato, ma comporterà la successiva attivazione contattando per telefono il supporto clienti. Il problema, però, è che non riesco a installare Windows 7. Se eseguo il boot da Dvd-Rom, l'installazione si blocca perché il disco è partizionato secondo lo schema Gpt. Dove sbaglio? Per poter utilizzare la partizione Gpt devo avviare l'installazione da una periferica Efi? È mai possibile che debba eliminare l'attuale struttura Gpt e perdere anche la partizione di recovery solo per installare Windows 7 con Ntfs? Se decidessi di formattare in Ntfs e poi volessi utilizzare i dischi di ripristino per reinstallare Windows 8, riuscirei a ripristinare il computer alle condizioni iniziali dopo aver eliminato la partizione di recovery e senza la possibilità di utilizzare una periferica Efi?

Giuseppe Giuliani

La tecnologia Gpt (*Guid partition table*) è stata introdotta contemporaneamente all'Uefi per il Bios delle schede madri allo scopo di aggirare le limitazioni del precedente schema di partizionamento Mbr che non consentiva di creare unità logiche più grandi di 2 Tbyte.

Allo stesso tempo, Gpt supera anche il numero massimo di 4 partizioni primarie previste dagli standard precedenti: ora, Windows può gestire fino a 128 partizioni sulla stessa memoria di massa. Il supporto a questa tecnologia, però, è differenziato: le versioni a 64 bit di Vista, Server 2003 con Service Pack 1, Server 2008, Windows 7 e 8 sono in grado di leggere, scrivere e avviare il sistema operativo da un disco con partizioni Gpt. Le relative versioni a 32 bit supportano anch'esse la tecnologia Gpt, ma solo per i dischi dedicati all'archiviazione dei dati. Non è quindi previsto l'avvio del sistema operativo da una memoria di massa partizionata secondo il nuovo schema. Allo stesso modo, Windows XP x64 può usare dischi Gpt solo per i dati, mentre la versione a 32 bit non è in grado di accedere a questo tipo di unità. Windows NT 4.0, 2000, 95 e 98, non sono compatibili con lo schema di partizionamento Gpt. Ovviamente, oltre al supporto specifico da parte del sistema operativo, il boot da partizioni Gpt è sempre subordinato alla presenza di un firmware Uefi in grado di rilevare e configurare correttamente il disco da cui si desidera caricare Windows. Al momento della configurazione della memoria di massa è necessario decidere quale sistema di partizionamento adottare: non è infatti possibile combinare partizioni Mbr e Gpt sullo stesso hard disk.

«Partizioni Mbr e Gpt non possono coesistere. La stessa tecnologia deve essere adottata per tutte le unità logiche di una memoria di massa.»

Lo schema di partizionamento Gpt prevede la presenza di un'intestazione, definita *Protective Mbr*, che assicura la retrocompatibilità. Non si tratta di una partizione vera e propria, ma solo di uno stratagemma per fare in modo che un disco Gpt sia rilevato come già utilizzato anche dai sistemi operativi delle generazioni precedenti, impedendo quindi ripartizionamenti e cancellazioni accidentali dei dati. Precisiamo che Gpt e Mbr sono schemi di partizionamento che consentono di suddividere lo spazio disponibile su disco e non devono essere confusi con il file system, che invece descrive la struttura con la quale sono archiviati i dati all'interno dell'unità logica. Indipendentemente dall'utilizzo della tecnologia Gpt o Mbr, è possibile formattare una partizione con il file system Fat o Ntfs. Purtroppo, se il sistema operativo scelto dal lettore non supporta in maniera specifica la tecnologia Gpt,

WINDOWS E I DISCHI GPT

Versione del sistema operativo	Partizione di boot	Partizione dati
95/98	×	×
NT 4	×	×
2000	×	×
XP 32 bit	×	×
XP x64	×	●
Server 2003 SP1 32 bit	×	●
Server 2003 SP1 64 bit	●	●
Server 2008 32 bit	×	●
Server 2008 64 bit	●	●
Vista 32 bit	×	●
Vista 64 bit	●	●
Windows 7 32 bit	×	●
Windows 7 64 bit	●	●
Windows 8 32 bit	×	●
Windows 8 64 bit	●	●
Server 2012 64 bit	●	●

Si ● No ×

Tutte le versioni a 64 bit di Windows possono accedere a partizioni Gpt contenenti dati. Le versioni a 64 bit di Windows Vista, 7, 8 e tutte le edizioni a 64 bit di Windows Server a partire da 2003 SP1 sono in grado di avviare il sistema operativo da una partizione Gpt. Le corrispondenti versioni a 32 bit e Windows XP x64 Edition sono compatibili solo con partizioni Gpt di dati.

