ΤΕΙ ΠΑΤΡΑΣ
ΣΧΟΛΗ : ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ : ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΘΕΜΑ

# «ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΥΜΑΤΩΝ»

ΕΙΣΗΓΗΤΗΣ :

Κα ΑΝΤΩΝΟΠΟΥΛΟΥ

ΣΠΟΥΔΑΣΤΗΣ:

ΔΟΥΡΗΣ ΚΩΣΤΑΣ

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ
ΒΙΒΛΙΟΘΗΚΗ

ΑΡΙΘΜΟΣ ΕΙΣΑΓΩΓΗΣ 2391

## ΠΕΡΙΕΧΟΜΕΝΑ

# ΠΡΟΛΟΓΟΣ

Η συνεχής ανάπτυξη των νέων τεχνολογιών και ιδιαίτερα της πληροφορικής επηρεάζει τις επιστημονικές και κοινωνικές εξελίξεις.

Ετσι με την εκσυγχρόνιση της πληροφορικής σε όλους τους τομείς δημιουργείται η ανάγκη για την κατοχύρωση του πολίτη από τις αρνητικές επιπτώσεις της πληροφορικής και την κατοχύρωση αυτή την παρέχει η ασφάλεια των πληροφοριακών συστημάτων.

Μια από τις διαστάσεις της πληροφορικής είναι αυτή που έχει σχέση με την τεχνολογία που μπορεί να επηρεάσει το δικαίωμα της κατοχύρωσης των πληροφοριών που αφορούν τα άτομα που ανήκουν σε κάποια επαγγελματική - κοινωνική ομάδα. Ο κίνδυνος αυτός οφείλεται σε ορισμένες δυνατότητες που προσφέρει η πληροφορική.

Πιο συγκεκριμένα η τεχνολογία της πληροφορικής διευκολύνει τη διασταύρωση και συνδυασμένη χρήση πληροφοριών που έχουν συγκεντρωθεί σε διαφορετικά μέρη για διαφορετικούς σκοπούς. Εδώ απεικονίζεται η ανάγκη εξασφάλισης των φυσικών προυποθέσεων δηλαδή των μέσων αποθήκευσης των επεξεργασιών και μετάδοσης πληροφοριών. Η τεχνική εξασφάλιση μπορεί να επιτευχθεί μέσα από την ανάπτυξη ασφαλών συσημάτων. Η ανάπτυξη αυτή δεν πρέπει να σκοπεύει στη στεγανοποίηση οποιουδή-

ποτε πληροφοριακού συστήματος. Αντίθετα αποβλέπει στην εξασφάλιση μόνον των συστημάτων για τα οποία υπάρχει μεγαλύτερη κοινωνική συναίνεση (π.χ πληροφορίες που αφορούν τα πολιτικά φρονήματα του πολίτη κ.λ.π).

Ενα χαρακτηριστικό παράδειγμα που τονίζει την ανάγκη για την αποτελεσματική εξασφάλιση ενός πληροφοριακού συστήματος αποτελεί η δημιουργία από διάφορα κράτη, ενιαίου κωδικού αριθμού μητρώου (ΕΚΑΜ). Για την απλούστευση της πολυπλοκότητας που χαρακτηρίζει τα πληροφοριακά συστήματα της Δημόσιας διοίκησης έχει προταθεί η χρήση ενός ενιαίου κωδικού αριθμού μητρώου. Η χρήση του ΕΚΑΜ υποστηρίζεται ότι μπορεί να συνεισφέρει στην ενοποίηση των λειτουργούντων πληροφοριακών συστημάτων και ως αποτέλεσμα αυτής της ενοποίησης προβάλλεται η βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών.

Εδώ πρέπει να αναφερθούμε σε ένα παράδειγμα που αφορά την Ολλανδία η οποία είχε σε ισχύ κάποιον ΕΚΑΜ από την εποχή του Δεύτερου Παγκοσμίου Πολέμου. Με την έναρξη του πολέμου οι εισβολείς απόκτησαν τη δυνατότητα χρήσης του συστήματος αυτού και το εκμεταλεύτηκαν, δυστυχώς, σε ενέργειές τους που αφορούσαν την Ολλανδική Εβραική κοινότητα.

Μετά από αυτήν την τραγική εμπειρία πολλοί πίστευαν ότι η Ολλανδία θα καταργούσε τη χρήση του ΕΚΑΜ. Ομως κάτι τέτοιο δεν έγινε. Η Δημόσια Διοίκηση της χώρας αυτής χρησιμοποιεί ΕΚΑΜ μέχρι και σήμερα, με η διαφορά ότι δίνει μεγάλη σημασία στις μεθόδους και διαδικασίες εξασφάλισης των βασικών αρχείων (master files) στα οποία συσχετίζεται ο ΕΚΑΜ με τα στοιχεία ταυτότητας του πολίτη που αφορά.

Εδώ βλέπουμε χαρακτηριστικά τις δυνατότητες οι οποίες μπορούν να προσδώσουν στο κοινωνικό σύνολο οι τεχνικές εξασφαλίσεις των πληροφοριακών συστημάτων. Αυτές οι τεχνικές εξασφάλισης είναι αποτελεσματικές, αλλά οπωσδήποτε δεν αποτελούν τον μοναδικό, ούτε τον πιο αποτελεσματικό στόχο δράσης για την ασφαλή λειτουργία ενός πληροφοριακού συστήματος. Απλά αποτελούν μια αποτελεσματική τεχνοκρατική προσέγγισή του, που συμπληρώνει την συνολικότερη κοινωνική επιδίωξη. Δεν είναι δυνατόν εξασφαλίζοντας πληροφοριακά συστήματα, να εξασφαλίσουμε και την κοινωνικά αποδεκτή χρήση τους.

Αντιθέτως ο στόχος είναι να επιδιώκεται ο έλεγχος και η διαφάνεια της λειτουργίας ενός συστήματος από το κοινωνικό σύνολο και στη συνέχεια να αποκτούνται οι τεχνικές εκείνες που διασφαλίζουν ότι η χρήση του συστήματος γίνεται για την εκπλήρωση των κοινωνικά επιθυμητών στόχων.

## 1. Η ΚΡΙΣΙΜΟΤΗΤΑ ΚΑΙ ΕΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Για μεγάλο χρονικό διάστημα τόσο οι επιστήμονες όσο και οιεπαγγελματίες του κλάδου της πληροφορικής και των Η/Υ έριχναν όλο το βάρος στην όσο το δυνατόν καλύτερη επεξεργασία δεδομένων, για κάποιο εργασιακό περιβάλλον. Αργότερα όμως έγινε αντιληπτό ότι αυτά τα δεδομένα ήταν στην πραγματικότητα πληροφορίες που είχαν ξεχωριστή αξία και η κατοχή των οποίων σήμαινε πρόσβαση σε πηγές εξουσίας.

Το πέρασμα από την "επεξεργασία δεδομένων" στην "επεξεργασία πληροφοριών" άργησε αρκετά να γίνει και αυτό δεν οφείλεται σε κάποια τεχνολογική μεταβολή. Ωφείλεται στη μεταβολή της φιλοσοφίας αντιμετώπισης των υποκειμένων επεξεργασίας.

Ετσι το πρόβλημα που δημιουργείται οφείλεται στο γεγονός ότι η ανάγκη εξασφάλισης πληροφοριακών συστημάτων οφείλεται σε αρνητικές εμπειρίες και όχι σε προβλέψεις.

Γι'αυτό οι επαγγελματίες του κλάδου πρέπει να στραφούν στο παρελθόν για να αναλύσουν τα αίτια του προβλήματος και να προτείνουν λύσεις.

Ετσι παρατηρείται πιθανή ανασφάλεια ενός πληροφοριακού συστήματος γι'αυτό πρέπει να υιοθετηθούν αποτελεσματικά μέτρα εξασφάλισης από κάθε ανεπιθύμητη ενέργεια.

## 2. ΠΩΣ ΕΞΑΣΦΑΛΙΖΟΝΤΑΙ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ

Μπορούμε να ορίσουμε κάποιους στόχους για τη διαδικασία εξασφάλισης ενός πληροφοριακού συστήματος.

Ως πιο σημαντικοί στόχοι μπορούν να θεωρηθούν :

α) Η διατήρηση της λειτουργίας και των παρεχόμενων υπηρεσιών ενός πληροφοριακού συστήματος μιάς υπηρεσίας ή ενός οργανισμού.

β) Η διασφάλιση ότι τα λειτουργούντα πληροφοριακά συστήματα δεν αποκλίνουν από τους προκαθορισμένους στόχους.

Ο όρος "διατήρηση" της λειτουργίας ενός πληροφοριακού συστήματος αφορά τις ενέργειες που πρέπει να πραγματοποιηθούν ούτως ώστε να υπάρχει εγγύηση για την εξασφαλισμένη λειτουργία του συστήματος.

Ο όρος "διασφάλιση" της λειτουργίας ενός πληροφοριακού συστήματος αναφέρεται στις διαδικασίες εκείνες που εγγυώνται τη χρήση του συστήματος από τους προκαθορισμένους χρήστες.

## 3. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

Εδώ θα αναφερθούμε σαν πρώτη φάση σε κάποιες βασικές

αρχές που πρέπει να διέπουν τη σχεδίαση του πληροφοριακού συστήματος για όσον το δυνατόν μεγαλύτερη εξασφάλισή του.

Συγκεκριμένα υπάρχουν τρεις βασικές αρχές οι οποίες αναλύονται στη συνέχεια :

## Α. ΑΠΟΚΕΝΤΡΩΣΗ (DISPERSION)

Για την ολοκληρωτική καταστροφή ενός αποκεντρωμένου πληροφοριακού συστήματος απαιτούνται πολλαπλές επεμβάσεις. Έτσι γι'αυτό το λόγο ο σχεδιασμός αποκεντρωμένων συστημάτων ελαχιστοποιεί τις απώλειες σε κάθε περίπτωση προσβολής. Τα τελευταία μοντέλα υπολογιστών είναι σχεδιασμένα πάνω σε αυτήν την αρχή.

## Β. ΥΠΑΡΞΗ ΑΝΤΙΚΑΤΑΣΤΑΤΗ (DUPLICATION)

Αυτή η αρχή βασίζεται στην ανάγκη συνεχούς λειτουργίας ενός πληροφοριακού συστήματος, έστω και αν πάψει κάποιο υποσύστημα να λειτουργεί. Αυτή η μέθοδος είναι εξαιρετικά αποτελεσματική στην ανίχνευση λαθών επεξεργασίας των πληροφοριών. Η μέθοδος που χρησιμοποιείται σήμερα περισσότερο είναι η παράλληλη λειτουργία δυο όμοιων Η/Υ (dualsystems) ή η παράλληλη χειρογραφική ροή των απαραίτητων υποσυστημάτων. Αυτά τα "διπλά" συστήματα παρέχουν δυνατότητα εφεδρείας στην περίπτωση που κάποιο από τα δυο βγει εκτός λειτουργίας.

## Γ. ΑΜΥΝΑ ΣΕ ΒΑΘΟΣ (DEFENCE IN DEPTH)

Αυτή η αρχή στηρίζεται στο γεγονός που απαιτεί την ύπαρξη πολλαπλών ελέγχων προτού ο μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση στο Π.Σ. Ιδιαίτερη εφαρμογή έχει στα συγκεντρωτικά Π.Σ.

Αυτές οι αρχές δεν εφαρμόζονται μόνο για την άμυνα Π.Σ αλλά για οποιοδήποτε σύστημα το οποίο χρειάζεται αυξημένη εξασφάλιση.

## 4. ΔΙΑΦΟΡΑ ΠΡΟΒΛΗΜΑΤΑ ΠΟΥ ΠΑΡΟΥΣΙΑΖΟΝΤΑΙ ΣΕ ΕΝΑ ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ

Οταν οι διαδικασίες εξασφάλισης ενός Π.Σ παραβιάζονται τότε είναι δυνατόν το σύστημα αυτό να παρουσιάσει κάποια απώλεια.

Η ακόμα όταν οι διαδικασίες εξασφάλισης προσβάλλονται από μη εξουσιοδοτημένο χρήστη παρέρχονται σε κρίση.

Οι απώλειες που είναι δυνατόν να παρουσιασθούν σε ένα Π.Σ ταξινομούνται σε τέσσερις κατηγορίες :

1. Αδυναμία χρήσης του Η/Υ.

   Οταν ο Η/Υ βρίσκεται εκτός λειτουργίας διακόπτονται οι παρεχόμενες υπηρεσίες του. Η αδυναμία χρήσης ενός Η/Υ και κατά συνέπεια του Π.Σ το οποίο υλοποιεί μπορεί να οφεί-

λεται στους εξής παράγοντες :

1α. Προσωρινή διακοπή λόγω πτώσης της τάσεως του ηλεκτρικού ρεύματος. Η αντιμετώπιση τέτοιων περιπτώσεων γίνεται συνήθως με γεννήτριες παροχής ηλεκτρικού ρεύματος και οι οποίες συνδέονται στο δίκτυο αυτόματα, όταν υπάρχει ανάγκη (Unlimitted Power Suppliers - UPS).

1β. Αδυναμία σύνδεσης με τον κεντρικό Η/Υ, λόγω υπερφόρτωσης των δικτύων τηλεπικοινωνίας. Το πρόβλημα αυτό βρίσκεται σε αποκεντρωμένα Π.Σ που λειτουργούν όμως με συγκεντρωτική μέθοδο επεξεργασίας π.χ δίκτυα τραπεζών.

1γ. Πρόβλημα υλικού εξαιτίας της μη καλής συντήρησης ή ανθρώπινου λάθους.

1δ. Πρόβλημα λογισμικού εξαιτίας επαγγελματικής ανεπάρκειας ή ανθρώπινου λάθους.

2. Απώλεια χρημάτων. Οταν κατατραφεί το Π.Σ ή υποβαθμισθεί η λειτουργία του τότε υπάρχει απώλεια χρημάτων η οποία μπορεί να εμφανισθεί με δυο μορφές :

2α. Χρήση του Η/Υ. Είναι σύνηθες φαινόμενο πολλά στελέχη ενός κέντρου πληροφορικής να ξεφεύγουνε από αυτό που τους ανατέθηκε να κάνουν και να χρησιμοποιούν τις δυνατότητες που έχουν για δικό τους σκοπό.

2β. Κλοπή του Η/Υ. Αν και είναι σπάνιο φαινόμενο είναι δυνατόν να γίνει.

3. Απώλεια αποκλειστικής χρήσης.

   Αν κάποιος χρησιμοποιήσει το Π.Σ για το οποίο δεν είναι εξουσιοδοτημένος τότε ο κάτοχός του παύει να έχει την αποκλειστική του χρήση. Πολλοί εργαζόμενοι π.χ παίρνουν μαζί τους τα προγράμματα που "δούλευαν" στην προηγούμενη δουλειά τους.

4. Παραβίαση δικαιωμάτων. Η παραβίαση ανθρωπίνων δικαιωμάτων μπορεί να οφείλεται σε προγράμματα που γράφτηκαν έχοντας σαν σκοπό τη διάκριση μεταξύ των πολιτών με βάση τις πολιτικές τους πεποιθήσεις κ.λ.π.

## 5. ΤΑΞΙΝΟΜΗΣΗ ΚΙΝΗΤΡΩΝ

Ενας μεγάλος αριθμός προσβολών αποβλέπει στο οικονομικό όφελος είτε άμμεσο είτε έμμεσο. Δεν χρησιμοποιείται συνήθως βία διότι οι γνώσεις αυτών που προσβάλλουν το Π.Σ είναι μεγάλες και το ποσόν που υπεξαιρείται είναι τις περισσότερες φορές σημαντικό.

Μπορούμε να κάνουμε μια διάκριση των κινήτρων σε δυο γενικές κατηγορίες :

A. Οικονομικό όφελος.

B. Δύναμη και εξουσία. Η πληροφορική δεν αποτελεί μόνο πηγή, αλλά μπορεί να γίνει ισχυρό όργανο κοινωνικού ελέγχου.

## 6. ΕΓΓΕΝΗ ΑΜΥΝΤΙΚΑ ΣΥΣΤΗΜΑΤΑ

Εχουμε τρια διακεκριμένα υπο-συστήματα εξασφάλισης :

1. ΥΠΟΣΥΣΤΗΜΑ ΣΥΝΑΓΕΡΜΟΥ (ALARM SYSTEM)

   Ο ρόλος του είναι να ειδοποιεί τον εξουσιοδοτημένο χρήστη για πιθανή απόπειρα προσπέλασης χωρίς εξουσιοδότηση και κατά συνέπεια να αποθαρρύνει τους μη εξουσιοδοτημένους χρήστες.

2. ΥΠΟΣΥΣΤΗΜΑ ΑΝΤΙΔΡΑΣΗΣ (RESPONSE SYSTEM)

   Ο ρόλος του είναι να οργανώνει την αντίδραση των εξουσιοδοτημένων χρηστών και να ελαχιστοποιεί τις συνέπειες της προσβολής.

3. ΥΠΟΣΥΣΤΗΜΑ ΕΠΑΝΟΡΘΩΣΗΣ (RECOVERY SYSTEM)

   Ο ρόλος του είναι να οργανώνει την αποκατάσταση της λειτουργίας των Π.Σ τα οποία έχουν προσβληθεί και να προετοιμάζει την επαναλειτουργία τους.

Σε συνδυασμό με αυτά τα υποσυστήματα λειτουργούν και οι λεγόμενοι ΔΑΚΤΥΛΙΟΙ ΑΜΥΝΑΣ (DEFENCE RINGS).

Οι δακτύλιοι είναι οι εξής :

1. Υλικό (hardware)
2. Σύστημα Τηλεπικοινωνιών

3. Προγράμματα εφαρμογών
4. Φυσική Ασφάλεια
5. Διαδικασίες χειρισμού
6. Διαδικασίες σχεδιασμού και ανάπτυξης
7. Ελεγχος

Ο εσωτερικός δακτύλιος άμυνας είναι το ΥΛΙΚΟ (hardware) που περιλαμβάνει εγγενής (built in) μηχανισμούς εξασφάλισής του.

Ακολουθεί το σύστημα τηλεπικοινωνιών που περιλαμβάνει τις διαδικασίες Αναγνώρισης και επαλήθευσης (INDENTIFICATION-AUTHENTICATION) των ταυτοτήτων των χρηστών που έρχονται σε επικοινωνία, καθώς και διαδικασίες που έχουν σχέση με την κρυπτογραφία.

Στη συνέχεια είναι τα ΠΡΟΓΡΑΜΜΑΤΑ ΕΦΑΡΜΟΓΩΝ που πρέπει να είναι βασισμένα σε πλήρεις λειτουργικές προδιαγραφές για να κάνουν σωστά αυτά για τα οποία σχεδιάστηκαν.

Ακολουθεί η ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ του Π.Σ που αναφέρεται κυρίως στην αντιμετώπιση σεισμών, πυρκαγιών κ.λ.π.

Οι ΔΙΑΔΙΚΑΣΙΕΣ ΧΕΙΡΙΣΜΟΥ του Π.Σ πρέπει να εξασφαλίζουν ότι δεν υπάρχει δυνατότητα προσπέλασης σε μη εξουσιοδοτημένους χρήστες.

Οι ΔΙΑΔΙΚΑΣΙΕΣ ΑΝΑΠΤΥΞΗΣ του Π.Σ πρέπει να έχουν τη δυνατότητα να εγγυηθούν ότι μόνο ελεγμένα και αξιόπιστα προγράμματα προστίθενται στο χρησιμοποιούμενο λογισμικό.

Ο ΣΧΕΔΙΑΣΜΟΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ καθορίζει τα όρια μέσα στα οποία μπορεί να λειτουργήσουν οι διαδικασίες εξασφάλισης.

Τέλος, ο ΕΛΕΓΧΟΣ όταν οι αμυντικοί δακτύλιοι λειτουργούν σωστά, είναι ένας από τους αποφασιστικότερους παράγοντες που καθορίζουν την εξασφάλιση ενός Π.Σ. Καμιά διαδικασία εξασφάλισης ενός Π.Σ δε μπορεί να είναι αποτελεσματική αν δεν διασφαλίζεται η πλήρης λειτουργίας της.

## 7. ΠΡΟΒΛΗΜΑ ΚΑΘΟΡΙΣΜΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΠΡΟΣΒΑΣΗΣ

Ενα από τα βασικότερα προβλήματα που εμφανίζονται κατά τη διάρκεια της λειτουργίας ενός Πληροφοριακού συστήματος (Π.Σ), είναι ο καθορισμός των δικαιωμάτων πρόσβασης κάθε χρήστη σε κάθε υποσύνολο δεδομένων, αρχείων ή εφαρμογών του Π.Σ.

Μια πρώτη προσέγγιση σε αυτό το πρόβλημα απαιτεί τον ορισμό και την περιγραφή του περιβάλλοντος ενός Π.Σ.

Υπάρχουν δυο βασικές φιλοσοφίες προσέγγισης. Η πρώτη χρησιμοποιεί την κατεύθυνση του καθορισμού διαβάθμισης, ανά χρήστη και αρχείο ή εφαρμογή.

Η δεύτερη χρησιμοποιεί γλώσσες ερωτοαναποκρίσεων για να καθορίσει τις "εικόνες" (views) στις οποίες έχει πρόσβαση κάθε χρήστης του Π.Σ.

Η Πρώτη προσέγγιση είναι γνωστή σαν Πολυ-επίπεδη Προσέγγιση Ασφαλείας και βασίζεται στις εξής έννοιες : χρήστες, μονάδες δεδομένων και πίνακες επιπέδων ασφαλείας.

Ο κάθε χρήστης έχει ένα επίπεδο προσπέλασης και κάθε

μονάδα δεδομένων έχει μια διαβάθμιση.

Η δεύτερη προσέγγιση που έχει εφαρμογή σε Π.Σ τα οποία χρησιμοποιούν βάσεις δεδομένων (Data Bases), απαιτεί βαθιά γνώση του συστήματος διαχείρισης της βάσης δεδομένων (Data Base Management System - DBMS) και του συγκεκριμένου μοντέλου δόμησης της βάσης δεδομένων.

## 8. ΑΝΑΓΝΩΡΙΣΗ - ΕΠΑΛΗΘΕΥΣΗ ΤΑΥΤΟΤΗΤΑΣ

Κάθε Π.Σ πλαισιώνεται από ένα σύνολο ανθρώπων οι οποίοι:

- είτε αναπτύσσουν τις δυνατότητες του διατιθέμενου υλικού και λογισμικού
- είτε το συντηρούν
- είτε χρησιμοποιούν τις υπηρεσίες που τους παρέχει

Για να ολοκληρωθεί η σύνδεση με τον υπολογιστή υπάρχουν τρια στάδια :

Πρώτο : Ταυτοποίηση (INDENTIFICATION). Ο χρήστης "αναγγέλει" στον Η/Υ ποιός είναι. Το στάδιο αυτό αποτελεί το στάδιο της "αναγνώρισης" .

Δεύτερο : Αυθεντικοποίηση (AUTHENTICATION). Ο χρήστης "βεβαιώνει" τον Η/Υ ότι είναι αυτός που ισχυρίζεται. Αυτό το στάδιο αποτελεί την "επαλήθευση" της ταυτότητας του χρήστη.

Τρίτο : Εξουσιοδότηση (AUTHORIZATION). Ο χρήστης "αξιοποιεί" τις δυνατότητες που του παρέχει το Π.Σ.

Η λεπτομερής διαδικασία που ακολουθείται φαίνεται στο σχήμα (1). Από το σχήμα φαίνεται ότι ενώ η ταυτοποίηση απαιτεί ένα χαρακτηριστικό του χρήστη που δεν είναι μυστικό - αντίθετα η αυθεντικοποίηση απαιτεί τη χρήση κάποιας τεχνικής.

Για την πραγματοποίηση της αυθεντικοποίησης υπάρχουν τρεις κατευθύνσεις.

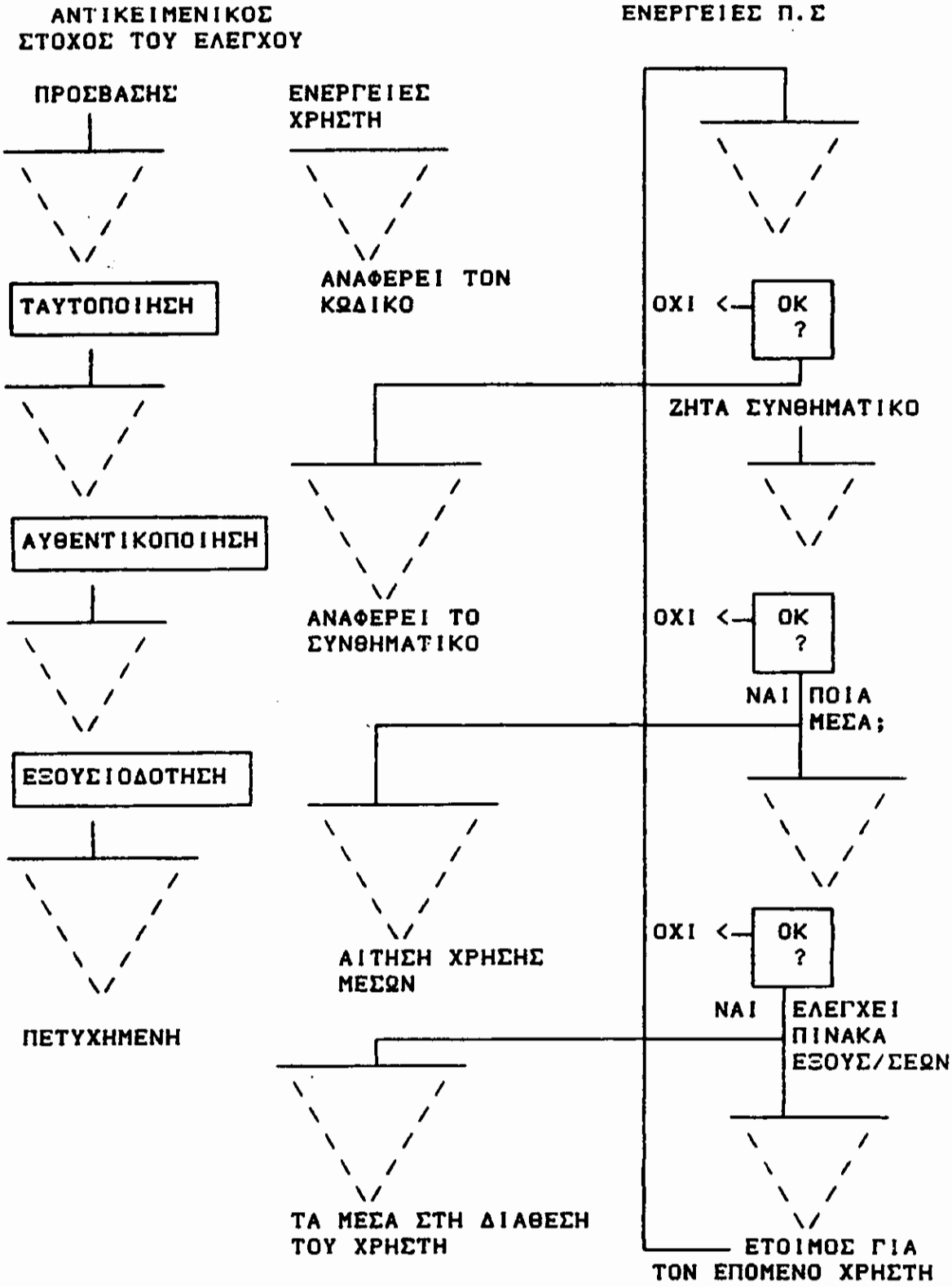
Σε κάθε μια από αυτές ο χρήστης χρησιμοποιεί κάτι :

α) που γνωρίζει (π.χ συνθηματικό)

β) που κατέχει (π.χ μαγνητική κάρτα κ.λ.π)

γ) που τον χαρακτηρίζει (π.χ συσκευή ανίχνευσης δακτυλικών αποτυπωμάτων, φωνής κ.λ.π).

