ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΓΙΑ ΣΧΗΜΑΤΩΝ Η/Υ

ΠΡΟΣΒΟΛΕΣ

Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΠΡΟΣΤΑΣΙΑ ΣΥΣΤΗΜΑΤΩΝ ΗΛΥ ΣΥΝΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΠΟ ΠΡΟΣΒΟΛΕΣ ΙΟΝ.

ΕΠΙΜΕΛΕΙΑ ΕΚΔΟΣΗΣ:
Καλλιτεχνική Επιμέλεια, Ηλεκτρονική Επεξεργασία Φωτογραφιών κα Εκτύπωση.

ΤΟΝΙΑ ΧΑΜΠΑ

ΜΕΣΟΛΟΓΓΙ, ΜΑΙΟΣ 2001.

ΠΕΡΙΕΧΟΜΕΝΑ ΥΛΗΣ

Μ Ε Ρ Ο Σ Π Ρ Ω Τ Ο

Η/Υ ΚΑΙ ΔΙΚΤΥΑ ΣΤΙΣ ΣΥΝ/ΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣΕΙΣ.

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

ΚΕΦΑΛΑΙΟ 1

ΚΕΦΑΛΑΙΟ 2

ΚΕΦΑΛΑΙΟ 3

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

ΠΡΟΣΦΟΡΕΣ ΣΥΣΤΗΜΑΤΩΝ Η/Υ ΣΤΙΣ ΣΥΝ/ΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΑΠΟ ΤΟΥΣ

ΚΕΦΑΛΑΙΟ 1

ΚΑΤΑΣΚΕΥΑΣΤΙΚΟΙ ΟΙΚΟΙ ΚΑΙ ΤΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥΣ.

ΚΕΦΑΛΑΙΟ 2

ΠΩΣ ΜΠΟΡΕΙ ΝΑ ΜΠΑΙΝΕΙ ΕΝΑΣ ΙΟΣ ΤΑ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ ΤΩΝ ΣΥΝ/ΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ.

ΚΕΦΑΛΑΙΟ 3

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΣΥΣΤΗΜΑΤΩΝ Η/Υ ΣΥΝ/ΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΙΩΝ.

ΠΡΟΛΟΓΟΣ

Η συγγραφή της ετούτης επιστημονικής εργασίας που έχει ως θέμα:΄΄**Προστασία συστημάτων Η/Υ συν/κων επιχειρήσεων από προσβολές ιών**΄΄, εντάσσεται στα πλαίσια του διδακτικού αντικειμένου που διδάχτικε μέσα σε εφτά εξάμηνα στο τμήμα Συν/κων Οργανώσεων και Εκμεταλλεύσεων του τεχνολογικού ιδρύματος Μεσολογγίου.Η ιδέα του θέματος αυτού προέκυψε από την ανάγνωση διαφόρων εντύπων για την επιστήμη των Η/Υ στον σύγχρονο εμπορικό κύκλο των επιχειρήσεων.Μια επιστήμη που θεωρείται ως μια πολυδιάστατη και πολύμορφη τάξη θεμάτων που ποικίλουν από τις εφαρμογές της πληροφορικής,του προγραμματισμού και τους υπολογισμούς ως την επίδραση των υπολογιστών στην κοινωνία και ειδικότερα στις επιχειρηματικές δραστηριότητες του ανθρώπου που υπάγονται μέσα σ' αυτήν.

Μια εισαγωγή σε τέτοια τάξη θεμάτων πρέπει να παρουσιάζει μία ευρεία εικόνα των πολλών χαρακτηριστικών διαστάσεων και των σχέσεων τους, δίνοντας στους μη-ειδικούς μια ενημερωτική σφαιρική άποψη για τις εφαρμογές των Η/Υ στον κόσμο των επιχειρήσεων και στους ενδιαφερόμενους φοιτητές μια κατάλληλη βάση μόρφωσης από την οποία μπορούν αργότερα να επιλέξουν ειδικευμένα θέματα πληροφορικής και να ακολουθήσουνε προχωρημένες σπουδές πληροφορικής στο πεδίο που τους ενδιαφέρει. Η εργασία αυτή έχει ως κύριο σκοπό να εξηγήσει με καθαρό τρόπο το σύγχρονο κόσμο των Η/Υ και να εστιάσει τα μειονεκτήματα τους στις συν/κες επιχειρήσεις που θα έχουν μεγαλύτερη επίδραση καθώς διανύουμε την τρίτη χιλιετηρίδα και τις νέες φάσεις της ΄΄επανάστασης των πληροφοριών΄΄.

Η κατανόηση του τρόπου επίδρασης, λειτουργίας και χρήσης των υπολογιστών και του τρόπου με τον οποίον τα υπολογιστικά συστήματα μπορούν να βοηθήσουν τον άνθρωπο στην λήψη αποφάσεων και επίλυση προβλημάτων, δεν θα πρέπει να περιορίζεται αποκλειστικά στην οπωσδήποτε σημαντική εργαστηριακή εξάσκηση για εκμάθηση χρήσης πακέτων λογισμικού.Η κατάλληλη παρουσίαση των βασικών εννοιών των υπολογιστών και η κριτική εξέταση υλικού, λογισμικού και υπολογιστικών συστημάτων, καθώς επίσης των τεχνικών που χρησιμοποιούνται για την αποδοτική

σύνδεσή τους, αποτελούν σημαντικούς παράγοντες κατανόησης και εκμάθησης του

τρόπου λειτουργίας και χρήσης των σύγχρονων υπολογιστών.Επειδή ακριβώς η χρήση Η/Υ και δικτύων είναι απαραίτητη στην σημερινή ζωή του άνθρωπου είναι υποχρεωμένος αν επιθυμεί να διασφαλίσει την ασφάλεια πληροφοριών συστημάτων Η/Υ να απομακρύνει τις διάφορες δυσλειτουργίες τους όπως είναι οι προσβολές των ιών με την εφαρμογή των σωστών μέτρων προστασίας για να αποφευχθούν οι δυσάρεστες συνέπειες στον άνθρωπο χρήστη και σε κάθε επιχείρηση συνεταιριστική.

Η εργασία αυτή χωρίζεται σε δύο μέρη:

Το πρώτο μέρος χωρίζεται σε τρία κεφάλαια.Το πρώτο κεφάλαιο περιέχει μια σύντομη ιστορική ανασκόπηση των υπολογιστών και μια ενδεικτική περιγραφή των πλεονεκτημάτων των Η/Υ στον σύγχρονο εμπορικό κύκλο των επιχειρήσεων.Το κεφάλαιο δυο περιγράφει τις εφαρμογές των Η/Υ στις συν/κες επιχειρήσεις εφόσον αναπτύσσουν επιχειρηματικές δραστηριότητες όπως όλες οι επιχειρήσεις, ενώ το τρίτο κεφάλαιο αναφέρεται στην ασφάλεια συστηματων Η/Υ σε συν/κες επιχειρήσεις όπου εγκαθίστανται αναγκαία να εφαρμόζεται ιδιαίτερα σ'αυτές τις επιχειρήσεις εφόσον ο σκοπός λειτουργίας τους βασίζεται στην διασυνεταιριστική συνεργασία.

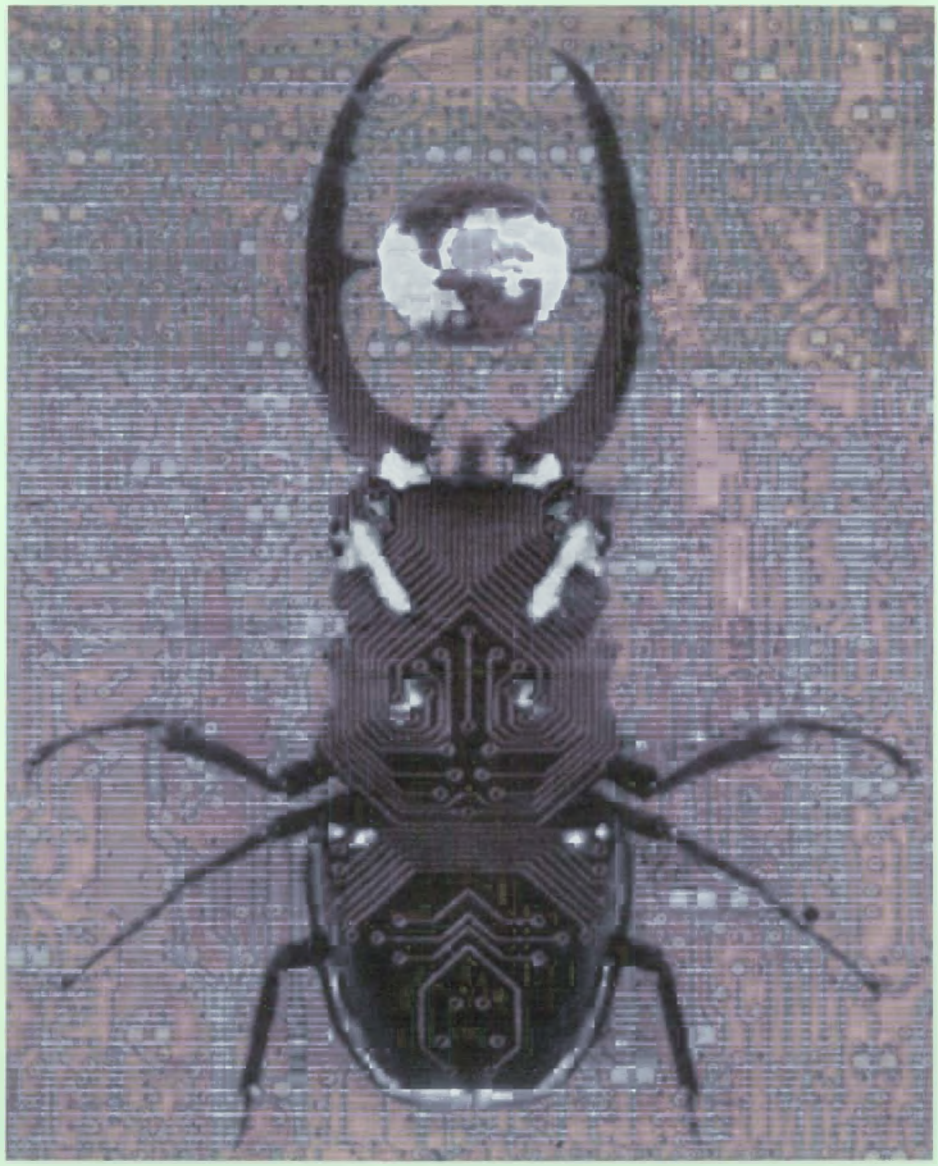
Το δεύτερο μέρος της εργασίας αυτής αποτελείται από τρία κεφάλαια.Το πρώτο κεφάλαιο εισάγει το φαινόμενο των ιών, τις διαστάσεις του προβλήματος, τα διάφορα είδη ιών, τα βλαπτικά προγράμματα,οι κακόβουλοι βάνδαλοι που προσπαθούν να θέσουν υπό τον έλεγχό τους τον υπολογιστή.Το δεύτερο κεφάλαιο εξηγεί τον τρόπο με τον οποίο ένας ιός μπορεί να εισβάλει τα υπολογιστικά συστήματα και πως οι ιοί ελέγχουν το πρόγραμμα ενός υπολογιστή.Τέλος στο τρίτο κεφάλαιο αναφέρεται στη διαδικασία αντιμετώπισης της κρίσης και καλύτερης στρατηγικής για την προστασία των δεδομένων, την πρόληψη,την διάγνωση και στην χρησιμοποίηση αντιβιοτικών για την προστασία των προγραμμάτων. Η συγγραφέας αυτής της εργασίας επιθυμεί να ευχαριστήσει όλους όσους βοήθησαν σ' αυτή την εργασία που συντέλεσαν σημαντικά στην βελτίωση των παρόντων κειμένων καθώς και εκείνους που βοήθησαν ποικιλόμορφα,ο καθένας από τη δική του θέση και με τη δική του ικανότητα στην παραγωγή αυτής της εργασίας.

Τέλος για οποιαδήποτε παράλειψη της εργασίας, την ευθύνη φέρει η συγγραφέας της, η οποία ευχαρίστως θα αποδεχόταν την όποια καλοπροαίρετη κριτική.

ΤΟΝΙΑ ΧΑΜΠΑ

ΜΕΡΟΣ Α΄

«Η/Υ ΚΑΙ ΔΙΚΤΥΑ ΣΤΙΣ ΣΥΝ/ΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ»



ΚΕΦΑΛΑΙΟ 1

ΧΡΗΣΗ Η/Υ ΚΑΙ ΔΙΚΤΥΩΝ ΣΤΟ ΚΟΣΜΟ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ.

1. Γενικά

Στην καθημερινή του ζωή κατακλύζεται κανείς από ακούσματα του τύπου ΄΄Ζούμε στη διαστημική εποχή΄΄ ή την ΄΄Εποχή του ατόμου΄΄ ή την ΄΄Εποχή της ηλεκτρονικής΄΄.Επίσης ακούει ή διαβάζει κανείς λέξεις και φράσεις του τύπου ΄Τεχνοτρονική εποχή΄΄, ΄΄Μετά-βιομηχανική κοινωνία΄΄, ΄΄Επιστημονικοτεχνική επανάσταση΄΄, ΄΄Υπερβιομηχανική κοινωνία΄΄… και άλλα εντυπωσιακά.

Κάθε τέτοιου είδους άκουσμα - και όχι μόνο - , πιθανότατα συνοδεύεται και από φράσεις του τύπου ΄΄… με βοήθεια Ηλεκτρονικού Υπολογιστή …΄΄, …΄΄ με την εισαγωγή Πληροφορικής …΄΄, ΄΄… με εισαγωγή Μηχανογραφημένου συστήματος…΄΄ με αποτέλεσμα να σχηματίζει δικαιολογημένα κανείς την άποψη ότι ΄΄κοινός παρονομαστής΄΄ όλων των παραπάνω είναι ο Η/Υ και η εποχή μας πάνω από όλα είναι η εποχή των πληροφοριών.

Πράγματι είναι γεγονός αδιαφιλονίκητο ότι η σημερινή ανθρώπινη κοινωνία είναι τόσο πολύ ΄΄έντασης πληροφοριών΄΄ όσο δεν ήταν ποτέ, μια και παράλληλα με τη μαζική παραγωγή υλικών αγαθών, παρατηρείται και μαζική παραγωγή πληροφοριών εκ των πραγμάτων απαραίτητων για την υποστήριξη των σημερινών ρυθμών ανάπτυξης των ανθρωπίνων δραστηριοτήτων .Για παράδειγμα, η αμερικάνικη τράπεζα που ήταν από τις πρώτες που εισήγαγαν υπολογιστές για τραπεζικές συναλλαγές ήδη απ' τη δεκαετία του '50, κατέληξε στην απόφαση αυτή μετά από μελέτη από την οποία προέκυψε ότι στο τότε βραχυπρόθεσμα μέλλον , θα χρειαζόνταν όλος ο ενήλικος πληθυσμός της Καλιφόρνιας

για τον χειρισμό των επιταγών της (!).Ανάλογες καταστάσεις συμβαίνουν και στις συν/κες επιχειρήσεις που αποτελούν μια μορφή επιχειρηματικής.Η χρήση Η/Υ και δικτύων στο κόσμο των συν/κων επιχειρήσεων είναι απαραίτητη για την συγκέντρωση πληροφοριών σε επαγγελματικό πάντοτε επίπεδο που διευκολύνει να γίνει πιο εύκολη η διαδικασία λήψη αποφάσεων σ' ένα πολύπλοκο επαγγελματικό θέμα .Διαφορετικά θα χρειάζονταν πολύ χρόνος και πνευματική κόπωση του εργαζόμενου για να διεκπεραιώσει την εργασία

Γενικά η χρήση των Η/Υ έχει εφαρμογές σ' όλους σχεδόν τους κλάδους της σύγχρονης επιχειρηματικής δραστηριότητας, στους επιστημονικούς και ιδιαίτερα στους τεχνικούς τομείς διότι τα διοικητικά στελέχη βλέπουν την πληροφορική σαν κάτι που γενικά αυξάνει την παραγωγικότητα και την ταχύτητα λήψης αποτελεσματικών αποφάσεων μια και μπορεί πλέον κανείς να έχει πρόσβαση σε μεγάλους όγκους στοιχειών από τα οποία να αντλεί πληροφορίες – και μάλιστα σε πολύ κατανοητή μορφή – με μικρή προσπάθεια και χρόνο, καθώς επίσης και να εξετάζει γρήγορα και με ακρίβεια εναλλακτικές λύσεις.Οι εργασίες αυτές χωρίς τη χρήση πληροφοριών συστημάτων κοστίζουν πολύ και συχνά είναι ανέφικτες.

Για τους άμεσους χρήστες συστημάτων του είδους, η πληροφορική είναι κάτι που κάνει γενικά την εργασιακή ζωή ευκολότερη, πιο παραγωγική και ίσως πιο ενδιαφέρουσα.Για τον απλό άνθρωπο που δεν έχει δουλέψει έστω και σαν χρήστης με κάποιον υπολογιστή, η πληροφορική είναι ίσως κάτι το μαγικό και μυστηριώδες που φαίνεται να μπορεί να κάνει τα πάντα μειώνοντας τις θέσεις εργασίας.

Τέλος σε επίπεδο κυβέρνησης γενικά, η σαρωτική σημερινή έλευση της πληροφορικής εισάγει τη γνωστή πλέον αντίφαση ότι αν αγνοηθεί η νέα τεχνολογία, οι βιομηχανίες και οι υπηρεσίες της χώρας θα μείνουν απαρχαιωμένες και άρα μη ανταγωνιστικές με αποτέλεσμα σε τελευταία ανάλυση ανεργία και πτώση του βιοτικού επιπέδου,γεγονότα που συμβαίνουν όμως και με την εισαγωγή πληροφορικής μια και οι νέες τεχνολογίες φαίνεται ότι, βραχυπρόθεσμα τουλάχιστον, εκτοπίζουν την ανθρώπινη εργασία.Όλα αυτά δε την στιγμή που η πληροφορική αποτελεί μονόδρομο μια και η εισαγωγή της είναι ήδη γεγονός σε μεγάλη έκταση στα λεγόμενα αναπτυγμένα κράτη.

Τα πρώτα βήματα της πληροφορικής για να γεννηθεί ο 21ος αιώνας.

Η ανάγκη για πληροφόρηση ώθησε τον άνθρωπο στην δημιουργία Η/Υ διότι ο κάθε άνθρωπος είτε είναι μαθητής ή επαγγελματίας αντιμετωπίζει ένα σύνολο προβλημάτων στις καθημερινές του δραστηριότητες, που είναι αναγκασμένος μέσα σε κάποιο χρονικό διάστημα να πάρει τις σωστές αποφάσεις .Για να μπορεί όμως να πάρει τις σωστές αποφάσεις χρειάζεται να έχει τις κατάλληλες πληροφορίες πάνω στο θέμα που θα αποφασίσει.Διότι η διαδικασία λήψη αποφάσεων απαιτεί κάποια συγκεντρωτικά στοιχεία που στην συνέχεια ο άνθρωπος θα τα επεξεργαστεί και έτσι θα επιλέξει την καλύτερη λύση για το πρόβλημα του.Και επειδή έχει αποδειχθεί επιστημονικά ότι ο ανθρώπινος νους λειτουργεί με μια έμφυτη καθυστέρηση που υπολογίζεται σε 80 χιλιοστά του δευτερολέπτου.Αυτό που νομίζουμε ότι βλέπουμε σε κάθε δεδομένη στιγμή στην πραγματικότητα επηρεάζεται από το μέλλον.Σαν τη ζωντανή τηλεοπτική μετάδοση που δεν είναι και τόσο ζωντανή, αφού η εικόνα έρχεται στο σπίτι μας με 3 δευτερόλεπτα καθυστέρηση και το μυαλό μας κατασκευάζει συνειδητή γνώση λίγο αργότερα από την οπτική πρόσληψη των εικόνων.Έτσι λοιπόν η αδυναμία του ανθρώπινου μυαλού σε μνήμη και σε ταχύτητα υπολογισμών τον οδήγησε να κατασκευάσει τον Η/Υ που θεωρείται προέκταση του μυαλού του.Οι αλλαγές όμως δεν έγιναν από τη μια στιγμή στην άλλη.Πέρασαν αρκετά χρόνια για να φτάσουμε στην υψηλή τεχνολογία του 21ου αιώνα.Ξεκινήσαμε πρώτα από έναν Η/Υ που λειτουργούσε ως μια απλή μηχανή υπολογισμού η οποία κατασκευάστηκε το 1940 από τον **John Atanasoff** και ονομάστηκε **ABC** (**A**tanasoff **B**erry **C**omputer).Οι καθηγητές **J.Ecket και J.Mauchly** το διάστημα 1942-1944 σχεδίασαν και κατασκεύασαν τον **ENIAC** (**E**lectronic **N**umerical **I**ntegrator **A**nd **C**alculator), που ζύγιζε 30 τόνους και κάλυπτε 140m^2, τον πρώτο Η/Υ που δεν είχε τμήματα να κινούνται ηλεκτρομαγνητικά παρά μόνο σε περιφερειακές μονάδες εισόδου-εξόδου.Αργότερα το 1949 κατασκευάστηκε στο πανεπιστήμιο του Cambridge ο πρώτος Η/Υ όπου ο επεξεργαστής περιείχε εκτός από την κύρια μνήμη και την βοηθητική που τότε σαν βοηθητική μνήμη χρησιμοποιούσαν τις μαγνητικές ταινίες που ήταν απαραίτητες ώστε τα δεδομένα να αποθηκεύονται σε μόνιμη βάση.Αυτός ο Η/Υ ονομάστηκε **EDSAL** (**E**lectronic **D**elay

Storage Automatic Computer) που αποτελούταν από μια γιγάντια οθόνη, από διάτρητες κάρτες (είναι το αντίστοιχο σημερινό πληκτρολόγιο) και τον επεξεργαστή.Ο πρώτος εμπορικά διαθέσιμος Η/Υ κατασκευάστηκε το 1951 από την **Sperry Rand Corporation** που ονομάστηκε **Universal Automatic Computer.**

Η βασική δομή ενός σημερινού υπολογιστή είναι η οθόνη 15 ή 17 ιντσών, το ποντίκι, το πληκτρολόγιο και ο επεξεργαστής.Η καρδιά του Η/Υ είναι ο επεξεργαστής που διαθέτει τρία βασικά χαρακτηριστικά: **1)** την κύρια μνήμη με συναίνεση την βοηθητική που σήμερα χρησιμοποιούν τους σκληρούς δίσκους διότι είναι άμεσοι προσπελάσιμοι δηλαδή όταν θέλει κάνεις να ακούσει ένα συγκεκριμένο κομμάτι από ένα CD δεν χρειάζεται να ακούσει όλα τα τραγούδια όπως συνέβαινε με την χρήση των μαγνητικών ταινιών.Ετσι λοιπόν η κύρια μνήμη χάρις της βοηθητικής μνήμης έχει την δυνατότητα χωρητικότητας μεγάλου όγκου δεδομένων η οποία μετριέται με βάση την μονάδα bytes που 1 bytes έχει 8 bits που είναι δυαδικό ψηφίο **2)** ελέγχει κάθε λειτουργία με τη μονάδα έλεγχου και **3)** εκτελεί αριθμητικές και συγκριτικές πράξεις με την αριθμητική μονάδαΕίναι αναμφισβήτητο ότι οι υπολογιστές διακρίνονται για την σπουδαιότητα της χρήσης τους και ότι έχουν εφαρμογές παντού, σ' όλες σχεδόν τις δραστηριότητες του άνθρωπου διότι ξεχωρίζουν για τα ιδιαίτερα χαρακτηριστικά που διακατέχονται.

Τα κύρια αυτά χαρακτηριστικά των υπολογιστών αποτελούν οι ακολουθεί πέντε βασικοί παράγοντες:

- **Ταχύτητα:** Ο υπολογιστής εφευρέθηκε ως μία μηχανή με υψηλές υπολογιστικές ταχύτητες.Αυτό οδήγησε στην λύση πολλών επιστημονικών προβλημάτων που ήταν προηγούμενα αδύνατον να επιλυθούν.Για παράδειγμα η διαδικασία προσσελήνωσης δεν θα ήταν πραγματοποιήσιμη χωρίς υπολογιστές, όπως επίσης η σημερινή επιστημονική προσέγγιση στην πρόγνωση του καιρού.Για την πρόγνωση του καιρού βραχυπρόθεσμα οι μετεωρολόγοι χρησιμοποιούν υπολογιστικά συστήματα για να εκτελέσουν γρήγορα τους αναγκαίους υπολογισμούς και αναλύσεις.Η ικανότητα της λήψης απαντήσεων αρκετά γρήγορα από τον υπολογιστή, έτσι ώστε ο χρήστης να έχει τον απαιτούμενο χρόνο για να ενεργήσει κατάλληλα επιτρέπει τους υπολογισμούς σε ''πραγματικό - χρόνο''.Οι ηλεκτρονικοί παλμοί ταξιδεύουν με πολύ μεγάλες ταχύτητες και επειδή οι υπολογιστές είναι ηλεκτρονικοί (χωρίς μηχανικές κινήσεις) η εσωτερική ταχύτητα τους είναι της τάξης μικρών-δευτερολέπτων (1 microsec = 10^{-6} sec), νάνο-δευτερολέπτων (1 nanosec = 10^{-9} sec) και τελευταία πίκο - δευτερολέπτων (1 picosec = 10^{-12} sec).Ο υπολογιστής

CDC 6600 π.χ. προσθέτει δύο 18 - ψήφους αριθμούς σε 300 περίπου νάνο - δευτερόλεπτα δηλ. περίπου 3 εκατομμύρια πράξεις το δευτερόλεπτο.Ως παράδειγμα μη - αριθμητικής εφαρμογής αναφέρεται ότι η καταχώρηση με δείκτες ενός συγγραφικού έργου περίπου 13 εκατομμυρίων λέξεων με το χέρι θα απαιτούσε 2000 άνθρωπο - έτη εργασίας π.χ. εργασία 13 ειδικών επί 20 έτη για να εκπληρωθεί, ενώ με την χρήση υπολογιστών η ίδια εργασία μπορεί να εκτελεστεί σε λιγότερο από ένα έτος από μερικούς ειδικούς.

- **Μνήμη:** Είναι γνωστό ότι ο ανθρώπινος εγκέφαλος από τις νέες γνώσεις που δέχεται,επιλέγει ότι θεωρεί σπουδαίο και άξιο να κρατηθεί στη μνήμη του, ενώ οι ασήμαντες λεπτομέρειες καταχωρούνται σε ΄΄δευτερεύουσες΄΄ περιοχές της μνήμης.Στους υπολογιστές, η εσωτερική μνήμη της CPU είναι αρκετά μεγάλη ώστε να χωρέσει ένα ορισμένο ποσό πληροφοριών, δηλ. έχει ορισμένα όρια.Όλα τα υπόλοιπα απαιτούμενα δεδομένα αποθηκεύονται έξω από την μνήμη της CPU σε βοηθητικές ή δευτερεύουσες μονάδες μνήμης.Μικρά τμήματα από το σύνολο των δεδομένων μπορούν να προσπελασθούν πολύ γρήγορα απο την CPU σε βοηθητικές ή δευτερεύουσες μονάδες μνήμης .Μικρά τμήματα από το σύνολο των δεδομένων μπορούν να προσπελασθούν πολύ γρήγορα από την CPU και να μεταφερθούν στην κύρια, εσωτερική μνήμη, όπως και όταν απαιτηθεί για την επεξεργασία.Η εσωτερική μνήμη είναι εγκατεστημένη σε Κ ισοδυναμεί με 1024 θέσεις μνήμης, π.χ. ο υπολογιστής CDC CYBER 73 έχει μνήμη 128 Κ (δηλ. 128 ×1024 θέσεις μνήμης).

- **Ακρίβεια:** Μηχανικά σφάλματα στους υπολογιστές είναι δυνατόν να συμβούν, αλλά λόγω της αυξανόμενης αποδοτικότητας στις τεχνικές που ανιχνεύουν σφάλματα, αυτά σπάνια οδηγούν σε λανθασμένα αποτελέσματα.Τα σφάλματα στους υπολογισμούς σε πολύ μεγάλο ποσοστό, οφείλονται σε ανθρώπινες μάλλον παρά τεχνολογικές αδυναμίες, π.χ. ανακριβή λογική στον προγραμματισμό, ανακριβή δεδομένα ή ακατάλληλα σχεδιασμένα συστήματα.

- **Λειτουργικότητα:** Οι υπολογιστές μπορούν να εκτελέσουν σχεδόν κάθε έργο με την προϋπόθεση ότι το έργο μπορεί να ελαττωθεί σε μία σειρά από λογικά βήματα.Για παράδειγμα, ένα έργο όπως η προετοιμασία ενός μισθολογίου ή ο

έλεγχος της ροής κίνησης μπορεί να χωρισθεί σε μια λογική ακολουθία από λειτουργίες.

α) **δίνει πληροφορίες στον εξωτερικό χώρο μέσω των μηχανών εισόδου/εξόδου,**

β) **μετακινεί δεδομένα εσωτερικά στην CPU,**

γ) **εκτελεί βασικές αριθμητικές λειτουργίες,**

δ) **εκτελεί λειτουργίες σύγκρισης.**

Κατά μία έννοια λοιπόν ο υπολογιστής έχει περιορισμένη λειτουργικότητα γιατί περιορίζεται στις παραπάνω τέσσερις βασικές λειτουργίες.Επειδή όμως ένα πολύ μεγάλο μέρος δραστηριοτήτων μπορεί να θεωρηθεί ότι καλύπτεται από αυτές τις λειτουργίες, ο υπολογιστής εμφανίζεται ότι λειτουργεί πάρα πολύ «έξυπνα».Ο προγραμματισμός μπορεί να θεωρηθεί ως η τέχνη που ελαττώνει ένα δεδομένο πρόβλημα σε μια κατανεμημένη συνεργασία των παραπάνω βασικών λειτουργιών.

