Virus, anno settimo

Correva l'anno di grazia 1986 quando fu scoperto il primo «virus informatico», un termine che all'epoca fece sorridere i più e forse causò un minimo brivido di eccitazione nei paladini a oltranza della vita artificiale.
Sette anni nel continuo spaziotemporale dell'informatica sono tantissimi; all'epoca cominciavano già a vedersi i primi 286, adesso guardiamo con scetticismo ai Pentium e ci chiediamo se valga poi davvero la pena questo ennesimo cambio di microprocessore; il DOS era alla versione 2.10, ora abbiamo una pletora di sistemi operativi dei quali spesso non sappiamo che fare, e li installiamo sui nostri PC supergonfiati di RAM, di cache e di mega o gigabyte soltanto per poter dire che noi li abbiamo installati

di Stefano Toria

Sette anni che hanno visto il venerdì 13 (ottobre 1989), il Michelangelo, le affermazioni dei guru prontamente smentite dai fatti, la nascita di pubblicazioni cartacee o elettroniche, poi conferenze, convegni, dibattiti televisivi sulla presunta fine dell'era informatica, e una valanga di sciocchezze.

Sette anni in cui, soprattutto, il fatto più rilevante si è svolto in silenzio: da quel primo Brain che fece la sua comparsa quasi silenziosa sui dischetti di alcuni turisti americani tornati dal Pakistan nel 1986 siamo arrivati oggi a tremila virus; la crescita è stata biologica, cioè esponenziale, e non sembra destinata ad arrestarsi per ora.

Anzi: proprio quest'anno un simpatico (!) ignoto ha pensato di fare un omaggio natalizio anticipato ai più noti ricercatori, inviando loro 250 nuovi virus. Nessuno di tali virus risulta effettivamente nuovo di per sé, dato che si tratta di virus piuttosto vecchi (dai due ai tre anni). Ma ciascun virus era stato lievemente modificato, in modo da renderlo invisibile allo Scan di McAfee.

VX BBS: una sigla, un incubo

Sembrerebbe che questa bravata sia la diretta conseguenza della pubblicazione, su un VX BBS, di un certo numero di stringhe utilizzate da McAfee nel suo antivirus.

Questo dei «virus exchange BBS» (abbreviato in VX) è un problema nel problema; non è possibile fare stime ma tutti gli esperti concordano nel ritenere che questi sistemi, più o meno clandestini, abbiano potenziato l'espansione del fenomeno dei virus, e che se fosse possibile chiuderli tutti da un giorno all'altro il problema dei virus non sarebbe certamente risolto ma verrebbe a cessare un pericoloso moltiplicatore.

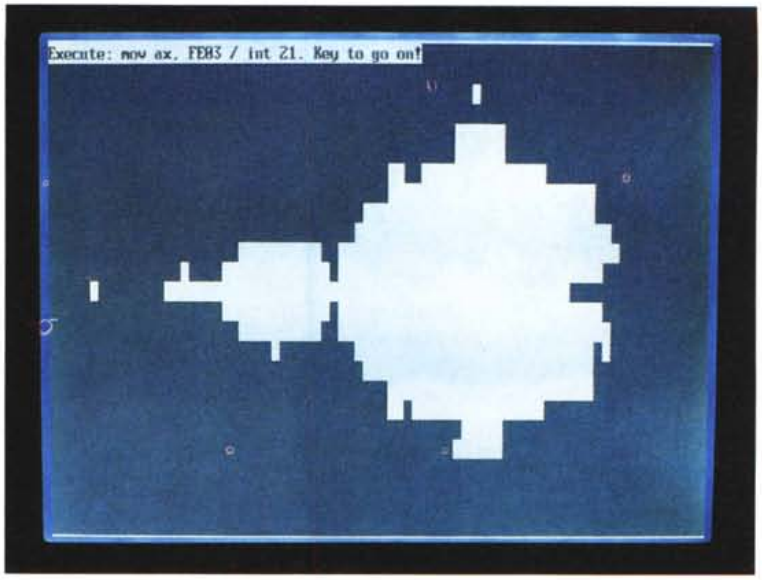
Il fatto più preoccupante, riguardo al «regalo di Natale» di cui parlavamo poc'anzi, è che i virus sono arrivati compressi in un file che si chiama PART1.ZIP, facendo supporre che si tratti soltanto della prima puntata. Già adesso molti programmi di scansione antivirus sembrano lì lì per scoppiare; un ritmo di crescita di duecentocinquanta nuove varianti ogni mese costituirebbe un banco di prova formidabile per i produttori, e andando avanti di questo passo si potrebbe ipotizzare per i prossimi mesi una morìa di programmi antivirus, che andrebbero ad aggiungersi ai diversi che sono già spariti negli ultimi tempi.