ΔΙΑΔΙΚΑΣΙΑ ΣΥΝΔΕΣΗΣ Η/Υ & ΧΡΗΣΤΗ




ΣΧΗΜΑ 1

Η κάθε μια από τις παραπάνω μεθόδους παρουσιάζει κάποια συγκεκριμένα πλεονεκτήματα και μειονεκτήματα που παρατίθενται συνοπτικά στο σχήμα 2.

| ΜΕΘΟΔΟΣ | ΚΡΙΤΗΡΙΟ | | | | |
|---|---|---|---|---|---|
| | ΚΟΣΤΟΣ | ΑΠΟΤ/ΤΑ | ΟΡΤ/ΣΗ | ΧΡΟΝΟΣ | ΤΕΧΝ/ΓΙΑ |
| ΣΥΝΘΗΜΑΤΙΚΑ | ΜΗΔΕΝ | ΚΥΜΑΙ-ΝΟΝΤΑΙ | ΝΑΙ | ΜΙΚΡΟΣ | ΝΑΙ |
| ΜΑΓΝΗΤΙΚΕΣ ΚΑΡΤΕΣ | ΑΡΚΕΤΟ | ΑΡΚΕΤΑ ΚΑΛΗ | ΚΑΠΟΙΑ | ΜΙΚΡΟΣ | ΝΑΙ |
| ΑΝΑΓΝΩΡΙΣΗ ΧΑΡΑΚΤΗΡ/ΚΩΝ | ΥΨΗΛΟ | ΜΕΓΑΛΗ | ΚΑΠΟΙΑ | ΑΡΚΕΤΟΣ | ΝΑΙ |

ΣΧΗΜΑ 2 : ΣΥΓΚΡΙΣΗ ΜΕΘΟΔΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Μια πρώτη ρεαλιστική εκτίμηση οδηγεί σε μια καλά οργανωμένη χρήση συνθηματικών (Passwords). Η προσέγγιση αυτή παρουσιάζει τα εξής πλεονεκτήματα :

* Χαμηλό κόστος, επομένως υιοθέτησή της και από μικρά και μεσαία κέντρα πληροφορικής,
* Πολύ καλή απόδοση, αν οργανωθεί σωστά,
* Εύκολη συντήρηση - τροποποίηση.

Στη συνέχεια θα ασχοληθούμε με τις βασικότερες τεχνικές και αρχές που πρέπει να διέπουν ένα Σύστημα Ασφαλείας που κάνει χρήση συνθηματικών.

## 9. ΑΡΧΕΣ ΧΡΗΣΗΣ ΣΥΝΘΗΜΑΤΙΚΩΝ

Αυτό που πρέπει να τονιστεί είναι ότι υπάρχει μεγάλος αριθμός τεχνικών χρήσης συνθηματικών με συγκεκριμένα πλεονεκτήματα και μειονεκτήματα η κάθε μια. Κάθε μια από αυτές τις τεχνικές κάνει διαφορετική επιλογή μεταξύ εννέα βασικών κριτηρίων που έχει καθορίσει η Διεθνής Υπηρεσία Προτύπων (National Bureau of standards), σε έκδοσή της που δημοσιεύτηκε στις ΗΠΑ το 1984.

Τα κριτήρια αυτά είναι :

α) Μήκος συνθηματικών

Σε έρευνα που έγινε στους χρήστες του λειτουργικού συστήματος UNIX της BELL LABORATORIES το 1979 αποδείχθηκε ότι το 89% των συνθηματικών μπορούσαν να προβλεφθούν από κάποιον που γνώριζε το χρήστη (το μικρό του όνομα, το τηλέφωνο του κ.λ.π). Ετσι αυτό το λειτουργικό σύστημα σχεδιάστηκε ώστε να προσθέτει από μόνο του στο σύνθημα έναν τυχαίο αριθμό. Με αυτή τη μέθοδο αυξάνοντας το μήκος του, αυξάνει την αξιοπιστία του χωρίς να αναγκάζει το χρήστη να πληκτρολογεί 16 ή 18 αλφαριθμητικά στοιχεία.

β) Σύνθεση Συνθηματικών

Εδώ οι επιλογές είναι περιορισμένες. Ενα συνθηματικό μπορεί να αποτελείται :

* μόνο από γράμματα
* από γράμματα και αριθμούς
* από γράμματα, αριθμούς και ειδικά σύμβολα (π.χ +, *, / κ.λ.π).

γ) Διάρκεια Συνθηματικών

Εδώ διακρίνουμε τρεις δυνατότητες. Η πρώτη αναφέρεται σε σταθερά συνθηματικά για όλες τις χρήσεις που αλλάζουν σε τακτά χρονικά διαστήματα ή μετά από μια ορισμένη ημερομηνία. Η δεύτερη αναφέρεται σε συνθηματικά που ζητούνται μόνον όταν απαιτηθεί προσπέλαση σε διαβαθμισμένο αρχείο. Η τρίτη αναφέρεται σε συνθηματικά που χρησιμοποιούνται σε κάποιο συνδυασμό των δυο πρώτων δυνατοτήτων.

δ) Πηγή Συνθηματικών

Οι δυνατότητες εδώ είναι δυο. Κατά την πρώτη το συνθηματικό επιλέγεται από τον ίδιο τον χρήστη. Κατά την δεύτερη το συνθηματικό είναι το αποτέλεσμα ενός προγράμματος που έχει γραφτεί και εκτελείται σε κατάλληλη χρονική στιγμή γι'αυτόν ακριβώς το σκοπό, χρησιμοποιώντας κάποιον αλγόριθμο ψευδοτυχαίων αριθμών. Πρέπει να τονιστεί ότι αν μια τέτοια γεννήτρια δίνει $2^{35}$ διαφορετικούς συνδυασμούς τότε όλα τα πιθανά συνθηματικά μπορούν να δοκιμασθούν σε 1 μόνο πρώτο λεπτό.

Αρα πρέπει να εξασφαλιστεί όσο το δυνατό μεγαλύτερος αριθμός πιθανών συνθηματικών. Κάτι άλλο πολύ σημαντικό είναι

ότι τα συνθηματικά πρέπει να μνημονεύονται εύκολα. Αν δεν συμβαίνει αυτό τότε είναι πολύ πιθανό οι χρήστες να τα καταγράφουν για να τα θυμούνται. Τέτοια γεννήτρια έχει προταθεί για το λειτουργικό σύστημα MULTICS, από το 1974.

ε) Μέθοδοι Διανομής Συνθηματικών

Οταν πρόκειται για Λ.Σ το οποίο είναι εγκατεστημένο και λειτουργεί σε κάποιο συγκεκριμένο χώρο και μόνο, τότε η διανομή των συνθηματικών γίνεται κατευθείαν στους χρήστες από τον υπεύθυνο Ασφαλείας ή το ειδικό πρόγραμμα - γεννήτρια. Αν το Λειτουργικό σύστημα παρέχει υπηρεσίες σε μια γεωγραφικά εκτεταμένη περιοχή, τότε η διανομή μπορεί να γίνει είτε με συστημένη αλληλογραφία ή με τη βοήθεια του προγράμματος - γεννήτριας και μιάς μεθόδου κρυπτογράφησης.

στ) Αποθήκευση - Μετάδοση Συνθηματικών

Εδώ διακρίνουμε τρεις δυνατότητες. Η πρώτη αναφέρεται στην αποθήκευσή τους σε κάποιο μέρος της μνήμης, έτσι όπως είναι π.χ Personal Computers. Η δεύτερη εξασφαλίζει ότι κανένας δεν έχει τη δυνατότητα να προσπελάσει το χώρο αυτό π.χ Bull DPS/6. Η τρίτη αναφέρεται στην κρυπτογράφηση του συνθηματικού και στην αποθήκευσή του στην κρυπτογραφημένη μορφή. Η μέθοδος αυτή παρουσιάζεται ως η πιο δημοφιλής. Το Λ.Σ UNIX για παράδειγμα ακολουθεί αυτήν ακριβώς τη μέθοδο και το αρχείο των κρυπτογραφημένων συνθηματικών είναι ελεύθερο στην προσπέλαση από κάθε χρήστη.

ζ) Εισαγωγή Συνθηματικών

Η εισαγωγή των συνθηματικών γίνεται με πληκτρολόγησή τους χωρίς να είναι ορατά στην οθόνη του τερματικού σταθμού ή

του προσωπικού υπολογιστή.

η) Συχνότητα αυθεντικοποίησης

Είναι δυνατόν κατά τη διάρκεια της εργασίας του χρήστη, να απαιτείται ανανέωση της αυθεντικοποίησης του, ιδιαίτερα μετά από παρατεταμένη αδράνεια. Αυτό γίνεται για να εξασφαλιστεί ότι κανένας δεν επωφελήθηκε από την απομάκρυνση ενός χρήστη για να χρησιμοποιήσει χωρίς εξουσιοδότηση τον τερματικό σταθμό του, που παρέμεινε ενεργός (ON LINE) στη διάρκεια της απουσίας του.

θ) Μορφή Συνθηματικών

Σε πολλά Π.Σ δεν αρκεί μόνο η πληκτρολόγηση ενός συνθηματικού αλλά ακολουθεί μια σειρά ερωτοαπαντήσεων οι οποίες ανταλάσσονται μεταξύ του υποψήφιου χρήστη και του Η/Υ.

Αυτή η μέθοδος είναι αρκετά χρονοβόρα, αλλά αυξάνει αισθητά την αξιοπιστία ενός συνθηματικού. Ενα παράδειγμα τέτοιας "συνομιλίας" παρατίθεται :

Η/Υ : ΠΟΙΟΣ ΕΙΝΑΙ Ο ΚΩΔΙΚΟΣ ΣΑΣ;

ΧΡΗΣΤΗΣ : AB102345

Η/Υ : ΣΩΣΤΑ, ΠΟΙΟΣ ΕΙΝΑΙ Ο ΑΡΙΘΜΟΣ ΤΑΥΤΟΤΗΤΑ ΣΑΣ;

ΧΡΗΣΤΗΣ : Ξ477211

Η/Υ : Η ΕΙΣΑΓΩΓΗ ΣΑΣ ΟΛΟΚΛΗΡΩΘΗΚΕ. ΘΕΛΕΤΕ ΝΑ ΑΛΛΑΞΕΤΕ ΚΑΠΟΙΑ ΑΠΟ ΤΙΣ ΕΡΩΤΗΣΕΙΣ; (Ν/Ο) Κ.Λ.Π

Με αυτήν τη μέθοδο ο χρήστης καλείται να απαντήσει και σε μια πρόσθετη ερώτηση. Αυτή η ερώτηση επιλέγεται στην τύχη από ένα σύνολο ερωτήσεων παρόμοιων. Επίσης μπορεί να τροποποιήσει τυχαία, μια μόνον από αυτές κάθε φορά που εισάγεται

στο σύστημα. Πρέπει να σημειωθεί ότι σε κάθε αποτυχημένη προσπάθεια εισαγωγής το Π.Σ επανέρχεται κάνοντας την ίδια πρόσθετη ερώτηση. Δεν είναι απαραίτητο να χρησιμοποιείται στην αρχική φάση αλλά μόνο όταν ζητείται πρόσβαση σε διαβαθμισμένα αρχεία.

# ΑΝΑΓΚΑΙΟΤΗΤΑ ΑΣΦΑΛΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

## ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ

Η πρώτη προσπάθεια για τη δημιουργία ψηφιακής μηχανής έγινε από τον Βρετανό μαθηματικό C.Babbage. Αν και ο Babbage ξόδεψε ολόκληρη τη ζωή και την περιουσία του για την τελειοποίηση της αναλυτικής του μηχανής δεν τα κατάφερε. Δεν πέτυχε το στόχο του διότι όπως συμβαίνει σχεδόν πάντα σε τέτοιες περιπτώσεις οι ιδέες του προηγούνταν της εποχής του. Ετσι ήταν αδύνατον να κατασκευαστούν τα απαραίτητα μηχανικά μέρη για τη σωστή λειτουργία της αναλυτικής μηχανής.

Στη συνέχεια ύστερα από αρκετά χρόνια γύρω στα μέσα της δεκαετίας του '40 κάποιοι επιστήμονες κατόρθωσαν να δημιουργήσουν υπολογιστικές μηχανές με τη βοήθεια λυχνίων. Ανάμεσα σε αυτούς ο Aiken, ο J.Von Newman, ο K. Zuse στη Γερμανία κ.ά.

Επειτα επακολούθησε η ανακάλυψη του transistor που είχε σα συνέπεια τη βαθμιαία εξέλιξη των υπολογιστικών μηχανών. Από τότε ξεκινάει περίπου και η εισαγωγή της έννοιας του λειτουργικού συστήματος. Χαρακτηριστικά λειτουργικά συστήματα εκείνης της εποχής το F.M.S και το IBSYS του IBM/7094.

Το λειτουργικό σύστημα εμφανίζεται με τη μορφή του

προγράμματος επίβλεψης. Γύρω στις αρχές της δεκαετίας του '60 η ανακάλυψη των ολοκληρωμένων κυκλωμάτων βοήθησε πολύ στην ώθηση των υπολογιστών.

Τα λειτουργικά συστήματα της γενιάς αυτής όπως το MULTICS, το CTSS, το OS/360 αλλά και το UNICS είχαν δυνατότητες όπως :

α) πολυπρογραμματισμού

β) χρονοδιαμέρισης

γ) διασωλήνωσης

Τέλος κατά τη διάρκεια της δεκαετίας του '80 αναπτύχθηκαν τα ολοκληρωμένα κυκλώματα ευρείας έκτασης. Χαρακτηριστικό λειτουργικό σύστημα που είναι και το πιο διαδεδομένο στον κόσμο σήμερα είναι το MS - DOS της Microsoft.

Χαρακτηριστικά αυτών των λειτουργικών συστημάτων είναι τα εξής :

i) Εχουν τη δυνατότητα να λειτουργούν σε δίκτυο

ii) Λειτουργούν με κατανεμημένη επεξεργασία

iii) Επιτυγχάνουν φιλικότητα προς τους χρήστες

Ετσι σαν ορισμό του Λειτουργικού συστήματος ενός υπολογιστή θα μπορούσαμε να πούμε πως ονομάζεται το προιόν Λογισμικού που ελέγχει την εκτέλεση των προγραμμάτων στον υπολογιστή και παρέχει υπηρεσίες αποσφαλμάτωσης, χρονοκατανομής, ελέγχου εισόδου - εξόδου, διαχείρισης μνήμης, μεταγλώτισης.

## ΙΔΙΟΤΗΤΕΣ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Οι ιδιότητες που πρέπει να έχει ένα λειτουργικό σύστημα επιγραμματικά είναι οι εξής :

1. Ευχρηστία
2. Γενικότητα
3. Αποδοτικότητα
4. Ορατότητα
5. Ευελιξία
6. Διαφάνεια
7. Ασφάλεια
8. Ακεραιότητα
9. Ευκινησία
10. Αξιοπιστία
11. Συντηρησιμότητα
12. Επεκτασιμότητα
13. Διαθεσιμότητα

## ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ - ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ

Οι πιο σημαντικές ιδιότητες από αυτές που αναφέρθηκαν παραπάνω για τα λειτουργικά συστήματα είναι :

α) Διαθεσιμότητα

β) Ασφάλεια

γ) Ακεραιότητα

Πιο συγκεκριμένα :

**α) Διαθεσιμότητα** είναι η ιδιότητα ενός λειτουργικού συστήματος να εξασφαλίζει στους χρήστες την πρόσβαση στα αντικείμενα του συστήματος που επιθυμούν με τον καλύτερο τρόπο.

**β) Ασφάλεια** ενός λειτουργικού συστήματος είναι η ιδιότητα

που έχει το σύστημα να επιτρέπει στους χρήστες προσπέλαση μόνον στα αντικείμενα που δικαιούνται.

Ετσι υπάρχουν δυο βασικές αρχές για την προστασία : η κατασταλτική και η προληπτική.

γ) Ακεραιότητα είναι η ιδιότητα του συστήματος να προστατεύει τους χρήστες και τα αντικείμενά τους κάτω από οποιεσδήποτε συνθήκες.

## Κατασταλτική προστασία

Η κατασταλτική προστασία πραγματοποιείται με χρήση μιάς σειράς μεθόδων.

Η πιο βασική από αυτές τις μεθόδους είναι αυτή της επίβλεψης (surveillance).

Αυτή η μέθοδος στοχεύει στην καταγραφή κάθε μη εξουσιοδοτημένης απόπειρας πρόσβασης στο λειτουργικό σύστημα. Επίσης στοχεύει στη διαρκή παρακολούθηση της συνολικής λειτουργίας του συστήματος, ώστε να εξασφαλίζεται, ότι οι μηχανισμοί προστασίας του λειτουργούν κανονικά. Η μέθοδος αυτή χρησιμοποιεί δυο τεχνικές : την παρακολούθηση των διαρροών (threat monitoring) και τον έλεγχο ασφαλείας (security audit).

Ο έλεγχος ασφαλείας αποτελεί μια περισσότερο παθητική τεχνική. Αποσκοπεί στην απλή καταγραφή των γεγονότων που σχετίζονται με την ασφάλεια ενός λειτουργικού συστήματος. Η καταγραφή αυτή εξασφαλίζει τα προβλεπόμενα ιστορικά στοιχεία, ώστε να εντοπιστεί κάποια παραβίαση εκ των υστέρων. Αν και η

τεχνική του ελέγχου ασφαλείας είναι παθητική παρόλα αυτά είναι πολύ χρήσιμη, γιατί βοηθά στην αποκάλυψη των μεθόδων που χρησιμοποιήθηκαν για την παραβίαση ενός συστήματος. Αυτή η τεχνική στηρίζεται σε ενέργειες όπως :

- Παρακολούθηση της λειτουργίας των διαδικασιών ασφαλείας,
- Αναγνώριση των παραβιάσεων και αναφοράς τους,
- Διάγνωση της φύσης της παραβίασης, κ.λ.π

## Προληπτική προστασία

Αυτή είναι περισσότερο σημαντική από ότι η κατασταλτική, γιατί αφορά παραβιάσεις που δεν πρόλαβαν να πραγματοποιηθούν. Επομένως το σύστημα δεν έχει υποστεί οποιαδήποτε συνέπεια. Πραγματοποιείται με βάση δυο αρχές :

- την αρχή της ελεγχόμενης προσπέλασης (controlled access)
- την αρχή του διαχωρισμού (isolution).

### Ελεγχόμενη προσπέλαση

Η ελεγχόμενη προσπέλαση επιτυγχάνεται με χρήση τεχνικών που επιτρέπουν σε κάθε εξουσιοδοτημένο χρήστη να αποκτά πρόσβαση μόνο στα αντικείμενα του συστήματος που δικαιούται.

Μια γνωστή και δημοφιλής τέτοια μεθοδολογία είναι η "ταυτοποίηση - αυθεντικοποίηση - εξουσιοδότηση". Στόχος της είναι να απαντηθεί η ερώτηση : "πως αποδεικνύεται, ότι

κάποιος χρήστης είναι πραγματικά αυτός που ισχυρίζεται;".

Διαχωρισμός

Η αρχή του διαχωρισμού στηρίζεται στη διαδικασία κατά την οποία ένα συστατικό ενός πληροφοριακού συστήματος διαχωρίζεται απολύτως από άλλα συστατικά στα οποία δεν πρέπει να έχει πρόσβαση. Οι συγκεκριμένοι στόχοι ενός τέτοιου διαχωρισμού εξαρτώνται από το συνδυασμό των αντικειμένων που αναγνωρίζουν με αυτά που αναγνωρίζονται σε κάποια συνεργασία. Οι στόχοι αυτοί είναι κατά περίπτωση :

1. Χρήστης από χρήστη. Ενας χρήστης ή μια ομάδα χρηστών πρέπει να μπορεί να εξασφαλίζει αποκλειστική προσπέλαση σε μια ομάδα αντικειμένων του συστήματος (π.χ προγραμμάτων).
2. Χρήστης από λειτουργικό σύστημα. Πρέπει να μπορούν να περιορισθούν οι αρμοδιότητες του λειτουργικού συστήματος στο χώρο ενός χρήστη.
3. Χρήστης από το περιβάλλον. Πρέπει να μπορεί να εξασφαλισθεί μια οθόνη για παράδειγμα από την έκθεσή της σε ηλεκτρομαγνητική ακτινοβολία. Πρέπει επίσης να αναγνωρίζεται θετικά το προσωπικό συντήρησης του μηχανικού εξοπλισμού.
4. Λειτουργικό σύστημα από χρήστη. Ο χρήστης δε θα πρέπει να μπορεί να ελέγξει πλήρως τις διαδικασίες ασφαλείας του λειτουργικού συστήματος.
5. Λειτουργικό σύστημα από λειτουργικό σύστημα. Σε

συνεργασία δυο λειτουργικών συστημάτων το εποπτεύον πρέπει να διαθέτει στο εποπτευόμενο μόνο τις λειτουργίες που είναι απόλυτα απαραίτητες για τη συνεργασία τους.

6. Λειτουργικό σύστημα από το περιβάλλον. Το λειτουργικό σύστημα πρέπει να είναι επαρκώς απομονωμένο από τις ενέργειες του προσωπικού συντήρησης του μηχανικού εξοπλισμού καθώς και των φυσικών φαινομένων που συμβαίνουν στο περιβάλλον του και μπορούν να το επηρεάσουν.
7. Πληροφορία από χρήστη. Πρέπει να μην είναι δυνατή για παράδειγμα η προσπέλαση όλων των χρηστών στις πληροφορίες που αφορούν την ασφάλεια του λειτουργικού συστήματος.
8. Πληροφορίες από το λειτουργικό σύστημα. Το λειτουργικό σύστημα πρέπει να περιορίζει την προσπέλαση χρηστών σε ορισμένα μόνον ευρετήρια του συστήματος. Επίσης πρέπει να διαγράφει φυσικά την κεντρική μνήμη πριν τη διαθέσει σε καινούργιο χρήστη.
9. Πληροφορίες από το περιβάλλον. Κανένα μέλος του προσωπικού υποστήριξης ή συντήρησης του πληροφοριακού συστήματος δεν πρέπει να διαθέτει πρόσβαση στις πληροφορίες ασφαλείας του συστήματος.
10. Φυσικά μέσα από το χρήστη. Τα προγράμματα των χρηστών δεν πρέπει να μπορούν να αποκτήσουν προσπέλαση στην κεντρική μονάδα επεξεργασίας

Κ.Μ.Ε (Central Processing Unit - CPU) ή στις συσκευές εισόδου - εξόδου εκτός αν έχουν ειδικά εξουσιοδοτηθεί.

11. Φυσικά μέσα από το λειτουργικό σύστημα. Πρέπει να διαχωρίζονται οι διαδικασίες ασφαλείας του λειτουργικού συστήματος από τις λειτουργίες ελέγχου εισόδου - εξόδου, καθώς και από τα φυσικά μέσα που περιέχουν την Κ.Μ.Ε.
12. Φυσικά μέσα από το περιβάλλον. Τα φυσικά μέσα που υλοποιούν τις διαδικασίες ασφαλείας πρέπει να διαχωρίζονται από το υπόλοιπο περιβάλλον και ιδαίτερα από το προσωπικό που εργάζεται εκεί.
13. Πληροφορίες από πληροφορίες. Οι πληροφορίες που είναι ζωτικές για την ασφάλεια του συστήματος πρέπει να είναι διαχωρισμένες από τις υπόλοιπες.
14. Φυσικά μέσα από φυσικά μέσα. Πρέπει να διαχωρισθούν τα φυσικά μέσα που περιέχουν την Κ.Μ.Ε, για παράδειγμα από άλλα μέσα.

Η συνύπαρξη των αρχών διαχωρισμού και διαφάνειας προυποθέτει στάθμιση των συγκυριών που διέπουν το πληροφοριακό σύστημα όπου οι αρχές θα εφαρμοσθούν. Ετσι σε άλλα συστήματα μπορεί να προκριθεί η υπεροχή της μιάς αρχής και σε άλλα της άλλης.

Υπάρχουν μέθοδοι που πετυχαίνουν το στόχο του διαχωρισμού σε αρκετό βαθμό. Χαρακτηριστικά παραδείγματα αποτελούν :

- η χρήση πυρήνα ασφαλείας (security kernes)
- η σχεδίαση ιδεατής μνήμης (virtual memory)
- η σχεδίαση κατανεμημένων συστημάτων (distributed systems).

## ΜΕΘΟΔΟΣ ΕΥΡΕΤΗΡΙΟΥ

Ενας απλός μηχανισμός για την προστασία των αντικειμένων ενός λειτουργικού συστήματος μοιάζει με ένα ευρετήριο αρχείων.

Κάθε αρχείο έχει ένα μοναδικό κάτοχο. Ο κάτοχος αυτός διαθέτει κάθε δικαίωμα στην αξιοποίηση του αρχείου αυτού.

Στα δικαιώματα αυτά ανήκει και το δικαίωμα να καθορίζει ποιός άλλος χρήστης μπορεί να έχει προσπέλαση στο αρχείο αυτό και το είδος της προσπέλασης. Ετσι, κάθε χρήστης διαθέτει ένα ευρετήριο ιδιόκτητων αρχείων, καθώς και κάποια αρχεία που του έχουν διατεθεί από άλλους χρήστες.

Τα ευρετήρια κάθε χρήστη βρίσκονται στη διάθεση του λειτουργικού συστήματος το οποίο ελέγχει αν τηρούνται τα καθορισμένα δικαιώματα πρόσβασης.

Τέτοια δικαιώματα πρόσβασης είναι τα ανάγνωσης, εγγραφής, εκτέλεσης προγράμματος καθώς και το Owner (ιδιοκτησίας).

Το βασικό πλεονέκτημα της μεθόδου αυτής είναι η ευκολία της εφαρμογής της. Αρκεί να τηρείται μια κατάσταση για κάθε

χρήστη, η οποία να περιέχει τα αρχεία που δικαιούται να προσπελαύνει με τα συγκεκριμένα δικαιώματα προσπέλασης σε καθένα από αυτά.

Μια πρώτη δυσκολία εμφανίζεται όταν το πληροφοριακό σύστημα περιέχει μεγάλο αριθμό αρχείων ή υπάρχουν πολλά αρχεία προσπελάσιμα από πληθώρα χρηστών.

