

M.C.S. Informa

Finalmente si avvicina Agosto e le sospirate vacanze

estive, pochi eletti stanno già godendo di un break ristoratore ma la maggior parte di noi è rimasta in ufficio a sopportare l'imprevedibile ondata di caldo.

M.C.S. Vi invita a "rilassarVi" e a trascorrere qualche minuto di pausa navigando nel nuovo cd



interattivo di Vertice^(R).

Un'ondata di novità a partire da Luglio Vi rinfrescherà, una nuova versione del cd-rom di Vertice^(R) completamente rinnovata...

“Un'ondata di novità!”

Come già anticipato nell'introduzione, a partire dal mese di Luglio e nei mesi seguenti Vi invieremo un nuovo aggiornamento di Vertice.

Le modifiche più importanti riguardano il modulo dei CESPITI ma la novità più rilevante per tutti gli utenti è rappresentata dalla veste grafica e interattiva del nuovo cd-rom: indice degli argomenti, file dei documenti in formato pdf, software freeware.

Nell'area "Software" troverete le schede tecniche di Vertice^(R); per ogni modulo della procedura potrete visionare le caratteristiche più interessanti; i prezzi di listino e approfondire alcune tematiche operative.

Una sezione è dedicata interamente agli utenti Vertice^(R): in "Release" potrete leggere tutte le implementazioni e le correzioni effettuate dalla versione 03.05.00 ad oggi e visualizzare e/o stampare le "Istruzioni" per effettuare gli aggiornamenti. Una collezione di documenti "Indispensabili" Vi guiderà ad operare nel miglior modo all'interno della procedura gestionale.

Troverete interessanti informazioni sui nostri "Servizi": l'avviamento all'uso del software gestionale, i corsi d'informatica e di contabilità per le aziende e i privati, gli interventi on site, l'hot-line, la teleassistenza... ovvero tutte le attività di M.C.S.

Per i fans del ns. periodico *MCS Informa*, tutti i numeri a partire dal 2002. Nella sezione "Applicativi" potrete scaricare programmi freeware (gratuiti):

OpenOffice per l'automazione d'ufficio (vedi *MCS Informa* di dicembre), Acrobat Reader per visualizzare i file in formato pdf e Norman antivirus in versione dimostrativa per 30gg. A proposito di sicurezza del Vs. PC Vi rimandiamo all'articolo allegato relativo ai virus informatici e alla scelta di un valido pacchetto antivirus per difendersi dagli attacchi indesiderati e proteggere i propri dati.

Ad agosto meritiamo anche noi un periodo di riposo pertanto saremo

CHIUSI PER FERIE
da lunedì 4 agosto

a lunedì 25 agosto *compreso*

Durante tale periodo sarà a disposizione un numero di **EMERGENZA** che Vi

verrà comunicato dalla segreteria telefonica attiva al numero **0121/79.44.19.**



BUONE
VACANZE!

A PROPOSITO DI SICUREZZA INFORMATICA



Un virus è un piccolo programma che tenta in modo illecito di bloccare alcune risorse fondamentali di un computer, alterando o cancellando ad esempio il contenuto dei dati memorizzati o inibendo il corretto funzionamento dell'intero sistema. Va detto però che nessun virus può danneggiare fisicamente una qualunque parte del PC. Oltre allo scopo di dar "fastidio" (ma spesso di recar danno) all'utente, scopo principale di un virus è quello di propagarsi, in modo da infettare quanto più possibile molti elaboratori. Tipicamente il virus rimane "invisibile" al sistema anche per molto tempo, in modo da potersi diffondere e magari infettare il più possibile. Poi, in base al verificarsi di qualche evento (una data, l'accensione del computer, l'avvio

di un certo programma, e così via), il virus si attiva e inizia la sua opera virale. In pratica, un virus si "aggancia" ad un programma e quindi si carica in memoria centrale quando questo viene lanciato in esecuzione; il virus rimane in memoria anche se il programma viene terminato, e quindi è in grado di infettare (cioè di "agganciarsi") altri programmi che successivamente vengono caricati ed eseguiti (che in un normale utilizzo sono sempre gli stessi), aumentando quindi la possibilità di essere residente in memoria e quindi di entrare in azione nel momento stabilito. I virus in circolazione sono di diversa natura, e si possono classificare in base ad alcuni fattori quali sistema operativo, algoritmo di funzionamento e capacità distruttive. Una prima distinzione si può fare tra virus che infettano programmi (cioè file con estensione .exe o .com), virus che infettano il settore di avvio dei dischi (cosiddetto boot sector), virus che infettano file di