Venti, duecento, tremila

Quando un utente inizia ad approfondire la propria conoscenza del computer, e scopre tra l'altro la vastità del problema dei virus, rimane stupefatto per via del numero di virus esistenti. Duemila, duemilacinquecento, tremila: dovunque egli legga, trova numeri differenti. Non ci sono due prodotti antivirus che riportino lo stesso numero di ceppi virali esistenti e riconosciuti. Due sono le domande che sorgono spontanee:

- Come è possibile che ci siano così tanti virus?
- Saranno veri i numeri stampati bene in vista sulle scatole degli antivirus?

La risposta alla prima domanda è la più semplice. Sì, è possibile che i virus siano così tanti perché il fenomeno si è diffuso ormai a macchia d'olio, man mano che progredivano le conoscenze medie di programmazione in linguaggio Assembler; che nascevano e si sviluppavano VX BBS un po' dappertutto, dai quali chiunque poteva prelevare campioni di virus esistenti per studiarli, analizzarli, modificarli; che persone senza scrupoli cercavano di cavalcare la tigre scrivendo e pubblicando libri che, sotto la bandiera di una malintesa «libertà di espressione e di informazione» e di una interpretazione forzata del Primo Emendamento della Costituzione degli Stati Uniti, fornivano in realtà istruzioni precise e dettagliate su come farsi da sé il proprio virus.



Virus «Tequila».

Per quanto attiene alla seconda domanda, la risposta è più complessa. La classificazione dei virus (la «tassonomia», prendendo un termine a prestito dalle scienze naturali) non è gestita da un organismo unico. Le persone che si occupano dell'analisi dei virus sono qua-

Passo per passo: come difendersi dai virus

Ci sono pochi argomenti che hanno dato origine a tanta informazione approssimata, per non dire disinformazione, quanto è accaduto per i virus.

L'utente meno esperto si rivolge a chi ne sa (o ne dovrebbe sapere) di più e riceve risposte confuse, approssimate, spesso contraddittorie; ne esce talvolta con la convinzione che il problema sia al di fuori della sua portata e che quindi l'unica soluzione consista nel fatalismo, nell'affidarsi alla fortuna; in altri casi ricava l'impressione che difendersi dai virus sia facilissimo, basta comprare il prodotto giusto.

C'è un briciolo di verità in entrambi questi punti di vista, come c'è al tempo stesso una grande imprecisione in tutti e due. Non è questione di fatalismo perché è possibile fare qualcosa di concreto e con successo, né basta acquistare un prodotto qualsiasi per essere automaticamente al sicuro perchè per sua natura il problema dei virus sfugge agli automatismi.

È vero tuttavia che la soluzione del problema passa per l'utilizzo di strumenti ben precisi, come anche è vero che l'utente deve sapere che in ogni caso, per quante precauzioni abbia preso, rimarrà comunque esposto a un rischio che le precauzioni possono minimizzare ma non escludere.