Μια δεύτερη δυσκολία της μεθόδου αυτής παρουσιάζεται κατά την ανάκληση ενός δικαιώματος κάποιου χρήστη, από ένα συγκεκριμένο αντικείμενο.

Για παράδειγμα έστω ότι ο χρήστης Α έχει παραχωρήσει δικαίωμα εγγραφής σε ένα αρχείο του οποίου είναι ιδιοκτήτης, σε κάποιους άλλους χρήστες. Κάποια στιγμή αποφασίζει να ανακαλέσει το δικαίωμα αυτό. Αν θελήσει να το ανακαλέσει από όλους τους χρήστες τότε δεν έχει πρόβλημα, παρόλο που το λειτουργικό σύστημα πρέπει να επεξεργασθεί όλες τις καταστάσεις όλων των χρηστών, για να εκτελέσει τη σχετική εντολή και η ενέργεια αυτή μπορεί να απαιτεί πολύ χρόνο.

Αν όμως θελήσει το δικαίωμα αυτό να το ανακαλέσει από ένα χρήστη, έστω τον Β, τότε αντιμετωπίζει ένα σημαντικό πρόβλημα. Θα ανακαλέσει το δικαίωμα του Β, αλλά δε θα γνωρίζει σε ποιούς άλλους έχει παραχωρήσει το ίδιο δικαίωμα, ο Β, άρα δε θα μπορεί να το ανακαλέσει και από αυτούς.

Μια τρίτη δυσκολία αφορά τα αρχεία με το ίδιο όνομα. Δυο χρήστες Χ και Υ είναι δυνατόν να έχουν ονομάσει με το ίδιο όνομα (έστω Κ), δυο διαφορετικά αρχεία τους. Αν κάποια στιγμή θελήσουν και οι δυο να παραχωρήσουν δικαίωμα προσπέλασης σε αυτό, στον ίδιο χρήστη Μ, τότε εμφανίζεται το

πρόβλημα. Το λειτουργικό σύστημα, αλλά και ο χρήστης, δε μπορούν να αναγνωρίσουν ότι τα αρχεία με το όνομα Μ προέρχονται από διαφορετικούς χρήστες, εκτός αν το όνομά τους είναι της μορφής <Κ,Χ>, <Κ,Υ>.

Μια άλλη λύση στο πρόβλημα αυτό είναι η μετονομασία των αρχείων που στέλνονται στο ευρετήριο του χρήστη Μ, έτσι ώστε το όνομά τους να καθίσταται μοναδικό. Έτσι, μπορεί το αρχείο Κ του Χ να ονομάζεται $K_1$ και το αρχείο Κ του Υ να ονομάζεται $K_2$. Η λύση αυτή ονομάζεται τεχνική των ψευδονύμων.

Η μέθοδος αυτή έχει ένα ενδιαφέρον πλεονέκτημα. Δυο χρήστες μπορεί να εμπιστεύονται σε διαφορετικό βαθμό έναν τρίτο. Έτσι είναι δυνατόν ο πρώτος να του παραχωρεί λιγότερα δικαιώματα σε ένα συγκεκριμένο αρχείο. Με τον τρόπο αυτό τα δικαιώματα του τρίτου χρήστη στο αρχείο Κ είναι τα δικαιώματα που του παραχωρεί ο χρήστης που τον εμπιστεύεται περισσότερο.

## ΤΙ ΜΠΟΡΕΙ ΝΑ ΣΥΜΒΕΙ ΣΕ ΕΝΑ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ

Γνωρίζουμε ότι το λειτουργικό σύστημα αποτελεί τον "ακρογωνιαίο λίθο" της σχεδίασης και της ασφαλούς λειτουργίας κάθε πληροφοριακού συστήματος.

Γι'αυτό το λόγο οι δυνατότητές του πρέπει να έχουν σχεδιαστεί μεθοδικά και να έχουν υλοποιηθεί κατά τρόπο που διευκολύνει τους χρήστες να κάνουν ασφαλέστερα και αποτελεσματικότερα τις εργασίες που επιθυμούν.

Αν ένα λειτουργικό σύστημα δε διαθέτει τις απαραίτητες δυνατότητες εξασφάλισης των χρηστών και των αντικειμένων του τότε υπάρχει κίνδυνος να υποστεί κάποια από τις εξής συνέπειες :

i) Να υποβαθμιστεί ή και να διακοπεί η λειτουργία του πληροφοριακού συστήματος προσωρινά ή και μόνιμα ακόμη

ii) Να επιτραπεί η προσπέλαση κάποιου χρήστη σε διαβαθμισμένα δεδομένα, τα οποία τηρούνται σε προστατευόμενη περιοχή

iii) Να επιτραπεί η τροποποίηση δεδομένων από χρήστες οι οποίοι δεν είναι εξουσιοδοτημένοι για κάτι τέτοιο.

Ετσι οι σχεδιαστές του λειτουργικού συστήματος πρέπει να γνωρίζουν τα σημεία ευπάθειας που αφορούν όλα τα λειτουργικά συστήματα. Τα σημεία αυτά είναι :

α) Προσπέλαση σε χρησιμοποιηθέντα χώρο

β) Ελλειπής έλεγχος κώδικα

γ) Ασύγχρονες διακοπές

δ) Ασύγχρονες προσβολές

## ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΤΑΤΕΥΕΤΑΙ ΚΑΙ ΠΩΣ

Η ανάγκη για την εξασφάλιση ενός υπολογιστικού συστήματος ή του λειτουργικού συστήματος που το επόπτευε δεν ήταν

η ίδια κατά την πρώτη εξέλιξη των πρώτων γενιών υπολογιστών. Αυτό συνέβαινε διότι ο χρήστης απασχολούσε το σύνολο ενός υπολογιστικού συστήματος για δική του και μόνο χρήση. Ετσι η ανάγκη για την εξασφάλιση των δεδομένων και των προγραμμάτων ήταν πολύ περιορισμένη.

Αργότερα όταν μάλιστα κατέστη δυνατόν πολλοί χρήστες να χρησιμοποιούν τους ίδιους πόρους του συστήματος οι συνθήκες αυτές άλλαξαν. Ηταν ορατή πλέον η ανάγκη για εξασφάλιση των δεδομένων, των αρχείων κ.λ.π. ενός χρήστη από τους υπόλοιπους.

Τα συστατικά ενός υπολογιστικού συστήματος που απαιτούν προστασία, όταν χρησιμοποιούνται από κοινού από άλλους χρήστες είναι τα εξής :

i) Αρχεία και ευρετήρια αρχείων
ii) Εκτελέσιμα προγράμματα
iii) Συσκευές υλικού, όπως οι δίσκοι
iv) Δομές δεδομένων όπως ο σωρός (stack)
v) Η μνήμη άμεσης προσπέλασης (RAM)
vi) Εντολές του λειτουργικού συστήματος οι οποίες καθορίζουν προνόμια στους χρήστες
vii) Δεδομένα του λειτουργικού συστήματος όπως πίνακες διευθύνσεων

Για να είναι δυνατή η προστασία των συστατικών αυτών πρέπει να έχει προηγηθεί κατάλληλη σχεδίαση του λειτουργικού συστήματος. Η σχεδίαση αυτή πρέπει να αποβλέπει στην κάλυψη ενός ή περισσοτέρων στόχων :

α) Φυσικός διαχωρισμός

β) Προσωρινός διαχωρισμός

γ) Λογικός διαχωρισμός

δ) Κρυπτογραφικός διαχωρισμός

Από αυτές τις μεθόδους η ασφαλέστερη μέθοδος είναι αυτή του Φυσικού διαχωρισμού και η λιγότερο ασφαλής του Κρυπτογραφικού διαχωρισμού. Ομως ο φυσικός διαχωρισμός υποβαθμίζει σοβαρά την αποδοτικότητα ενός υπολογιστικού συστήματος, ενώ αντίθετα ο κρυπτογραφικός διαχωρισμός, αν και είναι σχετικά ευπαθέστερη μέθοδος, διευκολύνει την ανταλλαγή δεδομένων και πόρων του υπολογιστικού συστήματος.

Η βαθμίδα ελέγχου είναι ένα άλλο ενδιαφέρον σημείο, στην εξέταση των μεθόδων που μπορεί να διαθέτει ένα λειτουργικό σύστημα για την εξασφάλιση των συστατικών του (αντικειμένων). Αν ένα λειτουργικό σύστημα πραγματοποιεί ελέγχους για παράδειγμα σε επίπεδο δυαδικού ψηφίου θα είναι αποτελεσματικότερο από το λειτουργικό σύστημα που πραγματοποιεί ελέγχους σε επίπεδο αρχείου (File), πεδίου (fields), εγγραφής (record). Αντίθετα όσο πιο κοντά στο κύτταρο της πληροφορίας γίνεται ο έλεγχος τόσο πιο δύσκολη είναι η σχεδίαση και η εφαρμογή του. Είναι λοιπόν προφανές ότι η εξασφάλιση των συστατικών (αντικειμένων) ενός υπολογιστικού συστήματος, αν και είναι δυνατή και τεχνικά εφικτή, απαιτεί αυξημένη προσπάθεια στη σχεδίαση του λειτουργικού συστήματος που το καθοδηγεί. Δεν πρέπει να ξεχνάμε πως απαιτεί επένδυση κόπου και χρόνου για την εφαρμογή της σε πραγματικό περιβάλλον.

Γίνεται έτσι κατανοητό πως η σχεδίαση ενός λειτουργικού συστήματος με αυξημένες δυνατότητες εξασφάλισης των αντικειμένων του δεν είναι μονόδρομος. Θα πρέπει να συνεκτιμηθεί το λειτουργικό περιβάλλον στο οποίο απευθύνεται το σύστημα, η επένδυση που απαιτείται για την ανάπτυξη του, καθώς και η γενικότερη εξέλιξη στον τομέα της ασφάλισης των πληροφοριακών συστημάτων.

## ΠΡΟΣΤΑΣΙΑ ΑΝΤΙΚΕΙΜΕΝΩΝ

Η προστασία των αντικειμένων που χρησιμοποιεί ένα λειτουργικό σύστημα είναι ένα γενικό πρόβλημα, μιας και τα αντικείμενα αυτά μπορεί να ανήκουν σε μια σωρεία μορφών (μνήμη, αρχεία δεδομένων, εκτελέσιμα προγράμματα, συσκευές εισόδου - εξόδου, εντολές και πίνακες του ίδιου του λειτουργικού συστήματος κ.λ.π).

Εκτός από τους βασικούς στόχους υπάρχουν και τρεις συμπληρωματικοί για την ασφάλεια των αντικειμένων ενός λειτουργικού συστήματος :

1. Ελεγχος κάθε προσπέλασης : Ο στόχος αυτός αποβλέπει στην εξασφάλιση της δυνατότητας του λειτουργικού συστήματος να ελέγχει κάθε απόπειρα προσπέλασης, οποιουδήποτε χρήστη, σε κάθε αντικείμενο του συστήματος.
2. Ισχύς ελάχιστων δικαιωμάτων : Για την κάλυψη του

στόχου αυτού πρέπει κάθε χρήστης να διαθέτει δικαίωμα προσπέλασης μόνο στα αντικείμενα που είναι απόλυτα απαραίτητα για την άσκηση των καθηκόντων του.

3. Επιβεβαίωση αποδεκτής χρήσης : Η δυνατότητα προσπέλασης σε ένα αντικείμενο είναι μια δίτιμη απόφαση. Αντίθετα η πράξη που εκτελείται σε ένα αντικείμενο μπορεί να ποικίλει. Ο στόχος του ελέγχου αυτού είναι να επιβεβαιώνει ότι η πράξη που εκτελείται σε ένα αντικείμενο είναι αποδεκτή.

## ΣΧΗΜΑΤΑ ΣΧΕΔΙΑΣΗΣ ΑΣΦΑΛΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

## ΠΡΟΥΠΟΘΕΣΕΙΣ ΣΧΕΔΙΑΣΗΣ ΑΣΦΑΛΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Για να γίνει μια ασφαλής σχεδίαση ενός λειτουργικού συστήματος είναι απαραίτητες κάποιες προυποθέσεις.

α) Πολιτική εξασφάλιση. Σε αυτήν την πολιτική πρέπει να περιλαμβάνονται οι στόχοι του σχεδιαστή του λειτουργικού συστήματος αφού θα είναι εξασφαλισμένη μια βασική δέσμη αρχών που θα εκφράζονται με σαφήνεια.

β) Ταυτοποίηση. Κάθε αντικείμενο του συστήματος πρέπει να μπορεί να αναγνωρισθεί θετικά.

γ) Σήμανση. Ολα τα αντικείμενα του συστήματος πρέπει απαραιτήτως να συνοδεύονται από ενδείξεις βαθμού εμπιστευτικότητας τους.

δ) Ελεγχότητα. Σε ένα λειτουργικό σύστημα πρέπει να καταγράφονται όλες οι ενέργειες οι οποίες αφορούν ή ακόμα μπορούν να επηρρεάσουν την ασφάλειά του.

ε) Διαβεβαίωση. Το υπολογιστικό σύστημα οπωσδήποτε πρέπει να περιέχει τεχνικές ρυθμίσεις για την υλοποίηση της πολιτικής εξασφάλισης του, οι οποίες να μπορούν να εκτιμηθούν ως προς την αποτελεσματικότητά τους.

στ) Συνεχής προστασία. Πρέπει να επιτυγχάνεται επιτυχής προστασία των τεχνικών εξασφάλισης του λειτουργικού συστήματος από κάθε ανεπιθύμητη μετατροπή.

Ενα πρότυπο εξασφάλισης ενός λειτουργικού συστήματος αποτελείται από ένα σύνολο αυστηρά καθορισμένων κανόνων που διέπουν τα αντικείμενα ενός συστήματος, τους χρήστες του συστήματος, καθώς και τις ενέργειες που δικαιούται να εκτελέσει φυσικά με κάποιες προυποθέσεις κάθε χρήστης σε κάθε αντικείμενο.

Τα πρότυπα εξασφάλισης πρέπει να ικανοποιούν τις απαιτήσεις των χρηστών και των σχεδιαστών ενός λειτουργικού συστήματος για διαθεσιμότητα, ασφάλεια και ακεραιότητα των αντικειμένων του.

## ΠΡΟΤΥΠΑ ΔΥΑΔΙΚΟΥ ΕΛΕΓΧΟΥ

Τα πρότυπα δυαδικού ελέγχου βασίζονται σε ένα απλό έλεγχο για την πρόσβαση σε ένα αντικείμενο του συστήματος. Ο έλεγχος αυτός στηρίζεται στη δυαδική λογική του "ναι" ή "όχι" δηλαδή στο αν επιτρέπεται ή όχι η πρόσβαση.

### Πρότυπο επίβλεψης

Σύμφωνα με αυτό το πρότυπο ο χρήστης που επιθυμεί να προσπελάσει ένα αντικείμενο του συστήματος για να εκτελέσει κάποια καθορισμένη ενέργεια ανακοινώνει στο σύστημα την επιθυμία του αυτή.

Βασικό πλεονέκτημα του προτύπου αυτού είναι η απλότητά του η οποία συνεπάγεται και την εύκολη εφαρμογή του.

Μειονέκτημά του αποτελεί η μεγάλη συχνότητα της κλήσης του. Για κάθε ενέργεια κάθε χρήστη καλείται το σύστημα να αποφασίσει αν δικαιούται να την εκτελέσει ή όχι. Έτσι και ο χρόνος ανταπόκρισης του συστήματος αυξάνεται και η φιλικότητά του τίθεται υπό αίρεση.

Το δεύτερο μειονέκτημα του προτύπου αυτού είναι ότι μπορεί να επιβλέψει μόνον άμεση προσπέλαση σε ένα αντικείμενο.

Το πρότυπο αυτό είναι ένα από τα πρώτα που προτάθηκαν και αφορούν την ασφάλεια των αντικειμένων ενός συστήματος. Στηρίζεται σε ιδέες που πρωτοεμφανίστηκαν μεταξύ 1969 και 1972. Εξαιτίας των αδυναμιών του, σύντομα το διαδέχτηκαν άλλα πιο αποτελεσματικά.

**Πρότυπο διαρροής πληροφοριών**

Αυτό το πρότυπο ελέγχει τις πληροφορίες που μεταδίδονται προς έναν χρήστη όταν αυτός κάνει χρήση του δικαιώματός του να προσπελάσει ένα αντικείμενο του συστήματος. Προέκυψε με βάση τη διαπίστωση ότι είναι δυνατόν κάποιος χρήστης να ζητάει πρόσβαση σε ένα αντικείμενο και με την πρόσβαση του αυτή να αντλεί πληροφορίες και για κάποιο άλλο.

Το πρότυπο διαρροής πληροφοριών έχει ιδιαίτερη σημασία γιατί μπορεί να ελέγξει καταστάσεις όπου ένας χρήστης δικαιούται να χρησιμοποιήσει ένα πρόγραμμα αλλά δεν δικαιούται να προσπελάσει τα δεδομένα που χρησιμοποιεί το πρόγραμμα αυτό.

Οι σχεδιαστές ενός λειτουργικού συστήματος μπορούν να εξασφαλίσουν με την εφαρμογή του προτύπου αυτού, ότι η κλήση των προγραμμάτων του συστήματος που διαχειρίζονται προστατευόμενα δεδομένα, δε μπορεί να οδηγήσει στη διαρροή των δεδομένων αυτών.

## ΠΟΛΥΕΠΙΠΕΔΑ ΠΡΟΤΥΠΑ ΕΞΑΣΦΑΛΙΣΗΣ

Τα προηγούμενα πρότυπα στηρίζονται στη δυαδική λογική του "ναι" ή "όχι". Στην πράξη όμως, απαιτείται μεγαλύτερη κλιμάκωση των απαντήσεων, στην απαίτηση για προσπέλαση σε ένα αντικείμενο του συστήματος. Τα πιο χαρακτηριστικά πολυεπίπεδα πρότυπα είναι δυο : α) το στρατιωτικό και β) το πρότυπο δικτυώματος.

### Στρατιωτικό πρότυπο

Το στρατιωτικό περιβάλλον για προφανείς λόγους έχει μια μακροχρόνια προϊστορία εξασφάλισης των πληροφοριών που διαχειρίζεται.

Συνήθως οι πληροφορίες αυτές κατατάσσονται σε τέσσερις κατηγορίες χωρίς να αποκλείεται και ακόμη ευρύτερη κλίμακα. Η ονομασία κάθε κλίμακας είναι i) άκρως απόρητη, ii) απόρητη, iii) εμπιστευτική και iv) αδιαβάθμητη.

Η φιλοσοφία του στρατιωτικού προτύπου στηρίζεται σε δυο αρχές :

α) Στην αρχή της ελάχιστης απαίτησης. Σύμφωνα με την αρχή αυτή κάθε χρήστης δικαιούται να χρησιμοποιεί τον ελάχιστο αριθμό αντικειμένων του συστήματος προκειμένου να ανταποκριθεί στις υποχρεώσεις του.

β) Στην αρχή του δικαιώματος γνώσης. Σύμφωνα με

την αρχή αυτή κάθε χρήστης δικαιούται προσπέλαση μόνο στις πληροφορίες που χρειάζονται για την επιτέλεση του έργου του.

Πρότυπο δικτυώματος

Το στρατιωτικό πρότυπο αποτελεί μέρος ενός γενικότερου προτύπου το οποίο ονομάζεται πρότυπο δικτυώματος. Εκτός όμως από το στρατιωτικό πρότυπο υπάρχει και μια σειρά άλλων που αποτελούν δικτυώματα. Για παράδειγμα οι διαβαθμίσεις κοινά γνωστοποιήσιμο, εμπιστευτικό και απόρητο που χρησιμοποιούνται για την προστασία του ιατρικού απορήτου, αποτελούν επίσης ένα δικτύωμα. Πολλά άλλα δικτυώματα χρησιμοποιούνται σε επιχειρηματικά περιβάλλοντα, σε κέντρα πληροφορικής εκπαιδευτικών ιδρυμάτων κ.ά.

## ΠΡΟΤΥΠΑ ΕΛΕΓΧΟΥ ΡΟΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Τα πρότυπα αυτά ελέγχουν και καθορίζουν ποιές πληροφορίες επιτρέπεται να μεταδίδονται σε ένα ασφαλές σύστημα.

Το πρότυπο Bell - Lapadulla στοχεύει στη διασφάλιση του συστήματος, ενώ το πρότυπο Biba στην εξασφάλιση της ακεραιότητάς του. Στην επιδίωξή τους να πετύχουν τους στόχους αυτούς υστερούν, αντίστοιχα στη διασφάλιση της ακεραιότητας και της ασφάλειας του συστήματος. Συνεπώς τα πρότυπα αυτά λειτουργούν με συμπληρωματικό τρόπο. Χρονικά προηγήθη-

κε η πρόταση του προτύπου Bell - Lapadula και ακολούθησε το πρότυπο Biba (1977).

Τα δυο αυτά πρότυπα αποτέλεσαν τη βάση για τη διαμόρφωση των Κριτηρίων Εξασφάλισης υπολογιστικών Συστημάτων που χρησιμοποιούνται από το υπουργείο Αμυνας των Η.Π.Α και ευρύτερα γνωστά ως "Orange book".

## ΠΡΟΤΥΠΟ BELL LAPADULLA

Το πρότυπο αυτό αποσκοπεί στον αυστηρό καθορισμό της δυνατής ροής κάθε πληροφορίας, έτσι ώστε το λειτουργικό σύστημα να είναι ασφαλές. Εφαρμόζεται με επιτυχία για την εξασφάλιση ενός συστήματος, το οποίο διαχειρίζεται αντικείμενα ποικίλων διαβαθμίσεων.

Το βασικό πλεονέκτημά του είναι ότι μπορεί να χρησιμοποιηθεί για τη σχεδίαση λειτουργικών συστημάτων, τα οποία έχουν τη δυνατότητα νε εκτελέσουν, παράλληλα δυο εργασίες, οι οποίες χρησιμοποιούν αντικείμενα διαφορετικής διαβάθμισης. Για την περιγραφή του προτύπου αυτού, ας κάνουμε τις εξής υποθέσεις :

- Εστω S το σύνολο των αντικειμένων και O το σύνολο των χρηστών του συστήματος
- Εστω ότι για κάθε αντικείμενο S και κάθε χρήστη O υπάρχουν καθορισμένες κλάσεις C(s) και C(o), διατεταγμένες με βάση τη σχέση διάταξης $\leq$ (οι κλάσεις αυτές μπορεί να αποτελούν δικτύωμα, αλλά

κάτι τέτοιο δεν απαιτείται).

Για να είναι ασφαλής η ροή των πληροφοριών στο σύστημα, πρέπει να ισχύουν οι παρακάτω κανόνες :

Κανόνας 1 : Ενας χρήστης S μπορεί να έχει δικαίωμα ανάγνωσης σε ένα αντικείμενο O, αν και μόνο αν ισχύει ότι C(o) ≤ C(s).

Παράδειγμα : Στο στρατιωτικό πρότυπο Ο ο κανόνας αυτός σημαίνει ότι πρόσβαση σε μια πληροφορία κάποιας διαβάθμισης επιτρέπεται μόνο σε όσους έχουν εξουσιοδότηση για τουλάχιστον την ίδια διαβάθμιση.

Κανόνας 2 : Ενας χρήστης S ο οποίος έχει δικαίωμα ανάγνωσης σε ένα αντικείμενο O, έχει δικαίωμα εγγραφής και σε ένα αντικείμενο p μόνο αν C(o) ≤ C(p).

Παράδειγμα : Στο στρατιωτικό πρότυπο ο κανόνας αυτός σημαίνει ότι κάποιος που διαθέτει πληροφορία μιας διαβάθμισης μπορεί να τη μεταδόσει μόνο σε χρήστες με διαβάθμιση τουλάχιστον ίση με τη δική του. Υπάρχει όμως και ένα βασικό μειονέκτημα του προτύπου αυτού. Στο στρατιωτικό πρότυπο για παράδειγμα φαίνεται με βάση το δεύτερο κανόνα ότι όταν κάποιος χρήστης λαμβάνει πληροφορίες κάποιας διαβάθμισης δεν πρέπει από εκείνη τη στιγμή, να ανταλλάσει οποιαδήποτε πληροφορία, με χρήστες που έχουν μικρότερη διαβάθμιση από αυτήν. Η ισχύς του κανόνα αυτού δεν είναι απαραίτητη άρα το πρότυπο Bell - Lapadula είναι πιο αυστηρό από όσο απαιτείται.

Για την άρση του μειονεκτήματος αυτού απαιτείται η συμπλήρωση - τροποποίηση του δεύτερου κανόνα, έτσι ώστε να αποσυνδέεται το δικαίωμα εγγραφής όταν οι πληροφορίες που γράφονται δεν εξαρτώνται από τις πληροφορίες που αναγνώσθηκαν.

Στο στρατιωτικό πρότυπο αυτό σημαίνει ότι επιτρέπεται η ανταλλαγή πληροφοριών μεταξύ δυο χρηστών διαφορετικής διαβάθμισης. Προυπόθεση, η ανταλλαγή αυτή να μην οδηγεί στην αποκάλυψη πληροφοριών, που γνωρίζει ο χρήστης με τη μεγαλύτερη διαβάθμιση και δε δικαιούται να γνωρίζει ο άλλος.

ΠΡΟΤΥΠΟ BIBA

Το πρότυπο Biba στοχεύει στην εξασφάλιση της ακεραιότητας των αντικειμένων ενός συστήματος, εμποδίζοντας τη μη εξουσιοδοτημένη τροποποίησή τους.

Αντίστοιχα με τους κανόνες που ορίζουν το σχήμα Bell Lapadula το πρότυπο Biba ορίζεται ως εξής :

Κανόνας 1 : Ενας χρήστης μπορεί να τροποποιήσει ένα αντικείμενο O, μόνο αν $\|(O) \leq \|(S)$

Κανόνας 2 : Αν ένας χρήστης S έχει δικαίωμα ανάγνωσης σε ένα αντικείμενο O τότε μπορεί να έχει δικαίωμα εγγραφής και στο αντικείμενο p μόνον αν $\|(p) \leq \|(O)$.

Βασικό μειονέκτημα του προτύπου αυτού είναι ότι δεν προστατεύει το σύστημα από την προσθήκη ανακριβών πληροφοριών. Ετσι, αν κάποιος χρήστης προσθέσει στο σύστημα μια ανακριβή πληροφορία μειώνει την αξιοπιστία του αντικειμένου στο οποίο την εγγράφει : Επίσης κάθε αντικείμενο που αντλεί πληροφορίες από το αναξιόπιστο αρχείο, υφίσταται και αυτό μείωση της αξιοπιστίας του.

## ΠΡΟΤΥΠΑ ΥΠΟΛΟΓΙΣΤΙΚΟΤΗΤΑΣ

Τα πρότυπα αυτά στηρίζονται στον εντοπισμό και τη συστηματική περιγραφή των ιδιοτήτων, που πρέπει να έχει ένα ασφαλές λειτουργικό σύστημα. Η θεωρητική τους βάση ανάγεται στη γενική θεωρία της υπολογιστικότητας. Από αυτά τα πρότυπα τρία είναι τα βασικά, το GD (Graham - Denning), το HRU πρότυπο των τεσσάρων δυνατοτήτων - 4Ω (Take - Grant). Χρονικά, τα σχήματα αυτά αναπτύχθηκαν το 1971 - 72 το πρώτο, το 1976 το δεύτερο και το 1977 - 81 το τρίτο.