- Αυτοματισμός: Όταν ένα πρόγραμμα είναι στη μνήμη του υπολογιστή, οι ατομικές οδηγίες μεταφέρονται η μία μετά από την άλλη για εκτέλεση στην μονάδα ελέγχου.Η CPU ακολουθεί τις οδηγίες μέχρι να συναντήσει μία τελευταία οδηγία που αναφέρεται στον τερματισμό της εκτέλεσης.Στη αναλυτική μηχανή του Babbage ο όρος ΄΄αυτόματη μηχανή΄΄ σήμαινε ότι όταν η επεξεργασία ενός προγράμματος είχε αρχίσει, θα συνεχιζόταν μέχρις ότου συμπληρωθεί, χωρίς την ανάγκη ανθρώπινης παρέμβασης.Σημειώνεται ότι ο υπολογιστής εκτελεί εξαιρετικά μεγάλους αριθμούς υπολογισμών με ακριβώς την ίδια ακρίβεια και ταχύτητα όπως εκτελεί τον πρώτο υπολογισμό.Οι υπολογιστές έχουν ήδη αποδείξει σήμερα ότι είναι ένα από τα καλύτερα εργαλεία του ανθρώπου και ότι οι δυναμικές ωφέλειες τους για το ανθρώπινο γένος είναι πολύ μεγάλες.Οι ωφέλειες όμως αυτές δεν θα αποδοθούν χωρίς την κατάλληλη προεργασία που απαιτεί εντατική και επίπονο προσπάθεια και μελέτη για την πληρέστερη κατανόηση των ευεργετημάτων από τους υπολογιστές.Θα πρέπει επίσης να μελετηθεί προσεκτικά η αποφυγή των κινδύνων που τυχόν συνοδεύουν την πρόοδο.Οι υπολογιστές έχουν αρχίσει να μπαίνουν σ' ένα στάδιο εξέλιξης που αναμένεται να επηρεάσει τη ζωή όλων των ανθρώπων.Οι υπολογιστές και οι σύγχρονες τεχνικές επεξεργασίας πληροφοριών μεγεθύνουν κυρίως την ικανότητα του ανθρώπου να χειρίζεται πληροφορίες και αναμένεται να προκαλέσουν αλλαγές στις οικονομικές, κυβερνητικές και κοινωνικές δομές ανάλογες με εκείνες που προκάλεσε η βιομηχανική επανάσταση.

Τα πλεονεκτήματα των Η/Υ στον σύγχρονο εμπορικό κύκλο των επιχειρήσεων.

Κάθε μέρα οι υπολογιστές και γενικότερα ΄΄οι καρποί της πληροφορικής΄΄, βοηθούν εκατομμύρια ανθρώπους να εργάζονται αποδοτικότερα και με λιγότερα στοιχεία ρουτίνας.Για παράδειγμα όλο και περισσότεροι εργαζόμενοι γραφείου και λογιστικών φύλλων και γενικά κάθε είδους πακέτων περατώνοντας αντίστοιχες εργασίες γρηγορότερα, αποδοτικότερα και ίσως πιο ευχάριστα.Όλο και περισσότεροι εργάτες εργοστασίου έχουν αντικαταστήσει τις μονότονα επαναλαμβανόμενες εργασίες παραγωγής σειράς με πιο ελκυστικές και δημιουργικές μέσω της χρήσης Η/Υ.Τα διευθυντικά στελέχη μπορούν να ελέγξουν γρήγορα ένα μεγάλο αριθμό εναλλακτικών λύσεων βασισμένων σε ακριβή και ενημερωμένα δεδομένα.

Θα πρέπει όμως να σημειωθεί ότι η αποφυγή μονότονων και χειρονακτικών εργασιών συχνά εξαργυρώνεται σε εντατικοποίηση της νοητικής προσπάθειας, με αποτέλεσμα ο εργαζόμενος να κοπιάζει περισσότερο, με την ίδια αμοιβή για περισσότερη δουλειά καλύτερης ποιότητας.

Επιπλέον υπάρχουν σοβαρές αρνητικές επιπτώσεις σε ορισμένα επαγγέλματα από άποψη ασφάλειας, κοινοτικού γοήτρου και ισχύος.Στο επίπεδο της συνολικής οικονομίας μιας χώρας αμβλύνονται οι αρνητικές επιπτώσεις από τις νέες θέσεις εργασίας που δημιουργούνται στον κλάδο παραγωγής προϊόντων πληροφορικής, καθώς επίσης και στην παραγωγή νέων προϊόντων και υπηρεσιών που προκύπτουν από τη διάδοση των υπολογιστών.

Έτσι λοιπόν η επανάσταση των πληροφοριών και η εφαρμογή των σύγχρονων τεχνολογιών πληροφορικής έχει άμεση επίδραση στις πολυποίκιλες δραστηριότητες του ανθρώπου στον σύγχρονο εμπορικό κύκλο των επιχειρήσεων.

Για παράδειγμα αναφέρονται:

Η απολαβή προϊόντων υψηλότερης ποιότητας. Η πληροφορική μπορεί να βοηθήσει στη βελτίωση της ποιότητας των προϊόντων που απολαμβάνει ο τελικός καταναλωτής .Η όλο και πιο διαδεδομένη χρήση συστημάτων σχεδίασης/παραγωγής με τη βοήθεια του υπολογιστή σε συνδυασμό με βιομηχανικά ρομπότ καταλήγει γενικά σε φτηνότερα προϊόντα υψηλότερα ποιότητας με πιο ομοιόμορφες ανοχές.Πέρα από τη χρήση συστημάτων αυτοματοποίησης της σχεδίασης-παραγωγής, η πληροφορική επιδρά και με διάφορους άλλους τρόπους στα προϊόντα του εμπορίου.Για παράδειγμα μικροεπεξεργαστές εγκαθίσταται σήμερα σε όλο και περισσότερα αυτοκίνητα για τον έλεγχο της ανάμιξης καυσίμου, το χρονισμό ανάφλεξης, τις εκπομπές καυσαερίων κ.λ.π.

Η διευκόλυνση άσκησης κυβερνητικού έργου. Τα προβλήματα που αντιμετωπίζει μια κυβέρνηση στο σημερινό πολύπλοκο και συνεχώς μεταβαλλόμενο κόσμο καθιστούν το κυβερνητικό έργο σήμερα ιδιαίτερα πολύπλοκο.Η πληροφορική μπορεί να βοηθήσει (αν υπάρχει πολιτική βούληση) αποτελεσματικά στην άσκηση του διευκολύνοντας τους ελέγχους, συμβάλλοντας στην λήψη σωστότερων αποφάσεων κ.λ.π.Στον αντίποδα των κινδύνων για παραβίαση της ιδιωτικής ζωής του πολίτη, η πληροφορική μπορεί να χρησιμοποιηθεί για τον περιορισμό της εγκληματικότητας.Φτάνει να τεθούν και να τηρηθούν αυστηρότητα τα σχετικά όρια.

Η καλύτερη εξυπηρέτηση. Η χρήση της πληροφορικής στους διάφορους οργανισμούς όπως για παράδειγμα οι τράπεζες, αεροπορικές εταιρίες κ.λ.π.καταλήγει γενικά σε μικρότερες γραμμές αναμονής.Επιπλέον παρέχονται ταχύτερα ακριβέστερες απαντήσεις στον πολίτη και γενικά η εξυπηρέτηση γίνεται αποδοτικότερη.Και αυτό βασίζεται ότι οι πληροφορίες ΄΄μακρών αποστάσεων΄΄είναι δυνατές μέσω των ειδικών δικτύων επικοινωνιών.Η χρήση οθονών τηλεοράσεων καθιστά δυνατή την ενημέρωση της κατάστασης τοπικών και διεθνών συνδέσεων σε μικρά χρονικά διαστήματα.Το δίκτυο, που σταθερά ακολουθεί την κίνηση, δραστηριοποιεί αυτόματα τηλεφωνικές κλήσεις

στην ένδειξη άρρυθμης λειτουργίας.Επισης με την εκτεταμένη χρήση των δίσκων CD-ROM, που διαθέτουν τεράστια ικανότητα αποθήκευσης πληροφοριών.Οσο μεγαλύτερος είναι ο όγκος των πληροφοριών προς επεξεργασία δεδομένων, τόσο πιο αποδοτική και πιο οικονομική γίνεται η χρησιμοποίηση του υπολογιστή.

Η αύξηση της ασφάλειας. Οι μικροεπεξεργαστές και ειδικό λογισμό, ενσωματώνονται σήμερα σε μια μεγάλη σειρά διατάξεων αυτοματισμών που αυξάνουν τα επίπεδα παρεχόμενης ασφάλειας σε οχήματα και συσκευές κάθε είδους, όπως για παράδειγμα στα συστήματα πυρανίχνευσης.

Οι αλλαγές στη λειτουργία των επιχειρήσεων. Η πληροφορική αναμφισβήτητα έχει επιφέρει μεγάλες αλλαγές στον τρόπο λειτουργίας των επιχειρήσεων.Ο αυτοματισμός γραφείου, μπορεί να θεωρηθεί ότι αποτελεί σήμερα μια σταδιακή επανάσταση στις δουλειές γραφείου.Με τη είσοδο τεχνολογιών **CAD/CAM** σημειώθηκαν ριζικές αλλαγές στις διαδικασίες σχεδίασης/παραγωγής προϊόντων.Οι εν λόγω αλλαγές τυπικά δεν είναι απαλλαγμένες από προβλήματα.Εμφανίζονται προβλήματα κατά τη μετάβαση που σχετίζονται κυρίως με τη συνηθισμένη αντίσταση ''στο καινούργιο '' εκ μέρους του προσωπικού, ενώ ενδέχεται να προκύψουν και προβλήματα ασφάλειας κατά τη λειτουργία (κλοπή πληροφοριών, διαγραφές, αλλοιώσεις κ.λ.π.) από το προσωπικό.Για τους παραπάνω λόγους, η μετάβαση που θα λαμβάνει σοβαρά υπόψη θέματα ασφάλειας, εργονομίας, εκπαίδευσης κ.λ.π.

Παρόλο αυτά στον σύγχρονο εμπορικό κύκλο των επιχειρήσεων – κυρίως στον εξωτερικό – η είσοδος της πληροφορικής έχει σαν αποτέλεσμα αλλαγές πολύ μεγάλης κλίμακας και σημασίας στις διαδικασίες παραγωγής, μια και σε πολλά αυτά μιλάμε πλέον για **Ολοκληρωμένη Παραγωγή με Υπολογιστή** (Computer Intergrated Manufacturing - **CIM**). Στην Ολοκληρωμένη Παραγωγή με Υπολογιστή η διοίκηση αποφασίζει την κατασκευή κάποιου προϊόντος βασιζόμενη σε σχετική έρευνα αγοράς, την τεχνογνωσία της επιχείρησης κ.λ.π.Στη συνέχεια στις εργασίες που ακολουθούν χρησιμοποιούνται σε μεγάλο βαθμό υπολογιστικά συστήματα:

Με ειδικά πακέτα Σχεδίασης με τη βοήθεια Υπολογιστή **(CAD)** αρχίζει ο σχεδιασμός του προϊόντος.Τα σχέδια που προκύπτουν τροφοδοτούν ένα σύστημα **Παραγωγής με βοήθεια Υπολογιστή** (Computer Alded Manufacturing - **CAM)** το οποίο επεξεργάζεται τις πρώτες ύλες όπως μέταλλα, πλαστικά, κ.λ.π. μορφοποιώντας τα σε

εξαρτήματα ή στοιχεία που προωθούνται για συναρμολόγηση.Για την συναρμολόγηση σε όχι λίγες περιπτώσεις – και όσο περνάει ο καιρός όλο και συχνότερα – χρησιμοποιούνται ρομπότ.Η διακίνηση των διαφόρων πρώτων υλών,τμημάτων και προϊόντων στο εργοστάσιο μπορεί να γίνεται και αυτή με ειδικά οχήματα – **ρομπότ.**Με τη βοήθεια υπολογιστή, η διοίκηση του εργοστασίου εποπτεύει την όλη παραγωγική διαδικασία, ελέγχοντας τις εισερχόμενες παραγγελίες, τα απαιτούμενα στοιχεία και υλικά, το σχεδιασμό και τη χρονοδρομολόγηση των λειτουργιών της παραγωγής κ.λ.π.

Τα συστήματα CIM οδηγούν σε σημαντική αύξηση της παραγωγικότητας και ελαχιστοποίηση της άμεσης ανθρώπινης εργασίας που χρειάζεται από το σύστημα παραγωγής.

ΚΕΦΑΛΑΙΟ 2

ΕΦΑΡΜΟΓΕΣ ΤΩΝ Η/Υ ΣΕ ΣΥΝ/ΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

1. Το συνεταιριστικό οικονομικό φαινόμενο αναπτύσσει επιχειρηματικές δραστηριότητες.

Πριν επιχειρήσουμε να δώσουμε τον ορισμό της συνεταιριστικής επιχείρησης θα πρέπει να σημειώσουμε ότι οι συνεταιρισμοί και ιδιαίτερα οι αγροτικοί συνεταιρισμοί ως μορφή οικονομικής οργάνωσης της παραγωγής αγαθών ή /και υπηρεσιών, λειτουργούν σε όλες τις χώρες του κόσμου με ενιαίες, λίγο έως πολύ, αρχές και κανόνες λειτουργίας, αλλά κάτω από διαφορετικές κοινωνικοοικονομικές

χρήστες των οργανώσεων π ένας συνεταιρισμός εμπορίας αγροτικών προϊόντων που παράγουν τα μέλη του.Ο βαθμός επιτυχίας του στόχου εξαρτάται, μεταξύ άλλων, και από το βαθμό χρήσης του συνεταιρισμού από τα μέλη.

3) Ο συνεταιρισμός αναγνωρίζει την αρχή της αναλογικότητας.Δηλαδή, στα πλαίσια της οργάνωσης και της λειτουργίας της συνεταιριστικής επιχείρησης τα μέλη (ιδρυτές – ιδιοκτήτες - πελάτες) μοιράζονται επιχειρηματικούς κινδύνους, χρηματοοικονομικές υποχρεώσεις και οικονομικά οφέλη ή ζημιές **ανάλογα με τον όγκο των συναλλαγών τους με το συνεταιρισμό.**

4) Ο συνεταιρισμός είναι ιδιωτική επιχείρηση.Όπως είδαμε, η ίδρυση του συνεταιρισμού είναι αποτέλεσμα της ιδιωτικής πρωτοβουλίας και συνεργασίας ατόμων.Επομένως η συνεταιριστική οργάνωση ανήκει στα μέλη και τα μέλη είναι ιδιοκτήτες των μέσων παραγωγής της οργάνωσης.**Αυτό σημαίνει ότι ο συνεταιρισμός δεν ανήκει στο κράτος, ούτε είναι δημόσια επιχείρηση.**Αν και σε διάφορες χώρες λειτουργούν συνεταιρισμοί που ανήκουν στο κράτος σαν δημόσιες επιχειρήσεις, κατά κανόνα δεν θεωρούνται συνεταιρισμοί γιατί δεν ανήκουν στα μέλη, και κατά κανόνα τα μέλη δεν είναι αυτά που αποφασίζουν για τις υποθέσεις των συνεταιρισμών.

5) Ο συνεταιρισμός είναι μία οικονομική επιχείρηση.Άτομα που θεωρούν ότι μπορούν να βελτιώσουν την οικονομική τους θέση μέσω της συνεργασίας, ιδρύουν μία συνεταιριστική οργάνωση η όποια ανήκει στα μέλη , ελέγχεται από τα μέλη, και στα μέλη διανέμονται τα κέρδη ή οι ζημιές.Όσοι συμμετέχουν στο συνεταιρισμό, το κάνουν επειδή αναμένουν κάποιο οικονομικό όφελος.**Επομένως, ο βασικός στόχος ενός συνεταιρισμού είναι η αύξηση του καθαρού εισοδήματος των μελών του.**Προς το σκοπό αυτό, η συνεταιριστική οργάνωση συνδυάζει παραγωγικούς συντελεστές και παράγει αγαθά ή / και υπηρεσίες για λογαριασμό των μελών της και με στόχο την αύξηση του εισοδήματος των συνεταίρων.

Έτσι λαμβάνοντας υπόψη τα παραπάνω χαρακτηριστικά, μπορούμε σε γενικές γραμμές να ορίσουμε τον συνεταιρισμό **ως την επιχείρηση που οργανώνονται από τη συνεργασία ατόμων –μελών, με στόχο την αύξηση του καθαρού εισοδήματος τους.Τα μέλη είναι ιδιοκτήτες – χρήστες – διαχειριστές της επιχείρησης και μοιράζονται οφέλη ανάλογα με το ύψος των συναλλαγών τους.**

Βλέπουμε λοιπόν ότι οι συνεταιρισμός λειτουργεί για λογαριασμό των μελών του και όχι για την απόκτηση κέρδους σαν μία ξεχωριστή οικονομική μονάδαΑυτό όμως δεν σημαίνει ότι ο στόχος του συνεταιριστικού πλεονάσματος (που αποτελεί και την πηγή οικονομικού οφέλους για τα μέλη) **αλλά ότι το συνεταιριστικό πλεόνασμα (κέρδος)**

ανήκει στα μέλη και μοιράζεται σε αυτά ανάλογα με το ύψος των συναλλαγών τους.

-Δεύτερον, ο στόχος του συνεταιρισμού συγχέεται με άλλους στόχους κοινωνικούς, πολιτικούς, πολιτιστικούς, κ.λ.π. θα πρέπει να τονιστεί ότι αν η οργάνωση και λειτουργία ενός συνεταιρισμού έχει κοινωνικές, πολιτικές ή άλλου είδους επιπτώσεις, αυτό είναι δευτερεύον αποτέλεσμα της επιτυχημένης δράσης του συνεταιρισμού ως οικονομικής μονάδας, των επιχειρηματικών δραστηριοτήτων και της δημιουργίας πλεονασμάτων και όχι ο σκοπός ίδρυσης του συνεταιρισμού.**Ο συνεταιρισμός δεν είναι σύλλογος ή σωματείο με στόχο την κοινωνική ή πολιτιστική αναβάθμιση των μελών του.**Βέβαια μία δραστήρια και επιτυχημένη συνεταιριστική οργάνωση μπορεί να δημιουργήσει τις προϋποθέσεις για την επίτευξη και των στόχων αυτών.Σε καμία περίπτωση, όμως μία τέτοια επιδίωξη δεν θα πρέπει να προηγείται της βασικής αποστολής της συνεταιριστικής επιχείρησης (που είναι μεγιστοποίηση του οικονομικού οφέλους), ούτε και να αντιστρατεύεται αυτήν

2 Η άσκηση επιχειρηματικής δραστηριότητας στους συνεταιρισμούς αναπτύσσει την χρήση Η/Υ.

Είναι εύλογο ότι η αλματώδη εξέλιξη της τεχνολογίας που άνθισε την επιστήμη της πληροφορικής να επιφέρει διάφορες αλλαγές σε πολλούς τομείς της ζωής .Στον επαγγελματικό κυρίως τομέα που υπάγονται και οι συν/κες επιχειρήσεις έχει διευκολύνει με την χρήση των υπολογιστών τον τρόπο παραγωγής ενός αγροτικού προϊόντος προς κατανάλωση και συνεπώς την άνοδο των κερδών των παραγωγών.Από την στιγμή που ο βασικός λόγος ύπαρξης μιας συν/κης επιχείρησης είναι η άσκηση επιχειρηματικής δραστηριότητας που δεν μπορεί να μην ακολουθεί τα βήματα της τεχνολογίας διαφορετικά δεν θα είναι άξια ανταγωνίστρια μεταξύ των άλλων συν/κων οργάνωσεων.Οι απαιτήσεις υψηλής ποιότητας προϊόντων από τους καταναλωτές, από την μία μεριά η απαίτηση των παραγωγών για υψηλά κέρδη οδηγήθηκαν στην χρήση Η/Υ διότι προσφέρουν αυτές τις υπηρεσίες με τα χαρακτηριστικά που διαθέτον που είναι τα εξής:η ταχύτητα, η μνήμη, η ακρίβεια, η λειτουργικότητα, και ο αυτοματισμός.

Από τότε που η χρήση Η/Υ και δικτύων έχει κατακλύσει τις συνεταιριστικές επιχειρήσεις έχει σημειώσει αλλαγές τόσο στον εργασιακό χώρο όσο και στην

οργάνωση της παραγωγής. Όσον αφορά πρωτα τις αλλαγές στις συνθήκες εργασίας του εργαζόμενου είναι οι εξής: έχει αντικαταστήσει τα χέρια με υπολογιστικά συστήματα χωρίς να χρειάζεται η καταβολή σωματικής και πνευματικής κόπωσης του εργαζόμενου.Επομένως η χρήση Η/Υ του προσφέρει εξοικονόμηση χρόνου και κόπου, περισσότερος ελεύθερος χρόνος.Επίσης έχει βελτιώσει τις συνθήκες εργασίες, με τα συστήματα ασφάλειας έχουν μειώσει τα εργατικά άτυχηματα.Γενικά συντέλεσε στην άνοδο του βιοτικού επίπεδου και στην βελτίωση του ανθρώπου.

Είναι εμφανές όμως ότι η ανάπτυξη των υπολογιστικών συστηματων ασκεί καταλυτική επίδραση στα κέρδη που εισπράττουν οι παραγωγοί των συν/κων επιχειρήσεων.Διότι αποτελούν μια κινητήρια δύναμη χάρις στην ταχύτητα που διαθέτουν στην βελτίωση των παραγόμενων προϊόντων και των παρεχόμενων υπηρεσιών, αύξηση της ποσότητα τους με μειωμένο κόστος για τον παραγωγό.Αυτό συμβάλλει στην μεγιστοποίηση των κερδών των συν/κων επιχειρήσεων με το χαμηλότερο δυνατό κόστος και στην και στην δημιουργία μιας συν/κης επιχείρησης με ισχυρή οικονομική ανεξαρτησία που διαθέτει άξια ανταγωνιστικά προϊόντα με υψηλή ποιότητα στο καταναλωτικό κοινό.Έτσι λοιπόν ο σκοπός δημιουργίας μιας συν/κης επιχείρησης και του ιδιοκτήτη της που είναι ο παραγωγός έχει επιτευχθεί(δηλ η όσο δυνατή κόστος μεγιστοποίηση των κερδών τους με το χαμηλότερο δυνατό κόστος για αυτούς με την χρήση υπολογιστικών συστηματων στον εργασιακό χώρο).

Η πληροφορική λοιπόν έχει προσφέρει στον άνθρωπο αφθονία αγαθών με την αξιοποίηση της στο επιχειρηματικό κόσμο των επιχειρήσεων παράλληλα έχει αναβαθμίσει το βιοτικό επίπεδο του.Αποτελεί ένα αξιόλογο επίτευγμα που τον βοήθησε να καταξιωθεί κοινωνικά μέσω του χρήματος.Ωστόσο όμως μέσα από την θετική της επίδραση ο άνθρωπος – παραγωγός μετατράπηκε σε τεχνοκράτη με συνέπεια να χάσει την εσωτερική του ελευθερία με αποτέλεσμα να αδυνατεί να ολοκληρώσει την προσωπικότητα του με τις αρνητικές επιπτώσεις που έχει επιφέρει αυτό το επίτευγμα παράλληλα με τα πλεονεκτήματα που έχει προσφέρει στον άνθρωπο και γενικότερα στην κοινωνία που περιβάλλει την κάθε συν/κη επιχείρηση.

ΚΕΦΑΛΑΙΟ 3

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ Η/Υ ΣΕ ΣΥΝ/ΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

1. Η αρχή της διασυνεταιριστικης συνεργασίας.

Η λειτουργία της συνεταιριστικής επιχείρησης διέπεται από ένα σύνολο αρχών, που είναι γνωστές ως συνεταιριστικές αρχές.Οι αρχές αυτές αποτελούν βασικά γνωρίσματα και χαρακτηριστικά των συνεταιρισμών που τους διακρίνουν, σε ένα βαθμό, από τις άλλες μορφές επιχειρηματικής δράσης.Οι αρχές αυτές φαίνεται ότι έχουν επηρεάσει τόσο το νομικό πλαίσιο ίδρυσης και λειτουργίας, όσο και τις διαδικασίες λήψης αποφάσεων στους συνεταιρισμούς.

Οι σύγχρονες συνεταιριστικές αρχές πηγάζουν από το σύνολο κανόνων λειτουργίας και πρακτικής του καταναλωτικού συνεταιρισμού του Rochdale της Αγγλίας (1844), που θεωρείται και ο πρώτος συνεταιρισμός σύγχρονης μορφής: **1) ελεύθερη είσοδος, 2) ένα άτομο – ψήφος, 3) θρησκευτική και πολιτική ουδετερότητα, 4) πώληση τοις μετρητοίς, 5) εκπαίδευση των μελών, 6) πώληση αγαθών σε τιμές λιανικής πώλησης, 7) καθόλου ή περιορισμένος τόκος ως αμοιβή του κεφαλαίου, 8) το κεφάλαιο καταβάλλεται από τα μέλη, 9) τα πλεονάσματα διατίθεται ανάλογα με τις συναλλαγές, 10) ισότιμη συμμετοχή των δυο φύλλων.**

Ωστόσο όμως η διεθνής Συνεταιριστική Ένωση το 1969 λαμβάνοντας υπόψη την εμπειρία και τη δράση των συνεταιρισμών σε παγκόσμιο επίπεδο αναθεώρησε τις

παραπάνω αρχές μπορεί από 10 να έγιναν 6 και να έγιναν κάποιες αφαιρέσεις και την θέση τους να πήραν άλλες αρχές.Ανάμεσα απ' αυτές τις 6 αρχές εκείνη η αρχή που θα μπορούσε να διευκολύνει την μεταφορά πληροφοριών χωρίς να διατρέχεται ο κίνδυνος παραπληροφόρησης από τους επιτήδειους «hackers» είναι η αρχή της διασυνεταιριστικής συνεργασίας η οποία στηρίζεται στην συνεργασία μεταξύ των συνεταιριστικών οργανώσεων σε τοπικό, εθνικό ή διεθνές επίπεδο.

Έτσι λοιπόν σύμφωνα με αυτή την συνεταιριστική αρχή, οι συνεταιριστικές οργανώσεις θα πρέπει να συνεργάζονται μεταξύ τους σε τοπικό, και διεθνές επίπεδο για την ικανοποίηση των στόχων τους, δηλαδή τη μεγιστοποίηση των ωφελειών για τα μέλη τους.Και επειδή η πρέπει να έχουν ως κύρια επιδίωξη τους την ασφάλεια των συστημάτων Η/Υ και την απομάκρυνση των εργαζόμενων που στοχεύουν σε κακόβουλες ενέργειες.Ένας συνεταιρισμός λοιπόν για να πετύχει τους σκοπούς του πρέπει να εκπαιδεύει τα μέλη του με βάση αυτή την συνεταιριστική χρήση των υπολογιστικών συστηματων έχει μπει στον κύκλο των συν/κων επιχειρήσεων θα αρχή.Ας σημειωθεί ότι στη σημερινή εποχή οι συνεταιριστικές επιχειρήσεις λειτουργούν σε πλαίσιο αυξημένου ανταγωνισμού, τόσο στην ενοποιημένη ευρωπαϊκή αγορά όσο και στην παγκόσμια αγορά, έχοντας επιπλέον να αντιμετωπίσουν και τις τάσεις συγκεντροποίησης – μονοπώλησης των αγορών εκ μέρους των μεγάλων ιδιωτικών επιχειρήσεων.Για το λόγο αυτό μια συν/κη επιχείρηση για οικονομικούς συνήθους λόγους μπορεί να προσβάλλει τα υπολογιστικά συστήματα ενός συν/σμου μ' ένα βλαπτικό πρόγραμμα μέσω INTERNET ή με τον δανεισμό μιας μολυσμένης δισκέτας που αυτοί οι δυο τρόποι είναι πιο σύνηθες για να διεισδύσουν έναν ιό στα υπολογιστικά του συστήματα που μπορούν να ανακάμψουν την ανοδική οικονομική πορεία του με πτώση κερδών.Αυτές τις επιπτώσεις δημιουργούν στις συν/κες επιχειρήσεις εάν οι επιτήδειοι «hackers» διαγράφουν
σημαντικά αρχεία ή τα κλέβουν κάνοντας ηλεκτρονικές ληστείες μέσω INTERNET τότε η κάθε επιχείρηση θα χάσει τον έλεγχο της και επομένως την οικονομική της ισορροπία. Για αυτό η διασυνεταιριστική συνεργασία καθίσταται επιβεβλημένη με την προϋπόθεση να μην αποτελεί περιοριστικό και δεσμευτικό παράγοντα στις κινήσεις των επιμέρους συνεταιριστικών επιχειρήσεων ώστε να μπορούν να επιβιώσουν και να λειτουργήσουν στο διεθνές ανταγωνιστικό κλίμα σαν αυτόνομες και δυναμικές επιχειρήσεις.

2. Ασφάλεια πληροφοριών συστημάτων Η/Υ.

Κατά τη διάρκεια της λειτουργίας ενός υπολογιστικού συστήματος είναι δυνατό – και όχι ασυνήθιστο να συμβούν διάφορες «έκρυθμες» καταστάσεις, που μπορούν να θέσουν σε κίνδυνο την ασφάλεια των δεδομένων και πληροφοριών που υπάρχουν στο σύστημα.Οι σύγχρονες απαιτήσεις που υπαγορεύονται από τη μεγάλη αξία των πληροφοριών στο σημερινό κοινωνικό περιβάλλον, αλλά και πιο ειδικά από λόγους εθνικής ασφάλειας, διαφύλαξης προσωπικών πληροφοριών κ.λ.π. ώθησαν σε εκτεταμένες μελέτες για την αντιμετώπιση του ολοένα και οξυνόμενου προβλήματος της ασφάλειας των πληροφοριακών συστημάτων.Δεν είναι τυχαίο άλλωστε το γεγονός ότι σχετικά υψηλό ποσοστό ερευνητικών προγραμμάτων περιλαμβάνουν θέματα ασφάλειας πληροφοριών.