Installare Windows 8 sul tablet WeTab

Sono in possesso di un tablet WeTab, un prodotto commercializzato qualche anno fa sul mercato tedesco. Il dispositivo è fornito di serie con il sistema operativo Meego, derivato da Linux, e tra le caratteristiche hardware salienti vi è il touchscreen da 11,6 pollici con risoluzione di 1.366 x 768 punti, le interfacce Bluetooth, Wi-Fi, Usb e il lettore di schede Sd. Vorrei eseguire l'aggiornamento a Windows 8 (alcuni hanno installato con successo anche Ubuntu Linux e Windows 7), perciò mi rivolgo a voi sperando che possiate fornirmi le istruzioni necessarie per quest'operazione.

Mario De Carlo

Il tablet WeTab è basato sulla piattaforma Intel Pineview ed è dotato di una Cpu Atom N450 a 1,66 GHz e di un adattatore grafico Intel Gma 3150. La memoria di massa è un Ssd da 16 o 32 Gbyte (quest'ultimo solo nel modello dotato di connettività 3G), le interfacce di connessione includono Wi-Fi 802.11n, Bluetooth 2.1 con funzionalità Edr, due porte Usb e un lettore di schede di memoria Sd/SDhc, oltre a un'interfaccia per Sim card e un connettore Hdmi. La Ram è solo 1 Gbyte. La potenza di elaborazione del WeTab è più o meno a livello di un netbook ed è appena sufficiente per Windows 8. Perciò, nonostante l'operazione desiderata dal lettore sia fattibile, il tablet consentirà di utilizzare solo le applicazioni più leggere, come i browser per la navigazione in Rete, i player multimediali per la riproduzione di musica e video e le applicazioni da ufficio. Gli utenti che hanno già installato Windows 8 consigliano di scegliere la versione a 32 bit, meno avida di risorse hardware e più capace di sfruttare la limitata quantità di Ram. La versione x64 dovrebbe essere considerata solo dagli utenti che hanno necessità di eseguire software a 64 bit. Tuttavia, molti applicativi a 64 bit che girano sotto forma di servizi all'interno del sistema operativo (per esempio, Microsoft Exchange Server) non sono compatibili. Per l'installazione di Windows 8 è necessario utilizzare la versione di aggiornamento. Quella Oem o completa sono state testate, ma, a quanto risulta, non contengono i driver che attivano lo schermo tattile.

non c'è modo di aggirare il problema. Si dovrà ripartizionare il disco fisso secondo il più conservativo schema Mbr ed eseguire l'installazione in questa configurazione. Esistono molte tipologie di dischi di ripristino. Alcuni produttori forniscono a corredo dei loro Pc lo stesso disco d'installazione di Windows distribuito da Microsoft, al quale sono aggiunti i driver delle componenti hardware e le applicazioni specifiche. Lanciando questi Dvd-Rom sarà avviata la normale procedura d'installazione, che porterà a termine il ripristino del computer senza utilizzare il materiale eventualmente già presente sull'hard disk. Altri produttori forniscono una copia immagine e in questi casi l'operazione di ripristino passa per un software di clonazione che riposiziona le partizioni all'interno del disco fisso. In altri casi ancora, invece, tra le opzioni del Bios vi è una funzione che consente di eseguire l'avvio da una partizione nascosta che contiene il materiale necessario. Non conoscendo la strategia scelta dal produttore del computer del lettore, consigliamo di archiviare l'attuale contenuto dell'hard disk facendo un'immagine con un software di clonazione, accertandosi di utilizzare una versione aggiornata che supporti la tecnologia Gpt. In questo modo sarà possibile, in caso di necessità, ripristinare il computer alla sua condizione iniziale.