### ΠΡΟΤΥΠΟ GRAHAM - DENNING (GD)

Το πρότυπο αυτό βασίζεται σε οκτώ βασικές εντολές πρόσβασης, οι οποίες ελέγχουν τη διαχείριση των αντικειμένων ενός συστήματος από έναν ή περισσότερους χρήστες.

Εστω S ένα σύνολο χρηστών O ένα σύνολο αντικειμένων, ενός συστήματος και R ένα σύνολο δικαιωμάτων. Εστω, επίσης, ένας πίνακας καθορισμού δικαιωμάτων πρόσβασης (ACM)A. Τα δικαιώματα πρόσβασης μπορούν να ορισθούν ως οι ενέργειες που δικαιούται να εκτελέσει ένας χρήστης σε άλλους χρήστες ή αντικείμενα του συστήματος.

Με βάση τις υποθέσεις αυτές, οι οκτώ βασικές εντολές του προτύπου ορίζονται ως εξής :

α) Δημιουργία αντικειμένου. Με την εντολή αυτή ο

χρήστης μπορεί να προσθέσει ένα νέο αντικείμενο στο σύστημα.

β)-δ) Δημιουργία χρήστη, διαγραφή χρήστη, διαγραφή αντικειμένου. Με την εντολή αυτή εξουσιοδοτείται ο χρήστης με τα σχετικά δικαιώματα.

ε) Ανάγνωση δικαιώματος πρόσβασης. Με την εντολή αυτή ο ιδιοκτήτης ενός αντικειμένου καθορίζει οποιοδήποτε δικαίωμα ενός άλλου χρήστη στο αντικείμενο αυτό.

ζ) Ακύρωση δικαιώματος πρόσβασης. Με την εντολή αυτή ένας χρήστης μπορεί να άρει τα δικαιώματα ενός άλλου χρήστη, σε ένα αντικείμενο. Προυπόθεση για την άρση αυτή είναι ότι το αντικείμενο είτε ανήκει στον αίροντα χρήστη, είτε ανήκει στον έλεγχό του.

η) Μεταφορά δικαιώματος πρόσβασης. Με την εντολή αυτή ένας χρήστης μπορεί να μεταφέρει κάποιο δικαίωμα που διαθέτει σε ένα αντικείμενο, σε έναν άλλο χρήστη. Το δικαίωμα που μεταφέρεται μπορεί να είναι επαναμεταφερτό ή όχι. Μόνο στην πρώτη περίπτωση μπορεί ο νέος κάτοχός του να το αναμεταδώσει σε τρίτο χρήστη.

Το σύνολο των εντολών αυτών μπορούν να αποτελέσουν τα συστατικά μιας "γλώσσας" με την οποία επικοινωνούν δυο μέρη, όταν υπάρχουν συνθήκες αμοιβαίας καχυποψίας.

Οι εντολές αυτές έχουν δυο σημεία τα οποία πρέπει να προσεχθούν ιδιαίτερα: τις προυποθέσεις υπό τις οποίες μπορούν να εκτελεσθούν και τις συνέπειες που έχουν όταν εκτελούνται. Για παράδειγμα, για να ισχύει η έκτη εντολή,πρέπει ο πρώτος χρήστης να είναι ιδιοκτήτης του αντικειμένου ενώ ο δεύτερος χρήστης δέχεται μόνον όσα δικαιώματα του αναθέτει ο πρώτος.

## ΠΡΟΤΥΠΟ HARRISON - RUZZO - ULLMAN (HRU)

Το πρότυπο HRU αποτελεί γενίκευση του προτύπου GD. Και αυτό στηρίζεται σε εντολές οι οποίες εκτελούνται σύμφωνα με κάποιες προυποθέσεις και έχουν συγκεκριμένες συνέπειες στα αντικείμενα και τους χρήστες του συστήματος. Μια μικρή διαφορά μεταξύ του προτύπου HRU και του GD είναι ότι στο πρώτο κάθε χρήστης μπορεί να είναι και αντικείμενο του συστήματος.

Αρα οι στήλες του πίνακα A.C.M αποτελούνται από όλους τους χρήστες καθώς και από όλα τα αντικείμενα του συστήματος που δεν είναι χρήστες.

Οι βασικές εντολές του HRU είναι :

α)-β) Δημιουργία χρήστη, δικαιώματος

γ)-δ) Ακύρωση χρήστη - δικαιώματος

ε) Ανάθεση δικαιώματος r στον A[S,O]

στ) Ακύρωση δικαιώματος r από τον A[S,O]

Τελικά το πρότυπο HRU δημιουργεί ένα σύστημα προστασίας το οποίο αποτελείται από χρήστες, αντικείμενα, δικαιώματα και εντολές.

Η φιλοσοφία προστασίας του λειτουργικού συστήματος UNIX βασίζεται σε ένα τέτοιο σύστημα προστασίας.

Η εφαρμογή ενός τέτοιου προτύπου οδηγεί σε δυο παρατηρήσεις. Η πρώτη στοιχειοθετεί πλεονεκτήματά του και η δεύτερη μειονεκτήματα.

1. Πλεονέκτημα : Αν οι εντολές του προτύπου αποτελούνται από

μια πράξη τότε είναι δυνατόν δοθείσας της αρχικής μορφής του ACM - να ελέγξουμε αν είναι δυνατόν ένας συγκεκριμένος χρήστης να αποκτήσει κάποιο συγκεκριμένο δικαίωμα, σε ένα συγκεκριμένο αντικείμενο. Αρα κάθε χρήστης είναι δυνατόν να βεβαιωθεί ότι κανένας άλλος χρήστης δε θα αποκτήσει κάποιο δικαίωμα προσπέλασης σε ένα αντικείμενο που τον ενδιαφέρει να προστατεύσει.

Με τον τρόπο αυτό είναι, επίσης, δυνατόν να ελεγχθεί αν κάποιος χρήστης χαμηλής διαβάθμισης μπορεί ή όχι να αποκτήσει δικαίωμα ανάγνωσης σε ένα αντικείμενο υψηλότερης διαβάθμισης.

2. Μειονέκτημα : Αν οι εντολές περιέχουν περισσότερες από μια πράξεις, τότε δεν είναι δυνατόν να ελεγχθεί η εξέλιξη της διάδοσης των δικαιωμάτων των χρηστών στα αντικείμενα του συστήματος. Το λειτουργικό σύστημα UNIX, για παράδειγμα, όπου εφαρμόζεται το σχήμα HRU, χαρακτηρίζεται από περιορισμένες δυνατότητες ασφαλείας αν και οι τεχνικές που χρησιμοποιεί εφαρμόζονται και γίνονται κατανοητές σχετικά εύκολα. Η αυστηρή απόδειξη και των δυο αυτών παρατηρήσεων είναι δυνατή με τη χρήση των αρχών λειτουργίας μιας μηχανής Turing.

ΠΡΟΤΥΠΟ ΤΕΣΣΑΡΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Το τελευταίο πρότυπο είναι αυτό των τεσσάρων δυνατοτήτων - 4Δ (Take - Grant). Στο πρότυπο αυτό υπάρχουν τέσσερις εντολές. Δυο από αυτές συναντώνται και στα πρότυπα

HRU και GD (οι δυο πρώτες), ενώ οι άλλες εισάγονται για πρώτη φορά.

Ας χρησιμοποιήσουμε τον ίδιο συμβολισμό που χρησιμοποιήθηκε και στα άλλα πρότυπα. Εστω S ένα σύνολο χρηστών και O ένα σύνολο αντικειμένων, τα οποία μπορεί με τη σειρά τους να είναι ενεργά ή ανενεργά. Επίσης, έστω R ένα σύνολο δικαιωμάτων. Κάθε χρήστης ή αντικείμενο σχεδιάζεται ως O κόμβος ενός γράφου. Τέλος τα δικαιώματα ενός χρήστη σε ένα αντικείμενο, σχεδιάζονται ως βέλη με φορά προς το αντικείμενο.

Οι τέσσερις εντολές είναι οι εξής :

1. Create (O,r). Με την εκτέλεση της πράξης αυτής προστίθεται ένα αντικείμενο O στο γράφο. Επίσης, συνδέεται ο χρήστης S με το O με δικαίωμα r.
2. Reroke (O,r). Η εκτέλεση της εντολής αυτής ακυρώνει το δικαίωμα r του χρήστη S στο αντικείμενο O.
3. Grant (O,p,r). Το αποτέλεσμα της πράξης αυτής είναι να αναθέτει από το χρήστη S στο αντικείμενο O, δικαίωμα r στο αντικείμενο p. Για να συμβεί αυτό πρέπει ο χρήστης S να έχει δικαίωμα grant στο αντικείμενο O και στο αντικείμενο p.
4. Take (o,p,r). Το αποτέλεσμα της πράξης αυτής είναι ότι ο χρήστης S αφαιρεί από το αντικείμενο O το δικαίωμα r, που είχε στο αντικείμενο p. Για να συμβεί αυτό πρέπει ο χρήστης S να έχει δικαίωμα take στο αντικείμενο p και το αντικείμενο O να έχει δικαίωμα r στο p.

Από τις εντολές αυτές οι grant και take ανήκουν και στο

σύνολο r, αποτελώντας δικαιώματα. Δυο πολύ σημαντικές παρατηρήσεις, που αφορούν την αξιοπιστία του προτύπου αυτού είναι οι εξής :

α) Ενας χρήστης είναι δυνατόν να μοιρασθεί ένα αντικείμενο, με έναν άλλο χρήστη, αν ισχύουν αθροιστικά οι εξής προυποθέσεις :

- αν υπάρχουν άλλοι χρήστες οι οποίοι διαθέτουν συνολικά, τα απαιτούμενα δικαιώματα πρόσβασης στο αντικείμενο
- αν ο πρώτος χρήστης είναι συνδεδεμένος με καθέναν από τους άλλους χρήστες

Υπάρχει μάλιστα αλγόριθμος ο οποίος μπορεί να υπολογίσει τη δυνατότητα από κοινού κατοχής ενός αντικειμένου μεταξύ κάποιων χρηστών. Ο υπολογισμός αυτός γίνεται σε χρόνο ανάλογο του μεγέθους του γράφου που σχηματίζεται από τη διασύνδεση των χρηστών αυτών.

β) Ενας χρήστης μπορεί - χωρίς να δικαιούται - να αφαιρέσει το δικαίωμα πρόσβασης ενός άλλου χρήστη σε κάποιο αντικείμενο, σε ορισμένες ακραίες περιπτώσεις. Και σε αυτήν την περίπτωση υπάρχει αλγόριθμος, ο οποίος μπορεί να εκτιμήσει την πιθανότητα αυτή με ακρίβεια.

Βασικό πλεονέκτημα του προτύπου 4Δ είναι ότι εντοπίζει τις προυποθέσεις εκείνες υπό τις οποίες ένας χρήστης μπορεί να προσπελάσει ένα αντικείμενο. Ετσι το πρότυπο είναι ιδιαίτερα χρήσιμο σε λειτουργικά συστήματα όπου απαιτείται ελεγχόμενη πρόσβαση σε από κοινού χρησιμοποιούμενες πληροφορίες.

# ΜΕΘΟΔΟΙ-ΣΧΕΔΙΑΣΗΣ ΑΣΦΑΛΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

## Βασικές διαπιστώσεις

Τα λειτουργικά συστήματα γενικά παρουσιάζουν σημαντική δυσκολία στο σχεδιασμό τους. Αυτό οφείλεται στο πλήθος των καθηκόντων που έχουν να εκτελέσουν, στην πληθώρα των διαχειριζόμενων διακοπών και μεταστροφών. Η διαχείριση των λειτουργιών αυτών πρέπει να γίνεται κατά τρόπο που να ελαχιστοποιεί το λειτουργικό κόστος του συστήματος.

Η μετάθεση της ευθύνης για την ασφαλή λειτουργία ενός πληροφοριακού συστήματος στο λειτουργικό σύστημα που το καθοδηγεί έχει ως αποτέλεσμα ακόμη μεγαλύτερη δυσκολία στη σχεδίασή του.

Ενα λειτουργικό σύστημα μπορεί είτε να σχεδιασθεί εξ'αρχής με βάση μια συγκεκριμένη μεθοδολογία και έτσι να καταστεί ασφαλές είτε να πλαισιωθεί - μετά τη σχεδίασή του από ορισμένους μηχανισμούς οι οποίοι το καθιστούν ασφαλές.

Αν επιλεγεί η πρώτη προσέγγιση, τότε το σχεδιαζόμενο λειτουργικό σύστημα πρέπει να καλύπτει το εξής πλαίσιο βασικών αρχών ασφαλούς σχεδίασης :

α) Αρχή της ελάχιστης από κοινού χρήσης.

Τα αντικείμενα που χρησιμοποιούνται από κοινού από πολλούς χρήστες μπορούν να αποτελέσουν φυσικά μέσα για τη

διαρροή διαβαθμισμένων δεδομένων. Το λειτουργικό σύστημα πρέπει να εμποδίζει τυχόν διαρροές.

β) Αρχή των ελαχίστων προνομίων.

Κάθε χρήστης πρέπει να διατηρεί τα ελάχιστα προνόμια, ώστε να ελαχιστοποιούνται, οι πιθανές αρνητικές συνέπειες από μια ενέργειά του.

γ) Αρχή της απλότητας

Οι τεχνικές εξασφάλισης που χρησιμοποιούνται πρέπει να είναι απλές, να υλοποιούνται εύκολα και να είναι φιλικές στους χρήστες.

δ) Αρχή του ανοικτού σχεδιασμού

Η ισχύς των μηχανισμών προστασίας δεν πρέπει να στηρίζεται στην άγνοια των χρηστών, τη σχετική με τις τεχνικές ασφάλειας που χρησιμοποιούνται, αλλά στην αποτελεσματική σχεδίαση των τεχνικών αυτών.

ε) Διαχωρισμός προνομίων

Αν η πρόσβαση του συστήματος πρέπει να βασίζεται στα διακεκριμένα προνόμια που οφείλει να διαθέτει κάθε χρήστης και τα οποία τον διαφοροποιούν από τους άλλους χρήστες.

στ) Αρχή της άρνησης προσπέλασης

Κάθε χρήστης πρέπει να μη διαθέτει δυνατότητα πρόσβασης σε ένα αντικείμενο του συστήματος εκτός αν καθορισθεί διαφορετικά.

## ΙΔΙΟΤΗΤΕΣ ΣΥΣΤΗΜΑΤΩΝ ΠΟΛΥΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ

Κάθε λειτουργικό σύστημα που διαθέτει δυνατότητες πολυ-προγραμματισμού εκτελεί πολλές λειτουργίες που σχετίζονται με την ασφάλειά του. Οι βασικότερες είναι :

1. Αυθεντικοποίηση των χρηστών

Το λειτουργικό σύστημα πρέπει να ταυτοποιεί θετικά κάθε χρήστη που ζητά άδεια προσπέλασης στο σύστημα.

2. Προστασία της μνήμης

Τα προγράμματα των χρηστών πρέπει να κάνουν χρήση περιοχών μνήμης που προστατεύονται από προσπέλαση από άλλους χρήστες.

3. Καταμερισμός και έλεγχος πρόσβασης

Μηχανισμοί του λειτουργικού συστήματος όπως ο συγχρονι-σμός και η συνεξέλιξη που διατίθενται στους χρήστες, πρέπει να ελέγχονται ώστε να μην προκαλούν αρνητικές επιπτώσεις σε άλλους χρήστες.

4. Υλοποίηση της από κοινού χρήσης δεδομένων

Οι μηχανισμοί του λειτουργικού συστήματος πρέπει να εξασφαλίσουν την ακεραιότητα των αντικειμένων του, ιδιαίτερα όταν αυτά χρησιμοποιούνται από πολλούς χρήστες.

5. Αποτελεσματική παροχή υπηρεσιών

Το λειτουργικό σύστημα πρέπει να εξασφαλίσει, ότι δεν υπάρχει χρήστης του οποίου η αίτηση για εξυπηρέτηση θα είναι διαρκώς τελευταίας προτεραιότητας.

Για την εξασφάλιση αυτή απαιτείται σωστή σχεδίαση των τεχνικών χρονοπρογραμματισμού.

6. Διαδιεργασιακή επικοινωνία και συγχρονισμός

Το λειτουργικό σύστημα πρέπει να εξασφαλίζει ότι οι εκτελούμενες διεργασίες έχουν τη δυνατότητα να επικοινωνούν και να συγχρονίζονται μεταξύ τους, με σκοπό τη βέλτιστη χρήση των πόρων του συστήματος.

## ΜΕΘΟΔΟΙ ΣΧΕΔΙΑΣΗΣ ΑΣΦΑΛΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

α) Μέθοδος του διαχωρισμού

Οπως έχουμε αναφέρει προηγουμένως υπάρχουν τέσσερις τρόποι για το διαχωρισμό των αντικειμένων του λειτουργικού συστήματος (φυσικός, προσωρινός, κρυπτογραφικός και λογικός).

Ενα λειτουργικό σύστημα που σχεδιάζεται για να είναι ασφαλές πρέπει να έχει τη δυνατότητα να υλοποιήσει και τα τέσσερα αυτά είδη διαχωρισμού. Αν μάλιστα είναι σύστημα πολυπρογραμματισμού τότε πρέπει απαραίτητα να απομονώνει κάθε χρήστη από όλους τους άλλους, επιτρέποντας μόνον ελεγχόμενες αλληλεπιδράσεις.

Στα περισσότερα λειτουργικά συστήματα η εντύπωση που δίνεται στους χρήστες είναι ότι τα προγράμματα του λειτουργικού συστήματος απαντώνται μια φορά στη μνήμη και το αντίγραφό τους αυτό χρησιμοποιείται από κοινού από όλους τους

χρήστες.

Η εντύπωση αυτή είναι διαφορετική στα λειτουργικά συστήματα που διαθέτουν δυνατότητες δημιουργίας πολλαπλών ιδεατών χώρων μνήμης. Στα συστήματα αυτά κάθε χρήστης έχει την εντύπωση ότι διαθέτει για αποκλειστική του χρήση ένα αντίγραφο του λειτουργικού συστήματος.

Το βασικό πλεονέκτημα της μεθόδου πολλαπλών ιδεατών χώρων μνήμης είναι η αποτελεσματικότητα στη διαχείριση της μνήμης. Ο χώρος που μπορεί να χρησιμοποιηθεί από κάθε χρήστη ισούται με το μέγιστο χώρο της μνήμης.

Αλλο πλεονέκτημα είναι η προστασία που μπορεί να παρέχεται στους χρήστες δεδομένου ότι στο χώρο που χρησιμοποιεί καθένας από αυτούς περιέχεται το λειτουργικό σύστημα, αλλά δεν περιέχεται χώρος άλλων χρηστών.

Μειονέκτημα της μεθόδου αυτής είναι ότι αφού χρησιμοποιείται το ίδιο αντίγραφο του λειτουργικού συστήματος από όλους τους χρήστες, τότε αν μεταβληθεί ένα πρόγραμμα του συστήματος από κάποιον από αυτούς, θα υπάρχουν επιπτώσεις για όλους τους υπόλοιπους που θα το χρησιμοποιήσουν.

β) Μέθοδος του πυρήνα ασφαλείας

Με τον όρο πυρήνα εννοούμε το τμήμα του λειτουργικού συστήματος το οποίο εκτελεί τις πιο θεμελιώδεις λειτουργίες του. Τέτοιες λειτουργίες είναι ο συγχρονισμός των διεργασιών, η επικοινωνία μεταξύ τους και η διαχείριση των διακοπών.

Ο πυρήνας ασφαλείας είναι ένα επιμέρους τμήμα του πυρήνα

του λειτουργικού συστήματος, το οποίο είναι επιφορτισμένο με την ευθύνη της υλοποίησης των τεχνικών εξασφάλισης όλων των αντικειμένων του λειτουργικού συστήματος.

Οι τεχνικές εξασφάλισης των αντικειμένων του λειτουργικού συστήματος είναι σκόπιμο να περιέχονται σε έναν πυρήνα ασφαλείας, γιατί με τον τρόπο αυτό πετυχαίνουμε μερικά πολύ σημαντικά πλεονεκτήματα όπως :

α) Διαχωρισμός των λειτουργιών ασφαλείας από τις άλλες λειτουργίες του συστήματος άρα περιορισμός στην αλληλεπίδρασή τους.

β) Ομοιομορφία στην εκτέλεσή τους μια και καθοδηγούνται από μια κεντρική διαδικασία.

γ) Ευκολία τροποποίησης λόγω της συγκέντρωσής τους σε ένα καθορισμένο σημείο.

δ) Συνεκτικότητα δεδομένου ότι ο πυρήνας ασφαλείας υπάρχει μόνο για ένα συγκεκριμένο λόγο και είναι απλό να διατηρηθεί όσο περιορισμένος επιθυμεί ο σχεδιαστής του.

ε) Επαληθευσιμότητα ότι εκτελούνται οι έλεγχοι που πρέπει, δεδομένης της ευκολίας στον αυστηρό έλεγχο των δυνατοτήτων του πυρήνα.

στ) Κεντρικός συντονισμός δεδομένου ότι κάθε λειτουργία ασφαλείας εκτελείται ή καθοδηγείται οπωσδήποτε από τον πυρήνα.

Από την άλλη πλευρά εκτός από τα πλεονεκτήματα παρουσιάζονται και κάποια μειονεκτήματα όπως :

α) Η κάποια πολυπλοκότητα που εισάγεται για τη σχεδίαση ενός λειτουργικού συστήματος που διαθέτει πυρήνα ασφαλείας.

β) Η σχεδίαση πυρήνα ασφαλείας δεν εξασφαλίζει από μόνη της ότι ο πυρήνας αυτός περιέχει όλες τις απαιτούμενες τεχνικές εξασφάλισης ούτε ότι όσες τεχνικές περιέχει είναι σωστά σχεδιασμένες.

γ) Σε πολλές περιπτώσεις η σχεδίαση ενός αποτελέσματικού πυρήνα ασφαλείας οδηγεί σε σημαντική αύξηση του μεγέθους του πυρήνα ασφαλείας καθοδηγεί και ελέγχει τις εξής βασικές λειτουργίες:

1. Συντονισμός ενεργοποίησης διαδικασιών.

   Ο πυρήνας ασφαλείας δίνει τον έλεγχο από μια διαδικασία σε άλλη, ενεργοποιεί καταστάσεις ελέγχου, προσπέλασης, ελέγχει την διαχείριση του περιεχομένου των καταχωρητών, κ.λ.π.

2. Κλήση των πεδίων διεργασίας

   Ο πυρήνας ασφαλείας καθοδηγεί την κλήση των πεδίων μιάς καλούμενης διεργασίας, προκειμένου να βεβαιωθεί ότι η καλούσα εκτελείται χωρίς να αποκτά πρόσβαση σε δεδομένα που δε δικαιούται.

3. Ο έλεγχος διαδικασιών Ε/Ε

   Ο πυρήνας ασφαλείας μπορεί να χρησιμοποιηθεί ώστε ο έλεγχος του λογισμικού να επεκταθεί και σε έλεγχο επί των συσκευών Ε/Ε.

Η σχεδίαση ενός πυρήνα ασφαλείας μπορεί, είτε να συνοδεύσει τη σχεδίαση του πυρήνα του λειτουργικού συστήματος, είτε να προηγηθεί και να αποτελέσει τη βάση για τη σχεδίαση ολόκληρου του λειτουργικού συστήματος.

Η πρώτη προσέγγιση συμβαίνει συνήθως σε λειτουργικά συστήματα που βρίσκονται σε λειτουργία, αλλά οι σχεδιαστές τους επιθυμούν την αναβάθμιση των παρεχόμενων τεχνικών εξασφάλισής τους. Σε αυτήν όμως την περίπτωση δεν είναι πάντα δυνατή η συγκέντρωση όλων των λειτουργιών ασφαλείας σε έναν πυρήνα, γιατί με τον τρόπο αυτό μπορεί να καταστραφεί η τμηματικότητα του υπάρχοντος λειτουργικού συστήματος.

Η δεύτερη προσέγγιση στηρίζεται στη σχεδίαση πρώτα του πυρήνα ασφαλείας και κατόπιν των υπόλοιπων συστατικών του λειτουργικού συστήματος. Με τον τρόπο αυτό είναι δυνατή η σχεδίαση πολύ ασφαλών λειτουργικών συστημάτων γύρω από τον πυρήνα ασφαλείας τους.

Σε ένα λειτουργικό σύστημα που διαθέτει πυρήνα ασφαλείας διακρίνονται τέσσερα πεδία επεξεργασιών, το υλικό, ο πυρήνας ασφαλείας, το λειτουργικό σύστημα και οι χρήστες.

Καθένα από τα πεδία αυτά είναι δυνατόν να υποδιαιρείται σε επιμέρους υποπεδία ή φλοιούς. Καθένας από τους φλοιούς αυτούς μπορεί να περιέχει ορισμένες τεχνικές ασφαλείας, είτε ανήκει στον πυρήνα ασφαλείας, είτε όχι.

Για παράδειγμα η αυθεντικοποίηση μπορεί να υλοποιηθεί σε ένα φλοιό εκτός του πυρήνα, ο οποίος έχει κατάλληλα ελεγχθεί για την αξιοπιστία του.

# ΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ DOS

## Γενικά στοιχεία

Ενα από τα πιο δημοφιλή λειτουργικά συστήματα που υπάρχουν σήμερα είναι το DOS (Disk Operating System) γνωστό είτε ως MS - DOS είτε ως PC - DOS.

## Η ΙΣΤΟΡΙΑ ΤΟΥ DOS

Το 1980 η Seattle Computer Products παραχώρησε τα δικαιώματα του λειτουργικού συστήματος 86 - DOS στην εταιρεία Microsoft. Η Microsoft το επεξεργάστηκε και το επανέκδοσε με το όνομα MS - DOS (Microsoft Disk Operating System).

Την ίδια περίοδο το πιο διαδεδομένο λειτουργικό σύστημα για υπολογιστές με μικροεπεξεργαστές των 8 bits ήταν το CP/M της Digital Research. Το 86 - DOS έμοιαζε πολύ με το CP/M. Η ομοιότητά τους εξασφάλιζε τη συμβατότητα των υπολογιστών που χρησιμοποιούσαν οποιαδήποτε από αυτά. Ετσι προγράμματα που εκτελούνταν υπό την εποπτεία του ενός συστήματος, μπορούσαν να εκτελεσθούν και υπό την εποπτεία του άλλου.

Η βασική διαφορά μεταξύ του CP/M και του 86 - DOS εντοπιζόταν στην αρχιτεκτονική των επεξεργαστών που χρησιμοποιούσαν. Ενώ το CP/M χρησιμοποιούσε επεξεργαστές των 8 bits το 86 - DOS έκανε χρήση των επεξεργαστών (16 bits) 8086 και 8088 της INTEL.