Vediamo in breve le cose che tutti gli utenti debbono sapere, anche se non hanno una conoscenza approfondita del funzionamento del proprio elaboratore.

1. Un virus è un programma come qualsiasi altro. Non si tratta di «creature» particolari, di cose al di fuori dell'immaginazione di tutti se non dei più audaci smanettatori di computer.

È concettualmente analogo ai programmi di cui l'utente si serve tutte le volte che mette mano al computer.

E poiché l'elaboratore è progettato per eseguire programmi, ne deriva che per l'elaboratore non c'è assolutamente alcuna differenza tra un virus e un programma di qualsiasi altro tipo. L'elaboratore non sa riconoscere un virus mentre lo sta eseguendo.

2. Siccome un virus è un programma come tutti gli altri allora non ci possiamo fidare al 100% del nostro elaboratore per identificare e scoprire i virus, nel senso che non possiamo delegare interamente a lui il compito di riconoscere un virus da un non-virus.

Questo, che sembra un sillogisma abbastanza banale, è in realtà un punto importantissimo in quanto stabilisce la necessità che siamo noi a preoccuparci attivamente di difenderci dai virus, perché non esiste alcuno strumento software che metta il nostro elaboratore in condizione di riconoscere con infallibile certezza tutti i virus e distinguerli con certezza altrettanto infallibile da tutto ciò che virus non è.

3. Se si delega all'elaboratore una parte della prevenzione del problema-virus si dovrà essere preparati a prendersi direttamente cura di un'altra parte della prevenzione.

È la conseguenza diretta del punto precedente. Siccome l'elaboratore non è in grado di fare tutto da solo, dobbiamo aiutarlo nel lavoro di prevenzione.

Come? Semplice: adottando alcune semplici norme di igiene informatica che vedremo ai punti prossimi.

4. La prima regola è: evitare che l'elaboratore esegua programmi che non è indispensabile eseguire.

Detto così suona ancora una volta banale, ma chiariamo meglio con un esempio. Molti utenti continuano a ignorare il fatto che tutti i dischetti formattati per i sistemi MS-DOS contengono un settore di avvio perfettamente valido, che consiste nel programma che scrive a video la frase «Disco non di sistema - sostituire e premere un tasto». Anche i dischetti «non di sistema» sono in realtà «di sistema», sebbene il sistema che viene eseguito da questi dischetti sia tutt'altro che sufficiente a far partire la macchina:

si sempre le stesse che sviluppano i programmi di difesa dai virus; la presenza di interessi commerciali ha impedito finora che si stabilisse una vera ed efficiente cooperazione tra i ricercatori.

A ciò bisogna aggiungere il fatto che molti virus sono frutto di un lavoro di trasformazione e rielaborazione di virus esistenti, anche se non sempre con scopo così manifestamente maligno come i duecentocinquanta di cui abbiamo parlato poc'anzi. Qualcuno, spinto da curiosità, oppure mosso dal desiderio di scrivere un virus ma non essendo in grado di partire da zero, ha preso un virus esistente e l'ha modificato in misura maggiore o minore.

Se le modifiche rispetto al «ceppo» originario sono minime, tutti i ricercatori concordano nel ritenere il nuovo virus variante del precedente. Ma in alcuni casi le variazioni sono tali e tante da indurre taluni ricercatori a considerarlo un nuovo virus, determinando uno scarto nella numerazione.

Informazione e prevenzione

Il migliore antivirus del mondo è l'utente, questo è uno dei pochi punti su cui gli esperti concordano in blocco. Anziché acquistare in blocco centinaia di copie di programmi antivirus, quindi, le grandi aziende trarrebbero maggiore beneficio da una massiccia campagna di informazione. Il software viene dopo, quando gli utenti hanno imparato cosa farci e come usarlo.

I corsi specializzati sui virus, tenuti da docenti effettivamente qualificati, sono ancora una rarità in Italia. Non è così in alcuni altri paesi, dove sono disponibili oltretutto informazioni precise e realmente utili.