Σε μια προσπάθεια κατηγοριοποίησης των κινδύνων που απειλούν τα πληροφοριακά συστήματα, θα μπορούσε να ισχυριστεί κανείς ότι σε μια πρώτη προσέγγιση αυτοί χωρίζονται σε κινδύνους από μη κακόβουλες ενέργειες και σε κίνδυνους από κακόβουλες ενέργειες.

2.1 Κίνδυνο από μη κακόβουλες ενέργειες.

Γενικά μπορεί κανείς να επισημάνει τρεις βασικές ομάδες κίνδυνων της κατηγόριας αυτής για τα σύγχρονα υπολογιστικά συστήματα:

α) Κίνδυνοι για τα δεδομένα που οφείλονται σε τυχαίους παράγοντες.

Στην κατηγόρια αυτή κίνδυνων εμπίπτουν οι βλάβες του εξοπλισμού που μπορούν να προκαλέσουν απώλεια ή αλλοίωση δεδομένων κατά τη μεταφορά από συσκευή σε συσκευή, κατά τη διάρκεια αποθήκευσης σε κάποιο είδος μνήμης, από πτώση τάσης του δικτύου κ.λ.π.

β) Κίνδυνοι για τα δεδομένα από λάθη χειρισμού χωρίς πρόθεση.

Κοίλια Χρ. – Σπ. Καλογεροπουλίδης "Το πρώτο βιβλίο της Πληροφορικής", Αθήνα 1995 σελ. 24 - 28

Οι συνηθέστεροι κίνδυνοι είναι αλλοίωση δεδομένων από προγραμματιστικό λάθος – ιδιαίτερα από κάποια μεταβολή σε κάποια εφαρμογή -,απώλεια μαγνητικού μέσου, κατά λάθος καταστροφή αρχείου με χρήσιμα δεδομένα από κακό χειρισμό, διαρροή εμπιστευτικών δεδομένων λόγω αμέλειας ή αφέλειας, ο μη χαρακτηρισμός δεδομένων σαν εμπιστευτικά κ.λ.π.

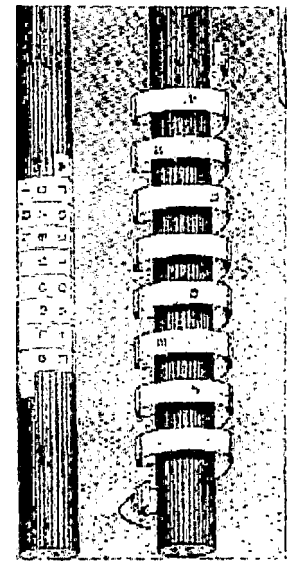
γ) Κίνδυνοι που απειλούν όλη την εγκατάστασης.

Στην κατηγορία αυτή εντάσσονται κίνδυνοι που προέρχονται από διάφορα φυσικά φαινόμενα όπως ζημιές στον εξοπλισμό από σεισμό, εκρήξεις, σοβαρές διαρροές νερού πυρκαγιές κ.λ.π.

2.2 Κίνδυνοι από κακόβουλες ενέργειες.

Εκτιμάται ότι η κατηγόρια αυτή κινδύνων για την ασφάλεια δεδομένων παρουσιάζει ιδιαίτερα ενδιαφέρον διότι τα περιστατικά επιθέσεων των «hackers» σε υπολογιστές έχουν καταγράφει από τις πρώτες ήμερες της διάδοσης των Η/Υ, αλλά το φαινόμενο της επέκτασης της ΄΄ηλεκτρονικής επιδρομής΄΄ είναι σχετικά πρόσφατο.Μέχρι τα μέσα της δεκαετίας του '80 η συγκεντρωτική υφή των υπολογιστικών συστηματων είχε το εξής αποτέλεσμα: Οι περισσότερες επιθέσεις στα υπολογιστικά συστήματα γίνονταν ΄΄εκ των έσω΄΄ άμεσα από κάποιον εργαζόμενα σε αυτά ή εν πάση περίπτωση μέσω κάποιου γνωστού που είχε πρόσβαση στο σύστημα. Κατά τα μέσα της δεκαετίας του '80 το φτηνό modem έδωσε τη δυνατότητα μετατροπής του μικροϋπολογιστή σε τερματικό μεγάλων συγκροτημάτων δικτύων.Με τον τρόπο αυτό δόθηκε η ευκαιρία σε ανώνυμους χρήστες σε κάθε σημείο της γης να επιχειρούν επιθέσεις σε υπολογιστικά συστήματα.Επιπλέον η εμφάνιση standard μηχανών εκτός των σημαντικών ωφελειών που επέφερε, αποτελεί παράλληλα και μια βάση δημιουργίας και διάδοσης ζημιογόνων προγραμμάτων (ιοί, λογικές βόμβες κ.λ.π.).Για την αντιμετώπιση των επιθέσεων επινοήθηκαν μια σειρά από μέθοδοι, μια σύντομη περιήγηση στις οποίες ακολουθεί.

Κρυπτογράφηση (encryption)



Με τη μέθοδο αυτή χρησιμοποιείται ένας αλγόριθμος και ένα κλειδί, που μετασχηματίζει το αρχικό κείμενο ενός μηνύματος σε κωδικοποιημένη μορφή (encrypted text) πριν αυτό φυλαχτεί στον δίσκο ή αποσταλεί μέσω μιας τηλεπικοινωνιακής γραμμής.Κατά την αντίστροφη διαδικασία χρησιμοποιείται ο ίδιος αλγόριθμος με το ίδιο κλειδί για να επαναφέρει (decryption)το μήνυμα στην αρχική του μόρφη.Ο αλγόριθμος παραμένει σταθερός, το κλειδί όμως μπορεί να αλλάξει στα δύο άκρα.Η ασφάλεια δεν στηρίζεται τόσο στον αλγόριθμο, που όσο και περίπλοκος να είναι, συνήθως είναι δημόσια γνωστός, αλλά στη μυστικότητα τήρησης του κλειδιού.Για το λόγο αυτό η ασφάλεια με κρυπτογράφηση πρέπει να συνοδεύεται και από σωστή διαχείριση (δημιουργίας, διανομή, κατάργηση κ.λ.π.) κλειδιών.

Με τον όρο **κρυπτανάλυση** εννοείται η επιστράτευση μεθόδων και σχετικής εμπειρίας για την ανακάλυψη των σκέψεων που βρίσκονται πίσω από τη μετατροπή καθαρού κειμένου σε κρυπτογραφημένο, χωρίς να είναι γνωστό το κλειδί.Ο ευρύτερος κλάδος των γνώσεων που συμπεριλαμβάνει την κρυπτογραφία και την κρυπτανάλυση αναφέρεται γενικά σαν **κρυπτολογία.**

Αν και κρυπτολογία αποκτά σήμερα ιδιαίτερη βαρύτητα λόγω των αυξημένων αναγκών για μυστικότητα στην σύγχρονη επικοινωνία και αποθήκευση πληροφοριών, θα πρέπει να σημειωθεί ότι σαν ιδέα δεν αποτελεί κάτι το καινούργιο .Η πρώτη καταγραμμένη χρήση της ανάγεται στο 400 π.χ στους Σπαρτιάτες, οι οποίοι χρησιμοποιούσαν ένα σύστημα ταινίας – σκυτάλης έγραφαν τα μηνύματα σε ταινίες πάπυρου τυλιγμένες σε μια σκυτάλη.Ο αγγελιαφόρος μετέφερε μόνο τον πάπυρο και ο παραλήπτης τύλιγε την ταινία σε σκυτάλη ίδιας διαμέτρου.Θεωρείται ότι η σύγχρονη κρυπτογραφία και η αντίστοιχη κρυπτοαλληλογραφία αρχίζει το 1200 μ.χ στην παπική αλληλογραφία.Το πρώτο εγχειρίδιο κρυπτογραφίας κυκλοφόρησε το 1379 και περιείχε τις τότε γνωστές μεθόδους κρυπτογραφίας.Πολλοί ισχυρίζονται ότι η κρυπτογραφία έπαιξε μεγάλο ρόλο στην έκβαση του Β'παγκοσμίου πολέμου: Οι βρετανοί με πρωτεργάτη τον Alan Turing μετά από πολλές προϋπόθεσης κατάφεραν να ''σπάσουν'' το γερμανικό σύστημα

κρυπτογραφίας ΄Enigma΄΄, ενώ οι ανάλογες επιτυχίες των Αμερικανών με τα κρυπτοσυστήματα των Ιαπώνων έπαιξαν καθοριστικό ρόλο στη νίκη των συμμάχων.

Σαν ένα απλό παράδειγμα μεθόδου κρυπτογραφίας θεωρείται το ακόλουθο:

καν.αλφαβ. Α Β Γ Δ Ε Ζ Η Θ Ι Κ Λ Μ Ν Ξ Ο Π Ρ Σ Τ Υ Φ Χ Ψ Ω →
ΚΡΥΠΤΟΓΡΑΦΙΑ
ολισθ.κατά 3 Δ Ε Ζ Η Θ Ι Κ Λ Μ Ν Ξ Ο Π Ρ Σ Τ Υ Φ Χ Ψ Ω Β Α Γ →
ΝΥΨΤΧΣΖΥΔΩΜΔ

Στην παραπάνω μέθοδο χρησιμοποιείται η ολίσθηση της αλφαβήτου, δηλαδή σαν κλειδί εδώ είναι το 3.

Στην πράξη βέβαια, τα χρησιμοποιούμενα συστήματα κρυπτογραφίας είναι πολύ πιο πελύπλοκα.Δύο από αυτά που ξεχωρίζουν σήμερα είναι το **DES** (Data Encryption Stadard) αναπτυγμένο από την IBM που αποτελεί εξέλιξη κλασικών μεθόδων και το **RSA** (**R**ivet, **S**hamir, **A**dleman) που είναι ένα σύστημα ΄΄δημόσιου κλειδιού΄΄ και βασίζεται στο γεγονός ότι η παραγοντοποίηση μεγάλων αριθμών εμπεριέχει ποσότητες υπολογισμών που απογοητεύουν τους επίδοξους κρυπτοαναλυτές.

Υπάρχουν πολλά συστήματα που χρησιμοποιούνται στο INTERNET για τη διασφάλιση των μεταδιδόμενων πληροφοριών.Στο web το SSL είναι το κυρίαρχο.Χρησιμοποιείται για την δημιουργία ενός κρυπτογραφημένου καναλιού από το οποίο μεταφέρονται κάθε είδους πληροφορίες.Αντίθετα το ΣΕΤ αποτελεί νεότερο πρωτόκολλο και χρησιμοποιείται αποκλειστικά με συστήματα πληρωμών μέσω πιστωτικών καρτών.Μερικά από τα πρωτοκόλλα που χρησιμοποιούνται για την μεταβίβαση πληροφοριών, αναφέρονται στον ακόλουθο πίνακα :

Πρωτόκολλο	**Στόχος**
Cybercash, Set	Ηλεκτρονικές Πληρωμές
SSL, PCT, TLS	Κρυπτογράφηση
PGP, S/MIME	E-mail TCP/IP
S-HTTP	Web browsing

SSL (Secure Sockets Layer)

Το SSL αποτελεί πρωτόκολλο το οποίο τοποθετείται στο επίπεδο δικτύου και εξασφαλίζει τη δημιουργία ενός ασφαλούς δίαυλου επικοινωνίας.Όλες οι εφαρμογές που τρέχουν επίπεδα θα μπορούν να εκμεταλλευτούν το ασφαλές αυτό κανάλι επικοινωνίας.Μέσα από το κανάλι αυτό μπορεί να μεταδίδεται πληροφορία από τους web servers και clients (HTTP) αλλά και κάθε άλλης μορφής (π.χ e-mail, news).

Το κανάλι εγγυάται ότι τα δεδομένα θα μεταφερθούν ακέραια, ότι το περιεχόμενο τους δεν πρόκειται να αλλάξει κατά τη διάρκεια της μεταφοράς και πιστοποιεί τον web server δηλαδή ο web browser επιβεβαιώνει ότι ο server είναι αυτός που δηλώνει ότι είναι.

Η πληροφορία πρώτα κρυπτογραφείται και έπειτα μεταδίδεται (ταυτόχρονα συμπιέζεται)για να αποκρυπτογραφηθεί από τον web browser.Αποτελεί αδιαφανή για το χρηστή διαδικασία, ο οποίος δεν αντιλαμβάνεται τίποτα από όλα αυτά, παρά μόνο τα σημάδια στον browser του :Το ΄΄έχει μετατρέπει σε ΄΄ https://΄΄και υπάρχει ένα σύμβολο κλειστής κλειδαριάς στο κάτω μέρος της οθόνης.

Όταν σε μια σύνδεση χρησιμοποιείται το SSL οτιδήποτε μεταφέρεται ανάμεσα στο χρήστη και τον web server είναι κρυπτογραφημένο, όπως το URL και τα περιεχόμενα του κειμένου που μεταδίδεται, τα περιεχόμενα που αποστέλλονται από το χρήστη μέσω φορμών (άρα και τα στοιχεία του πελάτη και ο αριθμός της πιστωτικής κάρτας τους)

Χρησιμοποιούνται δυο είδη κρυπτογράφησης:δημόσιου κλειδιού και συμμετρική .Με την
πρώτη επιτυγχάνεται πιστοποίηση των δυο μερών που θέλουν να επικοινωνήσουν μεταξύ τους.Με τη δεύτερη μεταφέρονται κρυπτογραφημένα τα δεδομένα ανάμεσα στα δυο μέρη, βάσει όμως μόνο ενός κλειδιού που κρυπτογραφούνται τα δεδομένα που μεταφέρονται.

Το SSL εγγυάται ότι οι πληροφορίες που εισάγονται σε μια φόρμα θα φτάσουν στον προορισμό της αναλλοίωτες.Για να το πετύχει αυτό, χρησιμοποιεί συμμετρική κρυπτογράφηση.Οι πληροφορίες που μεταδίδονται με βάση ένα μυστικό κλειδί που έχει δημιουργηθεί για την περίσταση, το οποίο γνωρίζουν ο browser του χρήστη και ο server.Επίσης, εγγυάται ότι οι πληροφορίες στέλνονται στο σωστό άνθρωπο και όχι σε τρίτους.Για να το πετύχει αυτό πιστοποιούνται τα δύο συναλλασσόμενα μέρη από κάποιον τρίτο, ο οποίος τυγχάνει να απολαμβάνει της εμπιστοσύνης και των δυο

μερών.Υπάρχουν εταιρείες οι οποίες πραγματοποιούν αυτά ακριβώς (όπως η Verisign, GET και άλλες).

Παρ' όλα αυτά υπάρχουν κάποια μειονεκτήματα που χαρακτηρίζουν το SSL, κυρίως σε ο,τι αφορά τη χρήση του ως πρωτόκολλο ηλεκτρονικών συναλλαγών.Παρά το ότι διασφαλίζει την ασφαλή μεταφορά των προσωπικών στοιχείων και των αριθμών των πιστωτικών καρτών, δεν βοηθά στο υπόλοιπο μέρος της συναλλαγής.Έτσι, δεν κάνει ελέγχους για την εγκυρότητα του αριθμού που αποστέλλεται, για το αν ο πελάτης είναι εξουσιοδοτημένος να χρησιμοποιεί τη συγκεκριμένη κάρτα, δεν αναφέρεται στην τύχη των αριθμών των πιστωτικών καρτών, μετά ôϊί άφιξή τους στον server του πωλητή κ.α.Μπορεί να έφτασε, για παράδειγμα, ο αριθμός χωρίς να τον έχουν δει τρίτοι κατά τη διάρκεια της συναλλαγής, αλλά ο πωλητής μπορεί να μην το αποθήκευσε σε ασφαλές μέρος, με αποτέλεσμα να υπάρχει η πιθανότητα κλοπής.

SET (Secure Electronic Transactions).

Με αντίθεση με το SSL το SET αποτελεί εξειδικευμένο πρωτόκολλο για τη διασφάλιση των ηλεκτρονικών συναλλαγών μέσω πιστωτικών καρτών.Κατασκευάζεται από τις Visa MasterCard, IBM, Netscape, Microsoft, GTE, Verisigen.Στο SET αυτοί που συμμετέχουν σε μια συναλλαγή είναι ο πελάτης, ο έμπορος, η τράπεζα του εμπόρου, καθένας από τους πρέπει να έχει ψηφιακά πιστοποιητικά έχει ψηφιακά πιστοποιητικά (digital certificates).

Με τη χρήση των ψηφιακών αυτών πιστοποιητικών επιβεβαιώνεται από τα συναλλασσόμενα μέρη (πωλητής και έμπορος) η ταυτότητα τους.Αυτό αποτελεί την φάση της συναλλαγής (αυθεντικοποίηση των δύο μερών).Οι πελάτες επιβεβαιώνουν ότι οι έμποροι από τους οποίους επιθυμούν να αγοράσουν είναι νόμιμοι, μέσα από ôϊί ψηφιακή ταυτότητα τους, όπως και οι έμποροι για τους πελάτες.Η εμπιστοσύνη αυτή εδραιώνεται μέσω των πιστοποιητικών που έχουν εκδοθεί από τρίτες αρχές (π.χ. τράπεζες).Ένα πιστοποιητικό περιέχει το όνομα του προσώπου για το οποίο εκδίδεται (έμπορος ή πελάτης), την ψηφιακή υπογραφή του, το δημόσιο (και το αντίστοιχο ιδιωτικό κλειδί του) και την υπογραφή της αρχής που εξέδωσε το πιστοποιητικό.Όταν ο πελάτης δώσει μια παραγγελία, ο browser του λαμβάνει το πιστοποιητικό του

προκειμένου να ελεγχθεί αν είναι όντως νόμιμος-αν σχετίζεται με κάποιον χρηματοπιστωτικό οργανισμό.Στη συνέχεια στέλνεται στον έμπορο η παραγγελία κρυπτογραφημένη με το δημόσιο κλειδί του εμπόρου.Στην τράπεζα στέλνεται η πληροφορία σχετικά με την πληρωμή, κρυπτογραμένη με το δημόσιο κλειδί της τράπεζας.Το μεγάλο πλεονέκτημα του SET είναι ότι με αυτόν τον τρόπο δεν στέλνεται πληροφορία με τον αριθμό της πιστωτικής κάρτας στον έμπορο.

Η παραγγελία χωρίζεται σε δύο μέρη.Το πρώτο μέρος αναφέρεται στην αίτηση παραγγελίας προς τον έμπορο και το δεύτερο οικονομικά-προσωπικά στοιχεία του πελάτη, τα οποία στέλνονται στον (έμπιστο) οικονομικό οργανισμό του εμπόρου.Από εκεί και έπειτα οι τράπεζες του πελάτη συνεργάζονται, προκειμένου να διασφαλιστεί η αυθεντικότητα των δύο μερών, και πραγματοποιούν τις υπόλοιπες χρηματοοικονομικές διαδικασίες περίπου με τον παραδοσιακό τρόπο.

Ο πελάτης πρέπει αφ'ενός να αποκτήσει ένα ψηφιακό πιστοποιητικό από κάποιο χρηματοπιστωτικό οργανισμό, με έναν τραπεζικό λογαριασμό και πιστωτική κάρτα, και αφ'ετέρου να εγκαταστήσει το λογισμικό του SET με τη μορφή plug-in, ActiveX control ή java applet.Ο έμπορος πρέπει να εγκαταστήσει στον Web server του το λογισμικό του SET.Το SET δεν έχει ακόμα χρησιμοποιηθεί ευρέως, σε αντίθεση με το SSL, το οποίο διατηρεί το μεγαλύτερο μερίδιο στις ασφαλείς ηλεκτρονικές.Σιγά σιγά εμφανίζονται προϊόντα από μεγάλες εταιρίες του χώρου που χρησιμοποιούν το πρωτόκολλο.

Σύμφωνα με τους κατασκευαστές του πρόκειται για ένα πολύ ασφαλές πρωτόκολλο.Εξάλλου μοιάζει πολύ με τον τρόπο που γίνονται οι συναλλαγές με πιστωτικές κάρτες σήμερα.Το βασικό μειονέκτημα, που ίσως το χαρακτηρίζει, είναι το γεγονός ότι είναι εξαρτώμενο και συνυφασμένο με το σύστημα συναλλαγών μέσω πιστωτικών καρτών.Έτσι, δεν μπορεί να χρησιμοποιηθεί για πολύ μικρές συναλλαγές, καθώς για κάθε τέτοια γίνεται χρέωση της πιστωτικής κάρτας.

Σύνθημα και ταυτότητα χρήστη (Password and user-id).

Όλα τα υπολογιστικά συστήματα σήμερα στα οποία εργάζονται πολλοί χρήστες, απαιτούν από τον κάθε χρήστη ορισμένα στοιχεία, χωρίς τα οποία δεν του επιτρέπουν προσπέλαση στο σύστημα.Συνήθως ο χρήστης υποχρεώνεται να πληκτρολογήσει μια ταυτότητα και στη συνέχεια που κρατούνται σε πίνακες, ώστε να βεβαιωθεί ότι ο

χρήστης είναι εφοδιασμένος με την εξουσιοδότηση που αιτείται.Το σύστημα αυτό παρουσιάζει το πλεονέκτημα της εύκολης δημιουργίας κατηγοριών χρηστών σε σχέση με τα δικαιώματα προσπέλασης.Η επιλογή του συνθήματος πρέπει να είναι τέτοιο (ικανό μήκος, άσχετη με το πρόσωπο που το χρησιμοποιεί, συχνή αλλαγή κ.λ.π.) ώστε να εξασφαλίζει ότι είναι δύσκολο να ΄΄μαντευθεί΄΄ από άλλο πρόσωπο.

Ψηφιακά πιστοποιητικά στα εταιρικά δίκτυα.

Με την ευκαιρία να αναφερθεί ότι τα ψηφιακά πιστοποιητικά μπορούν να χρησιμοποιηθούν όχι μόνο για ηλεκτρονικές αγορές αλλά και για τον καθορισμό της πρόσβασης των χρηστών σε εταιρικά δίκτυα (intranets), και μάλιστα πολύ αποτελεσματικά.Ένας οργανισμός μπορεί να ορίσει τέτοια πιστοποιητικά στους χρήστες του δικτύου του, λειτουργώντας ουσιαστικά ο ίδιος ως μια αρχή πιστοποίησης, καθορίζοντας την πρόσβαση που μπορεί να έχει ο καθένας από αυτούς στις πληροφορίες του οργανισμού μέσω πιστοποιητικών.

Από τα σημαντικότερα προβλήματα ασφάλειας που αντιμετωπίζουν οι οργανισμοί είναι η προστασία των ευαίσθητων δεδομένων που διατηρούν (οικονομικά στοιχεία, ιατρικά δεδομένα και ο έλεγχος της πρόσβασης σε αυτά).Με τη χρήση ψηφιακών πιστοποιητικών μπορεί να καθοριστεί ποιοι θα έχουν πρόσβαση με περισσότερο αξιόπιστο και αποτελεσματικό τρόπο σε σχέση με τα συνθηματικά (passwords).Τα συνθηματικά συχνά δεν επιλέγονται σωστά από το χρήστη.Συνήθως χρησιμοποιούνται απλές λέξεις, εύκολα ευρισκόμενες από προγράμματα που μαντεύουν συνθηματικά (crackers).Επίσης, ακόμα κι αν δημιουργηθούν σωστά (με πολλούς αλφαριθμητικούς χαρακτήρες και με την υπόδειξη του διαχειριστή του συστήματος), καθίσταται δυσκολομνημόνευτα από τους χρήστες, οι οποίοι τα γράφουν, σε βιβλία και προσωπικά σημειώματα, που ίσως πέσουν στα χέρια κακόβουλων χρηστών.

Το ψηφιακό πιστοποιητικό μπορεί να λειτουργήσει όπως μια κάρτα πιστοποίησης της ταυτότητας για δϊί είσοδο σε κτίρια με υψηλές απαιτήσεις ασφάλειας.Όπως μια τέτοια κάρτα καθορίζει σε ποιους χώρους έχει πρόσβαση ο χρήστης που την κατέχει, με αντίστοιχο τρόπο ο κάτοχος του πιστοποιητικού μπορεί να έχει πρόσβαση σε συγκεκριμένες πληροφορίες,ενώ απαγορεύονται ρητά εκείνοι για τους οποίους δεν έχει εκδοθεί ψηφιακό πιστοποιητικό.

Ο οργανισμός (ή η εταιρεία) που ενδιαφέρεται να εκδίδει ο ίδιος πιστοποιητικά για τους χρήστες του πρέπει να χρησιμοποιήσει προγράμματα, τα γνωστότερα από τα οποία είναι το Onsite, ο CA Workstation αποτελείται και από ξεχωριστό hardware για την αποθήκευση με τη μεγαλύτερη δυνατή ασφάλεια των κλειδιών που δημιουργούνται.Τα εν λόγω συστήματα δέχονται αιτήσεις των χρηστών για την έκδοση πιστοποιητικών και με τη σειρά τους αναλαμβάνουν να εκδώσουν τα πιστοποιητικά αυτά.Τα συγκεκριμένα πιστοποιητικά είναι άχρηστα εκτός του οργανισμού που τα εκδίδει,εκτός και αν ο οργανισμός έχει ο ίδιος πιστοποιητικό από κάποια CA.

Βεβαίωσης γνησιότητας (authentication).

Η μέθοδος αυτή χρησιμοποιείται πολύ σήμερα από τα τραπεζικά δίκτυα.Με τη μέθοδο αυτή δημιουργείται στο σημείο εκπομπής του μηνύματος μέσω λογισμικού ειδικό πεδίο βεβαίωσης γνησιότητας που προστίθεται στο μήνυμα που ταξιδεύει.Στο σημείο λήψης επαναλαμβάνεται η διαδικασία δημιουργίας και το αποτέλεσμα συγκρίνεται με το περιεχόμενο του πεδίου βεβαίωσης γνησιότητας.Εάν δεν είναι το ίδιο μήνυμα απορρίπτεται.

Εκτός από τις παραπάνω μεθόδους, χρησιμοποιούνται και μια σειρά άλλες όπως για παράδειγμα τήρηση μαγνητικών ταινιών που περιέχουν την κίνηση της ημέρας, την ταυτότητα κάθε συναλλαγής με μία περίληψη του τι ακριβώς έκανε και πότε κ.λ.π. που καθιστούν δυνατή την αναπαραγωγή με μεγάλη λεπτομέρεια των συνθηκών κάτω από τις οποίες έγινε κάποια παραβίαση ασφαλείας.

Παρά τα μέτρα όμως αυτά ασφαλείας μέχρι σήμερα δεν μπορεί να ισχυριστεί κανείς ότι έχει πετύχει πλήρη ασφάλεια από επιθέσεις μια και συνεχώς σημειώνονται παραβιάσεις συστημάτων που μάλιστα θεωρούνται ''καλά φρουρούμενα''.Και θα πρέπει να σημειώσει κανείς ότι οι παραβιάσεις που ''ακούγονται'' από το γεγονός αυτό και μόνο, θα πρέπει να θεωρηθούν αποτυχημένες...

Επίσης υπάρχει μια εφαρμογή, η οποία θα ελέγχει ποια προγράμματα θέλουν να στείλουν στο διαδίκτυο και θα επιτρέπει μόνο σε συγκεκριμένα από την πρόσβαση.Αυτή η εφαρμογή θα πρέπει να βρίσκεται ανάμεσα στον υπολογιστή που προστατεύει και στο διαδίκτυο και να ελέγχει κάθε bite που κινείται προς αυτόν.Όσο δύσκολη κι αν ακούγεται η παραπάνω δουλειά, είναι πραγματοποιήσιμη για την ακρίβεια, έχει ήδη πραγματοποιηθεί.Οι εφαρμογές που κάνουν αυτήν τη δουλειά

ονομάζονταν Firewalls.Δεν επιτρέπει σε τίποτα να περάσει προς τα ΄΄έξω΄΄ χωρίς την έγκριση του χρήστη.Αυτήν τη στιγμή **το Firewall είναι μία από τις καλύτερες** και **πιο εύκολες εφαρμόσιμες λύσεις** για την προστασία των υπολογιστικών συστημάτων.Μέχρι πριν από λίγο καιρό μια τέτοια εφαρμογή κόστιζε αρκετά χρήματα.Σήμερα όμως, υπάρχουν αρκετές εταιρείες που προσφέρουν τέτοιου είδους εφαρμογές εντελώς δωρεάν.Ένα αρκετά καλό και πολύ εύχρηστο Firewall είναι το **Zonealarm.**Μετά την εγκατάστασή του το Zonealarmμπορεί να ρυθμιστεί έτσι, ώστε να εμφανίζεται στο systemtray με κάθε εκκίνηση του υπολογιστή.Κύριο χαρακτηριστικό του είναι η αρκετά μεγάλη ευκολία στη χρήση και στη ρύθμιση του.Κάνοντας διπλό κλικ στο εικονίδιο του Zonealarm στο Systray, εμφανίζεται το κεντρικό μενού της εφαρμογής.

Επιλέγοντας, τώρα, ανάμεσα στα Alerts, Lock, Security, Programs και Configure, γίνεται εμφάνιση πληροφοριών στην κατηγορία που επιλέχθηκε.Κάνοντας κλικ στο πλήκτρο ''Alerts'', εμφανίζεται ο αριθμός των bytes που έχουν σταλεί (προς τα ''έξω'') και ο αριθμός των bytes που έχουν ληφθεί.Επίσης, εμφανίζονται όλα τα Alerts που έχουν σημειωθεί από την εκκίνηση των Windows και έπειτα.Εδώ μπορεί να ρυθμιστεί και η καταγραφή όλων των
Alerts σε ένα αρχείο.txt.Κάνοντας ένα απλό κλικ στο εικονίδιο που έχει τη μορφή ενός λουκέτου, διακόπτεται απευθείας κάθε επαφή με το Internet και αποκλείεται η διέλευση ακόμα και ενός byte από ή προς αυτό.