Είναι σημαντικό να τονίσουμε στο σημείο αυτό, ότι η επιλογή των επεξεργαστών INTEL και 8086/8088 των 16 bits, αντί του INTEL 8080 των 8 bits, αποτέλεσε μια κρίσιμη απόφαση των σχεδιαστών της IBM P.C.

Στις μέρες μας είναι φανερό ότι οι περιορισμένες δυνατότητες του INTEL 8080 θα αποτελούσαν ανασταλτικό παράγοντα στη διάδοση των προσωπικών υπολογιστών.

Η επιλογή μεταξύ του INTEL 8086 και 8088 έχει αρκετό ενδιαφέρον. Ο 8086 ως επεξεργαστής των 16 bits έπρεπε να συνεργάζεται εξωτερικά με εξαρτήματα που μπορούσαν να διαχειρισθούν 16 bits δεδομένων. Τον καιρό όμως που κατασκευάστηκε ο IBM PC υπήρχαν ελάχιστα και πολύ ακριβά τέτοια εξαρτήματα, σε αντίθεση με την αφθονία εξαρτημάτων των 8 bits.

Το πρόβλημα αντιμετωπίστηκε με τη σχεδίαση του INTEL 8088.

Ο επεξεργαστής αυτός έχει εσωτερικά όλες τις δυνατότητες ενός επεξεργαστή των 16 bits. Το σημαντικό χαρακτηριστικό του όμως είναι ότι μπορεί και συνεργάζεται με εξωτερικά εξαρτήματα των 8 bits.

Ο INTEL 8088 αποτέλεσε έναν επεξεργαστή "με ισχύ 16 bits και οικονομία 8 bits". Χρησιμοποιήθηκε στην κατασκευή των PC, XT, PORTABLE PC, καθώς και του PC Junior.

Τον επεξεργαστή αυτόν ακολούθησαν οι επεξεργαστές 80186, 80188, 80286, 80386, 80486, αλλά και άλλοι που βρίσκονται στο δρόμο από τα εργαστήρια προς την παραγωγή.

Τον Οκτώβριο του 1980 η IBM αναζητούσε λειτουργικό σύστημα για τον νέο υπολογιστή που κατασκεύαζε. Ο B. Gates ιδρυτής της Microsoft πρόσφερε το 86 - DOS με την ονομασία MS - DOS. Οταν ανακοινώθηκε ο πρώτος IBM - PC στα μέσα του 1981 η IBM τον συνόδευσε με το λειτουργικό σύστημα MS - DOS.

Ενα χρόνο μετά το φθινόπωρο του 1982 ανακοινώθηκε μια βελτιωμένη έκδοση του IBM PC εγκαινιάζοντας έναν αγώνα δρόμου μεταξύ των προσωπικών υπολογιστών της IBM και των συμβατών με αυτούς. Ολες οι εκδόσεις που ακολούθησαν από τότε είναι προσθήκες σε αυτήν την βασική φιλοσοφία.

## ΓΕΝΕΑΛΟΓΙΑ ΤΟΥ DOS

Κατά τη διάρκεια της σύντομης αλλά εξαιρετικά πετυχημένης καριέρας του, το DOS εξελίχθηκε διαμέσου τεσσάρων εκδόσεων. Ο πρώτος αριθμός που χαρακτηρίζει κάθε έκδοση, γνωστός σαν Version Number αλλάζει κάθε φορά που υπάρχει μια σημαντική επέκταση.

Ο δεύτερος αριθμός γνωστός σαν Release Number αλλάζει κάθε φορά που επιφέρονται μικρότερης κλίμακας διορθώσεις.

## ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Το DOS είναι ένα απλό, προσιτό στον άπειρο χρήστη και σχετικά φιλικό λειτουργικό σύστημα. Δεν παρέχει δυνατότητες πολυπρογραμματισμού και πολυεπεξεργασίας, αλλά στοχεύει στην κάλυψη των αναγκών κάποιου χρήστη με μεσαίες απαιτήσεις.

Στην εξέλιξή του όμως πλαισιώθηκε με βοηθητικά προγράμματα που αναβάθμισαν σε σημαντικό βαθμό τις δυνατότητές του.

Βασικό χαρακτηριστικό του MS - DOS είναι η δυνατότητα ελέγχου ενός ή περισσοτέρων μαγνητικών μέσων (δισκετών, δίσκων κ.ά) που λειτουργούν υπό τον έλεγχο των επεξεργαστών INTEL 8086 και 8088.

Το MS - DOS χρησιμοποιεί κατά τη λειτουργία του υπολογιστή, περίπου 32 KB κύριας μνήμης και πραγματοποιεί μεταξύ άλλων και τις εξής ενέργειες :

- Εγγραφή της ημερομηνίας και ώρας της τελευταίας αλλαγής ενός αρχείου
- Χωρισμός του δίσκου σε τμήματα
- Αυτόματη εκτέλεση μιάς σειράς επιλεγμένων εντολών
- Ελεγχος της πιστότητας της αποθήκευσης και ανακατασκευή ενός αρχείου όταν κάποια τμήματα του μέσου όπου είναι αποθηκευμένο έχουν κατατραφεί
- Δημιουργία σειράς αρχείων για επεξεργασία με περιφερειακές συσκευές.

## ΕΣΩΤΕΡΙΚΗ ΔΙΑΡΘΡΩΣΗ ΤΟΥ DOS

Το DOS αποτελείται από τρια βασικά μέρη :

α) τον επεξεργαστή εντολών

β) τον πυρήνα

γ) το βασικό σύστημα εισόδου - εξόδου

Ο επεξεργαστής εντολών είναι το τμήμα του λειτουργικού συστήματος που είναι υπεύθυνο για τη διαχείριση των εντολών που απευθύνονται στο σύστημα. Η ευέλικτη αρχιτεκτονική του DOS επιτρέπει την εναλλακτική χρησιμοποίηση διαφόρων επεξεργαστών εντολών. Ο επεξεργαστής εντολών που περιέχεται στο MS - DOS ονομάζεται COMMAND.COM και αποτελείται από τρια τμήματα.

Τα τμήματα αυτά φορτώνονται στη μνήμη κατά την εκκίνηση του υπολογιστή.

Τα τμήματα αυτά είναι τα εξής :

i) Το τμήμα εκκίνησης, με το οποίο εκτελείται το αρχείο εντολών AUTOEXEX.BAT

ii) Το μόνιμο τμήμα που διατηρείται μόνιμα στην κύρια μνήμη και περιλαμβάνει όλες εκείνες τις λειτουργίες που το DOS πρέπει να μπορεί να εκτελεί αμέσως. Το τμήμα αυτό περιλαμβάνει και όλα τα χρήσιμα μηνύματα για την ενημέρωση του χρήστη σχετικά με την εκτέλεση ενός προγράμματος.

iii) Το τρίτο τμήμα είναι το Μεταβατικό τμήμα το οποίο μπορεί να παραχωρεί εν μέρει ή συνολικά τη θέση του σε προγράμματα που χρησιμοποιούν μεγάλο χώρο μνήμης.

Ο πυρήνας του DOS είναι το τμήμα του λειτουργικού συστήματος που είναι υπεύθυνο για τη διαχείριση των αρχείων και των ευρετηρίων του, καθώς και για τη διασύνδεση των διαφόρων εφαρμογών και βοηθητικών προγραμμάτων του DOS.

Ο πυρήνας φορτώνεται στη μνήμη από το μαγνητικό μέσο όπου τηρείται, την πρώτη φορά που φορτώνεται το DOS διαμέσου του κρυφού αρχείου MS - DOS. SYS.

Το BIOS (Basic Input Output System) είναι το τμήμα του DOS που βρίσκεται στη ROM του υπολογιστή και το οποίο ρυθμίζει τις διαδικασίες εισόδου και εξόδου σημάτων δηλαδή των πληροφοριών από και προς το σύστημα.

Η ROM του συστήματος αρχίζει από τη διεύθυνση F000:0000 εκεί βρίσκεται και το BIOS. Ο υπολογιστής ξεκινά πάντοτε από τη διεύθυνση αυτή, γιατί εκεί βρίσκονται τα προγράμματα που επιτρέπουν στο λειτουργικό σύστημα να ενεργοποιηθεί.

Η οικογένεια των επεξεργαστών 8086/8088 στους οποίους απευθύνεται το MS - DOS διαθέτει καταχωρητές των 16 δυαδικών ψηφίων (bits). Κάθε καταχωρητής καταλαμβάνει χώρο δυο bytes, καθένα από τα οποία αποτελείται από 8 δυαδικά ψηφία.

Οι καταχωρητές που χρησιμοποιούνται από το DOS χωρίζονται σε πέντε κατηγορίες :

1. Γενικοί καταχωρητές
2. Δείκτες

3. INDEX
4. Καταχωρητές τμήματος
5. Καταχωρητές κατάστασης

## ΕΝΤΟΛΕΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ DOS

Οι κατασκευαστές του DOS, θέλοντας να δημιουργήσουν ένα ευέλικτο και απλό λειτουργικό σύστημα, δεν έδωσαν ιδιαίτερο βάρος στην ασφάλεια του. Μια επιφανειακή εξέταση του DOS δείχνει ότι ο χρήστης δε μπορεί να προστατευθεί με άλλον τρόπο εκτός από το χαρακτηρισμό των αρχείων και τη λήψη εφεδρικών αντιγράφων.

Ο χρήστης του DOS είναι εκτεθειμένος σε πολλούς κινδύνους ακόμη και από τις ίδιες τις εντολές του (DELETE, ERASE, FORMAT, κ.λ.π). Τυχόν λανθασμένη χρήση για παράδειγμα των εντολών του DOS που μεταβάλλουν τα περιεχόμενα των μαγνητικών μέσων αποθήκευσης (FORMAT), μπορεί να έχει καταστροφικά αποτελέσματα.

Ωστόσο το DOS παρέχει πολύ περισσότερες δυνατότητες στο χρήστη που γνωρίζει να αξιοποιήσει τη φιλοσοφία των διακοπών και των κλήσεων λειτουργιών για να δημιουργήσει ένα ασφαλέστερο περιβάλλον.

Συνεπώς η μελέτη της ασφάλειας του DOS μπορεί να γίνει σε δυο επίπεδα. Στο επίπεδο του απλού χρήστη με την παράθεση

και περιγραφή των στοιχειωδών εντολών εξασφάλισής του και στο επίπεδο του καταρτισμένου χρήστη με την ανάλυση των κρίσιμων διακοπών και λειτουργιών του.

## ΑΝΑΤΟΜΙΑ ΜΙΑΣ ΔΙΣΚΕΤΑΣ

Οι μαγνητικές δισκέτες αποτελούν ένα από τα φθηνότερα και πιο διαδεδομένα μαγνητικά μέσα αποθήκευσης δεδομένων. Το γεγονός ότι είναι φορητές και ανθεκτικές σε ένα μεγάλο εύρος θερμοκρασιών, τις καθιστά εύχρηστες στους χρήστες προσωπικών υπολογιστών. Κατασκευάζεται από εύκαμπτο πλαστικό σχήματος δίσκου, επιστρωμένο με κατάλληλο μαγνητικό υλικό. Ο δίσκος αυτός περικλείεται από πλαστικό περίβλημα, αφού πρώτα επεξεργασθεί κατά τρόπο που τον καθιστά ανθεκτικό στο στατικό ηλεκτρισμό.

Στο κέντρο του δίσκου υπάρχει άνοιγμα κυκλικού σχήματος. Μεταξύ του ανοίγματος αυτού και της δισκέτας υπάρχει ένας προστατευτικός δακτύλιος που οριοθετεί το τέλος του μαγνητικού υλικού.

Το άνοιγμα αυτό χρησιμοποιείται για την περιστροφή της δισκέτας περί τον άξονα της από τον οδηγό.

Στο κέντρο και στο κάτω μέρος της δισκέτας υπάρχει άνοιγμα ελλειπτικού σχήματος το οποίο αποκαλύπτει μέρος της μαγνητικής επίστρωσης της δισκέτας.

## ΤΟΠΟΛΟΓΙΑ ΕΝΟΣ DOS ΜΑΓΝΗΤΙΚΟΥ ΜΕΣΟΥ

Ενα μαγνητικό μέσο που πρόκειται να χρησιμοποιηθεί υπό τον έλεγχο του λειτουργικού συστήματος DOS μπορεί να έχει δυο μορφές. μπορεί να αποτελεί :

- την κύρια μνήμη του υπολογιστικού συστήματος
- τη βοηθητική μνήμη του υπολογιστικού συστήματος (δισκέτα, δίσκος κ.λ.π)

Η κύρια μνήμη του υπολογιστικού συστήματος χρησιμοποιείται ως ο "πάγκος εργασίας" του λειτουργικού συστήματος. Κατά την έναρξη της λειτουργίας του υπολογιστικού συστήματος τα περιεχόμενά της κατανέμονται σύμφωνα με συγκεκριμένη διάταξη, ως εξής :

α) Πίνακας διακοπών

β) Περιοχή όπου αποθηκεύονται δεδομένα του ROM - BIOS

γ) Περιοχή όπου αποθηκεύονται τα δεδομένα του λειτουργικού συστήματος

δ) Περιοχή όπου αποθηκεύεται ο κωδικός χαμηλού επιπέδου του BIOS

ε) Περιοχή των χειριστών των διακοπών του DOS

στ) Περιοχή των βοηθητικών μνημών

ζ) Περιοχή του COMMAND.COM

η) Περιοχή TSR προγραμμάτων

θ) Περιοχή εκτελέσιμων προγραμμάτων

ι) Περιοχή του αρχείου (κινητού) COMMAND.COM

κ) Περιοχή των καρτών γραφικών

λ) Πίνακας εξωτερικού κώδικα ROM

μ) Περιοχή πίνακα τμημάτων της A.T ROM

ν) Περιοχή της BASIC

ξ) Περιοχη του ROM - BIOS

Ο) Εντολή JMP

π) Ημερομηνία δημιουργίας του BIOS

ρ) Κωδικός ταυτοποίησης του IBM PC

## ΤΟΠΟΛΟΓΙΑ ΕΝΟΣ DOS ΜΑΓΝΗΤΙΚΟΥ ΜΕΣΟΥ

Μια δισκέτα ή η DOS διαμέριση (partition) ενός δίσκου περιέχουν δεδομένα με την εξής δομή :

α) Τομέας εκκίνησης (boot sector) του μέσου και φυλασσόμενοι (reserved) τομείς

β) Πίνακας κατανομής αρχείων (File Allocation Table - FAT)

γ) Αντίγραφο του FAT (η ύπαρξή του είναι προαιρετική και δε χρησιμοποιείται σε δίσκους RAM)

δ) Ευρετήριο των αρχείων του μέσου σε επίπεδο ρίζας (root directory).

ε) Περιοχή δεδομένων αρχείων προγραμμάτων κ.λ.π

Καθένα από τα τμήματα αυτά έχει μεταβαλλόμενο μέγεθος.

Τα δεδομένα που περιέχονται στα τρία πρώτα τμήματα είναι κρίσιμα για τη λειτουργία του υπολογιστικού συστήματος. Ενα ακόμη κρίσιμο σημείο του μαγνητικού μέσου είναι ο χώρος όπου αποθηκεύεται ο πίνακας διαμέρισής του (partition table).

## ΤΟΜΕΑΣ ΕΚΚΙΝΗΣΗΣ

Ο τομέας εκκίνησης ενός Dos μαγνητικού μέσου περιέχει τα εξής δεδομένα :

1) Μια εντολή JMP στην πρώτη εντολή του κώδικα εκκίνησης του λειτουργικού συστήματος (3 bytes)
2) Το όνομα της εταιρείας που κατασκεύασε το λειτουργικό σύστημα καθώς και η συγκεκριμένη έκδοση του (8 bytes)
3) Τον αριθμό των bytes ανά τομέα (2 bytes)
4) Τον αριθμό των τομέων ανά δεσμίδα (cluster) (1 byte)
5) Τον αριθμό των φυλασσόμενων τομέων, όσων δηλ. υπάρχουν πριν τον πρώτο FAT (2 bytes)
6) Τον αριθμό των FAT (1 byte)
7) Τον μέγιστο αριθμό αρχείων που ανήκουν στο ευρετήριο σε επίπεδο ρίζας, (2 bytes). Για κάθε τέτοιο αρχείο τηρείται χώρος 32 bytes.
8) Το πλήθος των τομέων που χρησιμοποιούνται από το Dos (2 bytes)

9) Ενα χαρακτηριστικό του μαγνητικού μέσου (1 byte)

10) Το πλήθος των κεφαλών ανάγνωσης εγγραφών (2 bytes)

11) Το πλήθος των τομέων ανά αυλάκι (2 bytes)

12) Το πλήθος των κρυμμένων (hidden) τομέων (2 bytes)

13) Το μέγεθος του τομέα εκκίνησης

14) Τον πραγματικό κώδικα εκκίνησης

15) Το πλήθος των τομέων που καλύπτουν ένα FAT (2 bytes)

Από αυτά τα δεδομένα το τρίτο ως το 10ο αποτελούν το σύνολο των παραμέτρων του BIOS και χρησιμοποιούνται για τον ορισμό οδηγών συσκευών.

Το χαρακτηριστικό του μαγνητικού μέσου (media descriptor) έχει ξεχωριστό ενδιαφέρον μια και αποτελεί το πρώτο byte και του FAT. Αποτελείται από 1 byte και οι πληροφορίες που παρέχει εξαρτώνται από τα τρία τελευταία δυαδικά ψηφία του byte αυτού.

Ο πίνακας κατανομής αρχείων είναι μια συνδεδεμένη λίστα (linked list) που χρησιμοποιείται από το Dos προκειμένου να εντοπίζεται η φυσική θέση κάθε αρχείου στο μαγνητικό μέσο και να υπολογίζεται ο ελεύθερος χώρος που απομένει στο μέσο αυτό.

Το 1ο byte της FAT είναι το χαρακτηριστικό του μαγνητικού μέσου που περιγράφηκε πιο πάνω. Τα επόμενα 5 ή 7 bytes έχουν την τιμή offH. Ο υπόλοιπος χώρος αποτελείται από κελιά (cells) που περιέχουν κυκλοφορίες που αφορούν κάθε δεσμίδα του δίσκου.

Οι πληροφορίες που τηρούνται στο FAT για κάθε αρχείο αποτελούν την είσοδο του αρχείου και απαρτίζονται από :

α) Το όνομα του αρχείου

β) Την επέκτασή του

γ) Το χαρακτηριστικό του

δ) Μια φυλασσόμενη περιοχή

ε) Την ώρα δημιουργίας του

στ) Την ημέρα δημιουργίας του

ζ) Τον αριθμό της δεσμίδας από όπου αρχίζει το αρχείο

η) Το μέγεθός του

η περιοχή FAT μπορεί να αναγνωρισθεί μέσω της διακοπής INT 25H CDX = 1 ή με τη βοήθεια εξειδικευμένων βοηθητικών προγραμμάτων.

Ο χώρος που διαθέτει ένα μαγνητικό μέσο (δίσκος) μπορεί να κατανεμηθεί σε τμήματα τα οποία λογικά είναι απομονωμένα μεταξύ τους. Αυτό σημαίνει ότι δεν είναι δυνατή η επικοινωνία μεταξύ των περιεχομένων δυο διαφορετικών τμημάτων ακόμη και αν οι δυο διαμερίσεις ελέγχονται από το ίδιο λειτουργικό σύστημα.

Ο πρώτος τομέας του μαγνητικού δίσκου περιέχει τη βασική εγγραφή εκκίνησης. Το τελευταίο μέρος του τομέα αυτού περιέχει τον πίνακα διαμέρισης του δίσκου με τη μορφή του πίνακα 4 θέσεων. Η διαχείριση του πίνακα διαμέρισης γίνεται από το πρόγραμμα FDISK του λειτουργικού συστήματος.

Κάθε μια θέση του πίνακα διαμέρισης περιέχει τα εξής δεδομένα :

1) Σημαία εκκίνησης. Αν είναι 0 τότε η διαμέριση δεν είναι ενεργή, αλλοιώς είναι ενεργή.
2) Συντεταγμένες της αρχής της διαμέρισης, οι συντεταγμένες αυτές αποτελούνται από την κεφαλή τομέα και αυλάκι που υποδεικνύει την αρχή εκκίνησης.
3) Κωδικοί λειτουργικού συστήματος. Αν είναι 0 τότε το λειτουργικό σύστημα είναι άγνωστο, αλλοιώς είναι το Dos.
4) Συντεταγμένες του τέλους διαμέρισης.
5) Ο αριθμός του σχετικού τομέα εκκίνησης.

Οι διαμερίσεις αρχίζουν σε αυλάκι με άρτιο αριθμό εκτός της πρώτης η οποία μπορεί να αρχίζει στο αυλάκι 0, τομέα 2.

## ΧΑΡΑΚΤΗΡΙΣΜΟΙ ΑΡΧΕΙΩΝ - ΕΝΤΟΛΕΣ ALTER, CHKDSK

Ο χαρακτηρισμός των αρχείων μπορεί να δοθεί είτε από το ίδιο το λειτουργικό σύστημα, είτε από το χρήστη. Αυτό γίνεται με τη χρήση μιας σημαίας, μήκους ενός byte. Κάθε δυαδικό ψηφίο του byte αυτού, αν ισούται με το 1 αποδίδει στο αρχείο κάποιο χαρακτηρισμό.

Συγκεκριμένα, το πρώτο από δεξιά δυαδικό ψηφίο χρησιμοποιείται για να χαρακτηρίσει το αρχείο ως Read - only, το δεύτερο για να το χαρακτηρίσει HIDDEN και το τρίτο για να το χαρακτηρίσει SYSTEM. Το τέταρτο bit χρησιμοποιείται ως είσο-

δος της ετικέτας του μέσου, το πέμπτο ως είσοδος υποευρετηρίου και το έκτο για να χαρακτηρίσει ένα αρχείο ως ARCHIVE. Οι χαρακτηρισμοί αυτοί έχουν της εξής σημασία :

1. ARCHIVE FILES (A):

   Τα αρχεία αυτά μπορούν να αναγνωσθούν ή να τροποποιηθούν και είναι ορατά στο χρήστη μέσω της εντολής DIR. Μπορούν επίσης να χρησιμοποιηθούν από κάθε εντολή του Dos.

2. READ - ONLY FILE (B):

   Τα αρχεία που έχουν το χαρακτηρισμό αυτό μπορούν μόνο να αναγνωσθούν. Δε μπορούν να αντιγραφούν, να τροποποιηθούν κ.λ.π.

3. HIDDEN FILES (H) :

   Τα αρχεία αυτά δεν εμφανίζονται όταν εκτελείται η εντολή DIR. Η παρουσία τους μπορεί να γίνει αντιληπτή με χρήση βοηθητικών προγραμμάτων ή με ανάλυση του χώρου που αναφέρεται ως ελεύθερος από την DIR.

4. SYSTEM FILE (S) :

   Ο χαρακτηρισμός αυτός αφορά τα αρχεία του λειτουργικού συστήματος IMBIO, COM και IMBDOS.COM και ισχύει για αυτά εξ'ορισμού. Τα αρχεία που έχουν το χαρακτηρισμό αυτό μπορούν να αναγνωσθούν μόνο, ενώ συχνά είναι κρυμμένα από το χρήστη.

Η χρησιμοποίηση των χαρακτηριστικών αρχείων για την προστασία τους είναι ικανοποιητική μόνο σε στοιχειώδες επίπεδο. Η εντολή CHKDSK/V έχει ως αποτέλεσμα την εμφάνιση όλων των αρχείων κάθε ευρετηρίου. Για την αντιμετώπιση του προβλήματος αυτού σε πολλά κέντρα πληροφορικής που χρησιμοποιούν

το Dos δεν υπάρχει η εντολή CHKDSK στα αρχεία του λειτουργικού συστήματος. Ομως το Dos είναι τόσο διαδεδομένο, ώστε η τεχνική αυτή είναι αποτελεσματική μόνο όταν οι υπάρχοντες προσωπικοί υπολογιστές δε διαθέτουν μονάδα δισκέτας (για να μη μπορεί να αντιγραφεί από εκεί στο δίσκο ένα αντίγραφό του.

## ΕΦΕΔΡΙΚΑ ΑΝΤΙΓΡΑΦΑ

### ΕΝΤΟΛΕΣ COPY, DISCOPY, BACKUP, RESTORE

Λέγοντας εφεδρικά αντίγραφα εννούμε ένα πρόσθετο αντίγραφο των αρχείων που βρίσκονται σε ένα μαγνητικό μέσο. Το αντίγραφο αυτό μπορεί να φυλάσσεται στο ίδιο ή συνήθως σε άλλο μέσο. Με την τήρηση εφεδρικών αντιγράφων είναι δυνατόν η διάσωση των δεδομένων του μέσου μετά από μια ενέργεια που προξένησε τη φυσική καταστροφή τους. Εφεδρικό αντίγραφο μπορεί να λαμβάνεται από ένα ή περισσότερα αρχεία ενός μέσου.

Η εντολή COPY μπορεί να χρησιμοποιηθεί για τη λήψη αντιγράφου ενός ή περισσοτέρων αρχείων.

Η DISCOPY χρησιμοποιείται για τη λήψη αντιγράφου ολόκληρου του μαγνητικού μέσου.

Μια πιο ολοκληρωμένη προσέγγιση στο θέμα των εφεδρικών αντιγράφων μπορεί να γίνει με τη διαδικασία BACKUP. Για την υλοποίηση της διαδικασίας αυτής απαιτούνται δυο εντολές του

DOS. Η εντολή BACKUP για τη λήψη αντιγράφου ενός αρχείου και η εντολή RESTORE για την επαναποθήκευσή του στο αρχικό μέσο.

## ΔΙΑΓΡΑΦΗ ΑΡΧΕΙΩΝ - ΕΝΤΟΛΕΣ ERASE - DELETE

Οι εντολές ERASE και DELETE αποσκοπούν στη διαγραφή ενός ή περισσοτέρων αρχείων από το ευρετήριο ενός μαγνητικού μέσου.

Συνεπώς αν κάποιος χρήστης διαγράψει ένα ή περισσότερα αρχεία και ο χώρος που καταλάμβαναν δε χρησιμοποιηθεί από κάποιο άλλο που δημιουργήθηκε στο μεταξύ τότε είναι δυνατή η αναδημιουργία τους.

## ΜΟΡΦΟΠΟΙΗΣΗ ΜΑΓΝΗΤΙΚΩΝ ΜΕΣΩΝ - ΕΝΤΟΛΗ FORMAT

Η εντολή FORMAT είναι απαραίτητη για την προετοιμασία οποιουδήποτε μαγνητικού μέσου που θα εργασθεί με το DOS.

Το DOS καθοδηγεί την εντολή FORMAT, ώστε να μορφοποιήσει μόνο τη μια ή και τις δυο πλευρές του μέσου και με συγκεκριμένη χωρητικότητα, αν αυτό είναι δισκέτα.

Παρόλα αυτά ο χρήστης μπορεί να κάνει τις δικές του υποδείξεις καθοδηγώντας ο ίδιος τις ενέργειες της FORMAT.