Da quando abbiamo iniziato a pubblicare questa rubrica, tre anni fa, siamo stati seguiti da molte altre riviste. Non tutti gli articoli che abbiamo avuto occasione di leggere ci hanno dato l'impressione di rispondere ai requisiti di precisione e utilità.

Se forse qualche appassionato, spesso inconsapevole dei rischi che corre e che fa correre a chi gli sta intorno, può trovare divertente capire come sono fatti i virus al loro interno, quali sono i meccanismi di replicazione e di mimetizzazione, è certo che per la massa degli utenti queste informazioni sono del tutto inutili. Come anche inutili e fuorvianti sono i vari «calendari» dei virus, che hanno il solo effetto di concentrare l'attenzione dell'utente su un particolare virus, che magari non è affatto diffuso, e distrarlo da altri che possono costituire per lui un maggiore pericolo.

Non ci sono «giorni a rischio» per i virus, l'abbiamo ripetuto diverse volte: ogni giorno in cui accendiamo il nostro computer è un giorno potenzialmente a rischio.

«Qual è il migliore programma antivirus?».

Ci siamo sentiti rivolgere questa domanda diverse centinaia di volte. Purtroppo non c'è una risposta, per una serie di ragioni che cercheremo di esporre in modo chiaro e sintetico.

Un programma antivirus, innanzitutto, è diverso da qualsiasi altro programma. Il tipo più diffuso di antivirus è lo «scanner»; non ha nulla a che vedere con il dispositivo che «legge» le immagini e le trasforma in file grafici, se non il fatto che hanno in comune il nome.

Uno scanner antivirus è un programma che riconosce le configurazioni di

al contrario, serve proprio a bloccarla per attirare l'attenzione dell'utente sul fatto che è stato inserito nel drive un dischetto che non contiene alcun sistema.

Questo minimo programma (sono poche istruzioni) è sufficiente per trasportare un virus, e in realtà i virus più diffusi sono proprio quelli di questo tipo.

Perché? È presto detto. Quante volte è accaduto a chi legge di vedersi comparire davanti la frase «Disco non di sistema etc.»? Bene, ogni volta che questa frase è comparsa è stato eseguito un programma che non era indispensabile eseguire, anzi era del tutto superfluo; e ogni volta che si è eseguito il programma che scrive questa frase si è corso il rischio di infettarsi con un virus.

I due virus numericamente più diffusi (Form e Stoned) sono proprio di questo tipo, perché i loro autori sapevano bene che tra le cattive abitudini degli utenti di computer c'è anche il fatto di accendere il computer senza aver tolto l'eventuale dischetto presente nel drive. Quindi

Regola Numero Uno: prima di accendere il computer verificare che i drive dei dischetti siano vuoti.

Deve diventare un riflesso, un tic. Mano al dispositivo di estrazione del dischetto, E POI all'interruttore: non viceversa. Quando poi il DOS sarà andato su, allora si potrà inserire il dischetto.

5. Evitare di eseguire programmi non indispensabili sembra una raccomandazione facile da seguire e forse un po' ovvia, eppure è altrettanto facile che venga trascurata. Nessuna infermiera di uno studio dentistico si sognerebbe di utilizzare i ferri del dentista per curarsi le unghie.

Ricordo di aver letto tempo fa che un operaio fu licenziato perché aveva bloccato il nastro trasportatore che portava delle parti dal magazzino all'officina di produzione, e vi si era sistemato sopra per farsi un sonnellino: nessuno si era stupito del provvedimento dell'azienda. Eppure pochi trovano inaccettabile che un elaboratore destinato a svolgere un lavoro produttivo venga utilizzato per giochi, prove di programmi procurati qua e là, e altre attività non pertinenti al lavoro.