Κάθε φορά που μια εφαρμογή προσπαθεί για κάποιο λόγο να συνδεθεί με το Internet, το Zonealarm τη σταματάει και ενημερώνει το χρήστη.Ο χρήστης τώρα έχει τρεις επιλογές.Μπορεί να επιτρέψει στην εφαρμογή αυτή να έχει πρόσβαση στο Internet ή όχι.Ακόμα μπορεί να κάνει τις απαραίτητες ρυθμίσεις, ώστε να μπορεί η εφαρμογή να έχει πάντα πρόσβαση στο Internet.

Εκτός από το Zonealarm, υπάρχουν και άλλα Firewalls που παρέχονται δωρεάν.Ωστόσο, το Zonealarm παρέχει όλες τις βασικές ρυθμίσεις που πρέπει να έχει ένα πρόγραμμα αυτού του είδους.Σίγουρα μερικές φορές αντιδρά λίγο υπερβολικά – αφού αντιλαμβάνεται ακόμα κι ένα απλό ping που έγινε από κάποιον στον υπολογιστή – όμως σημασία έχει το αποτέλεσμα :μια αρκετά καλή προστασία.

Επίσης υπάρχουν διάφοροι μηχανισμοί προστασίας από διάφορους περίεργους που βρίσκονται σε άμεση επαφή με τον υπολογιστή, σε περιπτώσεις δηλαδή, όπου η επίθεση δεν γίνεται μέσω του Διαδικτύου .Και αυτές οι περιπτώσεις είναι οι εξής:

Προστασία με Winzip, Winrar...

Πολλοί χρήστες προστατεύουν τα δεδομένα τους με τη βοήθεια κάποιου προγράμματος συμπίεσης, όπως είναι το πολύ δημοφιλές Winzip.Μάλιστα, πιστεύουν ότι επιλέγοντας τη ρύθμιση ΄΄Protect Zip with Password΄΄, τα δεδομένα τους είναι πλέον ασφαλή.Δυστυχώς,κάτι τέτοιο δεν ισχύει (!).Ο τρόπος, με τον οποίο γίνεται η κρυπτογράφηση των δεδομένων στα περισσότερα προγράμματα συμπίεσης, είναι εδώ και αρκετό καιρό γνωστός.Έχει σχολιαστεί και έχει δημοσιευτεί σε χιλιάδες ιστοσελίδες στο διαδίκτυο.Επίσης, έχουν κυκλοφορήσει αρκετές εφαρμογές που με ένα κλικ του ποντικιού στο ''προστατευόμενο'' αρχείο εμφανίζουν απευθείας τον κωδικό, με τον οποίο αυτό έχει προστατευτεί.Συνεπώς, **τέτοιους είδους προγράμματα δεν θα πρέπει να χρησιμοποιούντα για την προστασία πολύτιμων δεδομένων.**

Προστασία αλά Screensaver...

Η προστασία με τον Screensaver των Windows είναι αρκετά συνηθισμένη.Πολλοί εμπιστεύονται τον υπολογιστή τους στα 'χέρια'' του Screensaver των Windows ,εάν θέλουν να απουσιάσουν μερικά λεπτά από το γραφείο τους και δεν θέλουν να πειράξει κάποιος τον υπολογιστή τους.Αυτή η προστασία μπορεί να ενεργοποιηθεί πολύ γρήγορα στα Display Properties στη σελίδα ΄΄Screen Saver΄΄.Ωστόσο, τα μερικά λεπτά δεν πρέπει σε καμία περίπτωση να γίνουν μισάωρο, διότι σε αυτήν την περίπτωση η ασφάλεια που παρέχεται από τον Screensaver είναι παραπάνω από ελλιπής.Με τους σημερινούς υπολογιστές, που πραγματοποιούν ταχύτητα reboots, και με τη βοήθεια του πλήκτρου reset ο υπολογιστής θα είναι διαθέσιμος σε όλους σε 2-3 λεπτά(!).Υπάρχει, δηλαδή, χρόνος να διαβαστούν δεδομένα και να ξαναγίνει εκκίνηση του υπολογιστή.Οπότε, **αν θέλει κάποιος καλύτερη προστασία, εισάγει έναν κωδικό στο BIOS ή προστατεύει τον υπολογιστή με κάποια εφαρμογή που να ζητάει κάποιον κωδικό με την εκκίνηση των Windows.**Θα πρέπει να γνωρίζει ο κάθε χρήστης ότι ο τρόπος, με τον οποίο γίνεται κρυπτογράφηση του password του screensaver,είναι πολύ απλός και χρησιμοποιήθηκε στις πρώτες εφαρμογές κρυπτογράφησης.Η Microsoft θεωρεί επαρκή για την κρυπτογράφηση ενός password μια απλή κωδικοποίηση με ένα

XOR.Αυτή η μέθοδος συνεχίστηκε και στις επόμενες εκδόσεις των Windows, χωρίς να πραγματοποιηθούν ριζικές αλλαγές στον τρόπο κωδικοποίησης.Επομένως, είναι αρκετά εύκολο να βρεθεί ο κωδικός που έχει εισαγάγει κάποιος στον Screensaver του.Μάλιστα, το σημείο στη Registry, όπου αποθηκεύεται το password, είναι γνωστό και φανερώνεται, άλλωστε, και από το όνομα του.Στο κλειδί ''Screensaver Data'' βρίσκεται το password σε κωδικοποιημένη μορφή.Σίγουρα το παραπάνω δεν είναι και τόσο τραγικό, εφόσον, βέβαια δεν κάνει ο χρήστης του ίδιου password και αλλού για να προστατεύσει πολύτιμα δεδομένα.Ως εκ τούτου, μια άλλη πολύ χρήσιμη συμβουλή είναι **να μην χρησιμοποιούν παντού το ίδιο password**

Προστασία από το BIOS.

Σίγουρα η προστασία από το BIOS είναι μια αρκετά καλή λύση, ωστόσο έχει κι αυτή τις αδυναμίες της.Σχεδόν σε κάθε motherboard υπάρχει ένα jumper που επαναφέρει τις ρυθμίσεις του BIOS στις εργοστασιακές.Σε κάθε manual αναφέρεται ότι αυτή η επιλογή υπάρχει κυρίως για δϊί περίπτωση που ο χρήστης ξεχάσει το password που είχε επιλέξει.Δυστυχώς, όμως αυτό το jumper μπορεί να χρησιμοποιηθεί και από κάποιον κακόβουλο που έχει την περιέργεια να δει τι κρύβεται πίσω από αυτόν τον ''προστατευμένο'' υπολογιστή.Η μέθοδος κρυπτογράφησης που χρησιμοποιείται από τα περισσότερα BIOS είναι αρκετά καλή.Με την εισαγωγή ενός password στο BIOS γίνεται υπολογισμός μιας ''check sum'' και ύστερα γίνεται αποθήκευσή της.Το μόνο ελάττωμα αυτού του τρόπου κρυπτογράφησης είναι το ''check sum'' που έχει υπολογισθεί, αντιστοιχεί και σε περισσότερους κωδικούς.Έτσι, για παράδειγμα, μπορεί κάποιος να επιλέξει τη λέξη ''WINMAG'' και το ''check sum'' της να είναι ακριβώς το ίδιο με αυτό της ακολουθίας ''AZDJUA''.

Προστασία αλά Office 2000.

Από τις προηγούμενες κιόλας εκδόσεις του Office n Microsoft είχε δώσει στους χρήστες του τη δυνατότητα να προστατεύσουν τα έγγραφα τους μα έναν κωδικό.Η προστασία πραγματοποιείται γρήγορα κι εύκολα.Όταν θέλει κάποιος να αποθηκεύσει

ένα αρχείο και έχουμε πατήσει Save, πατάει το πλήκτρο ''Tools''και ύστερα επιλέγει ''General Options''.Στην οθόνη εμφανίζεται ένα παραθυράκι, στο οποίο μπορεί να επιλεγεί το password, με το οποίο θα θέλει να προστατέψει το αρχείο τους.Ως εδώ όλα φαίνονται μια χαρά, και η προστασία φαίνεται να λειτουργεί.Αν θέλει ο χρήστης όμως, να προστατέψει πολύ σημαντικά δεδομένα, δεν αρκεί, καθώς ο τρόπος, με τον οποίο κάνει κρυπτογράφηση το Office 2000, είναι γνωστός(!).

Τελικά παρατηρούμε ότι προστασίες που πολλοί θεωρούσαν επαρκείς, φαίνονται...γελοίες για κάποιον που έχει κάποιες γνώσεις γύρω από το θέμα ''ασφάλεια''.Επίσης σύμφωνα με όσα αναγράφονται αποδεικνύεται τελικά ότι ένας υπολογιστής είναι συχνά απροστάτευτος μπροστά σε διάφορους εισβολείς, που μπορούν αρκετές φορές να πάρουν εύκολα τον πλήρη έλεγχο ενός συστήματος.Παρ'όλα αυτά, εάν τηρηθούν κάποιοι κανόνες, μπορεί ο κάθε χρήστης να προσφέρει αρκετά μεγάλη ασφάλεια στον υπολογιστή και τα δεδομένα.

Το πιο βασικό είναι η χρήση ενός Firewall, όπως το Zonealarm που αναφέρθηκε παραπάνω.**Ένα Firewall σε συνδυασμό με ένα πολύ καλό Virus Scanner, όπως το Norton Antivirus, παρέχει αρκετά υψηλή προστασία.**Μια δεύτερη συμβουλή είναι να κατεβάζονται πάντα τις τελευταίες εκδόσεις προγραμμάτων που κάνουν χρήση του Διαδικτύου, γιατί διορθώνονται συνήθως bugs και διάφορα ''Security Holes''.

Για να προστατεύεται ο υπολογιστής από διάφορους ''εσωτερικούς'' εισβολείς καλό είναι να γίνεται η χρήση κάποιου προγράμματος που είναι εξειδικευμένο σε αυτόν τον τομέα.

Μπορούν επίσης να προστατευτούν συγκεκριμένα αρχεία σε έναν υπολογιστή με τη βοήθεια ενός προγράμματος κρυπτογράφησης.Έτσι, ακόμα κι αν κλαπούν με κάποιον τρόπο, Δε θα μπορέσουν να διαβαστούν ή να χρησιμοποιηθούν.

Τελικά, η ασφάλεια ήταν, είναι και θα είναι ένα λεπτό θέμα, και γι'αυτό καλό είναι ο να ενημερώνονται όλοι οι χρήστες ανά τακτά χρονικά διαστήματα για τις εξελίξεις σε αυτό τον τομέα.Εφαρμόζοντας, τα παραπάνω μέτρα ασφάλειας στα πληροφοριακά συστήματα των Η/Υ μειώνεται πάντως δραματικά η πιθανότητα κλοπής δεδομένων ή εισβολή σε ένα τέτοιο σύστημα.

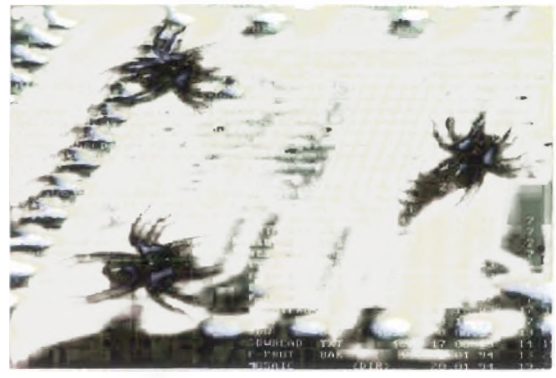
ΜΕΡΟΣ Β΄

«ΠΡΟΣΒΟΛΕΣ ΣΥΣΤΗΜΑΤΩΝ Η/Υ ΣΥΝΗΘΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΠΟ ΙΟΥΣ»

ΚΕΦΑΛΑΙΟ 1

ΚΑΤΑΣΤΡΕΠΤΙΚΟΙ ΙΟΙ ΚΑΙ ΤΑ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥΣ

1. Η δημιουργία των βιολογικών – τεχνολογικών ιών.



Οι βιολογικοί – Τεχνολογικοί ιοί δημιουργούνται με την βοήθεια του ανθρώπου και μεταδίδονται με τον ίδιο τρόπο προς τους βιολογικούς και Τεχνολογικούς οργανισμούς.Σε μια λεπτομερή σύγκριση των βιολογικών και των τεχνολογικών ιών, παρατηρούνται τρομακτικές ομοιότητες.

Θα έχετε αναμφισβήτητα παρατηρησει ότι οι βιολογικοί ιοί είναι δυσάρεστοι συγκάτοικοι του πλανήτη μας, που πολλαπλασιάζονται μόνο με την βοήθεια ενός οργανισμού, στον οποίο κατοικούν, και ονομάζεται ξενιστής.Από τους οργανισμούς αυτούς παίρνουν την ενέργεια που χρειάζονται για τον μεταβολισμό και τον πολλαπλασιασμό τους.Οι ιοί είναι κατά κανόνα, πολύ εξειδικευμένοι.Αυτό σημαίνει ότι δεν μπορούν να «Φιλοξενηθούν» οπουδήποτε, αλλά χρειάζονται ένα συγκεκριμένο ξενιστή.Έναν οργανισμό που προσφέρει τις κατάλληλες προϋποθέσεις για το μεταβολισμό του ιού.Μία ίωση συχνά δεν αναγνωρίζεται αμέσως.Υπάρχουν ιοί, με διάρκεια επώασης πολλών ημερών ή και εβδομάδων.Ακόμη όμως και όταν αναγνωριστεί η ασθένεια, τα προβλήματα συνεχίζονται.Οι ιοί έχουν μεγάλη αντοχή για αυτό η καταπολέμηση τους είναι εξαιρετικά δύσκολη.Επιπλέον οι ιοί εξαπλώνονται

τόσο γρήγορα που δύσκολα γίνονται αντιληπτοί από τα θύματα τους, θα έχουν ήδη διεισδύσει στους οργανισμούς για να εξαπλώσουν το μικρόβιο τους.Οι βιολογικοί ιοί, λοιπόν, είναι οργανισμοί που εγκαθίσταται σε έναν άλλο οργανισμό, και ζουν και πολλαπλασιάζονται με την βοήθεια, ή καλύτερα σε βάρος του.Κατά την διάρκεια της διαδικασίας αυτής και ανάλογα με τον ιό, ο ξενιστής υφίσταται μικρότερες ή μεγαλύτερες και στην οριακή περίπτωση πεθαίνει.

Οι ιοί των υπολογιστών τώρα, είναι και αυτοί προγράμματα, που έχουν όμως τη δυσάρεστη ιδιότητα να εγκαθίστανται σε άλλα προγράμματα.Αυτό σημαίνει ότι ο κώδικας του ιού εγκαθίσταται κάπου μέσα στον κωδικό του άλλου προγράμματος, κατά κανόνα στην αρχή ή στο τέλος του με συνέπεια το πρόγραμμα που έχει προσβληθεί να χάσει την πρόσβαση σε ορισμένες λειτουργίες, να μην εκτελείται όπως θα έπρεπε ή στην χειρότερη περίπτωση δεν θα μπορεί πια να εκτελεστεί.

Ο μεγαλύτερος λοιπόν εχθρός των συστηματων Η/Υ σε συν/κες επιχειρήσεις είναι οι ιοί με τις βλαβερές συνέπειες τους.Η καταστροφή τους μπορεί να ποικίλει και να είναι τόσο εκτεταμένη ώστε να απαιτείται η πλήρης ανοικοδόμηση όλου του συστήματος προγραμμάτων και δεδομένων.Για αυτό το λόγο οι ιοί των υπολογιστών είναι ένας πραγματικός κίνδυνος για την ευημερία της κοινωνίας μας.Ώστοσο πολλοί άνθρώποι δεν παίρνουν ακόμη στα σοβαρά τους ιούς των υπολογιστών.Ο κύριος λόγος γι'αυτό είναι η άγνοια, συνδυαζόμενη πολλές φορές και με την απάθεια.Ορισμένοι δε οι οποίοι έχουν εμπορικά ενδιαφέροντα στη βιομηχανία των υπολογιστών, δεν θέλουν να εστιάζεται η προσοχή του καταναλωτικού κοινού σ' αυτή την απειλή προφανώς φοβούμενοι την αρνητική δημοσιότητα για τα προϊόντα και τις υπηρεσίες τους για αυτό το λόγο κάνουν τα πάντα ώστε να αποπροσανατολίσουν την κοινή γνώμη από το φαινόμενο των ιών.Ώστοσο για να υπάρχει μία ισορροπημένη κοινωνία οφείλει ο κάθε άνθρωπος να έχει επαρκείς γνώσεις σχετικά Τι είναι ιός; και κυρίως για την ασφάλεια πληροφοριακών συστημάτων Η/Υ για την προστασία προσωπικών δεδομένων του υπολογιστή τους και γενικά για την ασφάλεια του μηχανικού και λειτουργικού μέρους του υπολογιστή.

2. Οι « Hackers ».

Οι περισσότεροι ιοί δημιουργούνται με μυστικότητα από άτομα χωρίς σημαντική οικονομική ισχύ.Είναι κατά κύριο λόγο μια δραστηριότητα μοναχικών ανθρώπων που έχει συνήθως την μορφή ηλεκτρονικού βανδαλισμού, κακόβουλης διασκέδασης ή εκδίκησης προς κάποιο συγκεκριμένο άτομο ή το κοινωνικό σύνολο.Η ζήλια και ο η αίσθηση κατωτερότητας είναι επίσης δύο στοιχεία που παίζουν μεγάλο ρόλο στην διαμόρφωση της συμπεριφοράς των δημιουργών των ιών.Ένας εισβολέας ο οποίος έχει δυσκολίες να επικοινωνήσει με τους άλλους ανθρώπους αισθάνεται ότι πρέπει να προστατέψει το περιβάλλον του υπολογιστή του, στο οποίο λειτουργεί πολύ άνετα, από τα να ελέγχεται από άλλα άτομα ή ατόμων που φθονεί. Καταστρέφοντας τους υπολογιστές άλλων επιβεβαιώνει ότι αυτός έχει τον έλεγχο και την απόλυτη ισχύ σε έναν χώρο που τον θεωρεί απόλυτα προσωπικό.

Αυτοί οι άνθρωποι που ασχολούνται με επιθέσεις σε υπολογιστικά συστήματα είναι γνωστοί γενικά σαν «hackers» μπορούν να χωριστούν σε τέσσερις κατηγορίες:σε εγκληματίες, σε ειδικούς, σε βάνδαλους και σε swappers.

1. Οι «εγκληματίες» είναι άτομα που εκμεταλλεύονται αδυναμίες συστημάτων.Τέτοια συστήματα μπορεί να είναι μία οποιανδήποτε επιχείρηση για παράδειγμα οι συν/κες επιχειρήσεις, που έχουν την ικανότητα να διεισδύσουν στο διαδίκτυο τους, με την χρήση του INTERNET κλέβοντας ότι σημαντικά στοιχεία που είναι δυνατόν να τα χρησιμοποιήσουν εναντίον τους.Κύριως διεισδύουν σε τραπεζικά συστήματα κάνοντας «ηλεκτρονικές ληστείες».Η ουσιώδης διάφορα με τις άλλες κατηγορίες είναι ότι δεν χρησιμοποιούν τις απλοποιημένες μεθόδους και μέσα που χρησιμοποιούν οι ερασιτέχνες και που είναι έως ένα βαθμό αντιμετωπίσιμες.
2. Οι «ειδικοί» είναι ελάχιστα άτομα που είναι ενημερωμένοι σε θέματα Η/Υ με επικοινωνίες δεδομένων και τηλεπικοινωνιών.Μπορούν να μπουν σ' ένα σύστημα με ερευνητικές μεθόδους.Αρκούνται στο «σπάσιμο» του συστήματος και μετά αποσύρονται.
3. Οι «βάνδαλοι» είναι μειοψηφία.Συνήθως μπαίνουν σε δίκτυα ή υπολογιστές και αφήνουν ανόητα μηνύματα ή διαγράφουν στοιχεία.Επίσης φτιάχνουν προγράμματα ελκυστικά ή αρκετά έξυπνα πιθανώς σαν παιχνίδια ή βοηθητικά προγράμματα έτσι ώστε να προκαλέσουν την προσοχή του χρήστη.Με αποτέλεσμα αυτά τα ελκυστικά

προγράμματα να καταλήγουν σε καταστροφές ή σ' ένα είδος ηλεκτρονικών σκουπιδιών ιών ή προπαγάνδας ή στην απόκτηση απορρήτων στοιχείων που τα χρησιμοποιούν για να προκαλέσουν ζημιές.

4. **Τέλος οι «swappers»** είναι πλειοψηφία και αποτελούνται από άτομα νεαρά ηλικίας που δρουν ακόμη με την νοοτροπία του παιχνιδιού.Γνωρίζουν συνήθως αρκετά γύρω από υπολογιστές.Δεν θεωρούν τους εαυτούς τους κλέφτες, άλλα σαν έξυπνους που ξεπερνούν τις στημένες δυσκολίες.Είναι πιο επικίνδυνοι από τους ειδικούς γιατί χρειάζονται πολύ λιγότερα κίνητρα για να περάσουν από την ακίνδυνη στην καταστρεπτική επέμβαση.

Συνήθως οι «hackers» χρησιμοποιούν συγκεκριμένα όπλα για να επιτεθούν στα θύματα τους ανάμεσα στα πιο χρήσιμα είναι πλέον τα Trojan horses ή εκμετάλλευση κάποιων bugs.Ένα Trojan horses είναι μία εφαρμογή γραμμένη σε μία γλώσσα προγραμματισμού, με σκοπό την εισβολή σ' ένα υπολογιστή.(Η λειτουργία ενός Trojan στηρίζεται σε δικτυακό πρωτόκολλο, απαιτεί την ύπαρξη ενός προγράμματος server και ενός client).Σε κάθε ΄΄μολυσμένο΄΄ υπολογιστή βρίσκεται ο server, ενώ ο επιτιθέμενος ελέγχει κάποιον υπολογιστή με την βοήθεια του client.Με την βοήθεια ενός Trojan μπορεί κάποιος να αποσπάσει εύκολα δεδομένα από έναν υπολογιστή και να τα ΄΄κατεβάσει΄΄ στο δικό του.Μπορεί να προκαλεί την αναπαραγωγή ήχων ή την εμφάνιση διαφόρων περίεργων μηνυμάτων στον υπολογιστή του θύματος.Ακόμα, με πολύ λίγο κόπο μπορεί να αποσπάσει το password δηλ.τον κωδικό πρόσβασης με τον οποίο συνδέεται ο χρήστης με τον προμηθευτή του και να προκαλέσει μεγάλη οικονομική ζημιά εις βάρος του πραγματικού κάτοχου του password.

Επιπλέον τα Bugs αποτελούν ένα θαυμάσιο όπλο για τους «hackers».Τα Bugs είναι διάφορα λάθη που γίνονται κατά τον προγραμματισμό μιας εφαρμογής.Πλλές φόρες μπορεί να προκαλέσουν το ΄΄κρέμασμα΄΄ ενός συστήματος ή τον τερματισμό μιας εφαρμογής.Σε μερικές περιπτώσεις, ωστόσο, ένα Bug, τα οποία εκμεταλλεύτηκαν διάφοροι ΄΄επιτήδειοι΄΄, προκειμένου να αποκτήσουν πρόσβαση σε κάποιους υπολογιστές.

Τελικά παρατηρούμε ότι ένας υπολογιστής μπορεί να είναι συχνά απροστάτευτος όταν ο έλεγχος τους περνιέται σ' άλλα χέρια στους «hackers» χωρίς να υπολογίζεται η έγκριση του δικαιούχου χρήστη.Η πράξη των «hackers» θεωρείται ποινικό αδίκημα αφού παραβιάζει το ιδιωτικό χαρακτήρα των ηλεκτρονικών επικοινωνιών.Μάλιστα και το έγκλημα της πληροφορικής αντιμετωπίζεται με το ποινικό δίκαιο χωρίς ωστόσο να είναι διαδεδομένο σ'όλες τις χώρες.Αυτοί λοιπόν οι νομικοί κανόνες μπορούμε να

πούμε ότι αποτελούν το δίκαιο της πληροφορικής.Ο νόμος συνήθως αποτελεί κίνητρο ώστε οι επιτήδειοι να περιορίσουν τις πράξεις τους για να ενισχυθεί η ασφάλεια στα υπολογιστικά συστήματα.

3. Τα διάφορα είδη Ιών.

Υπάρχουν αναμφίβολα πολλές δυνατότητες ταξινόμησης των ιών.Αλλά υπάρχουν δύο σημαντικές ταξινομήσεις με βάση τη μορφή της βλάβης που προκαλούν, και στη συνέχεια μα βάση τις περιοχές που προσβάλλουν.

Ταξινόμηση κατά το είδος της βλάβης:

1. **«Ακίνδυνοι Ιοί»** πρόκειται για ιούς που πιθανότητα προγραμματίστηκαν μάλλον από περιέργεια και διάθεση πειραματισμού.Ο προγραμματιστής δεν είχε σκοπό να προκαλέσει ζημιές με τον ιό του, αλλά ήθελε μονό να δοκιμάσει, αν ο αλγόριθμος του λειτουργεί.Και αυτοί βέβαια οι ιοί τροποποιούν τον κώδικα του προγράμματος που προσβάλλουν, και πολλαπλασιάζονται, αλλά δεν προξενούν ζημιές, Δε διαθέτουν δηλαδή «επιδραστικό μέρος».Τέτοιοι ιοί δηλώνουν άλλωστε κατά κανόνα αμέσως την ύπαρξή τους, με ένα μήνυμα που εμφανίζεται στην οθόνη.

Υπάρχουν επίσης πολλοί ιοί που κυκλοφορούν για παρουσίαση (Demo).Οι ιοί αυτοί εξυπηρετούν σκοπούς επίδειξης και εξαπλώθηκαν από κάποιους χρήστες από άλλους κατά λάθος, άλλα και από μερικούς σίγουρα σκόπιμα.Και αυτοί οι ιοί δεν **προξενούν** κατά κανόνα μεγάλες ζημιές, άλλα ασχολούνται κυρίως με τον πολλαπλασιασμό τους.Κυκλοφορούν όμως με τέτοιον τρόπο, ώστε τελικά να μπορούν να προξενήσουν μεγάλες ζημιές.

Παρατηρούμε όμως ότι οι ιοί που μεταδίδονται μέσου μολυσμένων δεν θεωρούνται ακίνδυνοι ιοί εφόσον δεν αλλάζουν τα προγραμματα που είναι αποθηκευμένα στον υπολογιστή.

2. **«Πειραματικοί ιοί»** πρόκειται για ιούς που δημιουργήθηκαν από τους ερευνητές ιών, για να μελετήσουν τον τρόπο εργασίας των ιών.Εξυπηρετούν την προσπάθεια βελτίωσης των ερευνητικών προγραμμάτων για αναγνώριση και απομάκρυνση ιών.Τέτοιοι ιοί συνήθως δεν κυκλοφορούν ευρύτητα, επειδή εξυπηρετούν μόνο ερευνητικούς σκοπούς, και γι' αυτό δεν μας ενδιαφέρουν ιδιαίτερα.

Oliver Wagner:''VIRUSCAN'', ''Εντοπίστε και Εκμηδενίστε τους Ιούς των Υπολογιστών'', Αθήνα 1997, σελ 42 -45

3. «Ιοί επικαλύπτουν αρχεία» αυτός ο τύπος ιού επικαλύπτει το μολυσμένο αρχείο με τον κώδικα του προγράμματος του ιού.Μερικοί ιοί αποδεικνύονται ιδιαίτερα συστηματικοί, και επικαλύπτουν ολόκληρο το προσβεβλημένο αρχείο, ενώ άλλοι πάλι επικαλύπτουν τμήματα μόνο του αρχείου.Φυσικά, το «μολυσμένο» πρόγραμμα με τον τρόπο αυτόν αχρηστεύεται και δεν μπορεί να αποδώσει την εργασία για την οποία δημιουργήθηκε, είτε μερικά, είτε και τελείως.Ανάλογα με το μέγεθος της επικάλυψης, οι ιοί αυτοί ανακαλύπτονται σχετικά εύκολα.Αυτό το είδος ιού γίνεται ολοένα και λιγότερο σημαντικό.

4. «Ιοί καταστρέφουν εσωτερικά δεδομένα» αυτό το είδος των ιών ιδιαίτερα επικίνδυνο, επειδή δεν καταστρέφουν στην τύχη οποιαδήποτε προγράμματα ή δεδομένα, αλλά στρέφονται εναντίον των στοιχείων εκείνων, που είναι πολύ σημαντικά για τη λειτουργία του συστήματος.Τέτοια δεδομένα βρίσκονται, για παράδειγμα, στον πίνακα κατανομής αρχείων (FAT) και στον πίνακα διαμερισμού.Αν καταστρέφουν οι πληροφορίες που περιέχονται στους πίνακες αυτούς, είτε η επανάκτησή τους γίνεται τόσο δύσκολη, ώστε να πρέπει να είναι πραγματικά ιδιαίτερα σημαντικά, για να αξίζει τον κόπο η προσπάθεια επανάκτησης τους.

Για παράδειγμα : ο FAT ο περιέχει τις βασικές πληροφορίες για το λειτουργικό σύστημα, σχετικά με τη θέση των αρχείων στη δισκέτα ή το σκληρό δίσκο.Αν τα δεδομένα αυτά καταστρέφουν, το λειτουργικό σύστημα δεν θα μπορεί πια να εντοπίσει κανένα αρχείο.