## Η ΦΙΛΟΣΟΦΙΑ ΤΩΝ ΔΙΑΚΟΠΩΝ

Οι διακοπές του λειτουργικού συστήματος DOS αποτελούν ένα χαρακτηριστικό του, που μπορεί να χρησιμοποιηθεί από κάποιον χρήστη με προωθημένες γνώσεις για την αύξηση της ασφαλείας των αρχείων ή εφαρμογών του.

Οι διακοπές των επεξεργαστών INTEL χωρίζονται σε τρεις κατηγορίες :

α) Εξωτερικές διακοπές υλικού, που προκαλούνται είτε από περιφερειακές συσκευές είτε από συν-επεξεργαστές.

β) Εσωτερικές διακοπές υλικού που προκαλούνται από συγκεκριμένα γεγονότα που συμβαίνουν κατά τη διάρκεια εκτέλεσης ενός προγράμματος. Η εκ-χώρηση αυτών των γεγονότων σε συγκεκριμένους αριθμούς διακοπών έχει γίνει μέσω υλικού και δε μπορεί να μεταβληθεί.

γ) Οι διακοπές λογισμικού συμβαίνουν με την εκτέ-λεση της εντολής INT. Η συγκεκριμένη λειτουρ-γία κάθε διακοπής περιγράφεται σε κώδικα που αποτελεί τη ρουτίνα εξυπηρέτησης ή το χειριστή της διακοπής.

## ΔΙΑΚΟΠΕΣ ΚΑΙ ΑΣΦΑΛΕΙΑ

Οι διακοπές μπορούν να χρησιμοποιηθούν για την προαγωγή της ασφάλειας του λειτουργικού συστήματος DOS με τρεις τρόπους :

1. Με την αξιοποίηση των ρουτίνων εξυπηρέτησής τους μέσα από προγράμματα του χρήστη.
2. Με αντικατάσταση των παρεχόμενων ρουτινών εξυπηρέτησης διακοπών με άλλες, γραμμένες από το χρήστη.
3. Με μετατροπή των παρεχομένων ρουτινών εξυπηρέτησης. Αυτό είναι σχετικά δύσκολο διότι οι ρουτίνες αυτές είναι εκτελέσιμα αρχεία.

## ΚΛΗΣΗ ΔΙΑΚΟΠΩΝ

Αν ο επεξεργαστής δεχθεί ένα σήμα διακοπής τότε έχουμε :

1. Αναγνώριση του σήματος της διακοπής. Στο βήμα αυτό ο επεξεργαστής πρέπει να αναγνωρίσει το σήμα και να εντοπίσει την πηγή.
2. Αναγνώριση της παρούσας κατάστασης. Ετσι τα περιεχόμενα των σημαντικών καταχωρητών και τα σήματα κατάστασης αποθηκεύονται προσωρινά στην

κύρια μνήμη.

3. Τοποθέτηση σχήματος διακοπών. Με χρησιμοποίηση μιάς τέτοιας μάσκας είναι δυνατόν να εμποδισθεί η εκτέλεση άλλων διακοπών όσο εξυπηρετείται η τρέχουσα διακοπή.
4. Αποστολή σήματος αναγνώρισης διακοπής προς την πηγή του σήματος της διακοπής.
5. Εξυπηρέτηση της διακοπής.
6. Ανάκληση των αποθηκευμένων τιμών των καταχωρητών και των σημάτων κατάστασης.

## ΑΛΛΑΓΗ ΡΟΥΤΙΝΑΣ

Αν ο χρήστης θέλει να εκτελεστούν κάποιες ενέργειες μετά την εκτέλεση της αυθεντικής ρουτίνας εξυπηρέτησης δεν έχει παρά να δημιουργήσει μια νέα ρουτίνα εξυπηρέτησης μέσω της οποίας να καλείται πρώτα η "αυθεντική" ρουτίνα και μετά να εκτελούνται οι επιθυμητές λειτουργίες.

Η διαδικασία αντικατάστασης μιας ρουτίνας εξυπηρέτησης έχει ως εξής :

α) Κατασκευή της νέας ρουτίνας εξυπηρέτησης της διακοπής

β) Αντιγραφή της διεύθυνσης της αυθεντικής ρουτίνας σε μια κενή θέση του πίνακα και αντιστοίχιση της διεύθυνσης αυτής σε έναν αριθμό που αντιστοιχεί

σε ελεύθερη διακοπή του DOS.

γ) Φόρτωση της ρουτίνας του χρήστη στη μνήμη και ορισμός της ως μόνιμης

δ) Αντιστοίχιση της θέσης του πίνακα της συγκεκριμένης διακοπής στη διεύθυνση της νέας ρουτίνας του χρήστη.

Τα ίδια βήματα ακολουθούνται και για τη συμπλήρωση της αυθεντικής ρουτίνας της διακοπής, με τη διαφορά ότι θα πρέπει να γίνει οπωσδήποτε αντιστοίχιση της διεύθυνσης της αυθεντικής ρουτίνας σε μια ελεύθερη διακοπή του DOS.

## ΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ UNIX

## ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

### ΣΥΝΟΠΤΙΚΗ ΑΝΑΦΟΡΑ ΣΤΟ UNIX

Το 1986 τα Bell Labratories, η General Electric και το Massachussets Institute of Technology είχαν ένα κοινό ερευνητικό πρόγραμμα με σκοπό το σχεδιασμό ενός νέου λειτουργικού συστήματος, του MULTI CS.

Κατά τη διάρκεια του σχεδιασμού, το Μάρτιο του 1969, τα

Bell Laboratories αποσύρθηκαν από το όλο πρόγραμμα. Ετσι εκείνο το έτος πρωτοσχεδιάστηκε στα Bell Laboratories το UNIX, από τους Ken Thompson και Dennis Ritchie και υλοποιήθηκε στο σύστημα DEC PDP -7. Το όνομα UNIX προέρχεται από τα αρχικά Uniplexed Information and Computer System.

Η δεύτερη έκδοση του UNIX εμφανίστηκε το 1971 στο σύστημα PDP - 11/20 και χρησιμοποιήθηκε για επεξεργασία κειμένου. Οι πρώτοι χρήστες του UNIX ήταν τα μέλη του τμήματος των Bell Laboratories που ήταν υπεύθυνο για τη διαδικασία υποβολής διπλωμάτων ευρεσιτεχνίας. Η συγκεκριμένη αυτή έκδοση συνοδεύτηκε από ένα εγχειρίδιο με συγγραφείς τους Thompson και Ritchie, το Νοέμβριο του 1971. Στην όλη διαδικασία συμμετείχαν επίσης και οι Rudd Canaday, Doug Mcllroy και Joe Ossana.

Η επόμενη έκδοση εμφανίστηκε τον Ιούνιο του 1972. Σε εκείνη τη χρονική περίοδο ο Thompson εργαζόταν στη γλώσσα προγραμματισμού B που χρησιμοποιήθηκε και για την ανάπτυξη του UNIX στο πρώτο στάδιο.

Στη συνέχεια δημιουργήθηκε η NB σα μια βελτίωση της γλώσσας B και έγινε προσπάθεια να επανεγγραφεί το λειτουργικό σύστημα σε αυτή.

Η συγκεκριμένη προσπάθεια απότυχε και οι εργασίες συνεχίστηκαν, γεγονός που αποτέλεσε την αρχή ανάπτυξης της γλώσσας προγραμματισμού C. Η C έδωσε νέα ώθηση στην ανάπτυξη του UNIX, με αποτέλεσμα ο πυρήνας του, και το 1973 όλο το UNIX, να ξαναγραφτεί σε C, ενάντια στην παράδοση σύμφωνα με την οποία όλα τα λειτουργικά συστήματα γράφονταν σε assebly.

Η έκτη έκδοση του UNIX διατέθηκε από την AT & T το Μάη του 1975. Μετά την έκτη έκδοση συνεχίστηκε η εργασία ανάπτυξης με διόρθωση ορισμένων σφαλμάτων που παρουσιάστηκαν κατά τη χρήση του. Αποτέλεσμα των προσπαθειών αυτών ήταν η σημαντική βελτίωση τόσο του συστήματος αρχείων, όσο και των διαδικασιών του. Ομως η κυριώτερη εργασία ήταν η επανεγγραφή του UNIX, ώστε να απαιτήσει την απαραίτητα μεταφερτότητα. Η εργασία αυτή έγινε στο σύστημα Interdaton 8/32. Η όλη εργασία τελείωσε το 1979 και αποτελεί το πρώτο ουσιαστικό πρότυπο του UNIX, την έβδομη έκδοση, η οποία είναι και η ευρύτερα διαθέσιμη εμπορική έκδοσή του. Η συγκεκριμένη έκδοση του UNIX μεταφέρθηκε σε ένα VAX 11/780 στο Berkley με αποτέλεσμα τη δημιουργία ενός νέου προτύπου του UNIX 4,3 BSD.

Ετσι το UNIX δεν αντιμετωπίζεται πλέον ως ένα λειτουργικό σύστημα με ακαδημαικό προσανατολισμό, αλλά ως ένα ισχυρό εμπορικό πρότυπο λογισμικού, αφού ο αριθμός των υπολογιστικών συστημάτων που το έχουν υιοθετήσει αυξάνεται τώρα περισσότερο από ποτέ.

Σήμερα το UNIX υποστηρίζει περίπου εκατό διαφορετικούς υπολογιστές και γι'αυτό το λόγο υπάρχουν υλοποιήσεις του. Υλοποίηση του UNIX είναι μια έκδοση του που είναι προσαρμοσμένη σε ένα συγκεκριμένο υπολογιστή. Κάθε υλοποίησή του βασίζεται σε μια από τις εκδόσεις του. Μερικές υλοποιήσεις του είναι το XENIX, PC/IX, ULTRIX, OSNIX κ.λ.π.

Πρέπει να υπογραμμισθεί στο σημείο αυτό, ότι στη συνέχεια δε θα περιορισθούμε στην παρουσίαση των δυνατοτήτων εξασφάλισης μιάς συγκεκριμένης υλοποίησης του UNIX. Αντίθετα

θα παρουσιάσουμε τις τεχνικές εξασφάλισης, που είναι σχετικά δημοφιλείς και παρουσιάζονται σε αρκετές από τις υλοποίησεις του.

Ο βασικός λόγος για την εμπορική επιτυχία του UNIX είναι κυρίως η δυνατότητα μεταφοράς του από υπολογιστή σε υπολογιστή χωρίς μεγάλες τροποποιήσεις. Αλλα σημαντικά πλεονεκτήματά του είναι ότι παρέχει :

- Δυνατότητα πολυεπεξεργασίας
- Δυνατότητα για πολλαπλή χρήση από διαφορετικούς χρήστες την ίδια χρονική στιγμή
- Πλούσια βιβλιοθήκη λογισμικού εφαρμογών
- Ηλεκτρονικό ταχυδρομείο
- Δυνατότητα επικοινωνίας χρήστη - χρήστη, χρήστη - υπολογιστή, υπολογιστή - υπολογιστή
- Καλή διαχείριση περιφερειακών
- Ανοικτή αρχιτεκτονική
- Προσαρμοστικότητα

## ΔΟΜΗ ΤΟΥ UNIX

Εσωτερικά το UNIX αποτελείται από τρία επίπεδα :

1. Τον πυρήνα : Είναι η καρδιά του συστήματος, ελέγχει το υλικό, ενεργοποιεί και απενεργοποιεί διάφορα μέρη του υπολογιστή κατευθύνει τις εισόδους/εξόδους κ.λ.π.

2. Το κέλυφος : Είναι ένα σύνολο προγραμμάτων που συνδέει και ερμηνεύει τις εντολές του χρήστη με τον υπολογιστή. Το κέλυφος ερμηνεύει τις εντολές του χρήστη και τις μεταφράζει σε εντολές κατανοητές από τον πυρήνα.
3. Διάφορα εργαλεία και εφαρμογές : Προσδίδουν ιδιαίτερες δυνατότητες στο σύστημα και ποικίλουν από σύστημα σε σύστημα (επεξεργαστές κειμένου, προγράμματα επικοινωνιών).

Οι λειτουργίες του κέλυφους που σχετίζονται άμεσα με το χρήστη είναι :

α) Εκτέλεση προγραμμάτων

β) Υποκατάσταση ονόματος αρχείου

γ) Επαναπροσδιορισμός Ε/Ε

Το κέλυφος χειρίζεται και τη διαδικασία επαναπροσδιορισμού εισόδου ή εξόδου πριν αρχίσει η εκτέλεση ενός προγράμματος, όταν αυτό καθορίζεται στη γραμμή εντολής

δ) Δίκτυο διοχετεύσεων

Το κέλυφος αναλαμβάνει την ευθύνη για τη διασύνδεση της προκαθορισμένης εξόδου ενός προγράμματος με την προκαθορισμένη είσοδο ενός δεύτερου, πριν τα δυο προγράμματα εκτελεστούν

ε) Ελεγχος περιβάλλοντος

Το κέλυφος παρέχει κάποια ευελιξία στην προσαρμογή των αναγκών του χρήστη. Ετσι είναι δυνατόν να προσδιοριστούν η διαδρομή του αρχικού καταλό-

γου, οι κατάλογοι αναζήτησης καθώς και ο χαρακτήρας προτροπής εισόδου εντολών

στ) Ερμηνευτική γλώσσα προγραμματισμού : Το κέλυφος εξασφαλίζει μια ισχυρή γλώσσα προγραμματισμού, επιτρέποντας είτε την άμεση εκτέλεση εντολών είτε εκτέλεση αρχείων εντολών.

## ΘΕΩΡΗΣΗ ΤΩΝ ΧΡΗΣΤΩΝ ΑΠΟ ΤΟ ΣΥΣΤΗΜΑ

Το λειτουργικό σύστημα UNIX, όπως έχει ήδη αναφερθεί, παρέχει τη δυνατότητα για πολλαπλή χρήση από διαφορετικούς χρήστες την ίδια χρονική στιγμή. Οι κατηγορίες χρηστών που μπορεί να υπάρχουν σε ένα τυπικό σύστημα UNIX είναι : α) χρήστες με τυπικές δυνατότητες και β) χρήστες με αυξημένες διαχειριστικές δυνατότητες.

Η τελευταία κατηγορία χρηστών σχετίζεται με τις διαχειριστικές λειτουργίες του συστήματος οι οποίες είναι δυνατόν να βρίσκονται υπό την ευθύνη ενός ατόμου ή κατανεμημένες σε περισσότερα από ένα άτομα με ανάλογες εξουσιοδοτήσεις.

Γενικά, οι χρήστες του συστήματος ομαδοποιούνται σύμφωνα με κάποια κριτήρια, με αποτέλεσμα κάθε χρήστης να ταυτοποιείται μέσω του ατομικού του αριθμού αναγνώρισης αλλά και μέσω του αριθμού αναγνώρισης της ομάδας στην οποία ανήκει.

## ΑΣΦΑΛΕΙΑ ΚΑΙ UNIX

Στα υπολογιστικά συστήματα στα οποία παρέχεται εύκολη πρόσβαση και δυνατότητες επικοινωνίας με άλλα συστήματα είναι δύσκολο να υιοθετηθεί κάποια αυστηρή πολιτική ασφάλεια. Ετσι, το επίπεδο ασφάλειας που παρέχουν τα συστήματα αυτά είναι πολύ χαμηλότερο από ότι θα μπορούσε να είναι. Αυτό εξαρτάται όμως και από άλλους παράγοντες ο σημαντικότερος από τους οποίους είναι η γνώση και η συμπεριφορά των διαχειριστών και των χρηστών του συστήματος.

Στόχος είναι να επιτυγχάνεται μια ισορροπία μεταξύ της ασφάλειας και της εύκολης και αποδοτικής χρήσης του συστήματος.

Οι σημαντικότεροι παράγοντες σε ότι αφορά στην ασφάλεια υπολογιστικών συστημάτων είναι :

- Φυσικός έλεγχος κάθε πρόσβασης και των δυνατοτήτων του συστήματος
- Διαχειριστικές υποχρεώσεις για θέματα ασφαλείας
- Επιμόρφωση των χρηστών σύμφωνα με το επιθυμητό
- Υπαρξη διαχειριστικών διαδικασιών που βοηθούν στην αύξηση της ασφάλειας

Το UNIX σχεδιάσθηκε με βάση τη φιλοσοφία των ανοικτών συστημάτων, έτσι είναι φιλικό στο χρήστη και οι περισσότερες τεχνικές εξασφάλισής του έχουν "θυσιασθεί" για χάρη της φιλικότητας αυτής. Το αποτέλεσμα είναι το UNIX να μην παρέ-

χει αυξημένες δυνατότητες ασφαλείας, αλλά να διαθέτει πρόσφορο πεδίο ανάπτυξης τέτοιων δυνατοτήτων.

Σε ένα υπολογιστικό σύστημα όπου υπάρχει διαχειριστής ή υπερχρήστης όπως στο UNIX θα πρέπει ο διαχειριστής αυτός να υιοθετεί μια συνεναιτική πολιτική ασφαλείας, ώστε :

- να επιτυγχάνεται η ομαλή εισαγωγή νέων χρηστών στο σύστημα
- να γίνεται αποτελεσματική διαχείριση των συνθηματικών
- να γίνεται αποτελεσματική διαχείριση των αδειών πρόσβασης στα αρχεία του συστήματος

Ετσι αν το σύστημα είναι σχετικά απομονωμένο από το εξωτερικό περιβάλλον και έχει ένα μικρό πλήθος χρηστών με τα ίδια ενδιαφέροντα, η πολιτική ασφαλείας μπορεί να είναι σχετικά χαλαρή.

Αντίθετα, σε μεγαλύτερα συστήματα όπου λειτουργούν μεγαλύτερες ομάδες χρηστών υπάρχει αρκετά μεγάλη δημόσια προβολή ή περιέχονται κρίσιμες πληροφορίες, τότε η πολιτική ασφαλείας θα πρέπει να είναι περισσότερο περιοριστική.

Η πρωταρχική ευθύνη για συμμόρφωση ανήκει σε κάθε χρήστη. Παρόλα αυτά, ένας υπεύθυνος διαχειριστής συστήματος μπορεί και πρέπει να αναπτύξει μια διαδικασία ελέγχου με ανατροφοδότηση παρεχόμενη από τους χρήστες.

Οι σημαντικότερες προσπάθειες για την ανάπτυξη προτύπων για την ασφάλεια του UNIX εντοπίζονται στις ΗΠΑ. Οι πιο ενδιαφέρουσες από αυτές αναφέρονται στην ανάπτυξη των εξής :

α) ISO JTC 1/SC 22 NG15 - Languages /90 SIX

Το έργο αυτό διεξάγεται στα πλαίσια του Διεθνούς Οργανισμού Προτύπων και αφορά στην ανάπτυξη διαδικασιών εξασφάλισης του λειτουργικού συστήματος UNIX

β) IEEE 1003.6(POSIX) Security Group

Το έργο αυτό αναπτύσσεται από μια ομάδα επιστημόνων της IBM και του Διεθνούς Ινστιτούτου Προτύπων και Τεχνολογίας των ΗΠΑ αλλά είναι ανοιχτό και σε κάθε άλλο ενδιαφερόμενο. Ως ένα αποτέλεσμα της ομάδας αυτής είναι η διατύπωση λειτουργικών προδιαγραφών, σύμφωνα με τις οποίες το UNIX κατατάσσεται στην κλάση B3 του συστήματος αξιολόγησης των ΗΠΑ.

γ) TRUSIX. Το έργο αυτό αφορά την ασφαλή λειτουργία του UNIX και αποσκοπεί στην πρόταση νέων προτύπων εξασφάλισης κ.λ.π Εκπονείται από μια κλειστή ομάδα αποτελούμενη από εκπροσώπους εταιρειών των ΗΠΑ.

δ) X - OPEN. Το έργο αυτό αποσκοπούσε παλιότερα, στον καθορισμό διοικητικών προτύπων για την ασφάλεια του UNIX. Σήμερα υποστηρίζεται το έργο του προγράμματος POSIX.

Η ανάπτυξη των παραπάνω προγραμμάτων βρίσκεται ακόμη σε εξέλιξη, αλλά αναμένεται να οδηγήσει σύντομα σε σημαντικά αποτελέσματα.

## ΕΛΕΓΧΟΣ ΤΟΠΙΚΗΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΣΥΣΤΗΜΑ

## ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΑΡΧΕΙΩΝ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Επειδή το UNIX είναι ένα σύστημα που σχεδιάστηκε για να ικανοποιεί πολλούς χρήστες, η πρώτη ενέργεια που θα πρέπει να κάνει ένας χρήστης που επιθυμεί να συνδεθεί με αυτό είναι να δηλώσει την ταυτότητά του μέσω ενός ονόματος εισόδου. Αυτό το όνομα εισόδου είναι μοναδικό και ταυτοποιεί κάθε συγκεκριμένο χρήστη. Κανείς άλλος χρήστης δε μπορεί να έχει το ίδιο. Οι απαιτήσεις που αφορούν το όνομα εισόδου είναι :

- να αποτελείται από λιγότερους από οκτώ αλφαριθμητικούς χαρακτήρες
- να μην κρυπτογραφείται αλλά να είναι δημόσια γνωστό

Αμέσως μετά την εισαγωγή του ονόματος εισόδου, δηλαδή μετά τη φάση της ταυτοποίησης απαιτείται η εισαγωγή ενός συνθηματικού, ώστε να είναι δυνατή η αυθεντικοποίηση του χρήστη. Η εισαγωγή του συνθηματικού είναι μη ορατή για ευνόητους λόγους.

Τα συνθηματικά βρίσκονται αποθηκευμένα σε κρυπτογραφημένη μορφή στο αρχείο των συνθηματικών σε τρόπο ώστε να είναι αδύνατη η κρυπτανάλυσή τους με μεθόδους ανάλυσης συχνοτήτων.

Μετά την εισαγωγή του από το χρήστη το συνθηματικό κρυπτογραφείται με ένα μονόδρομο μετασχηματισμό και συγκρίνεται με το κρυπτογραφημένο συνθηματικό που ήδη υπάρχει στο αρχείο των συνθηματικών.

Ενα σημαντικό πλεονέκτημα αυτής της διαχείρισης των συνθηματικών είναι ότι σε καμμιά περιοχή του συστήματος δεν καταγράφεται η μη κρυπτογραφημένη μορφή τους.

Αν οι φάσεις ταυτοποίησης και αυθεντικοποίησης ολοκληρωθούν με επιτυχία τότε το σύστημα επιτρέπει στο χρήστη να αξιοποιήσει τις δυνατότητες που του παρέχονται. Η διαδικασία αυτή επιτυγχάνεται μέσω μιάς διεργασίας που καλείται getty.

## ΤΟ ΑΡΧΕΙΟ ΤΩΝ ΣΥΝΘΗΜΑΤΙΚΩΝ

Οι πληροφορίες που ελέγχουν την είσοδο των χρηστών στο σύστημα βρίσκονται στο αρχείο /etc/passwd. Το αρχείο αυτό είναι συνήθως αναγνώσιμο από όλους τους χρήστες, αλλά μη εγγράψιμο.

Οι άδειες πρόσβασης του /etc/passwd πρέπει να διαχειρίζονται με προσοχή αφού πρόκειται για το σημαντικότερο αρχείο που σχετίζεται με την ασφάλεια του συστήματος.

Κάθε εγγραφή του /etc/passwd αναφέρεται σε έναν και μόνο χρήστη, εκτός από ορισμένες εγγραφές που χρησιμοποιούνται για την ορθή λειτουργία του συστήματος και περιέχονται σε αυτό ακόμη και πριν την εισαγωγή λογαριασμών χρηστών.

Οι εγγραφές αυτές δε θα πρέπει να διαγραφούν ή να μεταβληθούν, γιατί έτσι υπάρχει πιθανότητα καταστροφικών συνεπειών στο σύστημα. Στις περισσότερες περιπτώσεις μπορούν να μεταβληθούν μόνο τα συνθηματικά χωρίς να δημιουργηθούν προβλήματα.

Το όνομα αναγνώρισης, ο αριθμός αναγνώρισης του χρήστη και της ομάδας, το ευρετήριο σύνδεσης και το κέλυφος εισόδου, δε θα πρέπει να μεταβάλλονται σε εγγραφή που δεν ανήκει σε κάποιον χρήστη.

Σε μερικές εκδόσεις του UNIX το κρυπτογραφημένο συνθηματικό δεν περιέχεται στο etc/passwd, αλλά στο /etc/shadow, το οποίο είναι αναγνώσιμο μόνο από το root και ανήκει στο root.

Το /etc/shadow περιέχει το αναγνωριστικό εισόδου κάθε χρήστη, το κρυπτογραφημένο συνθηματικό, έναν αριθμητικό κώδικα που περιγράφει πότε έγινε η τελευταία αλλαγή στο συνθηματικό και τον ελάχιστο και μέγιστο αριθμό ημερών που απαιτείται μεταξύ των μεταβολών των συνθηματικών.

Υπάρχει αμφιμονοσήμαντη αντιστοιχία μεταξύ των εγγραφών του /etc/passwd και του /etc/shadow. Εάν υπάρχει το /etc/shadow στο σύστημα τότε το πεδίο που αντιστοιχεί στο συνθηματικό στο αρχείο /etc/passwd αντικαθίσταται από το χαρακτήρα X.

Το αρχείο /etc/shadow δημιουργείται μέσω της εντολής pwconv, η οποία έχει ως είσοδο το /etc/passwd. Κάθε φορά που μεταβάλλεται το /etc/passwd θα πρέπει να εκτελείται η προηγούμενη εντολή ώστε να ενημερώνεται το /etc/shadow.

## ΠΡΟΣΘΕΣΗ ΚΑΙ ΔΙΑΓΡΑΦΗ ΧΡΗΣΤΩΝ ΚΑΙ ΟΜΑΔΩΝ ΧΡΗΣΤΩΝ

Η διαδικασία πρόσθεσης νέων χρηστών στο σύστημα περιορίζεται μόνο στο διαχειριστή του συστήματος. Αρχικά απαιτείται η δημιουργία ενός ευρετηρίου σύνδεσης για το χρήστη για τον οποίο πρέπει να δοθούν κάποιες άδειες πρόσβασης.

Μετά τη δημιουργία του ευρετηρίου και τη μεταφορά των αρχείων σε αυτό μπορεί να γίνει η πρόσθεση μιάς εγγραφής στο αρχείο των συνθηματικών /etc/passwd, η οποία αφορά το νέο χρήστη. Εάν στο σύστημα υπάρχει το αρχείο /etc/shodow τότε πρέπει να εκτελεστεί η εντολή pwconv.

Συχνά το πεδίο του συνθηματικού είναι αρχικά κενό, ως την πρώτη φορά που θα εισέλθει ο χρήστης στο σύστημα. Η ενέργεια αυτή είναι αρκετά ανασφαλής, είτε λόγω της μη εισαγωγής του συνθηματικού από το χρήστη, είτε λόγω της μη εισαγωγής του εξουσιοδοτημένου χρήστη στο σύστημα για κάποιο χρονικό διάστημα.