Posta Hotmail irraggiungibile

Ho un notebook Asus X54C-SX289V con processore Intel Core i3-2350M e Windows 7 Home Premium a 64 bit con Service Pack 1. Per navigare uso Internet Explorer 9 e ho un account di posta elettronica con Hotmail. Qualche giorno fa, prima d'installare WinOptimizer 2013 allegato al numero 264 di PC Professionale, ho rimosso la versione precedente del software tramite il Pannello di controllo. Ho poi disinstallato anche le toolbar Bing e Babylon e ho caricato la nuova versione dell'utilità di Ashampoo. Con questa ho eseguito la scansione e la pulizia completa del computer, ma da quel momento non sono più riuscito ad accedere a Hotmail: la pagina non veniva caricata e rimaneva bianca. Ho tentato di aprirla partendo da Msn Italia, ma anche questa procedura non ha avuto l'esito sperato. La navigazione su altre pagine web avviene regolarmente. Ho provato ad aggiornare Internet Explorer alla versione 10, ma il

Le toolbar aggiuntive dei web browser modificano alcuni parametri operativi. In caso di una loro rimozione incompleta o non seguita dal pieno ripristino dei valori predefiniti del navigatore, l'accesso a siti e servizi web può essere compromesso.

problema si è riproposto. In alcuni forum ho letto che Google Chrome potrebbe risolverlo, ma non ho voluto installarlo per evitare di complicare ulteriormente le cose.

Emanuele Vetrone

È improbabile che il malfunzionamento sia riconducibile alle operazioni di pulizia eseguite con WinOptimizer 2013. Semmai potrebbe dipendere dalla disinstallazione delle barre strumenti per il browser. Per interfacciarsi con il programma di navigazione, queste utility modificano una serie di parametri operativi che, in caso di rimozione, devono essere ripristinati al valore predefinito. Se la procedura di disinstallazione non provvede a questa necessità, il browser potrebbe non essere più in grado di funzionare correttamente. Esistono inoltre anche alcuni cavalli di Troia che dissimulano la propria azione presentandosi sotto forma di toolbar. I software antivirus, pur essendo normalmente in grado di rilevare questi malware, si

Il problema non si verifica con il pacchetto di upgrade. Nei forum tecnici, sono state fatte molte ipotesi sui motivi per cui Microsoft abbia escluso i driver dalla versione completa del sistema operativo. Una delle più accreditate è che ciò impedirebbe agli assemblatori di Pc di fornire Windows 8 su touchscreen non ufficialmente certificati da Microsoft. La procedura d'installazione è eseguibile in più modi: se sul tablet è già presente una versione precedente del sistema operativo si può lanciare il Windows 8 Upgrade Assistant, disponibile sul sito di supporto tecnico di Microsoft. In caso contrario è necessario scaricare il pacchetto d'installazione da un altro computer. Una volta completato il download, si può avviare subito l'installazione oppure creare un pendrive Usb o un Dvd-R (lo scaricamento da Windows XP non prevede la creazione automatica del disco d'installazione). Prima di lanciare il setup è fondamentale installare tutti gli aggiornamenti disponibili mediante il sistema operativo residente del WeTab. Con questa operazione si aggiorna all'ultima versione (la 1006 mentre scriviamo) il firmware dello schermo, senza il quale in Windows l'interfaccia tattile non funzionerebbe. Se sul tablet è già presente Windows, la procedura è eseguibile tramite un'apposita utilità d'aggiornamento. La versione di upgrade di Windows 8 include la maggior parte dei driver necessari per il WeTab. Dopo l'installazione, in *Gestione dispositivi* saranno presenti alcuni componenti non configurati. I driver e le utilità necessarie si trovano sul sito di supporto tecnico di un tablet analogo, l'ExoPc, all'indirizzo exocommunity.com/forum/viewforum.php?f=59. Si dovranno installare i software di gestione del Wi-Fi e del Bluetooth di Atheros, il convertitore Chrontel per l'uscita Hdmi, l'audio Hd di Realtek, l'applet per la gestione del pulsante sul telaio e l'utilità Millennium, che gestisce l'accensione e lo spegnimento delle connessioni Wi-Fi e Bluetooth, la luminosità e l'orientamento automatico dello schermo. Nelle versioni del WeTab dotate di 3G e Gps si devono installare anche i driver per il Broadcom Crystal Hd video accelerator, il modem 3G Huawei EM770W e la relativa applet Gps. Nei forum dedicati all'ExoPc/WeTab si legge che alcune funzioni non sono supportate in Windows: tra queste, il sensore accelerometrico e i pulsanti aggiuntivi presenti sul telaio. Ciò impedisce l'esecuzione di applicazioni - per lo più ludiche - che richiedono questi componenti.