Non si vuole fare del moralismo, né suggerire un modo di lavorare simile a quello dell'Estremo Oriente, in cui la fedeltà e la dedizione assoluta all'azienda sono tutto. È una questione di utilità comparata. Una precauzione minima, quale quella che vuole separati lavoro e svago, quantomeno su due computer diversi e non comunicanti tra di loro, ripaga in termini di maggiore sicurezza del lavoro.

6. La maggior parte del costo di un incontro ravvicinato con un virus consiste nel tempo perso nel trovarlo, capire di che virus si tratta, poi eliminarlo, e infine ricominciare tutto da capo a breve scadenza perché il problema, che si credeva risolto, si è ripresentato dopo pochi giorni.

L'unico modo per ridurre al minimo questo costo è di sapere in anticipo quello che può succedere, ed essere pronti a fronteggiare l'evenienza.

I danni determinati dai virus possono essere raggruppati in due classi:

- danni diretti, immediati, all'atto dell'infezione; i programmi che l'utente aveva installato per eseguire il proprio lavoro sono modificati, alterati, resi provvisoriamente o - in alcuni casi - irreversibilmente inutilizzabili;
- danni successivi, che possono verificarsi qualora il virus responsabile dell'infezione preveda un meccanismo di innesco e danneggiamento; non tutti i virus lo fanno e comunque tra l'infezione e la determinazione di questo secondo tipo di danni può passare anche diverso tempo, con la possibilità di intercettare ed eliminare il virus prima che possa compiere questi danni.

Il metodo per prevenire le conseguenze di entrambi i tipi di danni è lo stesso, non presenta nulla di particolarmente innovativo e anzi è qualcosa che molti utenti si sono sentiti ripetere fino alla nausea:

Regola Numero Due: fare seriamente le copie di sicurezza.

Nel prossimo numero affronteremo le copie di sicurezza, spiegando come vanno fatte per ottenere il massimo del risultato con il minimo della perdita di tempo.

Accendere il computer senza precauzioni...

...può essere pericoloso.

istruzioni che fanno parte di un particolare virus; quando trova una di queste configurazioni, detta anche «firma» o «impronta», dentro un programma eseguibile, ne trae la conclusione che il programma è stato infettato da quel particolare virus.

Questa tecnologia di identificazione dei virus presenta un punto debole, che consiste proprio nelle impronte. Punto primo: per riconoscere tremila virus servono tremila impronte diverse. Questo fatto fa crescere a dismisura i programmi antivirus; alcuni produttori hanno cercato di sviluppare dei metodi di «riconoscimento generico» che presentano il vantaggio di non far crescere più di tanto la dimensione degli antivirus, ma per contro manifestano una minore precisione e possono occasionalmente lasciarsi sfuggire il riconoscimento di un virus, dando per buono un programma che in realtà è infetto (una «falsa certezza»).

Punto secondo: l'impronta deve essere determinata da un essere umano, il quale decide, in base alla propria competenza ed esperienza, che quella determinata sequenza di istruzioni si può trovare in quel virus e soltanto in quel virus. Ma questa affermazione è pericolosa, perché presupporrebbe, per essere fatta con assoluta certezza, che l'esperto abbia effettivamente visto tutti, proprio tutti i programmi esistenti al mondo (non so quante decine di milioni possano essere), compreso il programma che scriverò domattina.

Essendo ovviamente impossibile che l'esperto conosca a memoria tutto il software che esiste al mondo, dovrà basarsi su procedimenti euristici, e partorirà quella che «secondo lui» è una configurazione di istruzioni che «ragionevolmente» non si trova in nessun altro programma se non nei programmi infettati da quel particolare virus.

Nel 99% dei casi va tutto bene, ma occasionalmente viene segnalata la presenza di un virus in un programma che è tutt'altro che infetto (un «falso allarme»). È accaduto nel corso del 1993 con una nuova versione del famoso archiviatore/compressore PKZIP, nella cui versione 2.04c il Norton AntiVirus segnalava la presenza del virus «Maltese Amoeba» quando in realtà non c'era alcun virus.