Μια ασφαλέστερη διαδικασία είναι η δημιουργία ενός μη προστατευόμενου λογαριασμού άμεση εισαγωγή με το συγκεκριμένο όνομα εισόδου και δημιουργία ενός συνθηματικού με την passwd. Αμέσως έπειτα πρέπει να ακολουθήσει η ανακοίνωση του συνθηματικού στο χρήστη κατά τη διαδικασία αυτή ο διαχειριστής του συστήματος δεν είναι αναγκασμένος να εισέλθει στο σύστημα

κάνοντας χρήση του ονόματος εισόδου του νέου χρήστη, αλλά αρκεί να χρησιμοποιήσει την passwd με όρισμα το όνομα αυτό :

passwd < όνομα εισόδου του νέου χρήστη >

Για τη διαγραφή ενός χρήστη ακολουθείται η αντίστροφη διαδικασία. Για να αντιμετωπισθεί μια προσωρινή απομάκρυνση ενός χρήστη πρέπει να ασφαλιστεί η είσοδός του στο σύστημα. Μερικά συστήματα διαθέτουν για το σκοπό αυτό τις εντολές : addgrp και delgrp.

Το συνθηματικό χρησιμοποιείται κατά τη μετάβαση ενός χρήστη από μια ομάδα σε μια άλλη. Για να πραγματοποιηθεί αυτή η μετάβαση χρησιμοποιείται η εντολή newgrp. Σε κάθε χρονική στιγμή ένας χρήστης μπορεί να ανήκει σε μια μόνον ομάδα χρηστών.

Οταν προστίθεται ένας χρήστης σε μια υπάρχουσα ομάδα χρηστών δεν απαιτείται καμιά επιπλέον ενέργεια. Ομως εάν είναι απαραίτητη η δημιουργία μιας νέας ομάδας χρηστών πρέπει ο διαχειριστής του συστήματος να προσθέσει μια εγγραφή στο αρχείο /etc/group, η οποία θα περιγράφει τη νέα ομάδα. Το αρχείο αυτό θα πρέπει να είναι αναγνώσιμο, αλλά όχι εγγράψιμο.

## ΤΟ ΠΕΡΙΟΡΙΣΜΕΝΟ ΚΕΛΥΦΟΣ

Το τυποποιημένο κέλυφος παρέχει πολλές δυνατότητες στους χρήστες με βάση τις οποίες επιτρέπεται η μετακίνησή τους στο

σύστημα αρχείων, η εκτέλεση πολλών εντολών, η αλλαγή των τιμών πολλών μεταβλητών του κελύφους κ.λ.π.

Παρόλα αυτά το UNIX παρέχει και ένα άλλο επιπρόσθετο κέλυφος το rsh (περιορισμένο κέλυφος). Στην πραγματικότητα είναι το ίδιο εκτελέσιμο πρόγραμμα με το συνηθισμένο κέλυφος αλλά υπάρχει με δυο ονόματα στο ευρετήριο. Το πρόγραμμα αυτό ενεργεί ανάλογα με το όνομα που χρησιμοποιήθηκε για την κλήση του. Το rsh παρέχει λιγότερες δυνατότητες από ότι το κανονικό κέλυφος. Αν τεθεί δε, στο τελευταίο πεδίο κάθε εγγραφής για τους χρήστες του /etc/passwd, ως κέλυφος σύνδεσης το /bin/rch, τότε οι χρήστες θα χρησιμοποιούν αυτό το περιορισμένο κέλυφος. Το rsh διαφέρει από το κανονικό κέλυφος στα εξής :

1. Ο χρήστης δε μπορεί να χρησιμοποιεί την εντολή cd για αλλαγή ευρετηρίου. Ετσι περιορίζεται στο ευρετήριο σύνδεσης.
2. Ο χρήστης δεν έχει τη δυνατότητα αλλαγής της τιμής της μεταβλητής PATH με αποτέλεσμα να είναι δυνατή η εκτέλεση των εντολών που αυτή υποδεικνύει (η οποία μπορεί να προσδιορίζεται από το διαχειριστή του συστήματος).
3. Ο χρήστης δεν έχει τη δυνατότητα να χρησιμοποιεί πλήρη ονόματα αρχείων ή ευρετηρίων. Ετσι μόνο τα αρχεία στο ευρετήριο σύνδεσης και στα υποευρετήρια μπορούν να προσπελαστούν.
4. Ο χρήστης δε μπορεί να κάνει χρήση της επανακατεύθυνσης εξόδου με τη βοήθεια των > ή >>.

Οι περιορισμοί αυτοί επιβάλονται μετά την εκτέλεση του αρχείου εκκίνησης profile κάθε χρήστη. Ο διαχειριστής του συστήματος θα πρέπει να θέσει ένα περιορισμένο περιβάλλον στο profile κάθε χρήστη, συμπεριλαμβάνοντας το PATH που θα συνδέεται με ένα περιορισμένο ευρετήριο bin.

Ο διαχειριστής του συστήματος θα πρέπει στη συνέχεια να μεταβιβάσει την κυριότητα του profile στο λογαριασμό root. Το αρχείο profile θα πρέπει να είναι αναγνώσιμο από όλους, αλλά μη εγγράψιμο και εκτελέσιμο.

Παρόλα αυτά το rch δεν είναι τόσο ασφαλές και κάποιος χρήστης με αυξημένες γνώσεις μπορεί να μεταβεί στο κανονικό κέλυφος.

Η χρήση του περιορισμένου κελύφους για χρήστες χωρίς συνθηματικά δεν είναι αποτελεσματική. Συνεπώς η ασφάλεια του συστήματος δε μπορεί να βασίζεται στο rch.

Παρόλα αυτά το rch μπορεί να αποδειχθεί αρκετά χρήσιμο για την προστασία του συστήματος από απρόσεκτους χρήστες ή από χρήστες που δεν έχουν αυξημένες γνώσεις.

## ΕΠΙΛΟΓΗ ΣΥΝΘΗΜΑΤΙΚΩΝ

Το σύστημα διαχείρισης συνθηματικών επιτρέπει τη σύνθεση συνθηματικών με χρήση οποιουδήποτε χαρακτήρα (128 εναλλακτικές λύσεις). Τα συνθηματικά μπορούν να έχουν μήκος ως οκτώ χαρακτήρες, δίνοντας έτσι τη δυνατότητα για 128 διαφορετικούς

συνδυασμούς πιθανούς επιλογών.

Το UNIX ενθαρρύνει τους χρήστες του να χρησιμοποιούν συνθηματικά μήκους μεγαλύτερου των έξι χαρακτήρων αν χρησιμοποιούνται μόνον κεφαλαία γράμματα, των πέντε χαρακτήρων, αν χρησιμοποιούνται και μικρά γράμματα και των τεσσάρων αν χρησιμοποιούνται και ειδικά σύμβολα ή αριθμοί. Παρόλα αυτά αν κάποιος χρήστης δεν επιλέξει συνθηματικό το οποίο πληρεί τις παραπάνω προδιαγραφές το UNIX του επιτρέπει την πρόσβαση.

Με αυτά τα δεδομένα η κρυπτανάλυση των χρησιμοποιημένων συνθηματικών φαίνεται ότι γίνεται πραγματικά δύσκολο έργο. Ομως δεν είναι ακριβώς έτσι. Είναι ευρύτατα γνωστό και κοινά αποδεκτό ότι οι χρήστες δεν επιλέγουν τυχαία συνθηματικά, μειώνοντας έτσι δραστικά το συνολικό αριθμό των δυνατών επιλογών, που πρέπει να δοκιμαστούν, ώστε να εντοπιστεί το πραγματικό. Ετσι η ασφάλεια των συνθηματικών εναπόκειται στην επιλογή του χρήστη. Το γεγονός αυτό αναγορεύει το UNIX ως "φιλικό" λειτουργικό σύστημα αλλά από την άλλη πλευρά μειώνει σημαντικά την ασφάλειά του.

Στο UNIX όλοι οι χρήστες, ακόμη και οι διαχειριστές του συστήματος μπορούν να χρησιμοποιούν συνθηματικά. Συνεπώς η ευαισθησία τους σχετικά με το θέμα της ασφάλειας ενός Πληροφοριακού Συστήματος καθορίζει την αποτελεσματικότητα της επιλογής τους. Για την αντιμετώπιση του προβλήματος που δημιουργείται με δεδομένο, ότι οι περισσότεροι χρήστες θεωρούν ότι πρέπει να προστατεύονται επαρκώς, προτείνεται ο συνδυασμός δυο τεχνικών :

Η πρώτη τεχνική συνίσταται στη δημιουργία ενός προιόντος

λογισμικού που θα είναι εφοδιασμένο με ένα "λεξικό" πιθανών συνθηματικών τα οποία δεν πρέπει να χρησιμοποιούν οι χρήστες και το οποίο θα επεξεργάζεται το αρχείο των κρυπτογραφημένων συνθηματικών, ώστε μόλις εντοπίσει χρήση κάποιου που υπάρχει και στο λεξικό να ενημερώνει το χρήστη με κατάλληλο μήνυμα.

Η δεύτερη τεχνική συνίσταται στη χρήση ενός αλγόριθμου, ο οποίος θα δημιουργεί ψεύτικα και τυχαία συνθηματικά, με την ιδιότητα να είναι ευκολομνημόνευτα. Η κατασκευή ενός τέτοιου αλγόριθμου δεν παρουσιάζει σημαντικές δυσκολίες, αλλά οφείλει να τηρεί ορισμένες προυποθέσεις :

- Η διαδικασία πρότασης κάποιου συνθηματικού πρέπει να είναι φιλική, προαιρετική και να πείθει το χρήστη να τη χρησιμοποιήσει.
- Τα προτεινόμενα συνθηματικά πρέπει να είναι περισσότερα από ένα, ώστε να προσφέρουν δυνατότητα επιλογής.
- Η διαδικασία πρότασης πρέπει να είναι γρήγορη και τα προτεινόμενα συνθηματικά ευκολομνημόνευτα.
- Ο αλγόριθμος που χρησιμοποιείται για να τα παράγει πρέπει να μην είναι κοινοποιήσιμος.

## ΑΣΦΑΛΙΣΗ ΜΗ ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΩΝ ΕΙΣΟΔΩΝ

Αν κάποιες είσοδοι του συστήματος δε χρησιμοποιούνται ή δεν είναι απαραίτητη η ύπαρξή τους, τότε πρέπει να ασφαλί-

ζονται με μια από τις εξής ενέργειες :

- Διαγραφή των αντίστοιχων εγγραφών στο αρχείο των συνθηματικών /etc/passwd
- Αποκλεισμό προσπέλασης στις συγκεκριμένες εισόδους.

Η δεύτερη ενέργεια απαιτεί τη μετατροπή του αρχείου των συνθηματικών και πιο συγκεκριμένα τη μετατροπή του κρυπτογραφημένου συνθηματικού. Η τεχνική αυτή βασίζεται στην εγγραφή χαρακτήρων που δεν είναι δυνατόν να παραχθούν μέσω της διαδικασίας κρυπτογράφησης. Ετσι, κανένα συνθηματικό δε μπορεί να χρησιμοποιηθεί για τη συγκεκριμένη είσοδο. Οι χαρακτήρες αυτοί είναι δυνατόν να συνοδεύονται από μια επεξηγηματική ακουλουθία χαρακτήρων. Ετσι, είναι δυνατόν να χρησιμοποιηθούν οι εξής ακολουθίες χαρακτήρων για την αντικατάσταση του κρυπτογραφημένου συνθηματικού :

Locked : είναι η χαρακτήρας που δεν παράγεται από τη διαδικασία κρυπτογράφησης

Not valid : Ο χαρακτήρας που αντιστοιχεί στο κενό διάστημα (μεταξύ δυο λέξεων) δεν παράγεται από τη διαδικασία κρυπτογράφησης.

## ΚΑΤΑΓΡΑΦΗ ΜΗ ΕΠΙΤΥΧΩΝ ΠΡΟΣΠΑΘΕΙΩΝ ΕΙΣΟΔΟΥ ΣΤΟ ΣΥΣΤΗΜΑ

Μερικά συστήματα παρέχουν τη δυνατότητα καταγραφής ανεπιτυχών προσπαθειών εισόδου αποθηκεύοντας το όνομα

εισόδου, κάποια χρονική ένδειξη και τον αριθμό του τερματικού. Το συνθηματικό της αντίστοιχης εισόδου δεν καταγράφεται. Η διαδικασία αυτή είναι πολύ σημαντική, αφού έτσι παρέχονται πληροφορίες σχετικές με προσπάθειες μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Ενας λόγος για τον οποίο αποτυγχάνουν κάποιες προσπάθειες πρόσβασης είναι γιατί μερικοί χρήστες από αβλεψία, αντί για το όνομα εισόδου εισάγουν το συνθηματικό. Ετσι η συλλογή των ονομάτων εισόδου αποτελεί πολλές φορές συλλογή συνθηματικών. Κάποιος μπορί να μελετήσει την κατάσταση των ανεπιτυχών προσπαθειών και με τη βοήθεια του αρχείου των συνθηματικών να συμπεράνει ότι ονόματα εισόδου που δεν υπάρχουν στο αρχείο των συνθηματικών αποτελούν ίσως κάποια πραγματικά συνθηματικά.

Αυτή η διαδικασία καταγραφής είναι δυνατόν να συνοδεύεται από καταμέτρηση του αριθμού των συνεχόμενων ανεπιτυχών προσπαθειών εισόδου για ένα συγκεκριμένο χρήστη. Η καταμέτρηση αυτή μπορεί να χρησιμοποιηθεί για να εμποδίσει την πρόσβαση του συγκεκριμένου χρήστη στο σύστημα μετά από κάποιον αριθμό συνεχομένων ανεπιτυχών προσπαθειών.

## ΚΑΤΑΓΡΑΦΗ ΠΡΟΣΦΑΤΗΣ ΕΙΣΟΔΟΥ ΣΤΟ ΣΥΣΤΗΜΑ

Μερικά συστήματα παρέχουν την ημερομηνία της πιο πρόσφατης εισόδου στο σύστημα. Αυτή η στοιχειώδης πληροφορία βοηθάει να γίνει αντιληπτή η είσοδος στο σύστημα κάποιου μη

εξουσιοδοτημένου χρήστη. Αν ο χρήστης κατά τη φάση της εισαγωγής παρατηρήσει ότι η ημερομηνία της πρόσφατης εισαγωγής του στο σύστημα διαφέρει από την παρεχόμενη ημερομηνία, τότε θα πρέπει να αλλάξει συνθηματικό. Το χαρακτηριστικό αυτό υποστηρίζεται από το πρόγραμμα εισόδου, εφόσον επικυρωθεί το συνθηματικό. Το πρόγραμμα εισόδου χρησιμοποιεί γι'αυτό το λόγο κάποιο αρχείο μηδενικού μήκους, το οποίο καλείται lastlogin που βρίσκεται στο ευρετήριο σύνδεσης κάθε χρήστη. Το αρχείο αυτό ανήκει στο σύστημα και όχι σε κάποιο χρήστη. Οι εξουσιοδοτήσεις πρόσβασης που καθορίζονται γ'αυτό το καθιστούν αναγνώσιμο μόνο από το λογαριασμό SYS.

## ΕΙΔΙΚΑ ΔΙΑΧΕΙΡΙΣΤΙΚΑ ΣΥΝΘΗΜΑΤΙΚΑ

Υπάρχουν δυο μορφές πρόσβασης σε ένα σύστημα UNIX : είτε ενός ονόματος εισόδου που αντιστοιχεί σε έναν τυπικό χρήστη είτε μέσω του ονόματος εισόδου του διαχειριστή.

Οι σημαντικές δικαιοδοσίες του διαχειριστή είναι δυνατόν να περιορίσουν τις δικαιοδοσίες των χρηστών αυξάνοντας την ασφάλεια του συστήματος, αλλά μειώνοντας τη φιλικότητά του. Αρα θα πρέπει να επιδιώκεται μια ισορροπημένη οργάνωση παροχής δικαιωμάτων σε όσους σχετίζονται με το σύστημα. Αυτό επιτυγχάνεται με τη χρήση ειδικών εισόδων συστήματος καθώς και με τη σύνδεση ορισμένων κρίσιμων διαχειριστικών εντολών με συνθηματικά.

Τ.Ε.Ι. ΠΑΤΡΑΣ
ΒΙΒΛΙΟΘΗΚΗ

Το συνθηματικό του διαχειριστή του συστήματος αποτελεί ίσως τη σημαντικότερη πληροφορία πρόσβασης στο σύστημα. Σε αυτήν την περίπτωση αν κάθε προσπάθεια αποκάλυψης του συνθηματικού αποτύχει, θα πρέπει να ακολουθηθεί η διαδικασία επανατοποθέτησης του μέρους του λειτουργικού συστήματος, που είναι υπεύθυνο για την εκκίνηση με συνέπεια την απώλεια αρχείων του συστήματος.

Υπάρχουν κάποιες διαχειριστικές εντολές που αποτελούν και ονόματα εισόδου και θα πρέπει να προστατεύονται με χρήση συνθηματικών :

- Setup : χρησιμοποιείται για την εγκατάσταση του λειτουργικού συστήματος και θα πρέπει να ελέγχεται μετά την πρώτη εφαρμογή της.
- Sysadm : Επιτρέπει την πρόσβαση σε πολλές χρήσιμες διαχειριστικές λειτουργίες που δεν απαιτούν τη σύνδεση του χρήστη ως διαχειριστή.
- Powerdown : Χρήση για την απενεργοποίηση του συστήματος.
- Ckeckfsys : Χρησιμοποιείται για την εκκίνηση διαδικασιών ελέγχου συγκεκριμένου συστήματος αρχείων.
- Makefsys : Δημιουργεί νέα συστήματα αρχείων σε καθορισμένο φυσικό μέσο.
- Mountfsys : Χρησιμοποιείται για τη διασύνδεση συστημάτων αρχείων προς χρήση.

- Umountfsys : Χρησιμοποιείται για την αποσύνδεση συστημάτων αρχείων.

## ΠΑΡΑΚΑΜΨΗ ΣΥΝΘΗΜΑΤΙΚΩΝ - ΑΝΤΙΜΕΤΩΠΙΣΗ

Δεδομένου ότι το σύστημα των συνθηματικών αποτελεί το σημαντικότερο ίσως παράγοντα ασφαλείας σε συστήματα όπως το UNIX, το ενδιαφέρον των χρηστών επικεντρώνεται σε αυτό με τελικό στόχο την παράκαμψή του και τη μη εξουσιοδοτημένη εκμετάλλευση του πληροφοριακού συστήματος.

Τεχνικές οι οποίες είναι δυνατόν να υιοθετηθούν για το σκοπό αυτό είναι :

α) Κρυπτανάλυση συνθηματικών

Αποτελεί την πιο δύσκολη τεχνική εφόσον απαιτούνται υψηλού επιπέδου γνώσεις αλλά και ισχυρά υπολογιστικά συστήματα. Για την κρυπτογράφηση των συνθηματικών χρησιμοποιείται ένας αλγόριθμος που αποτελεί μια μορφή του D.E.S (Data Encryption Standard). Η ύπαρξη τεχνικών κρυπτανάλυσης του D.E.S αν και δεν είναι απίθανη δεν έχει αναφερθεί ως σήμερα.

β) Προγράμματα "Δούρειοι Ίπποι"

Πρόκειται για προγράμματα τα οποία αφού εγκατασταθούν σε ένα πληροφοριακό σύστημα χωρίς να γίνει αντιληπτή η παρουσία τους, επιχειρούν την αποκάλυψη ενός συνθηματικού χωρίς να γίνει κρυπτανάλυσή του. Τα προγράμματα αυτά δε διεκδικούν δάφνες πρωτοτυπίας αλλά στοχεύουν να υποδείξουν τη φιλοσοφία

λειτουργίας των Δούρειων Ιππων. Ενα άλλο κρίσιμο σημείο των προγραμμάτων Δούρειων Ιππων είναι η εντολή Su. Με την εκτέλεση της εντολής αυτής επιχειρείται μετάβαση από μια ταυτότητα εισόδου σε μια άλλη ακόμη και σε αυτή που αντιστοιχεί στο διαχειριστή του συστήματος.

Ειδικό ενδιαφέρον έχουν όσοι χρήστες προσπάθησαν να αποκτήσουν ταυτότητα διαχειριστή. Για τη διαχείριση αυτού του αρχείου διατίθεται η εντολή sulog. Το αρχείο sulog θα ήταν πραγματικά χρήσιμο για την αντιμετώπιση σημαντικών προσβολών του συστήματος, αν πραγματικά υπήρχε ανάγκη να επιχειρηθεί πρόσβαση στο σύστημα μέσω της εντολής SU. Ομως αυτή η ανάγκη δεν υπάρχει. Μόνο οι πιο άπειροι χρήστες θα χρησιμοποιούσαν την εντολή SU για την απόκτηση των προνομίων του διαχειριστή ή άλλου χρήστη, δοκιμάζοντας κάποιο συνθηματικό, ενώ θα μπορούσε να επιλεγεί η έμμεση προσέγγιση της κρυπτογράφησης του υποτιθέμενου συνθηματικού και σύγκρισης αυτού με το αντίστοιχο στο αρχείο των συνθηματικών, η οποία παρέχει επικύρωση, χωρίς να αφήνει "ίχνη".

γ) Προγράμματα τα οποία εφαρμόζουν επιλεκτική δοκιμή κάποιων πιθανών συνθηματικών.

Η επιλογή αυτή βασίζεται σε πληροφορίες που περιέχονται στο αρχείο των συνθηματικών /etc/passwd και είναι δυνατόν συνδυαζόμενες να αποκαλύψουν κάποιο συνθηματικό. Οι πληροφορίες που κύρια χρησιμοποιούνται είναι το όνομα εισόδου και τα σχόλια που περιέχονται σε κάθε εγγραφή του αρχείου. Τα προγράμματα αυτά είναι συνήθως χαμηλού κόστους και δρουν σε αρκετά μικρό χρονικό διάστημα.

Από όλα αυτά συμπεραίνουμε ότι η ασφαλής τήρηση συνθηματικών είναι έργο δύσκολο, αλλά μπορεί να αναβαθμιστεί αν υιοθετηθούν ενέργειες όπως :

- Προστασία του αρχείου των συνθηματικών ή των αντιγράφων του. Ετσι οι χρήστες δε θα έχουν την ευκαιρία να πειραματιστούν με κάποιο πρόγραμμα επιλεκτικών δοκιμών.
- Διασφάλιση των κρυπτογραφημένων συνθηματικών σε ξεχωριστό αρχείο και αντικατάσταση των αντίστοιχων χαρακτήρων στο αρχείο /etc/passwd με τυχαίες σειρές χαρακτήρων ίδιου μήκους. Αυτό θα έχει ως αποτέλεσμα, αν όχι να εμποδισθεί η αποκάλυψη των συνθηματικών, να δαπανηθεί σημαντικός χρόνος γι'αυτό.
- Απομάκρυνση των χρήσιμων πληροφοριών που περιέχονται στο πεδίο των σχολίων από κάθε εγγραφή του /etc/passwd. Η ενέργεια αυτή έχει σαν πρόσθετο θετικό αποτέλεσμα την αύξηση της ταχύτητας εκτέλεσης διαφόρων λειτουργιών του συστήματος που χρησιμοποιούν το αρχείο των συνθηματικών.
- Ματατροπή του προγράμματος εγκατάστασης συνθηματικών passwd και ενσωμάτωση διαδικασιών που αποτρέπουν τους χρήστες από την επιλογή ευνόητων ή γενικά ακατάλληλων συνθηματικών.
- Επιμόρφωση των χρηστών σχετικά με την επιλογή κατάλληλων συνθηματικών αλλά και τεχνικών διαφύλαξή τους.

Εκτός από τις μεθόδους αυτές είναι δυνατόν να χρησιμοποιηθούν για την παράκαμψη των συνθηματικών ειδικά εξωτερικά προγράμματα ή να αξιοποιηθούν χαρακτηριστικά του υλικού του συστήματος.

## ΧΡΟΝΙΚΗ ΕΞΑΡΤΗΣΗ ΣΥΝΘΗΜΑΤΙΚΩΝ

Η ασφάλεια που επιτυγχάνεται με τη χρήση συνθηματικών σε ένα σύστημα εξαρτάται άμεσα από το χρόνο ισχύος του συνθηματικού. Ετσι, αν ένα συνθηματικό διατηρείται σε ισχύ για μεγάλο χρονικό διάστημα τότε προκύπτουν κίνδυνοι όπως :

- Αυξάνονται τα χρονικά περιθώρια των μη εξουσιοδοτημένων χρηστών για την ανεύρεση του συνθηματικού.
- Αυξάνεται το χρονικό διάστημα δράσης ενός χρήστη, που έχει ήδη ανακαλύψει το συνθηματικό.

Για την αντιμετώπιση των πιο πάνω στοιχείων ανασφάλειας, τα περισσότερα συστήματα UNIX προσφέρουν έναν μηχανισμό που καλείται "ενηλικίωση συνθηματικών". Ο μηχανισμός αυτός ενεργοποιείται και ελέγχεται από το διαχειριστή του συστήματος και προκαλεί την αλλαγή των συνθηματικών των χρηστών μετά την παρέλευση κάποιου προκαθορισμένου χρονικού διαστήματος.

## ΕΛΕΓΧΟΣ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΣΥΣΤΗΜΑ

### Η ΑΣΦΑΛΕΙΑ ΤΟΥ ΥΠΟΣΥΣΤΗΜΑΤΟΣ U.U.C.P

Τα λειτουργικά περιβάλλοντα που απαρτίζονται από πολλά συστήματα, συνδεδεμένα μεταξύ τους είτε μέσω ενός ευρέως δικτύου TCP/IP είτε μέσω ενός τοπικού δικτύου, χαρακτηρίζονται από αρκετά σημεία ανασφάλειας.

Για παράδειγμα, σε πολλά δίκτυα UNIX επιτρέπεται η από απόσταση εκτέλεση εντολών σε κάποια συστήματα. Το χαρακτηριστικό αυτό εισάγει κινδύνους αλλά είναι αποδεκτό αν τα συστήματα λειτουργούν σε αξιόπιστο περιβάλλον. Τις περισσότερες φορές, μάλιστα, αρκεί ένα επιπλέον συνθηματικό πριν επιτραπεί προσπέλαση στο δίκτυο.

Συνήθως οι χρήστες ενός δικτύου συνδέονται με κάποια κοινή δραστηριότητα και έτσι αναπτύσσουν εργαλεία τα οποία επιτρέπουν εύκολο καταμερισμό αρχείων, δεδομένων και φυσικών μέσων μεταξύ τους. Τα υποσυστήματα επικοινωνίας δεδομένων UUCP είναι συνήθως αρκετά ανασφαλή μιάς και σχεδιάστηκαν αποκλειστικά για να επιτρέπουν απομακρυσμένη προσπέλαση.

Οταν το UUCP είναι ενεργό συνδέει ένα απομακρυσμένο σύστημα και εκτελεί εντολές από απόσταση σε αυτό διαβάζοντας και εγγράφοντας σε αρχεία, αν αυτό απαιτείται.

Ετσι αν το σύστημα ασφαλείας δεν είναι περιοριστικό,

ένας χρήστης μπορεί να προκαλέσει σημαντικά προβλήματα στο σύστημα. Εντούτοις σε πολλές περιπτώσεις το λογισμικό του UUCP είναι αρκετά ασφαλές αν έχουν ληφθεί οι απαραίτητες προφυλάξεις και περιορισμοί.