Nonostante la configurazione hardware minimale, sul tablet WeTab è possibile installare Windows 8 e sfruttare le funzionalità tattili offerte dal nuovo sistema operativo.

Il linguaggio Esc/P delle stampanti ad aghi

Sul lavoro ho necessità di utilizzare stampanti ad aghi per produrre moduli continui multicopia da 6 pollici. In passato, con Windows 2000 ho utilizzato una Star XB 24-250 e mi sono scontrato con un problema: la lunghezza della pagina stampata era di alcuni punti più corta rispetto ai 6 pollici impostati nel driver. Così dopo 3-4 pagine era necessario avanzare manualmente il carrello in modalità offline per riallineare il modulo continuo. Riuscii a correggere l'anomalia utilizzando un driver Epson compatibile con la stampante: con quello, la stampa rispettava perfettamente i 6 pollici anche dopo 300 pagine. In seguito ho sostituito la stampante con una Panasonic KX-P2624 e sono passato a un computer basato su Windows XP Professional. In questa configurazione il vecchio problema si è ripresentato e l'ho risolto usando il driver per la Epson LQ-1050. Recentemente ho eseguito l'aggiornamento a Windows 8 Professional e anche con questo sistema operativo il difetto si è riproposto. Com'è possibile che non sia stato ancora risolto?

Maurizio Dinosio

Il set di comandi Esc/P è stato introdotto con le stampanti ad aghi prodotte da Epson ed è stato poi adottato da altri produttori fino a diventare uno standard di fatto.



Nelle stampanti ad aghi il font predefinito di caratteri ha una dimensione pari all'altezza della testina di stampa. Questa caratteristica permette di stampare una riga a ogni passaggio in modalità testo. Per allineare la riga al modulo continuo si utilizza un set di comandi che consente di avanzare il cilindro su cui si avvolge la carta in base a una scala espressa in 1/216 di pollice. Con apposite macro è quindi possibile gestire la distanza tra

limitano a rimuoverli senza riparare eventuali danni arrecati al sistema. È quindi possibile che, nonostante il cavallo di Troia non sia più presente, gli effetti dell'infezione permangano. Di seguito daremo alcune procedure che consentono di ripristinare i parametri operativi predefiniti del programma di navigazione e che, nella maggior parte dei casi, dovrebbero consentire di ripristinare l'accesso alla casella di posta elettronica:

1. Nel menu *Strumenti* di Internet Explorer selezionare la voce *Opzioni*.
2. Entrare nella scheda *Protezione* e ripristinare il livello predefinito.
3. Chiudere tutte le finestre del browser e riavviare il programma.
4. Collegarsi a Hotmail.
5. Se il malfunzionamento persistesse, esaminare la configurazione del firewall o della suite di sicurezza informatica e verificare se sia stato inserito qualche indirizzo nella blacklist. Nel caso, cancellarli e riavviare il computer.
6. Verificare di nuovo il corretto funzionamento del browser. Consigliamo anche di azzerare il file *Hosts* secondo la procedura descritta nell'articolo 972034 della Knowledge Base di Microsoft.

Un'altra possibile causa del problema sono i software per il blocco dei popup e dei banner pubblicitari, che a volte

impediscono il collegamento anche a siti del tutto leciti e desiderati dall'utente. Si può provare a disabilitarli temporaneamente per verificare se ciò ripristini la normale funzionalità del browser.

Come ultima risorsa può essere utile rimuovere e reinstallare daccapo il browser, operazione che azzererà tutte le impostazioni e riporta l'applicativo nella sua condizione predefinita.

Purtroppo, ciò è impossibile con Internet Explorer, che è preinstallato nel sistema operativo. Anche gli aggiornamenti alle versioni successive dell'applicazione conservano le impostazioni preesistenti e con esse l'origine del malfunzionamento. Si potrà tentare d'installare un browser alternativo come Mozilla Firefox o Google Chrome, che non essendo presenti

nel sistema al momento dell'infezione non sono stati oggetto di modifiche da parte della toolbar o del cavallo di Troia. Inoltre, Firefox è provvisto di una funzione che, tramite la voce *Componenti aggiuntivi* del menu *Strumenti*, consente la scansione dei plugin installati nel computer e segnala versioni malfunzionanti o che richiedono un aggiornamento. Questa caratteristica spesso consente di risolvere problemi simili a quello segnalato dal lettore, altrimenti difficili da individuare.