Εξίσου μοιραία είναι η ζημιά στον πίνακα διαμερισμού.Στους σκληρούς δίσκους επιτρέπεται να γίνει διαμερισμός των δεδομένων σε δύο τουλάχιστον «σκληρούς δίσκους», τα λεγόμενα διαμερίσματα για τις εκδόσεις μάλιστα του DOS μέχρι την έκδοση 3.3, και για σκληρούς δίσκους με χωρητικότητα πάνω από 32 Mbytes, ο διαμερισμός είναι απαραίτητος, αλλιώς δεν μπορεί το λειτουργικό σύστημα να χειριστεί τα δεδομένα.Στον πίνακα διαμερισμού αποθηκεύονται οι πληροφορίες, που όπου αρχίζει το κάθε διαμέρισμα.Αν χαθούν τα δεδομένα αυτά, το DOS δε θα μπορεί πια να βρει ούτε και τον πίνακα κατανομής (FAT), με αποτέλεσμα και στην περίπτωση αυτή να χάνονται όλα τα αρχεία

Υπάρχουν και ιοί που μορφοποιούν αμέσως ολόκληρες δισκέτες ή σκληρούς δίσκους.Και στις περιπτώσεις αυτές τα δεδομένα χάνονται για πάντα, αν δεν έχουν

ληφθεί από πριν κάποια, προστατευτικά μέτρα.Τέτοια προστατευτικά μέτρα προσφέρουν για παράδειγμα προγράμματα όπως τα PC-Tools, που δημιουργούν ένα «Κάτοπτρο» (Mirror) στο σκληρό δίσκο.

Ένα τέτοιο αρχείο κατόπτρου περιέχει, σε γενικές γραμμές, τις πληροφορίες που κανονικά περιέχονται στον πίνακα διαμερισμού και στον πίνακα κατανομής αρχείων.Έτσι, αν χαθούν οι πληροφορίες αυτές, μπορούν να αντιγραφούν ξανά στην αρχική τους θέση.Εδώ πρέπει να σημειωθεί ότι κατά τη μορφοποίηση, όπως και κατά τη διαγραφή των αρχείων, αλλά απλώς σημειώνεται ο αντίστοιχος χώρος στον FAT ως ελεύθερος.Δυστηχώς αυτό δεν ισχύει για όλες εκδόσεις του DOS,και στο DOS, πότε για τις δισκέτες!

5. «Επιθετικοί ιοί» πρόκειται για ιδιαίτερα ύπουλους ιούς.Τέτοιοι ιοί δεν αναγνωρίζονται και από κανονικές συνθήκες δεν ανακαλύπτονται χωρίς βοηθητικά μέσα.Τροποποιούν τα υπάρχοντα δεδομένα μέσα σ'ένα σύστημα τόσο έντεχνα, ώστε ούτε να καταρρέει το εκτελούμενο πρόγραμμα, ούτε και να ανακαλύπτονται εύκολα οι χειρισμοί τους.

Για παράδειγμα, ιός dbase ττροποποιεί τα δεδομένα των αρχείων dbase.Ο ιός καταγράφει τις αλλαγές αυτές σ' ένα κρυφό αρχείο.

Με τον τρόπο αυτόν, ο ιός ξεγελά το χρήστη, και τον κάνει να πιστεύει ότι τα δεδομένα του – που έχουν ήδη επηρεαστεί – είναι σώστα.Αν όμως ο ιός απομακρυνθεί, τα δεδομένα dbase είναι πιο άχρηστα, επειδή ο ιός δεν μπορεί να διορθώσει όσα τροποποιήθηκαν, και ο χρήστης δεν μπορεί να γνωρίζει τι έχει αλλαχτεί.

Ταξινόμηση κατά τις περιοχές που προσβάλλονται.

Ενδιαφέρον παρουσιάζει και η ταξινόμηση των ιών με βάση τις περιοχές που προσβάλλονται, επειδή ανάλογη θα είναι και η στρατηγική αντιμετώπισης των ιών αυτών.Ακολουθεί μια τέτοια ταξινόμηση των ιών

1. «Ιοί αρχείων» οι αυτοί αντιγράφουν τον κωδικό τους σε εκτελέσιμα αρχεία, και πολλαπλασιάζονται με την κλήση των μολυσμένων αρχείων.Για την απομάκρυνση τέτοιων ιών αρκεί να αντικατασταθεί το μολυσμένο αρχείο με ένα καθαρό αντίγραφο του πρωτότυπου εκτελέσιμου αρχείου.

2. «**Ιοί εκκίνησης**» αυτό το είδος κρύβεται στην περιοχή εκκίνησης των δισκετών και των σκληρών δίσκων.Οι ιοί εκκίνησης προσβάλλουν όταν ενεργοποιηθούν, δισκέτες που είναι ακόμη καθαρές καθώς και, αν δεν έχουν ήδη μολυνθεί τους συνδεδεμένους σκληρους δίσκους.Οι ιοί εκκίνησης, λοιπόν, προσβάλλουν δισκέτες ή σκληρούς δίσκους και όχι αρχεία.

Η περιοχή εκκίνησης είναι μια από φυσική άποψη καθορισμένη περιοχή των δισκετών.Στην περιοχή αυτήν αναζητούνται κατά την εκκίνηση πληροφορίες, που δηλώνουν στο DOS, αν υπάρχουν και που βρίσκονται τα αρχεία του λειτουργικού συστήματος από τη μνήμη.Αυτός είναι ο λόγος που τέτοιοι ιοί μπορούν να εισχωρήσουν και σε δισκέτες που δεν περιέχουν ούτε ένα εκτελέσιμο αρχείο.Έτσι όμως δημιουργείται ένα σοβαρό πρόβλημα.Οι ιοί εκκίνησης είναι τα πρώτα προγράμματα που ενεργοποιούνται μόλις ανοίγει ένας υπολογιστής, δηλαδή ακόμη και πριν να φορτωθεί το λειτουργικό σύστημα.Τα προγράμματα καταπολέμησης των ιών, που ελέγχουν τις καταστάσεις των διακοπών, δεν έχουν καμιά τύχη να αντιμετωπίσουν τους ιούς εκκίνησης, επειδή ο ιός έχει ήδη δεσμεύσει τις διακοπές για τους σκοπούς του.Απαιτούνται λοιπόν ιδιαίτερα μηχανισμοί, για να γίνει δυνατή η αναγνώριση τέτοιων ιών.Δυστηχώς, στο μεταξύ ανακαλύφθηκαν και ιοί, που προσβάλλουν και προγράμματα, και περιοχές εκκίνησης.Αυτό έχει το αποτέλεσμα, να μπορούν οι ιοί αυτοί να εξαπλωθούν πιο γρήγορα και πιο εύκολα, και επιπλέον η απομάκρυνση τους να είναι πολύ πιο δύσκολη.

3. «**Αόρατοι Ιοί**» είναι ιοί που μπορούν να εμποδίσουν με πολύ έξυπνο τρόπο τον εντοπισμό τους.Με κατάλληλους μηχανισμούς δημιουργούν την εντύπωση, ότι ο κώδικας τους δεν βρίσκεται πια στο μολυσμένο πρόγραμμα.Με άλλα λόγια υποκρίνονται ότι ο κώδικας τους έχει διαγραφεί.Στη πραγματικότητα, όμως, ο κώδικας τους εξακολουθεί να βρίσκεται μέσα στο μολυσμένο αρχείο.

Βλέπουμε λοιπόν ότι οι ιοί έχουν πολλές δυνατότητες για να κρυφτούν σε κάποιο σύστημα των ηλεκτρονικών υπολογιστών όπως ένα τέτοιο σύστημα είναι οι συν/κες επιχειρήσεις.Μια και ο κίνδυνος των ιών θα αυξάνεται συνέχεια και δεν θα διαφαίνεται στο μέλλον ότι κάποιο λειτουργικό σύστημα θα κινδυνεύει από τους ιούς, παρότι που τα μέτρα προφύλαξης θα γίνονται όλο και πιο σημαντικά.

3. Βλαπτικά προγράμματα – Ιομορφίες

Ένας κίνδυνος για τα υπολογιστικά συστήματα είναι αυτός που περιλαμβάνει «μολύνσεις» των συστημάτων των συν/κων επιχειρήσεων.Οι μολύνσεις αυτές παίρνουν γενικά μια από τις παρακάτω μορφές:

1. **«Ιοί» (Viruses):** Ιός είναι ένα πρόγραμμα για υπολογιστές το οποίο έχει την ικανότητα να αναπαράγει τον εαυτό του.Μπορεί να έχει βλαβερή επίδραση πάνω στα δεδομένα και στα προγράμματα ενός υπολογιστή.Ένας ιός δεν μπορεί να κάνει τίποτα παραπάνω από αυτά που είναι γραμμένα μέσα στο πρόγραμμα του.Είναι η πνευματική δημιουργία κάποιου προγραμματιστή ακριβώς όπως είναι και το πρόγραμμα επεξεργασίας κειμένου ή το πρόγραμμα λογιστικών φύλλων.

2. **«Λογικές Βόμβες» (Logic bombs):** Οι λογικές βόμβες είναι μικρά προγράμματα που προστίθεται σε άλλα μπορούν να προκαλέσουν βλάβες σε αρχεία μετά από κάποιο προκαθορισμένο χρονικό διάστημα ή σε κάποια προκαθορισμένη ημερομηνία (π.χ Παρασκευή και 13).Τοποθέτηση των λογικών βομβών δεν γίνεται αυτόματα αλλά από κάποιο ανθρώπινο χέρι.

3. **«Δούρειοι Ίπποι» (Trojan horses):** Οι δούρειοι ίπποι είναι προγράμματα που φαινομενικά παράγουν χρήσιμο έργο αλλά στην πραγματικότητα περιέχουν κρυμμένοι κώδικα που εκτελεί ανεπιθύμητες ή ζημιογόνες λειτουργιες.Συχνά ένας ιός μπορεί να είναι κρυμμένος μέσα σε έναν δούρειο ίππο.Ένα πρόγραμμα **το οποίο** φαίνεται χρήσιμο, ενώ στην ουσία είναι το αντίθετο.Οι δούρειοι ίπποι διαφέρουν από τις λογικές βόμβες στο ότι οι τελευταίες ενεργοποιούνται κάθε φορά που εκτελείται το πρόγραμμα «φορέας» αλλά μόνο όταν τηρείται κάποια συνθήκη.

4. Οι πιο φημισμένοι ανά τον κόσμο ιοί.

Υπάρχουν εκατοντάδες τύποι διαφορετικών ιών που κυκλοφορούν στον κοσμο.Κάθε μέρα ο αριθμός των ιών και το οικονομικό μέγεθος της ζημιάς που προκαλούν, συνεχίζει, παγκοσμίως, να αυξάνεται.

Την τελευταία χρονιά μετρήθηκαν 10% περισσότεροι ιοί σε σχέση με το 1998 και το FBI εκτιμά ότι το συνολικό κόστος των ζημιών πλησιάζει τα δέκα δισεκατομμύρια δολάρια το χρόνο.

Από το 1986 μέχρι σήμερα σημειώθηκαν πολλές επικίνδυνες επιθέσεις.Μεγάλο βαθμό εξάπλωσης πέτυχαν κυρίως οι εξ :

1986: Ο ιός **«Brain» («Εγκέφαλος»)** χτυπά τους πρώτους δικτυωμένους υπολογιστές.Θεωρήθηκε ότι είχε δημιουργηθεί από δύο αδέλφια στη Λαχώρη του Πακιστάν.Ως αποτέλεσμα της επίθεσης εμφανίζονται ένα χρόνο αργότερα τα πρώτα προγράμματα προστασίας απέναντι στους Ιούς των ηλεκτρονικών υπολογιστών.

1988:Ο ιός Morris (σκουλήκι Μόρις ήταν για την ακρίβεια το όνομα του) τρυπώνει σε χιλιάδες υπολογιστές μέσω του ArpaNet, μιας πρόδρομης μορφής του Internet.

Μάρτιος 1992: Ο ιός **«Μικελάντζελο»** χτυπά τις αρχικές σελίδες δικτυακών τόπων και υπάρχουν φόβοι ότι έχει τη δυνατότητα να «ξεδοντιάσει» τον σκληρό δίσκο εκατομμυρίων υπολογιστών.Τελικά, επηρεάζονται μερικές μόνο χιλιάδες.

Μάιος 1996: Ο ιός **«Wazzu»** καταστρέφει τα αρχεία ηλεκτρονικών κειμένων, εισαγόμενος σε αυτά και πάλι μέσω e-mail.

1998: Μια ομάδα χάκερ υπό την επωνυμία «Η λατρεία της Νεκρής Αγελάδας» απελευθερώνει τον επικίνδυνο ιό **«Δούρειο Ίππο»**

1998: Στην επέτειο του πυρηνικού ατυχήματος στο Τσερνομπίλ, ο ιός **«CIN»** καταστρέφει τα λειτουργικά προγράμματα των Windows'95 και '98.

1999: Ο ιός **«Μελίσσα»** προκαλεί ζημιές 80 εκατομμυρίων δολαρίων σε χιλιάδες συνδεδεμένους υπολογιστές.

Το Δεκέμβριο του ίδιου έτους ο David Smith κηρύσσεται ένοχος ως δημιουργός του ιού, σε μια από τις λίγες περιπτώσεις που οι διωκτικές αρχές συλλαμβάνουν ένα δράστη.

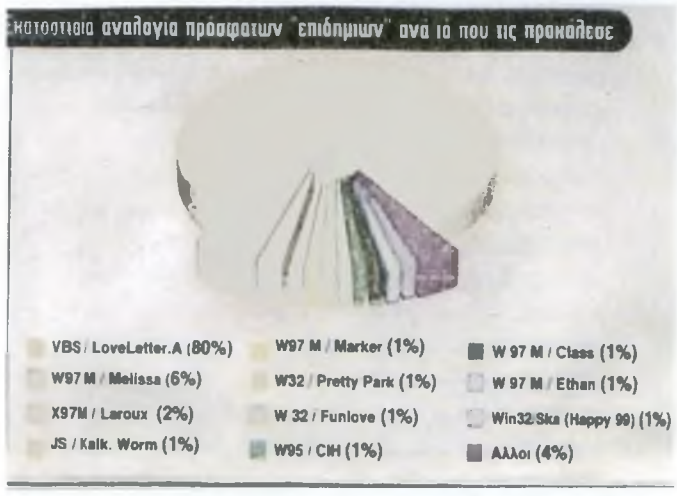
2000: Ο ιός της **«Αγάπης»** μεταλλάσσεται σε «Αστείο».Στην ουσία πρόκειται για ένα ακόμη όνομα του ιού, θελκτικό και αυτό προς τους χρήστες.Θεωρείται πιο καταστροφικός από τον Melissa ο οποίος είχε την ιδιότητα να εμφανιζόταν στην ηλεκτρονική αλληλογραφία και να επανεγγράφει τους φακέλους με ηχητικά δεδομένα ή φωτογραφίες, αντικαθιστώντας το περιεχόμενο τους με τους δικούς τους κωδικούς.Θεωρείται ο πιο διαδιδόμενος ιός που έχει μέχρι σήμερα εμφανιστεί στην ιστορία ανάλογων επιθέσεων και, σύμφωνα με κάποιες εκτιμήσεις η οικονομική ζημιά που προκάλεσε ανέρχεται σε 8-10 δισεκατομμύρια δολάρια ο δημιουργός του **«Love Letter»** ήταν ένας νεαρός φοιτητής από τις Φιλιππίνες όπου συλλήφθηκε από το FBI.

Εν κατακλείδι, από ό,τι φαίνεται το πρόβλημα των ιών θα συνεχίσει να υπάρχει, μάλιστα με δεδομένη την ολοένα μεγαλύτερη διασύνδεση υπολογιστικών συστημάτων το μόνο που πρέπει να κάνει ο κάθε χρήστης μεμονωμένα και η κάθε επιχείρηση να είναι ιδιαίτερα επιφυλακτικοί σ'ότι πρωτόγνωρο και ελκυστικό εμφανίζεται στην οθόνη τους ταυτόχρονα να προστατεύσουν τα υπολογιστικά τους συστήματα με τα σωστά μέτρα προφύλαξης.

5. Η αποκαλυπτική έρευνα των ιών.

Παρατηρούμε στις μέρες μας ότι η εμφάνιση νέων ιών που σε μερικές περιπτώσεις προκαλούν πραγματικές ΄΄επιδημίες΄΄, είναι συνηθισμένο φαινόμενο.Πώς δικαιολογείται όμως αυτό το φαινόμενο με δεδομένη την εξάπλωση των αντιβιοτικών

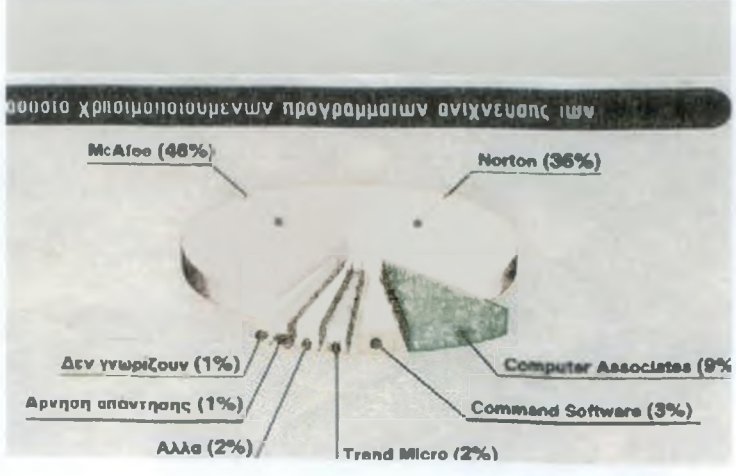
προγραμμάτων; Επιπλέον σε ποιο βαθμό οι ιοί προκαλούν όντως καταστροφές ή απλώς δυσλειτουργίες σε μεμονωμένους υπολογιστές και δίκτυα;Η πρόσφατη έρευνα του ανεξάρτητου οργανισμού ICSA δίνει απαντήσεις που βασίζονται σε ποσοτικά δεδομένα.



Ένα από τα πολλά αντικείμενα που αναφέρονται στην αποστολή των εργαστηρίων είναι και η παροχή προτύπων και μεθόδων ασφαλείας κατά των υπολογιστικών ιών.Στο πλαίσιο αυτό παρουσιάζουν κάθε χρόνο μια έρευνα που έχει σκοπό να περιγράψει το πρόβλημα των ιών στα δίκτυα υπολογιστών.

Τα αποτελέσματα της έρευνας έδειξαν ότι το πρόβλημα των ιών συνεχίζει να μεγαλώνει.Οι εταιρείες ολοένα συχνότερα αντιμετωπίζουν περιστατικά προσβολής από ιούς, σε βαθμό τέτοιο που η πιθανότητα αυτή έχει αυξηθεί στο διπλάσιο σε σχέση με τα προηγούμενα πέντε χρόνια, αυξάνοντας φυσικά και το αντίστοιχο κόστος.Τα αποτελέσματα της έρευνας για τους ιούς που σημειώθηκαν το 2000 έδειξαν ότι το 51% των ερωτηθέντων αντιμετώπισης μία καταστροφή λόγω ιών σε σχέση με το 48% της προηγούμενης χρονιάς.Αξιοσημείωτο είναι ότι το 80% από αυτές τις επιθέσεις αφορούσε σε ιούς που μεταδόθηκαν μέσω ηλεκτρονικού ταχυδρομείου.Αύξηση παρουσίασαν και τα περιστατικά μετάδοσης ιών μέσω του Internet, ενώ ήταν ελάχιστες οι περιπτώσεις μετάδοσης μέσω δισκετών.

Παρατηρήθηκε ότι όλες οι εταιρείες εκτός από μία, ανέφεραν ότι κατά τη διάρκεια της έρευνας είχαν τουλάχιστον ένα περιστατικό προσβολής από από ιό.Το μηνιαίο ποσοστό επεισοδίων για κάθε 1000 υπολογιστές για τους πρώτους δύο μήνες των ετών 1996 ως



2000 παρουσιάζει δραματική αύξηση της τάξεως του 800%, αφού τα 10 περιστατικά το μήνα το 1996 έγιναν 91 το 2000. Επίσης, 152 από τις 300 εταιρείες απάντησαν ότι κατά την περίοδο έρευνας αντιμετώπισαν περίπτωση επιδημίας δηλαδή την ταυτόχρονη εμφάνιση ιών σε περισσότερους από 25 υπολογιστές.

Ενδιαφέρον επίσης παρουσιάζουν οι απόψεις των ερωτηθέντων σχετικά με το πρόβλημα των ιών σε σχέση με το 1999. Η πλειονότητα απάντησε ότι όσον αφορά στους ιούς που σχετίζονται με το Ms-Word υπάρχει μια μικρή επιδείνωση, ενώ γι'αυτούς που σχετίζονται με το Ms-Excel η κατάσταση βελτιώνεται.

Επίσης η έρευνα έδειξε ότι η προσβολή του ιού προκαλεί σημαντικές επιπτώσεις στις επιχειρήσεις κυρίως στον οικονομικό τομέα.Είναι φανερό ότι η εμφάνιση κάποιου ιού σε ένα δίκτυο, αν δεν αντιμετωπιστεί άμεσα, θα οδηγήσει σίγουρα στο κλείσιμο κάποιων servers του δικτύου και ειδικά του mail server, με σκοπό την αποτροπή της εξάπλωσης του ιού στο ίδιο αλλά και σε εξωτερικά δίκτυα.Ο χρόνος που οι servers παραμένουν αδρανείς κυμαίνεται συνήθως μέχρι μια ώρα, ενώ δεν λείπουν οι περιπτώσεις που παραμένουν κλειστοί για 10 και 30 ώρες.Αποτέλεσμα της αδράνειας αυτής είναι να χάνονται πολύτιμες εργατοώρες.Η έρευνα έδειξε ότι σχεδόν το 75% των ερωτηθέντων ανέφεραν ότι χάθηκαν 10 ή λιγότερες εργάσιμες ημέρες.Το κόστος δε για μία εταιρεία κυμαίνεται συνήθως από 1000 έως 1500 δολάρια, ενώ δεν λείπουν και περιπτώσεις που το κόστος ξεπερνά τα 100.000 δολάρια.

Στον τομέα των επιπτώσεων μίας επίθεσης από ιό προηγείται η μείωση της παραγωγικότητας με ποσοστό 70% και 49% αντίστοιχα.

Τέλος η έρευνα ταξινομεί τα καλύτερα μέτρα προφύλαξης εναντίον των ιών σύμφωνα με τις απόψεις και με τις εμπειρίες της κοινής γνώμης.Και σύμφωνα με την έρευνα θεωρείται ως μοναδικό όπλο κατά της απειλής των ιών την χρησιμοποίηση λογισμικού προστασίας.Το 80% των ερωτηθέντων δήλωσαν ότι είχαν εγκαταστήσει στο 90% των υπολογιστών τους τέτοια προγράμματα, ενώ το περίπου 55% δήλωσαν ότι είχαν εγκαταστήσει σε όλους.Όσον αφορά τώρα στις προτιμήσεις των εταιρειών σε συγκεκριμένα προγράμματα ανίχνευσης ιών, η έρευνα έδειξε ότι τη μερίδα του λέοντος κατέχουν τα πολύ γνωστά σε όλους McAfee VirusScan και Norton Antivirus με 54% και 42% αντίστοιχα.Οι μηχανισμοί αποτροπής που χρησιμοποιούν οι περισσότερες εταιρείες είναι ο συνεχής έλεγχος καθ' όλη τη διάρκεια λειτουργίας του υπολογιστή σε ποσοστό 69% και ο έλεγχος κατά την εκκίνηση του υπολογιστή σε ποσοστό 68%.

Όπως ήταν αναμενόμενο η έρευνα φανέρωσε κάποιες αλήθειες σχετικά με το πρόβλημα των ιών.Παρά την ευρεία χρήση προγραμμάτων ανίχνευσης ιών, δεν κατέστη

δυνατόν να μειωθούν τα κρούσματα επιδημίας.Οι λόγοι φυσικά γι' αυτό είναι δυο: η συνεχής εμφάνιση νέων ιών και η λανθασμένη χρηση των προγραμμάτων προστασίας.Η εμφάνιση ιών που αναπαράγονται και μεταδίδονται με μεγάλη ταχύτητα μέσω του ηλεκτρονικού ταχυδρομείου καθιστά αναποτελεσματική τη χρήση οποιωνδήποτε μεθόδων προστασίας, αφού τις περισσότερες φόρες μέχρι να ανακαλυφθεί το αντίδοτο και να ενημερωθούν τα προγράμματα ο ιός έχει ήδη ''χτυπήσει''.Επίσης, πολύ συχνά, λόγω της μείωσης της απόδοσης των συστημάτων από τη συνεχή ανίχνευση των αρχείων, οι χρήστες απενεργοποιούν κάποιες από τις βασικές λειτουργίες των προγραμμάτων προστασίας με αποτέλεσμα να προσβάλλονται υπολογιστές που έχουν εγκατεστημένο τέτοιο πρόγραμμα.Επειδή, λοιπόν, η μετάδοση των περισσότερων ιών γίνεται σήμερα μέσω του ηλεκτρονικού ταχυδρομείου, κρίνεται απαραίτητη η συνεχής εκπαίδευση και ενημέρωση των χρηστών έτσι ώστε να προσέχουν και να μην ανοίγουν μηνύματα τα οποία προέρχονται από άγνωστους χρήστες ή έχουν παράξενους τίτλους.

Τα αποτελέσματα από την εξάπλωση κάποιου ιού στο δίκτυο μιας εταιρείας παραμένουν τα ίδια όλα αυτά τα χρόνια.Το βασικότερο από αυτά είναι η καταστροφή αρχείων δεδομένων, αφού πολλές φορές η επανεισαγωγή τους είναι αδύνατη ή πολύ χρονοβόρα.Για να περιοριστεί η απώλεια δεδομένων θα πρέπει, σε τακτά χρονικά διάστημα, να παίρνουν backup τόσο σε επίπεδο server όσο και σε επίπεδο προσωπικών υπολογιστών.

Εν κατακλείδι, από ό,τι φαίνεται το πρόβλημα των ιών θα συνεχίσει να είναι υπαρκτό και να αποτελεί την σοβαρότερη απειλή.Εντούτοις δύσκολα αντιμετωπίζεται το πρόβλημα στην ρίζα του χωρίς βλαβερές συνέπειες στα υπολογιστικά συστημάτα.Είναι τόσο ραγδαία η εξέλιξη του που ο ιός είναι εκείνος που εισχωρεί πρώτος στο σύστημα και είναι δύσκολο να αντιμετωπιστεί από χρήστες που δεν είναι ενημερωμένοι πάνω στο πρόβλημα των ιών.Ωστόσο αποτελούν ένα καλό κίνητρο για να ενημερωθούν όλοι!

ΚΕΦΑΛΑΙΟ 2

ΠΩΣ ΜΠΟΡΕΙ ΝΑ ΜΟΛΥΝΕΙ ΕΝΑΣ ΙΟΣ ΤΑ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ ΣΥΝ/ΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

1. Γενικά.

Πως εισχωρεί ένας ιός στα υπολογιστικά συστήματα και μετατρέπει την κανονική και υγιή συμπεριφορά σε μια μορφή ηλεκτρονικής ασθένειας; Η διαδικασία γίνεται πιο αντιληπτή όταν συγκριθεί με τον τρόπο που προσβάλλεται το ανθρώπινο σώμα από κάποιο μικρόβιο.

Η επικοινωνία ανάμεσα στον χρήστη και στον υπολογιστή, γίνεται με την χρησιμοποίηση προγραμμάτων (Software).Χωρίς αυτά, ο υπολογιστής είναι άπλα μία άχρηστη μηχανή.Το Software είναι τόσο το μέσον βάσει του οποίου δίνετε εντολές στον υπολογιστή, όσο και ο μηχανισμός ο οποίος δίνει την δυνατότητα σ'αυτό να διεκπεραιώνει αυτές τις εντολές σωστά το αντίστοιχο του μυαλού και του νευρικού συστήματος του ανθρώπου.Επειδή ο υπολογιστής είναι μία πολύπλοκη συσκευή, ικανή να κάνει πολλές διαφορετικές πράξεις, οι εντολές που τον εξαναγκάζουν να συμπεριφέρεται με τον επιθυμητό τρόπο τείνους επίσης να είναι πολύπλοκες.

Βασικά η δομή των υπολογιστικών συστημάτων αποτελείται από δύο τύπους προγραμμάτων:Το λειτουργικό που ονομάζεται Software στο οποίο ανήκουν διάφορα

προγράμματα και τα προγράμματα εφαρμογών που ανήκουν στο μηχανικό μέρος του hardware που είναι το αντίστοιχο σώμα μας.Όσον άφορα πρώτα το λειτουργικό σύστημα, είναι το κύριο πρόγραμμα που ελέγχει όλες τις βασικές λειτουργίες του υπολογιστή.Για παράδειγμα, εποπτεύει τη λειτουργία των οδηγών δίσκων.Όλοι οι υπολογιστές, από τους **Amigo και Macintosh** μέχρι τους **Mini και Mainframe** έχουν το δίσκο τους λειτουργικό σύστημα.Τα λειτουργικά συστήματα μπορεί να έχουν διαφορετική μεταξύ τους αρχιτεκτονική- όπως, για παράδειγμα, αυτό των Macintosh με αυτό των προσωπικών υπολογιστών, αλλά όλα εκτελούν παρόμοιες λειτουργίες.Αυτό σημαίνει ότι όλα τα λειτουργικά συστήματα είναι τρωτά στους ιούς των υπολογιστών.

Όσον αφορά τώρα το μηχανικό μέρος (Το hardware) του υπολογιστή είναι ισοδύναμο για να γίνει πιο κατανοητή η έννοια του με το ανθρώπινο σώμα.Όταν το ανθρώπινο σώμα βρίσκεται σε κατάσταση ύπνου, το μυαλό και το κεντρικό νευρικό σύστημα εκτελούν ένα ρόλο ανάλογο με αυτόν του λειτουργικού συστήματος του υπολογιστή, ελέγχοντας την κυκλοφορία του αίματος, την αναπνοή και άλλες ζωτικές λειτουργίες του ανθρώπινου οργανισμού.