Il programma antivirus perfetto è quello che presenta percentuali di falsi allarmi e di false certezze entrambe costantemente pari allo 0%.

Poiché un programma del genere non esiste né potrà mai esistere, ci si dovrà accontentare di un «buon» programma, e utilizzare almeno due programmi simultaneamente, per le ragioni che andiamo a esporre.

Perché due antivirus?

Mediamente ogni mese escono un centinaio di nuovi virus. Se dovesse stabilizzarsi il tasso di crescita gentilmente offerto dal simpatico ignoto di cui si parlava sopra, schizzeremmo a duecentocinquanta nuovi virus al mese: in ogni caso un numero formidabile, anche se si rimane agli attuali tassi di crescita.

Per aggiornare i propri software i produttori di antivirus debbono procurarsi i campioni dei nuovi virus. Non tutti se li procurano dalla stessa fonte; si produrrebbe una idilliaca situazione di mercato quasi perfetto, che nella realtà è ben lungi dall'esistere. Pertanto è verosimile che se in un mese escono i tre nuovi virus A, B e C uno dei produttori riesca ad averli tutti e tre immediatamente, un altro ottenga solo A e C, un altro ancora A e B e poco dopo una versione modificata di C, eccetera.

Per questo motivo non ci sono due programmi antivirus che offrano le stesse prestazioni in termini di riconoscimento di virus. L'uno ne riconoscerà di più, l'altro di meno; l'uno sarà più preciso nella distinzione tra varianti, l'altro più veloce, e così via.

Inoltre sono diverse le periodicità di aggiornamento degli antivirus. Alcuni produttori inviano ai propri abbonati una nuova versione regolarmente ogni mese, altri ogni due mesi o con periodicità variabili.

Pur non essendo di per sé sufficiente a risolvere il problema dei virus, il software antivirus è parte fondamentale della strategia di difesa. Ma risulta del tutto inutile se non è in grado di riconoscere il maggiore numero possibile di virus.

È evidente quindi che non è sufficiente affidarsi a un solo programma. Data la possibilità di andare incontro a false certezze o a falsi allarmi, possibilità che cresce insieme al crescere del numero di virus esistenti, è essenziale affidarsi a due programmi differenti.

«Allora, bastano due scanner?»

Il possesso di due programmi di scansione è indispensabile, ma non è affatto detto che sia sufficiente. Inoltre i sistemi di difesa dai virus non si limitano agli scanner.

Ci sono altre tipologie di programmi di supporto alla difesa dai virus, alcuni dei quali sono in grado di fornire un valido contributo. Alcuni di questi programmi sono stati scritti avendo in mente specificamente il problema-virus; altri sono prodotti di uso più generico, i quali tuttavia trovano una valida applicazione nella lotta ai virus.

Alla prima categoria appartengono i programmi di controllo di integrità. Il lo-

ro funzionamento si basa su un presupposto elementare: qualsiasi virus all'atto dell'infezione determina una modifica in qualche parte del sistema vittima. Un metodo infallibile per identificare un virus consiste nel predisporre un sistema che consenta di rilevare queste modifiche.

Descritta così sembrerebbe la soluzione finale; invece presenta non pochi problemi, come vedremo in un prossimo numero della rubrica quando esamineremo a fondo il funzionamento di questi programmi; tuttavia se correttamente installati e utilizzati i programmi di controllo di integrità sono in grado di fornire indicazioni preziose.

Se si dovesse pensare a un tipo di software utile nella lotta ai virus seppure non specificamente realizzato per essa, il primo che verrebbe in mente sarebbe il software per le copie di sicurezza. Ma non è il solo tipo di software generico che presenta funzioni di supporto alla difesa dai programmi aggressori; e anche questo argomento sarà ulteriormente sviluppato in uno dei prossimi articoli.