documenti (che contengono tipicamente macro, come i file di Word o Excel), virus che infettano reti di computer, e anche virus che hanno funzionalità miste o combinate tra quelle elencate. Altra distinzione può essere fatta tra Worm e Trojan: il primo è un particolare virus che ha il solo scopo di propagarsi il più possibile, non crea danni particolarmente seri ma infetta il contenuto di alcuni documenti o provoca sullo schermo l'apparizione improvvisa di messaggi o immagini di diversa natura, e tipicamente si diffonde tramite e-mail; il Trojan invece si ispira al famoso "cavallo di Troia" di epica memoria, ed è un virus un po' subdolo, in quanto si cela sotto le sembianze di un normale programma ma contemporaneamente si preoccupa di aumentare la vulnerabilità del sistema a possibili attacchi esterni, per esempio aprendo una porta di comunicazione non visibile dall'utente. I metodi di propagazione più diffusi sono tramite copia dell'applicativo o del file infetto su supporti di memorizzazione facilmente scambiabili quali quelli rimovibili (floppy disk, Cd-Rom, ecc...), oppure tramite allegati ai messaggi di posta elettronica, oppure tramite Internet. I più attivi dal punto di vista della diffusione sono certamente i virus che fanno uso dei client di posta per autoinviarsi ai contatti della rubrica, in questo modo la diffusione è enormemente facilitata, e in poche ore un virus può fare il giro del mondo. Per fortuna la pericolosità non è legata alla diffusione, anzi è spesso il contrario, ma **spesso viene messa in pericolo la privacy del malcapitato**, e non è un problema di poco conto. I nuovi ceppi virali sono programmati per auto allegarsi ai messaggi in uscita e inviarsi automaticamente a tutti gli indirizzi presenti nella rubrica del nostro client di posta. È necessario sottolineare che i messaggi di posta elettronica in formato tradizionale non sono in grado di trasmettere un virus a meno che non contengano in allegato un file eseguibile infetto. Le mail sono infatti costituite da testo in standard ASCII incapace di creare problemi virali. L'infezione legata alla posta elettronica è dovuta quindi all'esecuzione dell'allegato infetto, questa può avvenire in maniera esplicita dietro comando dell'utente, oppure automaticamente all'apertura del messaggio. Questa seconda modalità riscontrata soprat-

documenti (che contengono tipicamente macro, come i file di Word o Excel), virus che infettano reti di computer, e anche virus che hanno funzionalità miste o combinate tra quelle elencate. Altra distinzione può essere fatta tra Worm e Trojan: il primo è un particolare virus che ha il solo scopo di propagarsi il più possibile, non crea danni particolarmente seri ma infetta il contenuto di alcuni documenti o provoca sullo schermo l'apparizione improvvisa di messaggi o immagini di diversa natura, e tipicamente si diffonde tramite e-mail; il Trojan invece si ispira al famoso "cavallo di Troia" di epica memoria, ed è un virus un po' subdolo, in quanto si cela sotto le sembianze di un normale programma ma contemporaneamente si preoccupa di aumentare la vulnerabilità del sistema a possibili attacchi esterni, per esempio aprendo una porta di comunicazione non visibile dall'utente. I metodi di propagazione più diffusi sono tramite copia dell'applicativo o del file infetto su supporti di memorizzazione facilmente scambiabili quali quelli rimovibili (floppy disk, Cd-Rom, ecc...), oppure tramite allegati ai messaggi di posta elettronica, oppure tramite Internet. I più attivi dal punto di vista della diffusione sono certamente i virus che fanno uso dei client di posta per autoinviarsi ai contatti della rubrica, in questo modo la diffusione è enormemente facilitata, e in poche ore un virus può fare il giro del mondo. Per fortuna la pericolosità non è legata alla diffusione, anzi è spesso il contrario, ma **spesso viene messa in pericolo la privacy del malcapitato**, e non è un problema di poco conto. I nuovi ceppi virali sono programmati per auto allegarsi ai messaggi in uscita e inviarsi automaticamente a tutti gli indirizzi presenti nella rubrica del nostro client di posta. È necessario sottolineare che i messaggi di posta elettronica in formato tradizionale non sono in grado di trasmettere un virus a meno che non contengano in allegato un file eseguibile infetto. Le mail sono infatti costituite da testo in standard ASCII incapace di creare problemi virali. L'infezione legata alla posta elettronica è dovuta quindi all'esecuzione dell'allegato infetto, questa può avvenire in maniera esplicita dietro comando dell'utente, oppure automaticamente all'apertura del messaggio. Questa seconda modalità riscontrata soprat-