Όταν ενεργοποιείται το ανθρώπινο σώμα μετά από την κατάσταση ανάπαυσης, του δίνονται συγκεκριμένες οδηγίες – σήκω από το κρεβάτι, πιες καφέ και πήγαινε στην δουλειά.Αυτές οι εντολές τις οποίες ''φορτώνονται'' στο ανθρώπινο μυαλό είναι το ισοδύναμο ενός προγράμματος εφαρμογής που εκτελείται στους υπολογιστές.Όταν το σώμα είναι υγιές, τότε είναι όλα υπό έλεγχο και προβλέψιμα.Δίνονται οδηγίες στο σώμα να εκτελέσει συγκεκριμένες λειτουργίες και τα μέλη του συντονίζονται από το μυαλό και το κεντρικό σύστημα για να εκτελέσουν την κάθε μια εργασία.Εάν το σώμα κολλήσει μια μόλυνση, τόσο το ''λειτουργικό'' του σύστημα όσο και τα ''προγράμματα εφαρμογών'' θα δυσλειτουργούν.Το μυαλό τότε συναντάει δυσκολίες στον να ελέγχει τις βασικές λειτουργίες.

Έτσι λοιπόν ένας ιός των υπολογιστών, έχει παρόμοια επίδραση στα υπολογιστικά συστήματα.Μπορεί να καταστρέψει την ικανότητα του λειτουργικού συστήματος να ελέγχει τις βασικές λειτουργίες και όταν τρέχουν προγράμματα εφαρμογών μπορεί επίσης να τα παρακάμπτει.

2. Διαδικασία εισόδου του ιού σ' ένα σύστημα.

Ενώ ο ιός είναι κι αυτός ένα πρόγραμμα το οποίο ΄΄κλείνει΄΄ ηλεκτρονικά κυκλώματα ακριβώς όπως το λειτουργικό σύστημα και τα προγραμματα εφαρμογών, εντούτοις όμως διαφέρει σημαντικά από αυτά.Τα κανονικά προγράμματα βοηθάνε τους χρήστες να αγοράζουν με το απόλυτο λογικό σκεπτικό ότι ο καθένας που ενεπλάκη στην δημιουργία τους έχει τον ίδιο στόχο μ' αυτούς: την ομαλή διεκπεραίωση κάποιων εργασιών με τον υπολογιστή.

Οι δημιουργοί των ιών γράφουν τα προγράμματα τους με ένα εντελώς διαφορετικό κίνητρο.Επειδή έχουν την επιθυμία να προκαλούν ζημιές.Η μπορεί να γράφουν προγράμματα τα οποία εμφανίζουν ανόητα μηνύματα – ένα είδος ηλεκτρονικών σκουπιδιών ή προπαγάνδας.Τέτοιου είδους ζημιογόνα προγράμματα μπορεί να δείχνουν ενδιαφέροντα ή χρήσιμα – πιθανώς σαν παιχνίδια ή βοηθητικά προγράμματα – έτσι ώστε να προκαλούν την προσοχή του ανυποψίαστου χρήστη.Πολλά τέτοια προγράμματα ανακοινώνονται στα δίκτυα και κατόπιν διανέμονται στους χρήστες, οι οποίοι νομίζουν ότι βρήκαν κάποιο διασκεδαστικό ή χρήσιμο πρόγραμμα.

Είναι λογικό οι ιοί να σχεδιάζονται έτσι ώστε να εισβάλλουν στα συστήματα μέσω των αρχείων που είναι πιο πιθανό να συναντήσουν σ' αυτά.Έτσι, λοιπόν, τα COM, τα EXE και SYS αρχεία που είναι μέρος σχεδόν όλων των υπολογιστών με λειτουργικό σύστημα DOS είναι πιο εμφανείς στόχοι.Τα άλλα λειτουργικά συστήματα έχουν βέβαια παρόμοια τρωτά σημεία.Τα αρχεία εντολών του DOS (αυτά που έχουν επέκταση COM) καθώς και τα EXE είναι εκτελέσιμα προγράμματα που καθοδηγούν το DOS να εκτελέσει συγκεκριμένες λειτουργίες.Η επέκταση SYS δηλώνει τα αρχεία του συστήματος, τα οποία είναι επίσης πολύ ζωτικό μέρος του λειτουργικού συστήματος.

Πολλά εκτελέσιμα αρχεία έχουν την τάση να ενεργοποιούνται με την εκκίνηση του υπολογιστή.Συνεπώς, πολλοί ιοί σχεδιάζονται ώστε να κολλούν πάνω σε αυτά, η παρουσία των οποίων είναι πάντα δεδομένη, τρέχουν συνήθως κάθε φορά που ανοίγει ο υπολογιστής και οι λειτουργίες που επιτελούν είναι εξαιρετικά σημαντικές.

Πολλά προγράμματα εφαρμογών έχουν την δυνατότητα να δημιουργούν ή ακόμα να τροποποιούν τα ήδη υπάρχοντα αρχεία με ονόματα CONFIG.SYS και AUTOEXEC.BAT.Το DOS ψάχνει πάντα για τα δύο αυτά αρχεία κατά την διαδικασία εκκίνησης για να διαβάσει από αυτά πληροφορίες για την διαμόρφωση του συστήματος

ή οδηγίες για τα προγράμματα που θα εκτελέσει.Συνεπώς,ένας ιός μπορεί να τρέξει πριν από τα προγράμματα ανίχνευσης που μπορεί να έχει ο κάθε χρήστης στον υπολογιστή του,προκαλώντας την ζημιά σε κλάσματα του δευτερολέπτου καθώς εκκινείτε ο υπολογιστής.

Γιατί θα ήθελε κάποιος να δημιουργήσει ένα πρόγραμμα ιό; Το να γράψει κανείς ένα πρόγραμμα το οποίο θα προϋποθέτει την βιωσιμότητά του μέσα από διαδικασίες αυτόματης αναπαραγωγής και θα εκτελεί και διάφορες εργασίες που του έχουν ειπωθεί, είναι μία μεγάλη πρόκληση για την διανόηση του καθενός.Για να μπορέσει η τεχνολογία των υπολογιστών να συνεχίσει την ανάπτυξη της, χρειάζονται ευφυείς και δημιουργικούς ανθρώπους οι οποίοι θα
εξερευνήσουν το δυναμικό αυτής της νέας τεχνολογίας.Η δημιουργία αυτοαναπαραγόμενων προγραμμάτων είναι ένα σημαντικό μέρος της διαδικασίας ανάπτυξης, ειδικά αν σκοπεύει κανείς να δρέψει όλο αυτό το δυναμικό και να το αφιερώσει σε όλο και πιο ανταγωνιστικές εργασίες.Κατ' ακολουθία, πολλοί ιοί μπορεί να έχουν δημιουργηθεί από σοβαρούς και υπεύθυνους ερευνητές και να έχουν πιθανώς διαφύγει στο γενικότερο περιβάλλον των υπολογιστών.

Ορισμένοι ιοί δημιουργούνται αρχικά σαν αποτυχημένα παιχνίδια.Αυτοί έχουν δυνατότητα να κάνουν μεγάλες ζημιές, αν το πρόγραμμα περιέχει λάθη τα οποία το εξαναγκάζουν να φέρεται με καταστροφικό τρόπο και ειδικά εάν εξαπλώνεται αδιακρίτως σε κάθε μηχανή.

Οι ιοί αποτελούν επίσης ένα θαυμάσιο όπλο για όλα αυτά τα μέλη της κοινωνίας μας τα οποία επιδιώκουν να βλάψουν τους συνανθρώπους τους.Ορισμένοι από τους ανθρώπους αυτούς είναι βάνδαλοι καταστροφείς, άλλοι έχουν πολιτικά κίνητρα ή θέλουν να βλάψουν έναν φορέα που κατά την γνώμη τους έχει κάνει κάτι κακό.

Δεδομένου ότι το σύνολο των ανθρώπων που ασχολείται με τους υπολογιστές είναι πλέον μεγάλο, υπάρχουν μέσα του κακόβουλοι με και άνθρωποι αποξενωμένοι από το κοινωνικό σύνολο που έχουν τις απαραίτητες δυνατότητες να δημιουργούν και να διαδίδουν ιούς.

Υπάρχει επίσης και το φαινόμενο της αντιγραφής που θα πρέπει να λάβουμε υπ' όψη.Για παράδειγμα, εάν ένας ιός βάλει δηλητήριο σε ένα φάρμακο του εμπορίου, μπορεί να οδηγήσει κι άλλους ανθρώπους στο να τον μιμηθούν.Ανόμοια όμως με τη δηλητηρίαση φαρμάκων, δεν μπορούμε να σταματήσουμε την εξάπλωση των ιών βάζοντας σφράγισμα ασφαλείας στις δισκέτες των προγραμμάτων Είναι πολύ εύκολο οι επιτήδειοι να αναζητήσουν χιλιάδες μεθόδους ώστε να μεταδώσουν ιούς στα διάφορα

συστήματα που ένα απ' αυτά είναι και οι συν/κες επιχειρήσεις που αποτελούν την σημερινή μας κοινωνία και πλήττονται από το πρόβλημα των ιών.Αντιμέτωπες συν/κες επιχειρήσεις σ' αυτήν την απειλή συνίσταται σύμφωνα με τα παραπάνω να είναι ιδιαίτερα προσεκτικές σε πειραματικά προγράμματα που δεν είναι επίσημα αγορασμένα και στον δανεισμό δισκετών από τρίτα άτομα.Το πιθανότερο είναι ότι θα είναι πειραματικά ή προγράμματα ευρείας κυκλοφορίας τα οποία μπορεί και να έχουν μολυνθεί.Επίσης να εγκαταστήσουν στα υπολογιστικά τους συστήματα αντιβιοτικά προγράμματα ιδιαίτερα όταν γίνεται η χρήση του INTERNET διότι κρίνεται επικίνδυνη η μεταφορά μολυσμένων αρχείων μεταξύ των διασυνδεόμενων συστημάτων.Γενικά η χρήση του INTERNET είναι πιο ευάλωτη περιοχή στο μικρόβιο του ιού και κατά κάποιο τρόπο θεωρείται η μοναδική επικίνδυνη ζώνη, να απειλείται από τις εισβολές των ιών από τους « Hackers».Διότι η χρήση των δισκετών σήμερα έχει περιοριστεί με την χρησιμοποίηση CD-ROM.Έτσι λοιπόν η διαδικασία εισόδου του ιού σ'ένα σύστημα γίνεται ουσιαστικά μ' αυτούς τους δύο τρόπους που εκεί πρέπει να δοθεί ιδιαίτερη σημασία από τον κάθε χρήστη και από την οποιανδήποτε επιχείρηση.

3. Πως οι ιοί ελέγχουν ένα πρόγραμμα.

Η πιο ενοχλητική άποψη της επιδημίας των ιών είναι ότι ο μέσος όρος των χρηστών αρχίζει να χάνει τον έλεγχο του υπολογιστή τους.Οι εντολές τις οποίες δίνει ο χρήστης στον υπολογιστή του μπορούν να παραμορφωθούν από κάποιον ιό που έχει σχεδιαστεί γι αυτό τον σκόπο.Το χάσιμο του ελέγχου μπορεί να επιτευχθεί με πολλούς τρόπους, ανάλογα με το πώς είναι προγραμματισμένος ο ιός εισβάλλει στον υπολογιστή.Ούτε ο χρήστης ούτε το λειτουργικό σύστημα μπορεί να ελέγξει μία τέτοια κατάσταση, δεδομένου ότι ο ιός δεν είναι
σχεδιασμένος να ενεργεί με τα δικά του αθώα μέτρα και σταθμά.Μάλιστα μπορεί να δρα σαν τη πλειονότητα των μικρών παιδιών, που άλλα τους λες και άλλα κάνουνε.Μπορεί επίσης σκόπιμα να εξαθλιώσει τα αρχεία του υπολογιστή, καταστρέφοντάς τα ή παραμορφώνοντάς τα κατά τις επιθυμίες του.

Η λέξη κλειδί στο να γίνει αντιληπτό πώς λειτουργούν οι ιοί είναι έλεγχος.Οι ιοί που εισβάλλουν στα COM και EXE αρχεία, διακόπτουν την κανονική λειτουργία του υπολογιστή με την πρώτη ευκαιρία και παίρνουν τον έλεγχο του συστήματος ενώ ταυτόχρονα αντιγράφουν τους εαυτούς τους σε άλλα αρχεία των ίδιων τύπων.

Μπορεί να προσκολληθούν εξωτερικά σ' ένα αρχείο, ή μπορούν να βρουν χώρο στο εξωτερικό κάποιων προγραμμάτων όπου και αυτοεγκαθίσταται.

Η διαδικασία αυτή – της διακοπής της κανονικής λειτουργίας του υπολογιστή και της ανάληψης του ελέγχου από τον ιό για να αναπαραχθεί και να κολλήσει και σ' άλλα αρχεία και το ξαναπέρασμα μετά του ελέγχου στο λειτουργικό σύστημα ή τα προγράμματα εφαρμογών – μπορεί να συμβεί τόσο γρήγορα ώστε ο χρήστης να μην καταλάβει ποτέ ότι κάτι ανεπιθύμητο έχει συμβεί.

Ορισμένοι από τους εισβολείς των COM και EXE αρχείων παραμένουν μόνιμα στην μνήμη του υπολογιστή, έτσι ώστε να μπορούν να μολύνουν το κάθε πρόγραμμα που εκτελείται.Μπορούν να τροποποιήσουν τον τομέα εκκίνησης του δίσκου ώστε να δημιουργήσουν ένα πιο άνετο περιβάλλον για να δρουν και να αναπαράγονται.Μπορούν επίσης να τροποποιήσουν τα προγράμματα εφαρμογών για την περισσότερη άνεση τους.

Ένας ιός μπορεί επίσης να προσβάλει ένα αρχείο του συστήματος το οποίο είναι κρυφό ή ακόμα και να κρύψει ένα μολυσμένο αρχείο, το οποίο δεν θα εμφανίζεται πια στον κατάλογο του δίσκου.

Ορισμένοι ιοί κρύβουν ή τροποποιούν για δικούς τους σκοπούς το εσωτερικό ρολόι του υπολογιστή.Συχνά η πρώτη πράξη ενός ιού είναι να ελέγχουν την ημερομηνία και την ώρα του συστήματός για να δουν αν ταιριάζουν με την προγραμματισμένη ώρα ενεργοποίησης τους.

Πολλή από την εξάπλωση των ιών πάνω στα δίκτυα υπολογιστών ή στους οργανισμούς θα είχε αποφευχθεί αν γινόταν λιγότερη ανταλλαγή εκτελέσιμων προγραμμάτων.Για παράδειγμα, όταν ένας εκτυπωτής Laser μοιράζεται από περισσότερους του ενός χρήστες σ' ένα γραφείο, οι δισκέτες με τα περιεχόμενα της εκτύπωσης θα πρέπει να περιέχουν μόνο δεδομένα και όχι εκτελέσιμα προγράμματα.

Οι ιοί μπορεί να δρουν ταυτόχρονα με το λειτουργικό σύστημα ή τα προγράμματα που έχουν μολύνει, εκτελώντας τις κακές τους εργασίες είτε φανερά, είτε κρυφά.Υπάρχουν οι εισβολείς γενικής φύσεως προγραμματισμένοι να παίρνουν τον έλεγχο ενός προγράμματος όταν αυτό τρέχει, να κάνουν οποιανδήποτε αλλαγή είναι προγραμματισμένοι να κάνουν και κατόπιν να επιστρέφουν ξανά τον έλεγχο στα υπολογιστικά συστήματα.Οι ιοί αυτοί είτε κρύβονται μέσα στην εφαρμογή και καταλαμβάνουν μία ή περισσότερες από τις λειτουργίες της, ή πιο συχνά,

προσκολλώνται στην αρχή ή στο τέλος των αρχείων.Τα μολυσμένα προγράμματα γίνονται κατόπιν και τα ίδια ιοί διαδίδοντας την μόλυνση.

Ορισμένοι ιοί είτε παίρνουν τον έλεγχο του πίνακα κατανομής αρχείων ή καταστρέφουν την ικανότητά του να παρακολουθεί την φυσική τοποθέτηση των αρχείων στον δίσκο.Στην πραγματικότητα, ο ιός είτε ξανασχεδιάζει την εικόνα του δίσκου ή την καταστρέφει έτσι ώστε να μην μπορεί το λειτουργικό σύστημα να βρει τις θέσεις των αρχείων στο δίσκο.

Οι ιοί που στέλνουν αντίγραφα των εαυτών τους στην μνήμη RAM, την κύρια περιοχή εργασίας του υπολογιστή, μπορούν να μένουν εκεί κρυμμένοι περιμένοντας να εισβάλλουν σε ο,τιδήποτε ζητάει να εργαστεί στην μνήμη αυτή, όπως π.χ μία ''αμόλυντη'' δισκέτα που φορτώνεται σ' έναν οδηγό δίσκου.Κατά κάποιο τρόπο οι ιοί είναι σαν έντομα που κάθονται στο γρασίδι και περιμένουν να περάσει κάποιο ζώο για να του επιτεθούν.

Όταν ένας ιός προσβάλει ένα σύστημα, μπορεί να το εμποδίζει να λειτουργεί τόσο αποδοτικά όσο θα έπρεπε, ή μπορεί να προκαλέσει ακόμη πιο σοβαρά συμπτώματα ''ηλεκτρονικών ασθενειών'', ώστε να μην μπορεί πλέον να εκτελεί τις εργασίες που του αναθέτει.Ορισμένοι ιοί ''σκοτώνουν'' με τον πιο αποτελεσματικό τρόπο τους υπολογιστές, καταστρέφοντας όλα τα αρχεία που περιέχουν.Όμοια με ορισμένα βιολογικά μικρόβια, τα συμπτώματα μπορεί να κάνουν αρκετό καιρό για να εκδηλωθούν, δίνοντας έτσι αρκετό χρόνο στην μόλυνση να εδραιωθεί γερά και συνεπώς να είναι πιο δύσκολο να εξαλειφθεί.

Η καταστροφική δυνατότητα ενός ιού δεν είναι πάντα άμεση συνάρτηση της πολυπλοκότητας, του μεγέθους ή της ευφυΐας του.Ένας απλός ιός ο οποίος απλά τροποποιεί τον πίνακα κατανομής αρχείων, εκτελεί την εντολή Format στον σκληρό δίσκο ενός προσωπικού υπολογιστή ή ανακατεύει μερικά bytes στο αρχείο Desktop κι αν η πραγματική ζημιά είναι μικρή, οι συνέπειες μπορεί να είναι σοβαρές.Υπάρχουν ιοί οι οποίοι απλά αλλάζουν έναν χαρακτήρα δεδομένου εδώ κι εκεί με έναν υποχθόνιο και τυχαίο τρόπο, πράγμα που μπορεί να; κάνει πολύ καιρό να απομακρυνθεί.Τέτοιες καταστάσεις μπορεί να μην είναι πολύ σοβαρές αν οι αλλαγές φαίνονται να είναι μόνο μερικά ορθογραφικά λάθη σε κάποιο κείμενο.Οι συνέπειες θα ήταν πολύ πιο σοβαρές εάν τροποποιούνται αριθμοί σε λογιστικά φύλλα ή στην φόρμουλα παρασκευής ενός φαρμακευτικού προϊόντος.

Παρολλου αυτά οι μολύνσεις των υπολογιστών μπορούν να είναι πολύ περισσότερες κάτω από τον έλεγχο του χρήστη απ' ό,τι ορισμένες βιολογικές μολύνσεις που

προσβάλλουν τον ανθρώπινο οργανισμό.Δεν έχει βέβαια ακόμη βρεθεί μια άμεση τεχνολογική λύση, άλλα υπάρχουν όντως πολλά μέτρα άμυνας και καταστολής των ιών.Η μόλυνση από ιό δεν μπορεί ποτέ να είναι μοιραία για ένα σύστημα στο οποίο έχουν παρθεί επαρκείς προφυλάξεις.

4. Πως μεταδίδονται οι ιοί από το INTERNET.

Είναι αναμφισβήτητο γνωστό ότι το INTERNET στις μέρες μας έχει εξελιχθεί ραγδαία απ' ότι τα προηγούμενα χρόνια.Και αυτό επειδή αποτελεί ένα ταχύτατο μέσο επαφής, επικοινωνίας, ανταλλαγής πληροφοριών ιδεών και απόψεων άλλα και γνωριμίας, που δεν γνωρίζει σύνορα, φύλλο, ηλικία, τάξη και χώρα.Μια επικοινωνία, που συχνά ξεπερνά τα όρια – και την πλασματικότητα ίσως – του ίδιου του μέσου και γίνεται πραγματική καθημερινή διαπροσωπική επαφή.

Εντούτοις στην δεκαετία του '70 που εμφανίστηκε το INTERNET και τα δίκτυα μπορεί να μην ήταν ακόμη στο φόρτε τους, έτσι οι ιοί αυτοί μεταδίδονταν αλλά με μικρότερη ταχύτητα απ' ό,τι σήμερα, καθώς ο κυριότερος «ξενιστής» ήταν οι δισκέτες.Ίσως η απουσία του Διαδικτύου να μοιάζει με ευτυχή συγκυρία όμως παράλληλα περιείχε μια σημαντική αδυναμία.Οι εταιρείες που κατασκευάζουν τα προγράμματα αντιμετώπισης δεν μπορούσαν να ενημερώσουν άμεσα τους πελάτες τους με τις ενημερωμένες εκδόσεις των προϊόντων τους.Έτσι οι ιοί πολλαπλασιάζονται ανεξέλεγκτα και τα «εμβόλια» δεν έφταναν με ταχύτητα στους χρήστες.Έτσι οδηγούμαστε να πούμε ότι το INTERNET του 21ου αποτελεί τον κύριο αγωγό για τη μετάδοση των ιών και έγινε το μέσο για τη νίκη ενάντια στους δημιουργούς στην ίδια τους την έδρα.

Σήμερα υπάρχουν περίπου 18.000 διαφορετικοί ιοί οι οποίοι χωρίζονται σε δύο μεγάλες οικογένειες.Η πρώτη περιλαμβάνει τους ιούς που προσβάλλουν εκτελέσιμα προγράμματα και η δεύτερη τους μακροιούς που βασίζονται στα χαρακτηριστικά της Visual Basic και μολύνουν αρχεία δεδομένων όπως έγγραφα του Word ή φύλλα εργασίας του Excel.Στην οικογένεια των μακρο΄ίών ο τίτλος του ... πατριάρχη απονέμεται στον Concept.Εμφανίστηκε το1995 και προσέλαβε αρχεία του Word.Σε αντίθεση με ό,τι συνέβαινε στα προηγούμενα χρόνια, λόγω του INTERNET ο ιός έκανε αρκετές φορές το γύρο του κόσμου πριν να δημιουργηθούν τα σχετικά αντιοβιοτικά.Στην κατηγορία των μακρο΄ίών με ιδιότητες σκουληκιού περιλαμβάνεται

και ο διάσημος Melissa, ο οποίος έστελνε τον εαυτό του στις 50 πρώτες διευθύνσεις που διατηρούσε ο χρήστης – θύμα στο βιβλίο διευθύνσεων του προγράμματος Outlook.Μαζί με τον εαυτό του ο Melissa, έστελνε και ένα έγγραφο του Word με πορνογραφικές διευθύνσεις, ίσως γι'αυτό το λόγο να είχε τόση «επιτυχία».Ο «I Love you» δεν ήταν μακρύϊός, δεν μόλυνε αρχεία εγγράφων ή λογιστικά φύλλα, ωστόσο άφηνε τα ίχνη του στο μητρώο των Windows.Από τεχνικής άποψης «I Love you» είναι ένα μικρό πρόγραμμα γραμμένο σε Visual Basic.

Η περίπτωση του «I Love you» έφερε στην επιφάνεια μια σειρά από ενδιαφέροντα στοιχεία.Από το ρυθμό διάδοσης του ιού διαπιστώνεται κατ' αρχάς μια ευρεία χρήση των προγραμμάτων Outlook και Outlook Express της Microsoft.Οι παραλήπτες του παγιδευμένου μηνύματος έδειξαν ανυποψίαστοι σε βαθμό παρεξηγήσεως, αν και το συνημμένο αρχείο είχε την επωνυμία «iLove.txt.vbs» και όχι «iLove you.txt.».Η διαφορά μπορεί να είναι μόνο 3 γράμματα, αυτά όμως έχουν εξαιρετικά μεγάλη σημασία, αφού ορίζουν ποιο πρόγραμμα θα χρησιμοποιηθεί, από τα, Windows για την επεξεργασία του αρχείου.Έτσι, ένα αρχείο με επωνυμία «iLove you.txt» θα ανοιχτεί από το Notepad (ή Σήμειωταριο στην ελληνική έκδοση των Windows)και δεν θα προκαλέσει κανένα απολύτως πρόβλημα.Αντίθετα η προέκταση «.vbs» ορίζει ότι το συγκεκριμένο αρχείο είναι ένα τμήμα κώδικα της Visual Basic.Για το περιβάλλον των Windows στην ουσία το «.vbs» είναι πρόγραμμα, που με διπλό κλικ ενεργοποιείται.Μια Τρίτη παρατήρηση έχει να κάνει με το ότι οι υπεύθυνοι διαχείρισης των μεγάλων εγκαταστάσεων σε επιχειρήσεις και οργανισμούς πιάστηκαν κυριολεκτικά στον υπνό.Ο ιός «I Love you» έδειξε μια ιδιαίτερη προτίμηση σε αρχεία εικόνας τύπου .jpg και σε αρχεία mpeg (είτε πρόκειται για εικόνα είτε για ήχο).Προκάλεσε, όπως ήταν αναμενόμενο, πολλά προβλήματα σε επιχειρήσεις από κλάδους όπως η διαφήμιση, οι εκδόσεις και η επαγγελματική φωτογραφία.Επίσης με τις παρεμβάσεις του σε αρχεία όπως τα mp3 μάλλον ... πάγωσε των όσων χρησιμοποιούν τον υπολογιστή τους και για να κατεβάζουν τραγούδια από το δίκτυο.Αν και τα πράγματα θα ήταν διαφορετικά την εγκατάσταση ενός «φίλτρου» που θα απαγόρευε την αποστολή μηνύματος με το επικίνδυνο αρχείο – πρόγραμμα, ελάχιστοι προχωρούσαν στη λήψη αυτού του προληπτικού μέτρου.

Μια αναγκαία διευκρίνιση εδώ: Επί της ουσίας ο «I Love you» δεν είναι ιός με την κυριολεκτική ερμηνεία του όρου (που λεει ότι «ιός είναι ένα πρόγραμμα που έχει δημιουργηθεί για να αναπαράγει τον εαυτό του»).Όλες οι εταιρείες που ασχολούνται με την κατασκευή anti – virus προγραμμάτων τον χαρακτηρίζουν ως «σκουλήκι» (worm)

διότι σε αντίθεση με τους ιούς δεν χρειάζεται έναν ξενιστή αλλά μεταδίδεται μέσω δικτύου.Η ενεργοποίηση του γίνεται μόνο με την εκτέλεση του και όχι με την εκτέλεση άλλου προγράμματος στο οποίο έχει προσκολληθεί.Εκτός βέβαια αν θεώρησε πως το δίκτυο είναι ο ξενιστής, άλλα αυτό είναι τραβηγμένο.

Άλλος ένας τελευταίος ιός που έκανε πρόσφατη εμφάνιση στο Διαδίκτυο είναι εκείνος που έχει ως δημιουργούς, τους Έλληνες και Τούρκους χάκερς που δίνουν καθημερινά τη δική τους μάχη στο Διαδίκτυο.Η Ελλάδα και η Τουρκία διασταυρώνουν καθημερινά τα ξίφη τους στο Διαδίκτυο.Όσο κι αν φαίνεται απίστευτο ένας ακήρυκτος μυστικός πόλεμος ανάμεσα στην Ελλάδα και την Τουρκία βρίσκεται σε εξέλιξη σε καθημερινή βάση.

Μόνο που τα παραδοσιακά όπλα και οι μέχρι σήμερα γνωστές μέθοδοι της κατασκοπίας έχουν αντικατασταθεί από τις εισβολές των χάκερς.Και οι αντίπαλοι, αντί για τόξα, οβίδες και βόμβες, ανταλλάσσουν ηλεκτρονικούς «ιούς»!

Έχουν γνώση, όμως, οι φύλακες στο ελληνικό Πεντάγωνο.Αντί των ηρωικών ταγμάτων των ευζώνων, οι σύγχρονοι ηλεκτρονικοί εύζωνοι του Συστήματος Διοικήσεως Ελέγχου Πληροφοριών (ΣΔΕΠ) έχουν μέχρι στιγμής αποκρούσει με επιτυχία κάθε προσπάθεια εισβολής.Ως πότε, όμως; Αυτό είναι ένα από τα βασικά ερωτήματα και προβληματίζει τους επιτελείς.

«Σε σχέση με την Τουρκία, είμαστε μπροστά», δήλωσε πρόσφατα στο περιοδικό «TOMORROW» ο ταξίαρχος Κωνσταντίνος Γεροκωστόπουλος, διευθυντής του ΣΔΕΠ στο ΓΕΣ.«Εκείνο όμως που μας βασανίζει είναι για πόσο καιρό θα καταφέρουμε να κρατήσουμε την πρωτοπορία.Γιατί την Τουρκία την 'πονάει' πολύ αυτό, αφού το ΣΔΕΠ θεωρείται πλέον οπλικό σύστημα», συνέχισε.Πόλεμος των «ποντικιών» των ηλεκτρονικών υπολογιστών στα κατάλληλα χέρια μπορούν να κάνουν θαύματα και να τελειώσουν έναν πόλεμο πριν ακόμα αρχίσει.Πόλεμος «ταύρων», θα λέγαμε εμείς, αφού οι χάκερ, παθιασμένοι με τους υπολογιστές, ως ταύροι σε υαλοπωλείο μπροστά στις οθόνες τους, βάζουν στοίχημα με τους εαυτούς τους να σπάσουν τους κωδικούς και να μπουν στα απόρρητα αρχεία των Επιτελείων και όχι μόνο.Μια από τις κυριότερες απειλές για την ασφάλεια της χώρας τους θεωρούν οι Αμερικανοί μία οργανωμένη επίθεση στον κυβερνοχώρο τους και υποχρεώθηκαν μόνο το 1996 να αλλάξουν περισσότερους από 35.000 κωδικούς, αφού το αμερικανικό Πεντάγωνο έχει πέσει πολλές φορές θύμα μεμονωμένων, ευτυχώς γι' αυτούς, παραβιάσεων.Το NATO, από την πλευρά του, έχει ήδη αρχίσει από διετίας να πραγματοποιεί ασκήσεις αντιμετώπισης τέτοιων περιστατικών.Συμμετεχεί και η Ελλάδα, αφού τόσο η υποδομή

του ΣΔΕΠ όσο και το προσωπικό που το επανδρώνει, έχουν όλα τα στοιχεία που χρειάζεται για μια τέτοια συμμετοχή.