Privacy e sicurezza sulle reti wireless

Oggi gli istituti bancari propongono comode applicazioni per accedere al proprio conto online anche da smartphone e tablet via Wi-Fi e 3G. I dati scambiati tramite questi canali sono crittografati fin dall'origine? È sufficiente che compaia la stringa *Https* per essere certi di essere connessi in modo sicuro? Utilizzando un access point gratuito, come quelli forniti da alberghi o reti cittadine, credo che almeno la tratta da smartphone/tablet al router non sia crittografata ed esponga al rischio d'intercettazione da parte di terzi. La soluzione proposta in questi casi è l'uso di una Vpn o la navigazione "in incognito" (Chrome) o "anonima" (Firefox), ma in questi casi si ha la certezza dell'anonimato e non della cifratura. Mi chiedo allora se il collegamento sia cifrato solo nel caso

«Reinstallare il web browser dopo averlo rimosso spesso ripristina la piena funzionalità dell'applicazione. Solo IE non è disinstallabile.»

le righe in maniera flessibile e adattarla ai moduli personalizzati. Ancora oggi, infatti, per produrre documenti ufficiali in formati speciali si utilizza questo tipo di periferiche. Il set di comandi per eseguire queste operazioni è noto con il nome di Esc/P (*Epson standard code for printers*), un linguaggio sviluppato dalla società giapponese per gestire le stampanti ad aghi e a getto d'inchiostro. Nel periodo di massima diffusione è stato adottato anche da altri produttori e molti dispositivi lo implementano tuttora. È per questo motivo che il lettore ha potuto configurare le stampanti Star e Panasonic utilizzando un driver Epson che, evidentemente, implementa le funzioni di avanzamento del modulo continuo con maggiore precisione di quello nativo di Windows. Purtroppo, le stampanti ad aghi sono ormai relegate a compiti molto specifici e anche lo sviluppo dei driver si concentra più sulla gestione della stampa bitmap piuttosto che sulla modalità testuale e sulla gestione dei moduli continui. Riteniamo quindi improbabile che i driver per queste periferiche saranno aggiornati per eliminare i malfunzionamenti riscontrati. Tuttavia, vista l'ampia compatibilità di questi dispositivi con lo standard Esc/P, non dovrebbero presentarsi inconvenienti anche continuando a utilizzare il driver di stampa di Epson.



Le reti Wi-Fi aperte espongono gli utenti al rischio d'intercettazione dei dati personali. È buona norma collegarsi esclusivamente alle reti wireless pubbliche protette da password e trasmettere informazioni sensibili solo su connessioni di tipo Https.

di connessioni Https. Quali sono le tratte protette? Esistono sistemi per crittografare fin dall'origine? Le connessioni dati su rete cellulare (scheda Sim) garantiscono maggior sicurezza?

Stefano Greco

L'utilizzo delle connessioni wireless pone con forza la questione della privacy e della sicurezza dei dati personali. I gruppi di lavoro che hanno progettato gli standard Ieee 802.11 ne erano coscienti e, insieme ai protocolli di trasmissione, hanno sviluppato appositi schemi di codifica. Purtroppo, la crittografia è uno dei

compiti più gravosi e le implementazioni degli standard Ieee 802.11, ratificate nel 1999, potevano contare su processori con limitate capacità di elaborazione. È per questo motivo che i primi sistemi crittografici per le connessioni Wi-Fi, noti con il nome di Wep (*Wired equivalent privacy*, in italiano *Riservatezza equivalente alla rete cablata*), nonostante il nome rassicurante offrivano una protezione debole. Con l'evoluzione dei processori integrati nei dispositivi Wi-Fi la potenza di calcolo è aumentata ed è stato possibile implementare algoritmi più sicuri come il

HI TECH SENZA SEGRETI

www.pcprofessionale.it



I volantini sottocosto delle grandi catene di distribuzione visionarli e commentarli da PC Professionale. Scopri i "pacchi" e le offerte "vere".