A PROPOSITO DI SICUREZZA INFORMATICA

tutto con Outlook e Outlook Express rende praticamente obbligatorio l'utilizzo di un antivirus ed è evitabile rimanendo costantemente aggiornati sulle patch rilasciate per le varie versioni di Outlook. Ma perché un normale utente dovrebbe aprire un allegato infetto? Semplicemente perché non sa che è infetto! La maggior parte dei virus ricevuti per posta elettronica ci vengono infatti inviati da persone conosciute che hanno contratto il virus via mail e in altri modi, e non è nemmeno detto che il nostro amico ci abbia mandato la mail infetta di sua volontà visto che alcuni virus sono in grado di replicarsi e rispedirsi automaticamente a tutti i contatti della rubrica. Se riceviamo una mail da un amico ci poniamo senza dubbio molti problemi in meno ad aprire l'allegato rispetto a una mail ricevuta da uno sconosciuto. Non bisogna dimenticare il classico metodo di scambio file che per anni è stato il veicolo migliore per infettare nuovi Pc. Bastava un floppy infetto scambiato tra amici per colpire velocemente molte macchine e contribuire così alla diffusione di virus informatici.

Quindi "prevenire è meglio che curare" e un buon antivirus, periodicamente aggiornato, è la soluzione più indicata.

Gli antivirus sono un categoria di software molto particolare che, con il trascorrere del tempo, si sta fondendo sempre più con altri programmi di utilità dedicati alla sicurezza informatica, non è raro quindi trovare piccoli firewall personali integrati nei programmi o estensioni della protezione a script maligni. Internet può essere il veicolo migliore per la diffusione dei virus ma anche la soluzione più rapida per debellarli infatti da alcuni anni la maggior parte degli antivirus è in grado di aggiornarsi collegandosi alla rete. Questa funzionalità è più o meno curata a seconda dei vari software ma è sempre comunque in grado di aggiornare il prodotto; la modalità di aggiornamento migliore è quella completamente automatica, oppure programmabile a date determinate in cui si prevede di essere collegati alla rete e il computer sia acceso. Le operazioni da svolgere per eseguire questi aggiornamenti nel caso non vengano eseguiti automaticamente sono comunque molto semplici, e si risolvono il più delle volte con pochi clic del mouse. In alcuni casi possono essere richiesti i dati delle licenze del prodotto, mentre in altri il tutto avviene senza alcuna richiesta. Con questa indubbia comodità

avremo sul nostro computer un software sempre aggiornato con le ultime firme virali senza compiere nessuna operazione. Gli aggiornamenti messi a disposizione dalle varie software house sono molto frequenti, in alcuni casi addirittura giornalieri, e ci consentono di lavorare al computer con relativa sicurezza. Diverso come concetto ma non come sistema di aggiornamento è l'upgrade del motore di scansione vero e proprio, se infatti le firme virali sono importanti per scovare nuovi virus l'algoritmo utilizzato per effettuare la ricerca lo è altrettanto. L'aggiornamento del motore di scansione può inoltre essere necessario non solo per effettuare migliorie alla precedente versione ma anche per correggere eventuali errori che potrebbero compromettere la sicurezza del sistema.



In conclusione il software antivirus ottimale deve fare solamente un semplice compito: proteggere il computer dal problema dei virus.

Norman, azienda norvegese leader nel settore della sicurezza informatica propone NVC, Norman Virus Control, un antivirus progettato per analizzare e difendere "workstation" e "server" dai virus, anche quelli non ancora completamente identificati e garantire un buon livello di sicurezza soprattutto per quei PC vulnerabili 24 ore su 24 per 365 giorni l'anno.

Dal sito Norman (<http://www.norman.com>) potrete scaricare e installare la versione dimostrativa di **NVC IN PROVA PER 30 GG.**

NORMAN

Oppure potrete richiedere il CD per l'installazione al ns. Ufficio Commerciale il quale rimane a Vs. disposizione per fornirVi maggiori informazioni (tel. 0121,794419).