Από την πλευρά της, η Τουρκία ετοιμάζεται να ξοδέψει δισεκατομμύρια, προκειμένου να εκσυγχρονίσει την πληροροφοριακή υποδομή της.Η δυνατότητα να συνεργάζεται καλύτερα με τα Νατοϊκά υπερδίκτυα είναι η επίσημη δικαιολογία της.Και η κρυφή ελπίδα της ότι κάποτε θα μπορέσει να μπει επιτέλους στα άδυτα του ελληνικού Πεντάγωνου!

Έτσι λοιπόν το Διαδίκτυο σήμερα αποτελεί πλέον την μοναδική πηγή μετάδοσης ιών από τους χάκερς και κρίνεται περισσότερο επικίνδυνο απ' ότι οι δισκέτες διότι υπάρχουν πολλοί χρήστες που έχουν πρόσβαση σήμερα στο Διαδίκτυο λόγου της χρησιμότητας των υπηρεσιών της και με το μειονέκτημα να μην γίνεται εύκολα αναγνωρίσιμη η ταυτότητα τους ώστε να καθίσταται δύσκολη η σύλληψη αυτών των επιτηδείων που μολύνουν τα υπολογιστικά συστήματα μ' ένα είδος «ηλεκτρονικών σκουπιδιών».Μια αξιοσημείωτη από τις πολλές που κάνει η IBM για να εξαλείψει αυτούς τους ιούς που αξίζει να αναφερθεί είναι εκείνη που στοχεύει στη δημιουργία ενός περιβάλλοντος «εικονικού Internet» που ονομάζεται «Internet σ' ένα κουτί».Σκοπός, η ανάλυση της γενιάς ιών που μεταδίδονται μέσω Internet.

Σε αντίθεση με τις προηγούμενες γενιές, οι ιοί του Internet, αναζητούν καταλόγους διευθύνσεων ηλεκτρονικού ταχυδρομείου και αποστέλλονται χωρίς την παρέμβαση του χρήστη σε όλους όσοι ατυχώς βρέθηκαν καταχωρισμένοι στο μολυσμένο υπολογιστή.Η ιδιότητα αυτή των ιών του Internet, να αυτοπολλαπλασιάζονται, καθιστά το ανοσοποιητικό της Symantec.

Το «Internet σ' ένα κουτί» αποτελεί προέκταση του ανοσοποιητικού συστήματος.Ωστόσο, οι ιοί του Internet παρουσιάζουν πολύ μεγαλύτερες δυσκολίες στην ανάλυση, διότι απαιτείται η παρακολούθηση της εξάπλωσής τους σε πολλούς υπολογιστές.

Προγράμματα σαν το ανοσοποιητικό σύστημα μπορεί να εξαλείφουν τους κινδύνους για ολοσχερή καταστροφή από μια επίθεση ιών, ωστόσο μπορεί να αποδειχθούν ανίσχυρα σε περιπτώσεις όπως οι πρόσφατοι πολυμορφικοί μακροιοί, που είχαν την ιδιότητα να μεταλλάσσονται καθώς εξαπλώνονταν.Η ανθρώπινη ευφυΐα και δεξιότητα θα είναι πάντα απαραίτητη σε τέτοιες περιπτώσεις για να δίνει τη λύση.

5. Ιοί και νόμος.

Στο κεφάλαιο αυτό αναπτύσσεται το θέμα των ιών των υπολογιστών, από την οπτική γωνία των νομικών προβλημάτων που παρουσιάζονται στην Γερμανία που είναι από τις λίγες χώρες που εφαρμόζεται ο νόμος κατά τους εισβολείς των ιών, ενώ κάτι τέτοιο δεν ισχύει και στη Ελλάδα.Ένα από τα συμπεράσματα της δημοσκόπησης σχετικά με τους ιούς ήταν ότι σύμφωνα με την γνώμη πολλών, δεν επιβάλλονται αρκετά αυστηρές ποινές σε όσους προωθούν και κατασκευάζουν ιούς.Στο εδάφιο αυτό εξηγείται σε συντομία, το γιατί αυτή η άποψη δεν είναι σωστή.Το κεντρικό πρόβλημα είναι να βρεθεί ο υπαίτιος ή οι υπαίτιοι.Στο πρόβλημα αυτό προστίθεται και το ότι πρέπει να γίνει μια μήνυση, για να καταδιωχθούν τα άτομα αυτά.Ο εισαγγελέας δεν επεμβαίνει αυτεπάγγελτα, όπως γίνεται για παράδειγμα στην περίπτωση των ναρκωτικών, αλλά πρέπει να έχει προηγηθεί μια μήνυση.

Καταρχήν, και σύμφωνα με το γερμανικό ποινικό κώδικα τιμωρείται όποιος παράνομα διαγράφει, εξαφανίζει αχρηστεύει ή τροποποιεί δεδομένα ή όποιος παρενοχλεί μια ιδιωτική επιχείρηση ή μια δημόσια υπηρεσία καταστρέφοντας, αχρηστεύοντας, εξαφανίζοντας ή τροποποιώντας ένα σημαντικό γι' αυτούς φορέα δεδομένων ή μια εγκατάσταση επεξεργασίας δεδομένων.

Όποιος διαπράττει κάτι από τα παραπάνω, τιμωρείται με φυλάκιση μέχρι πέντε έτη ή με καταβολή προστίμου.Αξίζει να σημειωθεί ότι τιμωρείται ακόμη και η απόπειρα τέλεσης μια από τις παραπάνω πράξεις και με τις ίδιες ποινές.Ούτε οι συνεργοί μένουν ατιμώρητοι.Όποιος παροτρύνει, βοηθά ή συνεργάζεται σε μια μόλυνση από ιό, τιμωρείται ακριβώς όπως και ο κύριος ένοχος.

Αυτή είναι η σκοπιά του ποινικού δικαίου.Από την άποψη του αστικού δικαίου, ο αστικός κώδικας υποχρεώνει τον ένοχο να πληρώσει αποζημίωση για τις βλάβες, που προξενήθηκαν από τον ιό.Είναι αναγκασμένος να αναλάβει όλα τα έξοδα, τα οποία πρέπει να καταβάλλει ο χρήστης, για να επαναφέρει το σύστημά του στην κατάσταση που βρισκόταν πριν τη μόλυνση.Όποιος ασχολείται με το θέμα αυτό, γνωρίζει ότι τα έξοδα που πρέπει να καταβληθούν για την επανόρθωση τέτοιων ζημιών είναι τεράστια.Αυτός που υπέστη τη ζημιά έχει την επιλογή να ζητήσει αποζημίωση από ένα μόνο άτομο ή από όλους τους συνενόχους.

Ο προγραμματισμός ιών, όμως, δεν τιμωρείται.Ο προγραμματιστής τιμωρείται μόνο από τη στιγμή που μόνο από τη στιγμή που ο ιός του θα εντοπιστεί σε ξένο σύστημα ακόμα και αν ως εκείνη τη στιγμή δεν έχει δημιουργηθεί καμιά ζημιά

Γενικά, είναι καλό να μη δίνει κανείς σε άλλους χρήστες μεταγλωττισμένους ιούς ή τους πηγαίους κώδικές των ιών.Κι αυτό, επειδή σε μια τέτοια περίπτωση, ο νομοθέτης δέχεται ότι ο παραλήπτης μπορεί να μην είναι επαρκώς πληροφορημένος για την καταστροφική δύναμη του υλικού που του παραδίδεται.Ακόμη και αν ο παραλήπτης ενός μεταγλωττισμένου ιού μολύνει το ίδιο του το σύστημα, μπορεί, κάτω από ορισμένες προϋποθέσεις να μηνύσει αυτόν που του έδωσε αυτόν τον ιό.

Πέρα όμως από τη νομική πλευρά, πρέπει να αναφερθεί και το ηθικό μέρος.Η πείρα του παρελθόντος έδειξε ότι είναι καλύτερο να μη δημοσιεύονται πηγαίοι κώδικες ιών.Πολλοί ιοί που κυκλοφορούν,- ανάμεσά τους και ιδιαίτερα επικίνδυνοι – είναι μάρτυρες του γεγονότος ότι υπάρχουν αρκετοί ανεύθυνοι και μάλιστα ερασιτέχνες «προγραμματιστές», που πειραματίζονται και κυκλοφορούν κάποιο μεταλλαγμένο κώδικα ιού, που έχει κοινοποιηθεί.Γενικά η ευθύνη για το πρόβλημα των ιών διακρίνεται με βάση την ιδιότητα του κάθε επιτήδειου που επιδιώκει να μόλυνσει τα υπολογιστικά συστήματα.Έτσι έχουμε την ευθύνη των εμπόρων προγραμμάτων, την ευθύνη συντονιστών ηλεκτρονικών γραμματοθυρίδων, την ευθύνη του παραγωγού λογισμικού και την ευθύνη εμπόρων.

6.1 Η Ευθύνη των Εμπόρων Προγραμμάτων Public Domain.

Ο νομοθέτης θεωρεί ότι ένας έμπορος δε θα βλάψει συνειδητά τον εαυτό του, πουλώντας εν γνώσει του μολυσμένα προγράμματα.Συνεπώς, οι έμποροι δεν τιμωρούνται, με την προϋπόθεση ότι δε διέσπειραν κάποιον ιό εν γνώσει τους.

Η κατάσταση είναι διαφορετική σε ό,τι αφορά απαιτήσεις αποζημίωσης από τον έμπορο προγραμμάτων Public Domain.Αν ο έμπορος μπορούσε να διαπιστώσει χωρίς μεγάλο κόπο, π.χ εκτελώντας μια φορά το πρόγραμμα, ότι το πρόγραμμα ήταν μολυσμένο, μπορεί κάλλιστα να του υποβληθεί μήνυση και να καταδικαστεί στην πληρωμή αποζημίωσης.Όλα αυτά τα νομικά θέματα αφορούν τη νομική κατάσταση στη Γερμανία.

6.2 Ευθύνη Συντονιστών Ηλεκτρονικών Γραμματοθυρίδων.

Κατά κανόνα, ούτε οι συντονιστές γραμματοθυρίδων (Mailbox System Operators) διαπράττουν κάτι εκ προμελέτης και γι'αυτό δεν τιμωρούνται.Σε ό,τι αφορά τις

απαιτήσεις για τους εμπόρους των Public Domain.Σε πολλές ηλεκτρονικές γραμματοθυρίδες παρέχεται η δυνατότητα απόθεσης προγραμμάτων, για να μπορούν ελεύθερα να χρησιμοποιούνται από άλλούς συνδρομητές της ηλεκτρονικής γραμματοθυρίδας.Ο συντονιστής του συστήματος δεν έχει τη δυνατότητα να δοκιμάζει τα προγράμματα αυτά.Συνεπώς είναι πολύ πιο δύσκολο να τεκμηριώσει κανείς ένα, αίτημα αποζημίωσης από το συντονιστή της ηλεκτρονικής γραμματοθυρίδας.

6.3 Ευθύνη του Παραγωγού Λογισμικού.

Καταρχήν θεωρείται δεδομένο ότι ο παραγωγός λογισμικού γνωρίζει άριστα τα προγράμματα που δημιουργεί, και συνεπώς μπορεί και να αποφύγει τη μόλυνσή τους από ιούς.Μπορεί πάντως να συμβεί, ένας παραγωγός λογισμικού να διαθέσει στην αγορά ένα μολυσμένο πρόγραμμα.Κάτι τέτοιο μπορεί να συμβεί εύκολα σε περίπτωση δολιοφθοράς.Το αποτέλεσμα είναι ότι, ένας παραγωγός λογισμικού μπορεί να τιμωρηθεί ευκολότερα από τους εμπόρους προγραμμάτων Public Domain και τους συντονιστές ηλεκτρονικών γραμματοθυρίδων.Αυτό που έχει τελικά σημασία είναι βέβαια το ύψος της αποζημίωσης.

6.4 Ευθύνη Εμπόρων.

Οι έμποροι είναι μια ενδιάμεση ομάδα μεταξύ των εμπόρων PD και των παραγωγών λογισμικού.Η προσφορά τους είναι αριθμητικά μικρότερη απ' αυτήν των εμπόρων PD, αλλά μεγαλύτερη από του παραγωγού.Και οι έμποροι πάντως φέρουν ευθύνη για ζημιές, αν αποδειχτεί ότι δεν ανταποκρίθηκαν στην υποχρέωση τους, να προφυλάσσουν τους πελάτες τους.

Είναι αξιοσημείωτο να αναφερθούν κάποιες διαφορές που υπάρχουν σχετικά με την νομοθεσία των ιών στο διαδίκτυο στις διάφορες χώρες του κόσμου.Κάθε κυβερνητικό στέλεχος που αξίζει τα λεφτά του φαίνεται να έχει δικό του σχέδιο για τη νομοθεσία σχετικά με το διαδίκτυο.

Η Νιγηρία θέλει ένα «Σχέδιο Μάρσαλ», σύμφωνα με το οποίο οι φόροι των πλουσιότερων χωρών θα «καλωδίωναν» την Αφρική.Η Ολλανδία θέλει να περιορίσει τον «εμπορικό χαρακτήρα» του δικτύου και η Σιγκαπούρη ελπίζει να πείσει τους πάντες να ακολουθήσουν τη γραμμή της και να περιορίσουν τα ερωτικά Site μια προσπάθεια των κυβερνήσεων να βρουν κοινό έδαφος, θα συναγωνιστούν για τον καλύτερο δυνατό τρόπο νομοθεσία σε μια συνάντηση των Ηνωμένων Εθνών στο Παρίσι.Ένα βασικό ζήτημα σχετικά με «Το Διαδίκτυο και τις νέες υπηρεσίες» σε ένα διήμερο κορυφαίων νομοθετών που φιλοξένησε ο Εκπαιδευτικός Επιστημονικός και Πολιτιστικός Οργανισμός των Ηνωμένων Εθνών είναι το κατά πόσον η κυβερνητική πίεση στη βιομηχανία υπολογιστών είναι επαρκής ή μήπως χρειάζεται πιο επίσημη νομοθεσία.

Τα αισθήματα περιπλέκονται, σύμφωνα με περισσότερες από 60 χώρες που απάντησαν σε προωθημένα ερωτηματολόγια που προώθησε η γαλλική κυβέρνηση.Το Ανώτατο Οπτικοακουστικό Συμβούλιο της Γαλλίας συγκέντρωσε τις απαντήσεις και ετοίμασε μία περίληψη, την οποία διέθεσε για να συγκεντρώσει παρουσίες.Εντουτοίς υπάρχουν κάποιες περιοχές συμφωνίας.Σχεδόν όλοι φαίνεται να πιστεύουν – σύμφωνα με την έκτασης της τριάντα σελίδων έκθεση του Συμβουλίου – ότι η «μεταφορά» νομοθεσίας που είχε δημιουργηθεί για την τηλεόραση και το ραδιόφωνο είναι το καλύτερο «έδαφος» για οποιανδήποτε προσπάθεια να υιοθετηθεί ένα νομοθετικό πλέγμα σχετικά με τα Sites.

Κάποια σημεία που αξίζει να επισημανθούν είναι τα έξεις:

1. **Η Μάλτα** θέλει να συγκεντρώσει απεσταλμένους για να δημιουργήσει ένα «προσχέδιο συνεδρίου» προκειμένου να νομοθετήσει τις εκπομπές μέσω Διαδικτύου.Το έγγραφο θα προωθούνταν εν συνεχεία στην UNESCO ώστε να αποκρυσταλλωθεί σε μια επίσημη διεθνή επιστήμη.

2. Μπορεί να μην αποτελεί ξεχωριστή χώρα, αλλά **το Κεμπέκ** αξίζει να αναφερθεί ιδιαίτερα.Θέλει περισσότερη «προώθηση πολιτιστικού περιεχομένου» στο διαδίκτυο.

3. **Το Ολλανδικό Comissarjaat voor de Media** υποστηρίζει ότι «είναι εξίσου σημαντικό η πληροφόρηση να μην υπαγορεύεται από επιχειρηματικές επιρροές».Η Ολλανδία υποστηρίζει ότι οι καταναλωτές θα έπρεπε να είναι σε θέση να εμπιστεύονται τις πληροφορίες που διαβάζουν, ενώ «κάποιες βασικές αρχές των εκπομπών πρέπει να μεταφερθούν στο διαδίκτυο, όπως για παράδειγμα ο διακριτός χαρακτήρας των κρατικών οργανισμών μετάδοσης εκπομπών» .

4. **Η Γκαμπόν** φαίνεται να θέλει να περιορίσει την ανωνυμία, προβάλλοντας «την αναγκαιότητα να κατονομάζεται κάθε υπεύθυνο πρόσωπο» αναφορικά με συνδέσεις πολυμέσων που διατίθεται μέσω του Διαδικτύου.

Βλέπουμε λοιπόν ότι η νομοθεσία σχετικά με τους ιούς δεν είναι ίδια για όλες τις χώρες.Αλλά εξαρτάται από το μέγεθος των συνεπειών που θα υποστεί η κάθε χώρα και από το πόσο αναπτυγμένες είναι οικονομικάΓιατί ακριβώς αυτές έχουν ένα μεγάλο αριθμό αξιοσημείωτων υπολογιστικών συστημάτων που θεωρούνται ιδιαίτερα ευαίσθητες από τις εισβολές των «Hackers» και αποτελούν τον πιο σύνηθες στόχο τους.Και αυτό επειδή υπάρχουν πολλά οικονομικά κίνητρα για τους «Hackers» να ΄΄χτυπήσουν΄΄ τα υπολογιστικά συστήματα των αναπτυσσόμενων παρά των μη αναπτυσσόμενων χώρων.

ΚΕΦΑΛΑΙΟ 3

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΥ ΣΥΝΔΕΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΠΟ ΙΟΥΣ ΙΟΥΣ

1. Πρόληψη

Υπάρχουν πολλές διαφορετικές πηγές που μπορούν να ελαχιστοποιήσουν τον ρίσκο μόλυνσης των ιών στα υπολογιστικά συστήματα.Και αυτό ακριβώς επειδή υπάρχουν πολλοί διαφορετικοί ιοί.Ο κάθε ιός πρέπει να αντιμετωπίζεται ανάλογα με τον τύπο του.

Γενικά η προστασία των υπολογιστικών συστημάτων είναι ένα θέμα που παραμένει πάντα λεπτό και ευαίσθητο.Αυτό βέβαια οφείλεται στις σημαντικές ζημιές που προκαλεί ένας εισβολέας.Δεν είναι λίγες φορές που εξαιτίας κάποιας απροσεξίας προγραμματιστών κατά τη δημιουργία μιας εφαρμογής ή εξαιτίας κάποιου εισβολέα προκλήθηκαν ανεπανόρθωτα ζημιές τεράστιου κόστους.Ωστόσο όμως με μερικές γνώσεις και με την βοήθεια ορισμένων εφαρμογών μπορεί ο κάθε χρήστης και η οποιανδήποτε συνεταιριστική οργάνωση να εμποδίσουν κάποιον να εισβάλλει στον υπολογιστή τους και να δουν κάτι που δεν θα έπρεπε.Υπάρχουν τέσσερις βασικοί τρόποι για να ελαχιστοποιηθεί το ρίσκο μόλυνσης των συστημάτων από του ιούς:

1.1 Έλεγχος με Ανιχνευτή Ιών.

Μια σε μεγάλο βαθμό ασφαλής και σχετικά απλή μέθοδος, είναι να ελέγχει κανείς με ένα ενημερωμένο πρόγραμμα ανίχνευσης ιών την κάθε, μα πραγματικά την κάθε,

δισκέτα και το κάθε πρόγραμμα, που εισάγει μέσω μόντεμ στο σύστημά του, πριν την πρώτη κλήση τους ή την εγκατάσταση τους στο σύστημα.Αν θέλει κάποιος να είναι απόλυτος ασφαλής, θα πρέπει να επαναλάβει τη διαδικασία ακόμη μια φορά μετά την εγκατάσταση, επειδή υπάρχουν προγράμματα, που διαμορφώνονται μετά την εγκατάσταση από τη σύνθεση διαφόρων ενοτήτων και μπορεί καμιά φορά να μην αναγνωριστούν οι ιοί, που περιέχονται στις ενότητες.Επιπλέον κάποιος μπορεί να εκτελέσει και να αρχειοθετήσει διαγνωστικούς ελέγχους με το πρόγραμμα Validate.Με τον τρόπο αυτό θα έχει αργότερα στη διάθεση του δεδομένα για σύγκριση, που θα τον διευκολύνουν – ως ένα σημείο τουλάχιστον – σε ορισμένους έλεγχους.

1.2 Προστασία με εμβολιασμό.

Συχνά συνιστάται επίσης και ο εμβολιασμός αρχείων.Η μέθοδος αυτή αξιοποιεί το γεγονός, ότι οι ιοί προσβάλλουν ένα αρχείο, κατά κανόνα μόνο μια φορά.Για να αναγνωρίζεται όμως ο ιός, αν έχει ήδη προσβάλει κάποιο αρχείο, τοποθετεί σε ένα ειδικό μέρος του αρχείου, σαν χαρακτηριστικό σημάδι του ιού, μια ακολουθία από Byte.Αν γνωρίζει κανείς για ποια ακολουθία χαρακτήρων πρόκειται, και σε ποιο μέρος τοποθετείται, μπορεί να εισαγάγει τεχνητά αυτήν την ακολουθία χαρακτήρων και να ξεγελάσει έτσι τον ιό, ότι έχει ήδη προσβάλλει το αρχείόΕνα τέτοιο αρχείο δε θα ξαναπροσβληθεί από τον ιό αυτόν.Η μέθοδος αυτή όμως, έχει ένα μεγάλο μειονέκτημα.Οι ιοί της ίδιας οικογένειας τοποθετούν τις περισσότερες φορές το χαρακτηριστικό τους στο ίδιο σημείο, αλλά χρησιμοποιούν κάθε φορά διαφορετική ακολουθία κώδικα.Για το λόγο αυτό δεν είναι δυνατό να γίνει ταυτόχρονα εμβολιασμός εναντίον πολλών ιών της ίδιας οικογενείας.Γι' αυτό και ο εμβολιασμός δεν προσφέρει αρκετά ασφαλή προστασία.

1.3 Μετονομασία Αρχείων.

Μια άλλη δυνατότητα, την οποία χρησιμοποιούν μερικοί χρήστες, είναι μετονομασία αρχείων.Με αυτή τη μέθοδο μπορούν να αλλάξουν για παράδειγμα, όλες τις προεκτάσεις COM σε ΕΝΑ και όλες τις προεκτάσεις ΕΧΕ σε ΔΥΟ.Για να εκτελεστεί

Olivier Wager: «VIRUSCAN», Εντοπίστε και Εκμηδενίστε τους Ιούς των υπολογιστών, Αθήνα 1991, σελ. 69 - 72

αυτό το ομαδικό αρχείο, θα πρέπει να δίνεται σαν παράμετρο, το όνομα του προγράμματος που επιθυμεί κάποιος χρήστης να εκτελέσει, χωρίς την προέκταση του.Η αρχή της διαδικασίας αυτής βασίζεται στο γεγονός, ότι υπάρχουν ακόμη πολλοί ιοί, που ελέγχουν μόνο την προέκταση των αρχείων κατά την αναζήτηση προσβεβλημένων αρχείων.Τέτοιοι ιοί εντοπίζουν κανένα αρχείο COM και EXE, και συνεπώς, και κανένα αρχείο – ξενιστή.

Παρ' όλα αυτά πρέπει να είναι κανείς προσεκτικός.Πρώτο, δεν πέφτουν πια όλοι οι ιοί σε αυτήν την παγίδα, και δεύτερο, δεν μπορεί κάποιος να μετονομάσει τα αρχεία του λειτουργικού συστήματος, στην περίπτωση που κάποια προγράμματα χρησιμοποιούν τα αρχεία αυτά.Αυτό ισχύει κυρίως για το αρχείο COMMAND.COM.Φυσικά, ένα ακόμα μειονέκτημα είναι ότι, για να εγκαταστήθει μια τέτοια διαδικασία, απαιτείται ανάλογα με το σκληρό δίσκο, και μια όχι αμελητέα προετοιμασία.

Στις μέρες μας πια, η κάθε εταιρία συστημάτων καθώς και ο κάθε έμπορος προγραμμάτων Public Domain ή Shareware, ελέγχει για την ύπαρξη ιών στις δισκέτες του, πριν τις διανείμει στην αγορά πολλοί φτάνουν στο σημείο να προμηθεύουν τα πρωτότυπα προγράμματα σε ειδικές δισκέτες με προστασία εγγραφής – ο κίνδυνος όμως από τους ιούς εξακολουθεί να μην εξορκιστεί.Πιστευετε ότι είναι θέμα χρόνου μέχρις ότου οι εταιρείες αυτές να δηλώνουν ότι το λογισμικό τους έχει ελεγχθεί και βρεθεί ελεύθερο από κάποιους συγκεκριμένους ιούς.Η βασικότερη, όμως, προϋπόθεση, για την εξάπλωση των ιών, θα εξακολουθεί να είναι η απροσεξία και η άγνοια των χρηστών σε θέματα ιών.Για να ανακοπεί λοιπόν, η εξάπλωση των ιών, θα πρέπει να ενημερωθούν σωστά και **αναλυτικά**, όλοι όσοι χρησιμοποιούν υπολογιστές.

1.4 Οι Δέκα Χρυσοί Κανόνες για την Ασφαλή Χρήση των Υπολογιστών.

1. Ποτέ μην φορτώνετε άγνωστες δισκέτες στο σύστημά σας, ούτε να το επιτρέπετε σε άλλους, εκτός κι αν είστε εκατό τοις εκατό σίγουροι ότι δεν έχουν ιό.

2. Μην χρησιμοποιείτε τις δισκέτες σας σε αλλά συστήματα, χωρίς να είναι προστατευμένες από εγγραφή με το μικρό αυτοκόλλητο.

3. Μην δέχεστε προγράμματα από άλλους, εκτός κι αν είστε απόλυτα σίγουροι ότι δεν έχουν ιό.Προσπαθήστε να κρατάτε όλα σας τα προγράμματα σε ξεχωριστές δισκέτες απ' ότι τα δεδομένα.

4. Να είστε πολύ προσεκτικοί αν νοικιάζεται κάποιον υπολογιστή ή χρησιμοποιείται κάποιον από ένα κέντρο ηλεκτρονικών επιτραπέζιων εκδόσεων (desktop publishing) που δεν έχει τόσο αυστηρές διαδικασίες ελέγχου.

5. Εάν πρέπει να ανταλλάξετε δισκέτες ή να χρησιμοποιήσετε προγράμματα ή δεδομένα σε συστήματα που δεν ξέρετε, υιοθετήστε μία αποτελεσματική διαδικασία απομόνωσης.Για παράδειγμα, μην τρέχετε ποτέ δισκέτες που είναι πιθανό να είναι μολυσμένες στο κεντρικό σας σύστημα, ειδικά αν έχει σκληρό δίσκο.Ελέγξτε τις **πρώτα** σε ένα όχι τόσο ζωτικό, απομονωμένο σύστημα, π.χ ένα φορητό υπολογιστή που δεν έχει σκληρό δίσκο, ούτε δισκέτα στον δεύτερο οδηγό.Εάν τρέχετε τα προγράμματά σας ή χρησιμοποιείται τα δεδομένα σας σε συστήματα που σας είναι άγνωστα, κάντε πρώτα αντίγραφα ασφαλείας τους τα οποία θα χρησιμοποιήσετε στο άλλο σύστημα και θα τα καταστρέψει αμέσως μετά την ολοκλήρωση της εργασίας.

6. Μην φορτώνεται προγράμματα από δίκτυα τα οποία δεν έχουν σωστή διαχείριση ούτε σωστές διαδικασίες πρόληψης των ιών.Εάν είναι αναγκαίο, ρωτήστε τον χρήστη του αλλού συστήματος για τις διαδικασίες πρόληψης ιών που χρησιμοποιεί.

7. Μην επιτρέπεται κανένα άλλον να χρησιμοποιήσει τον υπολογιστή σας χωρίς την δική σας επίβλεψη, ειδικά όταν πρόκειται να φορτώσει δικές του δισκέτες.Να θυμάστε ότι η μόλυνση μπορεί να μεταδοθεί από τα χέρια του καλύτερου σας φίλου!

8. Ψάξτε για ανεξήγητες αλλαγές στον τρόπο λειτουργίας του υπολογιστή σας – για παράδειγμα, η χωρίς λόγο δραστηριότητα των οδηγών δίσκων.

9. Χρησιμοποιήστε πάντα τα μικρά αυτοκόλλητα προστασίας από εγγραφή και δημιουργήστε ετικέτες όπου θα καταγράφετε το μέγεθος των αρχείων σας.Να ελέγχετε τα μεγέθη των δίσκων τακτικά για ανεξήγητες αλλαγές που θα μπορούσαν να σημαίνουν αναπαραγωγή ιών.