La vostra foto migliore. Date spassosetti di fotografia digitale? Inviatela le vostre tre foto migliori e le pubblicheremo o le esporremo a Smau in una speciale mostra fotografica.



Panasonic Eluga - gli scatti per valutare la fotocamera
Le foto dello smartphone Panasonic Eluga in prova sul numero di Agosto di PC Professionale. Scarica...
13 luglio 2012 - 2 Agosto 2012 - 0 commenti

Gli speaker da 4 pollici secondo M-Audio
Le AV40 sono un sistema di altoparlanti 2.0 adatto a qualsiasi applicazione multimediale.
Antiprima...
13 luglio 2012 - 24 luglio 2012 - 0 commenti

Leggi altre notizie da questo canale



Aprire automaticamente le pagine preferite
I principali browser offrono, di solito tramite estensioni e plug-in, molti modi...
13 luglio 2012 - 6 Agosto 2012 - 0 commenti

Modificare più parti di un documento con OpenOffice.org
Word offre da moltissimi anni la possibilità di dividere la sua finestra in due...
13 luglio 2012 - 3 Agosto 2012 - 0 commenti

Leggi altre notizie da questo canale

**Non perderti
le ultime notizie
dal mondo
della tecnologia**

Wpa (Wi-Fi protected access) e il successivo Wpa2. La principale differenza tra questi due metodi crittografici è la lunghezza delle chiavi utilizzate per generare il codice e si ritiene che la seconda variante, pubblicata nel 2004, offra tuttora un buon livello di protezione per la maggioranza degli utenti. La crittografia Wep, invece, è ormai obsoleta e i dispositivi che non offrono che questa soluzione dovrebbero essere sostituiti al più presto con altri di produzione più recente.

Purtroppo, molte reti Wi-Fi pubbliche, per semplificare le cose agli utenti, non prevedono password di accesso. È un'abitudine deprecabile perché, in assenza di questo elemento, tutto il traffico trasmesso da ogni client all'access point (e viceversa) viaggia in chiaro e può essere facilmente intercettato. L'impostazione di una password, anche se banale, attiva invece gli schemi crittografici e complica l'azione dei pirati informatici. Con la protezione Wpa/Wpa2, i dati in transito sono crittografati dall'adattatore di rete Wi-Fi del computer dell'utente, trasmessi in codice all'access point che li riceve, li decodifica e li instrada verso la loro destinazione in Rete.

Quindi, utilizzando la crittografia Wap/Wap2, i dati sono protetti nel tragitto tra client e access point, ma sono ancora soggetti ad attacchi del tipo "man in the middle" nel tratto tra access point e sito di destinazione attraverso la rete locale cui è collegato il router Wi-Fi e successivamente in Rete.

Il protocollo Https è un altro layer che si sovrappone alla crittografia Wap/Wap2 e codifica i dati trasmessi dal client con una chiave che è a disposizione solo del sito di destinazione. Pertanto, usando il protocollo Https i dati viaggiano crittografati per tutto il tragitto da un corrispondente all'altro (per esempio, dall'utente alla sua banca). Il problema del protocollo Https è che la maggior parte dei siti inizia dapprima la connessione col protocollo Http, per poi attivare successivamente la cifratura dei dati. Ciò lascia l'utente privo di protezione crittografica nelle fasi iniziali della connessione. È per questo motivo che è consigliabile utilizzare in ogni caso entrambi gli schemi: il Wpa/Wpa2 per cifrare tutto quello che viene trasmesso verso il router/access point e l'Https per avere uno scambio di dati riservato con il sito corrispondente e, allo stesso tempo, difendersi anche dall'eventuale curiosità di chi offre la connessione wireless

pubblica. L'utilizzo di app per collegarsi all'home banking tramite smartphone offre generalmente un buon livello di protezione: il software provvede a verificare l'identità dell'utente in locale prima di consentire l'accesso al servizio e crittografa tutte le interrogazioni e i relativi risultati. Con questo metodo di fruizione, il flusso dei dati è completamente codificato da una estremità (l'utente) all'altra (la banca) ed è possibile utilizzare algoritmi di crittografia personalizzati e quindi ancor più sicuri rispetto a quelli standard implementati da Wpa/Wpa2 e Https.