Fidarsi è bene, etc.

Un rischio che molti utenti corrono, in una fase o nell'altra della propria crescita informatica, è di diventare lievemente paranoici riguardo ai virus. Paradossalmente moltissimi corrono anche il rischio opposto, cioè di ritenere che sia tutta una gran paranoia e quindi non vale la pena prendere tante precauzioni, perché tanto tutti questi scambi di dischetti non li si fa, e comunque soltanto con persone fidate.

L'atteggiamento più saggio, manco a dirlo, sta nel mezzo. Un pizzico di paranoia non guasta, ogni tanto; e la nostra è tutt'altro che una battuta, se lo scorso settembre, all'autorevole Terzo Convegno Internazionale sui Virus organizzato dall'autorevolissimo «Virus Bulletin», un ancor più autorevole rappresentante della più autorevole delle Università, l'Università di Oxford, ha sintetizzato il proprio intervento nello slogan «It Pays to Be Paranoid» (essere paranoici conviene).

Lo stesso relatore ha espresso sotto forma di slogan un altro concetto fondamentale nella prevenzione dei virus: «Anche il vostro migliore amico può avere un virus nel computer e non saperlo».

Abbiamo assistito a talmente tanti casi del verificarsi di questo fatto da considerarlo ormai una regola. Quando ci viene assicurato che «non è possibile che il virus sia stato portato da XY, è una persona fidata» quasi sempre finiamo con lo scoprire che il virus è arrivato proprio da XY.

E sovente questo XY è il consulente informatico della ditta, una persona cioè di cui ci si fida.

Quando questo accade, è difficile convincere l'utente che il consulente non ha alcuna colpa, se non forse quella di essere stato forse un po' incauto; in ogni caso la lezione è quasi sempre utile, perché ha l'effetto di insegnare all'utente (e al consulente) che un po' di sicurezza in più non guasta.

MC

Stefano Toria è raggiungibile tramite MC-link alla casella MC0170 e tramite Internet all'idirizzo MC0170@mclink.it

Le nostre stampa
perché abbiamo sem

SISTEMA LASER

nti vivono meglio plificato la loro vita.

SISTEMA LED

OL 400ex

La vita delle tradizionali stampanti laser è piuttosto difficile. Infatti si basa ancora su di un complicato meccanismo di specchi, lenti e raggi, con un sistema di rifrazione molto delicato, perché prevede numerosi passaggi dalla sorgente laser al tamburo.

E' quindi bisognoso di una attenta e frequente manutenzione. Insomma una vita segnata dalle preoccupazioni.

Le stampanti OKI LED, invece, vivono decisamente meglio. Hanno una sola lente e una barra fissa dove sono collocati i diodi emettitori di luce, per cui vengono eliminate le parti in movimento, più soggette ad usura, e tutti i problemi a questo connessi, con riduzioni di ingombro e peso.

Di conseguenza hanno una maggiore affidabilità ed una migliore durata nel tempo. Non a caso le stampanti OKI sono garantite 5 anni sull'unità LED, contro i soli 3 anni delle altre. Tutto questo significa una qualità di stampa con eccellenti livelli di definizione e risoluzione finale, perfettamente comparabili agli standard più diffusi.

La grande differenza sta nel fatto che il sistema OKI LED di seconda generazione è stato concepito anche per rispondere alle più attuali esigenze di risparmio energetico e ambientale.

Una stampante OKI LED, per esempio, consuma in media 80 watt contro i 400 watt di molte stampanti, con la totale assenza di emissioni di ozono, tipiche di altri sistemi. Una evoluzione nella direzione della semplicità, della affidabilità e della tranquillità.

E quando le stampanti vivono più serene, rendono più serena anche la vita di chi sta accanto a loro.

OKI

People to People Technology

IN ITALIA OKI E' ... STAMPANTI, TELEFAX E TELEFONI CELLULARI.