10. Για να προστατευτείτε ενάντια στην απώλεια δεδομένων, **κρατήστε** αντίγραφα ασφαλείας των δεδομένων σας σε δισκέτες που δεν περιέχουν καθόλου κώδικα προγραμμάτων .Καθαρίστε οποιανδήποτε μόλυνση από όλα τα μαγνητικά μέσα αποθήκευση και μην χρησιμοποιείτε ούτε τα αντίγραφα ασφαλείας αν δεν τα ελέγξτε πρώτα.

Τα μέτρα που περιγράφονται στη συνέχεια, έχουν εφαρμογή τόσο για τον ανεξάρτητο χρήστη, όσο και για τις επιχειρήσεις.Στις επιχειρήσεις όμως, πρέπει να λαμβάνονται και πρόσθετα προστατευτικά μέτρα.Πάντως αποδείχθηκε ανεπιτυχής η προσπάθεια να απαγορευτεί στους εργαζομένους η χρήση δισκετών, με προέλευση εκτός του χώρου της επιχείρησης.Αφού δεν είναι πρακτικό να σφραγιστούν οι είσοδοι των οδηγών δισκετών, είναι προτιμότερο η κάθε επιχείρηση να παρέχει στους συνεργάτες της σύγχρονα προγράμματα ανίχνευσης ιών, με τα οποία θα ελέγχεται κάθε δισκέτα πριν χρησιμοποιηθεί.Η εφαρμογή ενός τέτοιου μέτρου γίνεται ευκολότερα αποδεκτή όταν υλοποιηθεί.Αν όμως δεν είναι απαραίτητοι οι οδηγοί δισκέτας οι χρήστες να τις αποσυνδέσουν, ενώ αν τις χρησιμοποιεί μόνο σπάνια, να τις κλειδώσουν για να εμποδίσουν την πρόσβαση κάθε μη εξουσιοδοτημένου χρήστη, με κάποιον ειδικό διακόπτη, για παράδειγμα στην πηγή ρεύματος.

Υπάρχει επίσης η δυνατότητα να προστατευτούν και οι σκληροί δίσκοι.Για το σκοπό αυτόν, πρέπει να εγκαταστήθει ένας δεύτερος σκληρός δίσκο στο μηχάνημα που θέλει κάποιος να προστατεύσει.Ύστερα θα τοποθετηθεί στον σκληρό δίσκο C το λειτουργικό σύστημα και όλα τα αρχεία προγραμμάτων, ή όλα τα αρχεία που δεν χρειάζονται μεταβολές.Στη συνέχεια, με έναν ειδικό διακόπτη, εμποδίζεται η δυνατότητα εγγραφής σε αυτόν το σκληρό δίσκο.Στον άλλο σκληρό δίσκο, το D να αποθηκευτούν όλα τα δεδομένα του χρήστη.Με αυτόν τον τρόπο ο κάθε χρήστης θα είναι βέβαιος ότι ο υπολογιστής τους δεν έχει ιούς, αρκεί να ξεκινά από το σκληρό δίσκο επιπλέον θα εξασφαλιστεί ότι κανένα πρόγραμμα στον σκληρό δίσκο C δεν έχει υποστεί αλλαγές – ούτε από ιό, ούτε από κάποιο σφάλμα χειρισμού.Από πλευράς υλικού δεν δημιουργούνται κατά την εφαρμογή αυτού του μέτρου, γιατί τώρα πια σχεδόν κάθε ελεγκτής δίσκων μπορεί να συνεργάζεται με δυο τουλάχιστον σκληρούς δίσκους.

Πέρα απ' αυτά, είναι σκόπιμο η κάθε επιχείρηση ενημερώνει και να ευαισθητοποιεί τους συνεργάτες της σχετικά με τα προβλήματα και τους κινδύνους που ξεκινούν από τους ιούς.Για να μην ξεχνιέται το θέμα αυτό, θα πρέπει ο κάθε χρήστης να επανέρχεται τακτικά, και με την κατάλληλη μορφή.Για παράδειγμα η επιχείρηση μπορεί να κάνει

Oliver Wagner: «VIRUSCAN»,'' Εντοπίστε και Εκμηδενίστε τους Ιούς των Υπολογιστών'', Αθήνα 1991, σελ. 72 -74

μια ενημέρωση για ιούς και τις επιπτώσεις τους ή σχετικά με τα αποτελέσματα μιας μόλυνσης που έγινε γνωστή στην εταιρία τους, ή σε άλλες επιχειρήσεις.Η ενημέρωση των συνεργατών θα πρέπει να επικεντρώνεται στην γνώση των πραγμάτων, που πρέπει να προσέχουν κατά την εργασία τους με τον υπολογιστή, για να αποφύγουν μια μόλυνση ή να αναγνωρίσουν έγκαιρα κάποια νέα μόλυνση.Παράλληλα, η εταιρία είναι σκόπιμο να καταρτίσει ένα πρόγραμμα αντιμετώπισης των ιών – κάτι ανάλογο με το πρόγραμμα αντιμετώπισης μιας πυρκαγιάς.Το πρόγραμμα αυτό θα καθορίζει, τι πρέπει να γίνει αν υπάρχει υποψία μόλυνσης ενός υπολογιστή, καθώς και ποιοι θα πρέπει να ενημερώνονται αμέσως σε μια τέτοια περιπτωση.Το πρόγραμμα αυτό πρέπει επίσης να ορίζει έναν υπεύθυνο, που θα ειδικεύεται στην καταπολέμηση των ιών και θα είναι πάντα έτοιμος να πάρει τα απαραίτητα μέτρα, για να καθαρίσει το προσβεβλημένο σύστημα και να το επαναφέρει σε κατάσταση σωστής λειτουργίας.

Και μια ακόμη πρόταση για προστασία από τους ιούς, που παρουσιάζει ενδιαφέρον μόνο για όσους έχουν δεδομένα μεγάλης σημασίας στον υπολογιστή τους.Η μέθοδος αυτή απαιτεί έναν ελεύθερο, ενδεχομένως ανεξάρτητο υπολογιστή.Επειδή πολλοί ιοί δεν προσβάλλουν δισκέτες αλλά μόνο σκληρούς δίσκους, ο υπολογιστής αυτός θα πρέπει να έχει ένα σκληρό δίσκο.Στο σκληρό δίσκο του υπολογιστή αυτού, ο χρήστης μπορεί να αντιγράψει, να ταξινομήσει σε περισσότερους υποκαταλόγους, διάφορα αρχεία EXE, COM, SYS.Πρέπει να είναι βέβαιο ότι κανένα από αυτά τα αρχεία δεν έχει προσβληθεί.Μπορεί να δημιουργήσει ένα εφεδρικό αντίγραφο του σκληρού δίσκου, να αντιγράψουν όλα αυτά τα αρχεία σε μιαν άδεια δισκέτα και να ενεργοποιήσουν την προστασία εγγραφής, που δεν πρέπει πια να απενεργοποιηθεί ποτέ.Κατόπιν να αντιγραφτούν μερικά από αυτά τα προγράμματα σε μιαν άλλη δισκέτα.Από αυτήν πάλι, να δημιουργήσουν ένα ακριβές αντίγραφο με τη διαταγή diskcopy και για σιγουριά να το ελέγξουν αμέσως με την diskcomp.Να φυλαχτούν σε ασφαλές μέρος τη μια από αυτές τις όμοιες δισκέτες, μαζί με το εφεδρικό αντίγραφο του σκληρού δίσκου, καθώς και με τη δισκέτα με τα προγράμματα.

Όταν θελήσει τώρα ο χρήστης να δοκιμάσει μια νέα δισκέτα, να εγκαταστήσετε πρώτα το πρόγραμμα που περιέχει η δισκέτα στο σκληρό δίσκο του υπολογιστή δοκιμών.Στην συνέχεια να εκτελέσει μερικές φορές το πρόγραμμα.Καλό είναι να αλλάζει ενδιαμέσως και την ημερομηνία του συστήματος «Κατάλληλες» (δηλαδή, επικίνδυνες) ημερομηνίες είναι Παρασκευή και 13, η Πρωταπριλιά, τα Σάββατα, τα Χριστούγεννα και άλλες ημερομηνίες με κάποια ιδιαιτερότητα.Σκόπιμα επίσης είναι να αλλάζει και τη χρονολογία, επειδή ορισμένοι ιοί ενεργοποιούνται μόνο σε συνδυασμό με ορισμένα έτη.Αφού θα αλλάξουν μερικές φορές την ημερομηνία, θα ξαναξεκινήσουν

τον υπολογιστή.Μην ξεχάσουν να καλέσουν μερικές φορές και κάποια από τα προγράμματα των ταυτόσημων δισκετών, για να αναγνωρίσουν πιθανούς ιούς εκκίνησης.

Αφού καλέσουν αρκετές φορές τα προγράμματα, κάτι που μπορεί να αυτοματοποιηθεί σε μεγάλο βαθμό με τη χρήση ομαδικών αρχείων – από έμπειρους μάλιστα προγραμματιστές αντίγραφα των αρχείων ελέγχου που βρίσκονται στο σκληρό δίσκο.Με τη διαταγή του DOS Comp να συγκριθούν με τα αρχεία που βρίσκονται στο σκληρό δίσκο.Κατόπιν να τα συγκρίνουν με τη διαταγή diskcomp τις δυο όμοιες δισκέτες.Αν τα αρχεία και οι δισκέτες εξακολουθούν να ταιριάζουν απόλυτα μεταξύ του, μπορεί να είναι βέβαιοι ότι η νέα δισκέτα δεν είναι μολυσμένη.

Να προσέξει ο κάθε χρήστης να βρει έναν καλό συμβιβασμό μεταξύ αριθμού αρχείων και απαιτούμενου χρόνου.Όσο πιο συχνά καλέσουν το πρόγραμμα και όσα περισσότερα αρχεία ελέγχου να τα αντιγράψει στο σκληρό δίσκο, τόσο περισσότερες πιθανότητες υπάρχουν να αποκαλυφθεί ο ιός.Η μέθοδος αυτή φυσικά μπορεί να χρησιμοποιηθεί και με το σύστημα, όπου εργάζονται συνηθως.Τότε όμως, ενώ θα διαπιστώσουν την παρουσία ιού, όταν υπάρχει, ο ιός θα βρίσκεται ήδη στο σύστημα και όχι απλώς σε έναν υπολογιστή, που δεν περιέχει σημαντικά δεδομένα.

Μόλις ολοκληρωθεί η δοκιμή ενός νέου προγράμματος, ο υπολογιστής θα πρέπει να ετοιμαστεί ξανά για την επόμενη δοκιμή.Για μεγαλύτερη ασφάλεια, να εκτελέσουν μια μορφοποίηση χαμηλού επιπέδου του σκληρού δίσκου και με τη διαταγή restore, να επαναφέρουν τα δεδομένα από τη δισκέτα με το εφεδρικό αντίγραφο.Αν χρειαστεί, να δημιουργήσετε με diskcopy, ένα νέο αντίγραφο των δύο όμοιων δισκετών.Για τις διαταγές restore και diskcopy, θα χρησιμοποιήσουν φυσικά τις δισκέτες που είχαν δημιουργήσει και προστατεύονται από εγγραφή.

Όπως βλέπουμε, η φασαρία είναι μεγάλη.Η ανταμοιβή όμως, εφόσον η διαδικασία γίνει σωστά, είναι η ασφάλεια των ζωτικών δεδομένων όλων των χρήστων.Η ακεραιότητα των δεδομένων τους όταν εργάζονται σε δίκτυο υπολογιστών, είναι φυσικά πολύ πιο σημαντική από τους μεμονωμένους υπολογιστές.

2. Κατά την διάρκεια της μόλυνσης.

Βοήθεια

1. Κλείστε αμέσως τον υπολογιστή σας εκτός κι αν πρέπει να σώσετε την τρέχουσα εργασία σας.Η κατάσταση δεν μπορεί να γίνει χειρότερη όταν ο υπολογιστής είναι

κλειστός ή σώστε τη τρέχουσα εργασία σας σε μία δισκέτα εάν μπορείτε και μετά κλείστε τον υπολογιστή.

2. Τοποθετήστε όλες τις δισκέτες που έχετε χρησιμοποιήσει για αυτήν την εργασία σε έναν φάκελο με τίτλο ΄΄Πιθανώς μολυσμένες από ιό΄΄.

3. Ενώ έχετε ακόμη φρέσκα τα γεγονότα, καθίστε και **γράψτε** μία σύντομη περιγραφή συμπτωμάτων που προκάλεσαν τις υποψίες σας.

4. Κάντε κατάλογο όλων των αρχείων που έχετε **προσπελάσει** πρόσφατα μέσω δικτύου ή modem, των περίεργων CD – ROM ή δισκετών που πιθανόν να έχετε χρησιμοποιήσει, των ονομάτων των ανθρώπων που έχουν χρησιμοποιήσει τον υπολογιστή σας πρόσφατα, των δισκετών σας που χρησιμοποιήσετε σε κάποιον άλλο υπολογιστή και μετά στον δικό σας, ή οποιεσδήποτε άλλες επικίνδυνες περιπτώσεις.

5. Τηλεφωνήστε στον διευθυντή μηχανογράφησης, ή τον υπεύθυνο του δικτύου ή σε όποιων άλλο εσείς έχετε καθορίσει σαν επαφή για επείγουσες περιπτώσεις.

6. Απομονώστε το σύστημα σας από οποιοδήποτε δίκτυο είστε συνδεδεμένοι να είστε προσεκτικοί γιατί μπορεί να δημιουργηθούν προβλήματα σε άλλα συνδεδεμένα δίκτυα.

7. Τοποθετήστε στον οδηγό δισκέτας Α ένα προστατευμένο από εγγραφή αντίγραφο της αυθεντικής δισκέτας του DOS.Έχοντας την δισκέτα του DOS στον οδηγό Α, θα παρακάμψετε την διαδικασία φορτώματός του από τον σκληρό δίσκο, οποιοιδήποτε ιοί που προσβάλλουν τον τομέα εκκίνησης θα πρέπει τώρα να βρίσκονται μέσα στο φάκελο των πιθανώς μολυσμένων δισκετών που έχετε δημιουργήσει σε κάποιο προηγούμενο βήμα.

8. Εκκινήστε τον υπολογιστή σας, ψάχνοντας για τυχόν αποκλίσεις από την κανονική διαδικασία εκκίνησης.Το DOS θα αρχίσει να ελέγχει το σύστημα σας, εμφανίζοντας τον τίτλο του, το σήμα του και άλλες λεπτομέρειες, βρίσκοντας μόνο του την ημερομηνία ή ζητώντας την από εσάς.Οποιαδήποτε διαφορετική από τις συνηθισμένες ενέργειες θα μπορούσε να σημαίνει μόλυνση.

9. Τρέχτε το πρόγραμμα καταπολέμησης που έχετε και ακολουθήστε τις οδηγίες του προσεκτικά.Αν χρησιμοποιήσετε το Virus Scan θα δείτε ότι είναι τοποθετημένο σε μια προστατευμένη από την εγγραφή δισκέτα ώστε να αποφευχθεί η πιθανή μόλυνση του.Τοποθετήστε την δισκέτα αυτή σε έναν από τους οδηγούς δισκετών και πληκτρολογήστε : Scan C: για να αρχίσει να ελέγχει την ύπαρξη ιών στον σκληρό σας δίσκο.

10. Πληκτρολογήστε την εντολή Sys C: στην γραμμή εντολής.Εάν η μεταφορά γίνει ομαλά θα λάβετε το μήνυμα : System trashferred.Αν αποτύχει η εντολή Sys κάνετε αντίγραφα ασφαλείας όλων των δεδομένων σας πριν προχωρήστε στο επόμενο βήμα.

11. Για να ξαναφορτώσετε τον σκληρό δίσκο **ανατρέξτε** στο εργαστήριο του DOSκαι ακολουθήστε την διαδικασία που αναφέρει.

2. Μετά την μόλυνση.

Πολλά πράγματα μπορούν να πάνε στραβά με τους υπολογιστές, με τα πιο πολλά με τα πιο πολλά να προκύπτουν από λάθη προγραμμάτων ή δυσλειτουργίες του hardware.Όμως, όταν εμφανίζονται δύο ή περισσότερα συμπτώματα προβλημάτων που πιθανόν να οφείλονται σε ιούς, οι πιθανότητες να έχετε μολυνθεί αυξάνονται σημαντικά και είναι τότε καιρός να ελέγξει ο χρήστης το σύστημα του με κάποιο ΄΄αντιβιοτικό΄΄ πρόγραμμα.

Τα ακόλουθα είναι τα πιο κοινά συμπτώματα:

1. Ο χρόνος φόρτωσης των προγραμμάτων παίρνει περισσότερο από το κανονικό.Ορισμένοι ιοί καταλαμβάνουν τον έλεγχο των διαδικασιών εκκίνησης κάποιου συστήματος ή προγράμματος.Όταν το σύστημα εκκινεί, ή φορτώνεται ένα πρόγραμμα εφαρμογής, οι ιοί αυτοί εκτελούν τις δικές τους ενέργειες, μεγαλώνοντας του χρόνο που χρειάζεται αυτό για να φορτωθεί κατά μερικά δευτερόλεπτα.

2. **Οι προσπελάσεις** στους δίσκους διαρκούν υπερβολικά ακόμη και σε απλές εργασίες.Για παράδειγμα, το να σώσετε μία σελίδα κειμένου απαιτεί συνήθως περίπου ένα δευτερόλεπτο, αλλά ο ιός επεκτείνει αυτό τον χρόνο κατά ένα ή δύο ακόμη δευτερόλεπτα.Δώστε ιδιαίτερη προσοχή στην μείωση των χρόνων που απαιτούνται για ôïí προσπέλαση καταλόγων δίσκων και για τις διαδικασίες ενημέρωσης.

3. **Εμφανίζονται** ασυνήθιστα μηνύματα λάθους.Μπορεί να δείτε το μήνυμα write protect error on drive A το οποίο υποδηλώνει ότι κάποιος ιός στο σύστημα σας προσπαθεί να προσπελάσει έναν δίσκο για να τον μολύνει.Η εμφάνιση ενός τέτοιου μηνύματος θα πρέπει να σας κάνει να ψάξετε για μόλυνση από ιό, ειδικά αν το μήνυμα εμφανίζεται συχνά.

4. **Τα λαμπάκια** των οδηγών δίσκων ανάβουν χωρίς να υπάρχει προφανής λόγος.Εάν, για παράδειγμα, το λαμπάκι κάποιου οδηγού δίσκου αναβοσβήνει όταν δεν κάνετε καμία προσπέλαση για εγγραφή ή ανάγνωση από αυτόν, τότε πολύ πιθανό να είστε θύμα κάποιου ιού.

5. **Ελαττώνεται** η μνήμη του συστήματος.Ορισμένοι ιοί καταναλώνουν υπολογισμοί ποσά μνήμης.Εάν τρέχετε μεγάλα προγράμματα χωρίς προβλήματα και ξαφνικά λαμβάνετε ένα μήνυμα που σας λεει ότι δεν υπάρχει αρκετή μνήμη διαθέσιμη στο σύστημα, αυτό θα μπορούσε να σημαίνει μόλυνση από ιό.

6. **Εξαφανίζονται** μυστηριωδώς αρχεία.Ορισμένοι ιοί σβήνουν αρχεία, είτε με τυχαίο τρόπο, είτε βάση οδηγιών.Εάν ένα αρχείο έχει εξαφανιστεί από τον κατάλογο του δίσκου χωρίς λόγο, τότε θα πρέπει να υποπτευθείτε την ύπαρξη κάποιου ιού.Επίσης, ελέγξτε το σύστημα σας όταν δείτε ότι εμφανίζονται ανεξήγητα αρχεία.

7. **Ελαττώνεται** ο χώρος των δίσκων χωρίς προφανή λόγο.Αυτό είναι ένα κοινό προειδοποιητικό σήμα ότι ένας ιός έχει εισβάλει στο σύστημα σας κι έχει αρχίσει να αναπαράγεται.

8. **Αλλάζει** το μέγεθος των αρχείων εκτελέσιμων προγραμμάτων.Κανονικά, τα προγράμματα αυτά διατηρούν το ίδιο μέγεθος, αλλά αν έχετε μολυνθεί από ιό, μπορεί να γίνουν μεγαλύτερα, με το πλήθος των bytes τους να αυξάνεται.Ορισμένοι ευφυείς ιοί

αυξάνουν μεν το μέγεθος των αρχείων, αλλά το νούμερο που εμφανίζουν είναι το κανονικό μέγεθος τους αρχείου.

9. Τα εικονίδια αλλάζουν την εμφάνιση τους.Μία μεγάλη αδυναμία των δημιουργών ιών είναι να κάνουν ξαφνικές αλλαγές των γνωστών εικονιδίων των υπολογιστών Mac, όπως για παράδειγμα, να δώσουν στο εικονίδιο απλού κείμενου μορφή σκύλου. Παρόμοια συμπτώματα μπορούν να εμφανιστούν και σε άλλους υπολογιστές που χρησιμοποιούν γραφικά συστήματα επικοινωνίας με τον χρήστη.

Οι δυσλειτουργίες του hardware και τα λάθη των προγραμμάτων μπορούν επίσης να προκαλέσουν συμπτώματα που να μοιάζουν με αυτά των ιών και να μπερδεύουν την διάγνωση.

Με τα παραπάνω συμπτώματα που προδιαγράψαμε σχετικά με του ιούς των υπολογιστικών συστημάτων μπορεί κάνεις να αντιληφθεί έγκαιρα τον ιό και να περιορίσει σ' ένα μεγάλο ποσοστό την εξάπλωση της μόλυνσης του υπολογιστή του.Για αυτό το πρόβλημα υπάρχουν μέτρα που μπορεί κάνεις να πάρει ΄ύστερα από την επαναφορά του υπολογιστή στην προηγούμενη κατάστασή του.Για το λόγο αυτό θα πρέπει να δημιουργήσει κάνεις εγκαίρως ένα υπόβαθρο, που θα περιέχει όλες τις σημαντικές πληροφορίες για τη δομή και την οργάνωση του σκληρού δίσκου .Τέτοιες πληροφορίες είναι:

- Ο διαμερισμός του σκληρού δίσκου.Αν εκτελεστεί ο διαμερισμός με το πρόγραμμα FDISK, δεν είναι πρόβλημα να σημειωθούν οι αντίστοιχοι κύλινδροι κάθε διαμερίσματος.
- Η δομή των καταλόγων κάθε σκληρού δίσκου.Τη δομή αυτή μπορεί κάνεις εύκολα να την τυπώσει σε χαρτί, για παράδειγμα δίνοντας τη διαταγή tree c:\.> prn.
- Ένας πίνακας των προγραμμάτων, που έχουν αποθηκευτεί σε κάθε κατάλογο.
- Καθώς και ένας πίνακας των αντίστοιχων αρχείων.Μπορεί επίσης να τυπώσει σε χαρτί και τους δυο αυτούς πίνακες με τη διαταγή dir>prn.

ΕΠΙΛΟΓΟΣ

Η λίστα των επιπτώσεων της Πληροφορικής σίγουρα δεν τελειώνει με τη πιο πάνω σταχυολόγηση.Πολλοί επισυνάπτουν στις αρνητικές επιπτώσεις της Πληροφορικής και την έμμεση συμβολή της στα μεγάλα προβλήματα της σημερινής ανθρώπινης κοινωνίας.Άλλοι επιμένουν ότι αποτελεί κύρια συνιστώσα στην προσπάθεια για την επίλυση τους.Η άποψη μας ταυτίζεται με αυτή των Nora και Minc, ότι δηλαδή η Πληροφορική είναι τεχνολογία υποδομής.Σαν τέτοια από μόνη της απλά αποτελεί ένα τμήμα της μηχανής που ο ίδιος ο άνθρωπος κατασκεύασε και έθεσε σε λειτουργία σαν απάντηση στην πρόκληση για καλύτερη ζωή.Το αν η μηχανή τελικά τρέχει γρηγορότερα από τον ίδιο ή περισσότερο θέμα πολιτικών επιλογών.

Σχεδόν πάντα οι τεχνολογίες αναπτύσσονταν πολύ γρηγορότερα από τον αντίστοιχο ιδεολογικό προβληματισμό σχετικά με το ρόλο τους.Το ΄΄εν δυνάμει΄΄ πρόβλημα με Πληροφορική είναι το γεγονός ότι τη δυνατότητα στον άνθρωπο να ωθήσει τις γνώσεις σε σημεία που μπορούν να χαρακτηριστούν σχεδόν οριακά.Οι γνώσεις αυτές μπορούν να χρησιμοποιηθούν όμως κατά τρόπο που θα οξύνει την αλλοτρίωση του ανθρώπου και τις υπάρχουσες ανισορροπίες οδηγώντας σε ένα σύγχρονο τεχνοκρατικό ολοκληρωτισμό.Για να επωφεληθεί η ανθρωπότητα από την πρόκληση ΄΄Πληροφορική Εποχή΄΄ απαιτούνται πνευματική καλλιέργεια ανάλογη των τεχνολογικών εξελίξεων, σωστή ενημέρωση και ευαισθησία του μέσου πολίτη του πλανήτη μας.

Η ίδια η γνώση του ανθρώπου οδήγησε την βιομηχανία των υπολογιστών στο πρόβλημα των ιών και να χάσει τα νεωτεριστικά χαρακτηριστικά της, τα οποία σε προηγούμενες εποχές έδιναν την δυνατότητα σε μικρού μεγέθους προσπάθειες να παράγουν εξαιρετικά αποτελέσματα και προϊόντα τα οποία έμπαιναν γρήγορα στην αγορά, ενθουσιάζοντας τους πάντες – από τους επενδυτές μέχρι τους τελικούς αγοραστές.Αυτοί οι τολμηροί πρωτοπόροι των υπολογιστών, που έκαναν έδρα της

επιχείρησής τους τα γκαράζ των σπιτιών τους και χρηματοδοτούνται αποκλειστικά με δάνεια, έχουν πλέον αντικατασταθεί από μέσης κατηγορίας μάνατζερ, των οποίων οι στόχοι οδηγούνται κατά βάση όχι από την αγάπη για την τεχνολογία αλλά από πιο πεζά και υλικά ενδιαφέροντα.Αντί να ρισκάρουν γενναία τα πάντα, πολλοί από αυτούς προσπαθούν απλώς να προστατεύσουν τους εαυτούς τους με τον πιο συμφέροντα τρόπο.Το πνεύμα της συναδέλφωσης και της αφοσίωσης σ' έναν σκοπό που είναι λόγος ύπαρξης μιας συν/κης επιχείρησης έχει αρχίσει σήμερα να καταρρέει.

Έτσι λοιπόν η βιομηχανία των υπολογιστών δεν οδηγείται πλέον από τους επιστήμονες.Οι ευγενείς στόχοι ενός συνεταιρισμού έχουν αντικατασταθεί από άλλους, πιο υλιστικούς και εγωιστικούς.Οι νέοι ηγέτες της ζητούν και θα ζητούν να διατηρήσουν την ψευδαίσθηση ότι όλα θα πηγαίνουν καλά στο μέλλον, κι έτσι κανείς δεν θα ασχολείται με την ολοένα αυξανόμενη απειλή των ιών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αντίθετα με το κοντινό παρελθόν, σήμερα η βιβλιογραφία στο χώρο της Πληροφορικής χαρακτηρίζεται από εξαιρετικό πλούτο και ποικιλία.Μόνο ο αριθμός των σχετικών με υπολογιστές περιοδικών διπλασιάζεται κάθε τέσσερα χρόνια, ενώ ο αντίστοιχος χρόνος για άλλα επιστημονικά και τεχνικά περιοδικά είναι 10 με 12 χρόνια.Εκτός από περιοδικά οι πάσης φύσεως εκδόσεις γύρω από την Πληροφορική εμφανίζουν μια εντυπωσιακή αύξηση.

Σε μια προσπάθεια να βοηθηθεί ο αναγνώστης που αποφάσισε να ασχοληθεί σε μεγαλύτερο βάθος με την Πληροφορική, παραθέτουμε ορισμένα στοιχεία που εκτιμούμε ότι θα τον βοηθήσουν στην περιήγηση του στον κυκεώνα της σχετικής βιβλιογραφίας.Σημειώστε ότι πολλά από τα βιβλία και περιοδικά που αναφέρονται πιο κάτω, χρησιμοποιήθηκαν και σαν βιβλιογραφία για τη συγγραφή του παρόντος.

ΕΛΛΗΝΙΚΑ – ΒΙΒΛΙΑ

- Κοίλια Χρ.- Στρ.- Καλαφατούδη: «Το πρώτο βιβλίο της Πληροφορικής, Νέες Τεχνολογίες Αθήνα 1995.
- Λυπιτάκης Α.Ηλίας: «Ο Σύγχρονος κόσμος των υπολογιστών », Αθήνα 1997.

ΞΕΝΑ- ΒΙΒΛΙΑ

- Colin Haynes: «Τεχνικές προστασίας από τους ιούς υπολογιστών », Μ. Γκιούρδας, Αθήνα 1991.
- Oliver Wagner: «VIRUSCAN».΄Εντοπίστε και Εκμηδενίστε τους Ιούς των Υπολογιστών΄΄, Κλειδάριθμος Αθήνα 1991.

ΠΕΡΙΟΔΙΚΑ

- Ένθετο: «Ο κόσμος του Internet ».Ασφάλεια και Ηλεκτρονικό Εμπόριο,΄Αθήνα 1999.
- Ένθετο: « Computer για όλους », Αθήνα 2000.
- Ένθετο: « Winplus », Αθήνα 2000.

ΕΦΗΜΕΡΙΔΕΣ

- « Έθνος » ,της 6ης Μαΐου 2000.
- « Ελευθεροτυπία », της 23ης Μαΐου 2000.
- « ESPRESSO », της 14ης Απριλίου 2001.

ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΜΑΤΩΝ

- Τσουραμάνης Χρήστος:΄΄Ο Οδηγός για την συγγραφή μιας επιστημονικής εργασίας΄΄, Μεσολόγγι 2000.
- Πατρώνης Βασίλης:΄΄Διευθύνσεων Συνεταιριστικών Οργανώσεων και Επιχειρήσεων΄΄, Μεσολόγγι 1995.