Le Vpn (Virtual private network) potenzialmente offrono un livello di sicurezza ancora superiore, ma richiedono software appositi e la disponibilità di un sito corrispondente che riceva il traffico per poi reinstrarlo verso la destinazione. Si tratta quindi di una soluzione meno generale rispetto alla crittografia Wpa/Wpa2 e Https.

Le funzioni di navigazione anonima, invece, hanno uno scopo completamente diverso: esse servono a evitare che sul computer (tablet, smartphone o altro dispositivo) sul quale è eseguito il browser rimangano tracce dei siti visitati. Normalmente, ogni sito viene aggiunto alla cronologia e i file Html e le immagini che compongono le pagine Web sono archiviate in apposite directory sul disco, in modo da velocizzare le successive consultazioni del sito. Questa strategia, però, espone al rischio che altri utenti del computer possano rovistare nella cache del browser. Con la navigazione anonima, l'applicazione provvede a cancellare tutte le tracce alla chiusura del programma senza lasciare materiale sensibile archiviato. Questa funzione non ha alcuna influenza sui dati trasmessi dal client all'access point o al sito di destinazione, che senza le tecnologie di cifratura dei dati di cui sopra viaggiano in chiaro e senza protezione.

I dati trasmessi tramite rete cellulare (2G o 3G) sono anch'essi crittografati, ma il livello di protezione è abbastanza debole. In Europa e Usa l'algoritmo di codifica più comune è l'A5/1, che, pur essendo più robusto dell'A5/2 utilizzato nel resto del mondo, rimane comunque vulnerabile agli attacchi di pirati informatici particolarmente tenaci. Anche in questo caso è quindi consigliabile, durante operazioni che coinvolgono dati sensibili, come l'home banking, utilizzare metodi crittografici aggiuntivi quali l'Https o eventualmente le Vpn. •

Antivirus Avast e posta Tls/Ssl



L'antivirus Avast! è ora in grado di eseguire la scansione della posta elettronica codificata con i protocolli crittografici Ssl/Tls. La finestra dell'applicazione che notifica questa nuova funzionalità potrebbe essere scambiata per un messaggio d'errore.

Qualche giorno fa è stato rilasciato un aggiornamento per l'antivirus Avast che utilizzo sul mio computer. Di solito eseguo manualmente il download del database delle definizioni dei virus, ma in questo caso, per qualche strano motivo, l'applicazione ha deciso in modo autonomo di scaricare la nuova versione, che comprende un'interfaccia utente rinnovata. Oltre all'eccesso di verbosità e di comunicazione, ho subito notato un messaggio d'errore che mi informava che la protezione mail di Avast! era ora in grado di analizzare la posta elettronica anche quando Ssl/Tls era abilitato nel client email. Se in precedenza Ssl/Tls era stato disabilitato per permettere alla funzione di protezione di analizzare la posta, era possibile riabilitarlo e cancellare gli account Ssl nelle impostazioni della funzione. La finestra mi dava come unica opzione il pulsante Ok, che sono stato obbligato a premere per continuare, senza aver capito l'origine del problema. Come faccio a ripristinare la modalità operativa precedente che ha sempre funzionato bene?

Lettera firmata

Anche se il messaggio si presenta con l'inquietante icona della croce bianca su sfondo rosso, non si tratta propriamente di un errore. Molti fornitori del servizio di posta elettronica supportano i protocolli crittografici Ssl/Tls per la trasmissione dei messaggi, a volte in maniera obbligatoria, a volte facoltativa. Le versioni precedenti di Avast! non erano in grado di eseguire la scansione della posta quando venivano utilizzati questi protocolli e ciò obbligava a rinunciare alla crittografia oppure alla protezione antivirus. La nuova versione è invece in grado di gestire anche la posta inviata con Ssl/Tls e il messaggio in questione informava di questa nuova funzionalità e invitava l'utente, se lo avesse desiderato, a riattivare la funzione Ssl/Tls. Si tratta solo di un consiglio ed è possibile continuare a utilizzare il proprio client di posta elettronica nel modo consueto senza alcuna controindicazione. In alternativa, se il server di posta elettronica lo prevede, si potranno attivare i protocolli Ssl/Tls all'interno delle opzioni relative al proprio account email per migliorare ulteriormente il livello di protezione della privacy.