## ΣΥΝΘΗΜΑΤΙΚΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ

Συνήθως η προβολή ενός σχηματισμού συνδεόμενων συστημάτων πραγματοποιείται από κάποιους χρήστες ενός συστήματος οι οποίοι επιθυμούν να υπερβούν τα όρια που τους έχουν καθορισθεί. Η απόκτηση πληροφοριών, η χρήση τους, η απόκτηση κάποιων προνομιούχων θέσεων με στόχο καταστροφική δράση και η χρήση των δυνατοτήτων του υπολογιστικού συστήματος χωρίς οικονομική επιβάρυνση, αποτελούν στόχους όσων υπερβαίνουν τις δικαιοδοσίες τους. Το σενάριο που ακολουθείται για σκοπό αυτό είναι το ακόλουθο.

Κάποιος χρήστης χρησιμοποιεί έναν κωδικό σύνδεσης και πειραματιζόμενος προσπαθεί να ανακαλύψει κάποια είσοδο μη προστατευόμενη από συνθηματικό. Αν η διαδικασία αυτή πετύχει, τότε προσπαθεί να αποκτήσει κάποια ισχυρά προνόμια, ώστε να θέσει υπό τον έλεγχό του τα μέσα για την πραγματοποίηση των στόχων του.

Πολύ συχνά τα αρχεία του συστήματος αλλοιώνονται, τα δικαιώματα δε αυτά τροποποιούνται ή προστίθενται στο σύστημα αλλοιωμένες εντολές, ώστε η πρόσβαση σε αυτό μετά από κάποιο

χρονικό διάστημα να μην απαιτεί δύσκολη προσπάθεια.

Πολλές φορές, επίσης, ερευνούνται οι συνθέσεις του δικτύου, ώστε να εντοπισθούν και να προσπελασθούν και άλλα συστήματα.

Για την αποτροπή τέτοιων ενεργειών θα πρέπει οι διαδικασίες επικοινωνίας από απόσταση, οι διαδικασίες δημιουργίας δικτύων, αλλά και όλες οι ενέργειες που σχετίζονται με τη λειτουργία του δικτύου να αντιμετωπίζονται πάντα με γνώμονα την απαιτούμενη αυξημένη ασφάλεια.

## ΤΟ ΠΡΟΒΛΗΜΑ ΤΩΝ ΙΩΝ ΑΥΞΑΝΕΤΑΙ

Στην εποχή μας η πληροφορική εξαπλώθηκε με μεγάλους ρυθμούς και τα ωφέλη της ηλεκτρονικής επεξεργασίας δεδομένων έφτασαν μέχρι τον απλό άνθρωπο.

Καθώς συνδέουμε όλο και πιο πολύ την τεχνολογία των υπολογιστών με την καθημερινή μας εποχή μπορεί να αποδειχθεί ότι είναι εποχή στην οποία αγωνιζόμαστε να διατηρήσουμε τον έλεγχό μας από βανδάλους σαμποτέρ και κοινωνικά αναπροσάρμοστα άτομα.

Η ζημιά που μπορούν να προκαλέσουν οι ιοί είναι τεράστια. Πρέπει να λαμβάνονται σοβαρά υπόψη.

Οι ιοί έχουν κοστίσει πολλά εκατομμύρια δολλάρια σε οργανισμούς, εταιρείες και εκπαιδευτικά ιδρύματα για την πρόληψη και την αντιμετώπισή τους. Εχουν την δυνατότητα να εισβάλλουν και να καταστρέφουν συστήματα και δίκτυα υπολογιστών τα οποία είναι ζωτικής σημασίας για τις επικοινωνίες - για παράδειγμα, τις τηλεφωνικές υπηρεσίες, υπηρεσίες πρόληψης πυρκαγιών και άλλων καταστάσεων ανάγκης, τις στρατιωτικές επικοινωνίες και τον έλεγχο εναέριων συγκοινωνιών.

Οι ιοί προσβάλλουν πολλούς τομείς των επιχειρήσεων, της κυβέρνησης και της επιστημονικής έρευνας αλλά είναι αδύνατον να μετρηθεί επ'ακριβώς το μέγεθος της εισβολής διότι πολλά από τα θύματα αποκρύπτουν το γεγονός ότι προσβλήθηκαν, λόγω της αρνητικής δημοσιότητας που μπορεί αυτό να έχει.

Εγινε σκληρή προσπάθεια να αποκτηθεί ακριβής ποσοτικός προσδιορισμός για την έκταση του προβλήματος αλλά η έλλειψη αναφοράς τέτοιων περιστατικών δείχνει ότι αυτή τη στιγμή υπάρχει μόνο μια θολή εκτίμηση του προβλήματος, δεδομένου ότι μόνο μερικές χιλιάδες από τις μολύνσεις έχουν αναφερθεί στην επιτροπή.

Δεν υπάρχει αμφιβολία ότι ο ρυθμός μολύνσεων αυξάνει συνεχώς. Διάφορες στατιστικές αναφέρουν χαρακτηριστικά το δεκαπλασιασμό της αύξησης των μολύνσεων. Προκύπτει ακόμη κι ένα θέμα ηθικής από το πρόβλημα της μόλυνσης από ιούς : το δικαίωμα του καθενός να διατηρήσει κρυφό τον ιδιωτικό του βίο ενάντια στην ανάγκη να υπάρχουν μαρτυρίες οι οποίες να αποδεικνύουν τέτοιου είδους εγκληματικές δραστηριότητες.

## ΛΥΝΟΝΤΑΣ ΤΟ ΠΡΟΒΛΗΜΑ ΤΩΝ ΙΩΝ - ΟΧΙ ΗΜΙΜΕΤΡΑ

Ο Joseph Tomphins, Πρόεδρος του Αμερικανικού Συνδέσμου Πρόληψης Εγκλημάτων υπολογιστών είναι της άποψης ότι οι νομικές κυρώσεις και η επιβολή του νόμου αποτελούν μόνο ένα μέρος της λύσης του προβλήματος των ιών. Επισήμανε τη δυνατότητα να τροποποιηθούν οι υπάρχουσες νομοθεσίες σχετικές με παραπτώματα, εγκληματική αδιαφορία, απάτες για να δημιουργηθούν νέες μορφές νόμων.

Η εισαγωγή νομικών κυρώσεων θα μπορούσε να βοηθήσει στην καταδίωξη των δημιουργών ιών, με το σκεπτικό ότι αν οι επι-

χειρήσεις μπορούσαν να απαιτήσουν αποζημίωση για τις ζημιές που υφίστανται από τους ιούς, θα είχαν πολύ ισχυρά κίνητρα για να αποκαλύπτουν τις περιπτώσεις των μολύνσεων. Στην πραγματικότητα, είναι συνήθως αδύνατο να βρεθούν οι δημιουργοί των ιών ή αυτοί που είναι υπεύθυνοι για τη διάδοσή τους σε συγκεκριμένα συστήματα.

Οι περισσότεροι ιοί δημιουργούνται με μυστικότητα. Είναι μια δραστηριότητα μοναχικών ανθρώπων που έχει συνήθως τη μορφή ηλεκτρονικού βανδαλισμού, κακόβουλης διασκέδασης ή εκδίκησης προς κάποιο συγκεκριμένο άτομο ή το κοινωνικό σύνολο.

Η αμερικάνικη κοινότητα που ασχολείται με τους υπολογιστές έχει πάρει ελάχιστη εως καθόλου βοήθεια από κυβερνητικές υπηρεσίες όπως το Ομοσπονδιακό Γραφείο Ερευνών, το Υπουργείο Αμυνας και τον Οργανισμό Εθνικής Ασφάλειας, μολονότι η προστασία είτε από οικείους είτε από εξωτερικούς ιούς είναι θέμα εθνικής σημασίας.

Ορισμένοι από τους ειδικούς που κατέθεσαν στο Κονγκρέσο πιστεύουν ότι η έρευνα περί των ιών είναι καλύτερο να αφεθεί σε ανθρώπους οι οποίοι γνωρίζουν πραγματικά την τεχνολογία και όχι σε κυβερνητικές υπηρεσίες. Υπήρξε έντονη κριτική για τους ειδικούς ασφαλείας υπολογιστών οι οποίοι δεν μπόρεσαν να διδαχθούν από την τρώτότητα του UNIX σε μολύνσεις ιών, όπως αποδείχθηκε από την πολυδιαφημισμένη υπόθεση της μόλυνσης του δικτύου INTERNET. Εαν το internet υπήρξε ένα μάθημα γι'αυτούς όπως θα έπρεπε, τότε δε θα έπρεπε να πάθει τα ίδια ένα σύστημα της NASA σχεδόν ένα χρόνο μετά.

## ΠΩΣ ΜΟΛΥΝΕΙ ΕΝΑΣ ΙΟΣ ΤΟΝ ΥΠΟΛΟΓΙΣΤΗ ΣΑΣ

Πως εισχωρεί ένας ιός στον υπολογιστή σας και μετατρέπει την κανονική και υγιή συμπεριφορά του σε μια μορφή ηλεκτρονικής ασθένειας;

Η διαδικασία γίνεται αντιληπτή όταν συγκριθεί με τον τρόπο που προσβάλλεται το ανθρώπινο σώμα από κάποιο μικρόβιο.

Για να επικοινωνήσουμε με τον υπολογιστή χρησιμοποιούμε προγράμματα (software). Χωρίς αυτά ο υπολογιστής είναι απλά μια άχρηστη μηχανή. Το software είναι τόσο το μέσο βάση του οποίου δίνουμε τις εντολές στον υπολογιστή, όσο και ο μηχανισμός ο οποίος δίνει τη δυνατότητα στον υπολογιστή να διεκπεραιώνει αυτές τις εντολές σωστά.

Επειδή ο υπολογιστής είναι μια πολύπλοκη συσκευή, ικανή να κάνει πολλές διαφορετικές πράξεις, οι εντολές που τον εξαναγκάζουν να συμπεριφέρεται με τον πιο επιθυμητό τρόπο τείνουν επίσης να είναι πολύπλοκες.

Για να γίνει η χρήση των υπολογιστών ευκολότερη και γρηγορότερη, χρησιμοποιούμε δυο τύπους προγραμμάτων. Ο πρώτος είναι το λειτουργικό σύστημα, το κύριο πρόγραμμα που ελέγχει όλες τις βασικές λειτουργίες του υπολογιστή. Για παράδειγμα, εποπτεύει τη λειτουργία των οδηγών δίσκων. Όλοι οι υπολογιστές από τους Amica και Manintosh μέχρι τους mini και mainframe έχουν το δικό τους λειτουργικό σύστημα. Τα

λειτουργικά συστήματα μπορεί να έχουν διαφορετική μεταξύ τους αρχιτεκτονική αλλά όλα εκτελούν παρόμοιες λειτουργίες. Αυτό σημαίνει ότι όλα τα λειτουργικά συστήματα είναι τρωτά στους ιούς των υπολογιστών, οι Macintosh μολύνονται από τον ιό McMag ενώ οι προσωπικοί υπολογιστές IBM και οι συμβατοί τους μολύνονται από τον ιό Jerusalem.

Υπάρχει μόνο ένας συγκεκριμένος αριθμός λειτουργικών συστημάτων, ενώ υπάρχουν πολλά προγράμματα από τη δεύτερη κατηγορία, τα προγράμματα εφαρμογών. Αυτά λειτουργούν σε συγκεκριμένα λειτουργικά συστήματα και διεκπεραιώνουν συγκεκριμένες εργασίες, όπως η επεξεργασία κειμένου, η δημιουργία λογιστικών φύλλων, τα παιχνίδια και τα γραφικά.

Οταν ενεργοποιήσετε το σώμα σας μετά από την κατάσταση ανάπαυσης, του δίνετε συγκεκριμένες οδηγίες - σήκω από το κρεββάτι, πιές καφέ και πήγαινε στη δουλειά. Αυτές οι εντολές που φορτώνετε στο μυαλό σας είναι ισοδύναμες με τα προγράμματα εφαρμογής που εκτελείται στους υπολογιστές.

Οταν το σώμα σας είναι υγιές όλα είναι υπό έλεγχο και προβλέψιμα. Δίνεται οδηγίες στο σώμα σας για 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 σας κολλήσει μια μόλυνση τόσο το λειτουργικό σύστημα όσο και τα προγράμματα εφαρμογών θα δυσλειτουργούν. Το μυαλό θα συναντήσει δυσκολίες στο να ελέγχει τις βασικές λειτουργίες.

Ενας ιός υπολογιστών έχει παρόμοια επίδραση στον υπολογιστή σας. Μπορεί να κατατρέψει την ικανότητα του λειτουρ-

γικού συστήματος να ελέγχει τις βασικές λειτουργίες και όταν τρέχουν προγράμματα εφαρμογών μπορεί επίσης να τα παρακάμψει.

## ΠΩΣ ΕΙΣΑΓΩΝΤΑΙ ΙΟΙ ΣΤΟ ΣΥΣΤΗΜΑ ΜΑΣ

Ενώ ο ιός είναι και αυτός πρόγραμμα το οποίο ανοίγει και κλείνει ηλεκτρονικά κυκλώματα ακριβώς όπως το λειτουργικό σύστημα και τα προγράμματα εφαρμογών, εντούτοις όμως διαφέρει σημαντικά από αυτά. Τα κανονικά προγράμματα είναι οι βοηθοί σας.

Οι δημιουργοί των ιών γράφουν τα προγράμματά τους με ένα εντελώς διαφορετικό κίνητρο.

Επειδή έχουν την επιθυμία να δημιουργούν μπελάδες γράφουν προγράμματα που αντί να σας βοηθούν, σας προκαλούν ζημιές. Η μπορεί να γράφουν προγράμματα τα οποία εμφανίζουν πολλές φορές ανόητα μηνύματα - ένα είδος ηλεκτρονικών σκουπιδιών ή προπαγάνδας. Καθώς κανείς δε τα θέλει, ούτε χρειάζεται τέτοιου είδους προγράμματα - και σίγουρα δεν αγοράζονται, ούτε τα δεχόμαστε ως δώρα - οι δημιουργοί τους θα πρέπει να τα φτιάχνουν ελκυστικά και αρκετά έξυπνα ώστε να σας ξεγελούν.

Η παράξενη συμπεριφορά του υπολογιστή σας μπορεί πολύ συχνά να οφείλεται σε λάθος ενός προγράμματος και όχι σε ιούς. Ελέγξτε το αρχείο οδηγιών του προγράμματος ή καλέστε την υπηρεσία υποστήριξης της εταιρείας από την οποία το

προμηθευτήκατε για να εξακριβώσετε αν είναι κάποιο λάθος του προγράμματος ή ιός.

Δε χρειάζεται παρά ένα άτομο να φορτώσει τον ιό από το ηλεκτρονικό ταχυδρομείο του δικτύου για να αρχίσει αυτός να εξαπλώνεται.

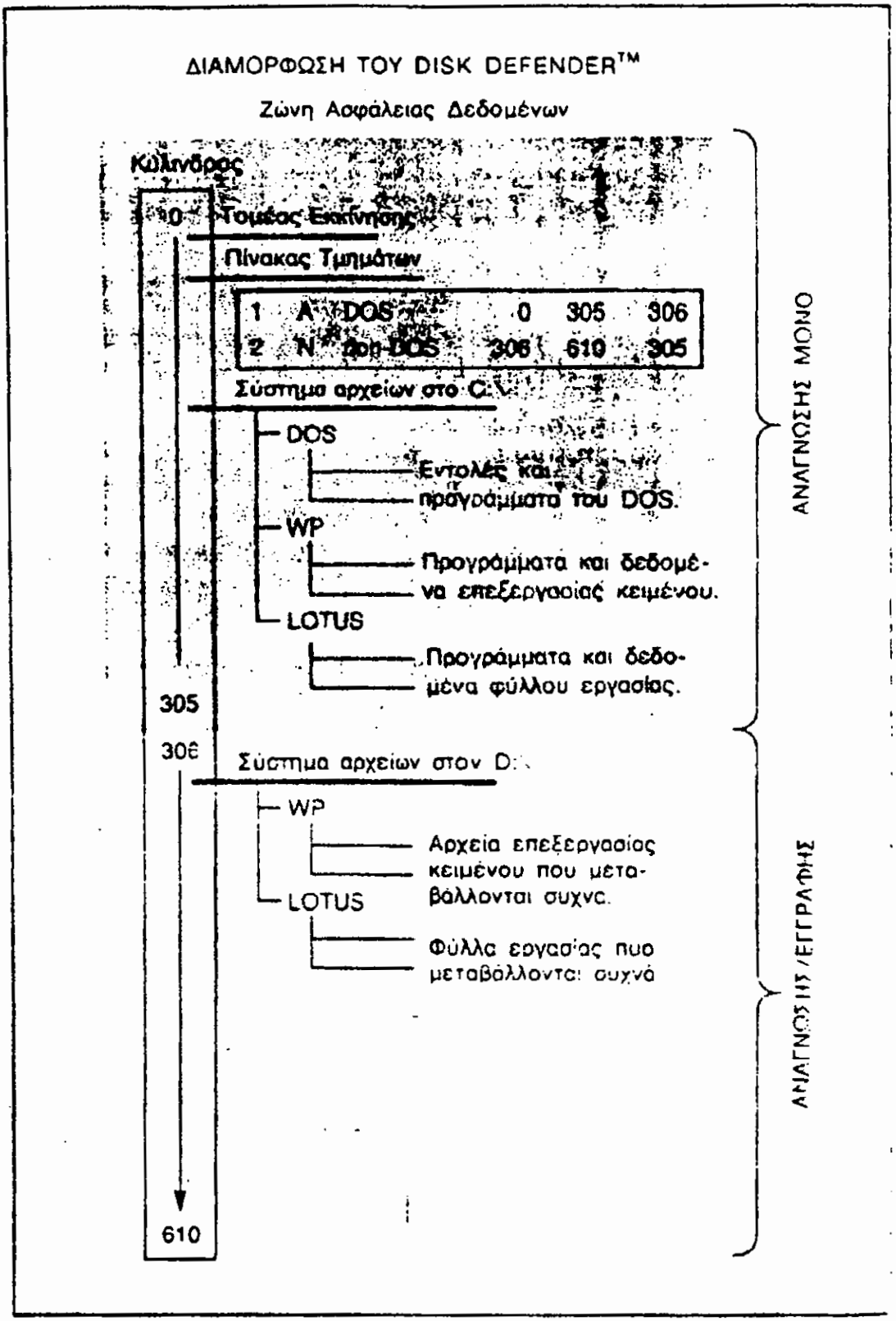
Αφού μπει μέσα στον υπολογιστή αυτού του ατόμου μπορεί να μολύνει τα αρχεία του σκληρού δίσκου του, αλλά και των δισκετών. Κατόπιν όταν το πρώτο θύμα επικοινωνήσει με κάποιον άλλον χρήστη του δικτύου ή δανείσει κάποιες από τις μολυσμένες δισκέτες σε έναν φίλο ο ιός εξαπλώνεται έχοντας έτσι πολύ περισσότερες ευκαιρίες να κάνει ζημιά.

Με την επιδημία των ιών βλέπουμε πλέον πολλές χιλιάδες υπολογιστών να μην τρέχουν δυο αλλά τρία είδη προγραμμάτων, τα λειτουργικά συστήματα, τις εφαρμογές που έχουν σκόπιμα εγκατασταθεί από τον χρήστη και τους ανεπιθύμητους εισβολείς-τους ιούς. Αφού εισβάλλει σε ένα σύστημα ένας ιός μπορεί να συμπεριφερθεί με πολλούς διαφορετικούς τρόπους, είτε αποκαλύπτοντας αμέσως την παρουσία του, είτε παραμένοντας κρυμμένος εν'όσω θα κάνει καταστροφές και θα αναπαράγει τον εαυτό του.

Είναι λογικό οι ιοί να σχεδιάζονται έτσι ώστε να εισβάλλουν στα συστήματα μέσω των αρχείων που είναι πιο πιθανό να συναντήσουν σε αυτά. Έτσι λοιπόν τα COM, τα EXE και τα SYS αρχεία που είναι μέρος σχεδόν όλων των υπολογιστών με λειτουργικό σύστημα DOS είναι εμφανές στόχος. Τα άλλα λειτουργικά συστήματα έχουν βέβαια άλλα τρωτά σημεία.

Πολλά προγράμματα εφαρμογών έχουν την δυνατότητα να δημιουργούν η ακόμα να τροποποιούν τα ήδη υπάρχοντα αρχεία με

ονόματα CONFING.SYS και AUTOEXEC.BAT. Το DOS ψάχνει πάντα για τα δυο αυτά αρχεία κατά τη διαδικασία εκκίνησης για να διαβάσει από αυτά πληροφορίες για τη 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 έχετε, προκαλώντας τη ζημιά σε κλάσματα του δευτερολέπτου καθώς εκκινείτε τον υπολογιστή σας, και πριν προλάβει να τρέξει κάποιο πρόγραμμα ανίχνευσης.


ΔΙΑΜΟΡΦΩΣΗ ΤΟΥ DISK DEFENDER™
Ζώνη Ασφάλειας Δεδομένων
Κύλινδρος
0
Τομέας Εκκίνησης
Πίνακας Τμημάτων
1 A DOS 0 305 306
2 N Δοκ DOS 306 610 305
Σύστημα αρχείων στο C:\
DOS
Εντολές και προγράμματα του DOS.
WP
Προγράμματα και δεδομένα επεξεργασίας κειμένου.
LOTUS
Προγράμματα και δεδομένα φύλλου εργασίας.
305
306
Σύστημα αρχείων στον D:\
WP
Αρχεία επεξεργασίας κειμένου που μεταβάλλονται συχνα.
LOTUS
Φύλλα εργασίας που μεταβάλλονται συχνά
610
ΑΝΑΓΝΩΣΗΣ ΜΟΝΟ
ΑΝΑΓΝΩΣΗΣ/ΕΓΓΡΑΦΗΣ

## ΠΩΣ ΟΙ ΙΟΙ ΕΛΕΓΧΟΥΝ ΤΟ ΠΡΟΓΡΑΜΜΑ ΣΑΣ

Η πιο ενοχλητική άποψη της επιδημίας των ιών είναι ότι ο μέσος όρος των χρηστών αρχίζει να χάνει τον έλεγχο του υπολογιστή τους. Τις εντολές τις οποίες δίνει ο χρήστης στον υπολογιστή του μπορούν να παραμορφωθούν από κάποιον ιό που έχει σχεδιαστεί γι'αυτόν το σκοπό. Το χάσιμο του ελέγχου μπορεί να επιτευχθεί με πολλούς τρόπους, ανάλογα με τον τρόπο που είναι προγραμματισμένος ο ιός που εισέβαλλε στον υπολογιστή σας. Ούτε ο χρήστης, ούτε το λειτουργικό σύστημα μπορεί να ελέγξει μια τέτοια κατάσταση, δεδομένου ότι οι ιοί είναι σχεδιασμένοι να λειτουργούν με τα δικά τους μέτρα και σταθμά. Μπορεί επίσης σκόπιμα να εξαθλιώσει τα αρχεία σας, καταστρέφοντάς τα ή παραμορφώνοντάς τα κατά τις επιθυμίες του.

Η λέξη κλειδί στο να καταλάβετε πως 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 του ιδίου τύπου.

Μπορεί να προσκολληθούν εξωτερικά σε ένα αρχείο, ή μπορούν να βρουν χώρο στο εξωτερικό κάποιων προγραμμάτων όπου και αυτοεγκαθίστανται.

Η διαδικασία αυτή - της διακοπής της κανονικής λειτουργίας του υπολογιστή και της ανάληψης του ελέγχου από τον ιό για να αναπαραχθεί και να κολλήσει σε άλλα αρχεία και το ξεπέρασμα 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 στη μνήμη του υπολογιστή, έτσι ώστε να μπορούν να μολύνουν το κάθε πρόγραμμα που επιτελείται.

Μπορούν να τροποποιήσουν τον τομέα εκκίνησης του δίσκου ώστε να δημιουργήσουν ένα πιο άνετο περιβάλον για να δρουν και να αναπαράγονται.

## ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΛΗΨΗ ΤΩΝ ΜΟΛΥΝΣΕΩΝ

Στην πραγματικότητα, μπορείτε να μειώσετε τον κίνδυνο έκθεσης στις μολύνσεις ιών κατά 90% τουλάχιστον. Αυτό όμως που είναι ακόμη καλύτερο είναι ότι ακόμη και αν γίνεται θύμα, θα έχετε τη δυνατότητα να ανακτήσετε σχετικά εύκολα τα δεδομένα σας και να ελαχιστοποιήσετε τη ζημιά.

Τα καλύτερα πάντως νέα είναι ότι μπορείτε να διατηρήσετε το πιο πολύτιμο συστατικό ολόκληρου του συστήματός σας - τα δεδομένα - ενάντια στους περισσότερους από τους φυσικούς κινδύνους και τις τεχνικές καταστροφές που είναι πιθανόν να

συναντήσετε.

Το κόστος της οικονομικής επένδυσης ωχριά μπροστά στην αξία των δεδομένων που το Hardware μαζί με τα προγράμματα σας δίνουν τη δυνατότητα να παράγετε. Τα δεδομένα αυτά είναι μοναδικά. Το hardware και πιθανώς και τα προγράμματα εφαρμογών του συστήματος μπορούν εύκολα να αντικατασταθούν. Σε περιπτώσεις πολλών καταστροφών υπολογιστών, η αντικατάσταση μπορεί και να μην κοστίσει τίποτα παραπάνω από μια απλή ενόχληση, δεδομένου ότι οι απώλειες καλύπτονται από την ασφάλεια.

Εντούτοις δεν υπάρχει κανενός είδους εταιρεία η οποία να μπορεί να σας αντικαταστήσει τα δεδομένα σας. Η προστασία των δεδομένων σας, του πιο πολύτιμου ηλεκτρονικού αγαθού είναι εντελώς δικιά σας ευθύνη. Ευτυχώς αυτό δεν είναι και πολύ δύσκολο ούτε απαιτεί ειδικές τεχνικές γνώσεις, ενώ στοιχίζει σχεδόν τίποτα.

## ΧΡΗΣΙΜΟΠΟΙΗΣΤΕ ΦΥΣΙΚΕΣ ΜΕΘΟΔΟΥΣ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΨΕΤΕ ΤΟ ΣΥΣΤΗΜΑ ΣΑΣ

Οι τεχνικές προτάσεις που δημιουργεί το θέμα των υπολογιστών και των ιών ειδικότερα τείνουν πολλές φορές να παραμερίσουν το γεγονός ότι οι ιοί είναι κατά βάση ένα ανθρώπινο πρόβλημα. Ο πρώτος κανόνας πρόληψης των ιών είναι να προστατεύεται το σύστημα από τους ανθρώπους που μπορεί να το

εκθέσουν σε μολύνσεις, είτε σκόπιμα, είτε από ατυχία.

Οπως το αυτοκίνητο είναι εκτεθειμένο σε κίνδυνο είτε κινείται, είτε όχι, έτσι ο υπολογιστής διατρέχει τους ίδιους περίπου κινδύνους. Καθορίστε τους επικίνδυνους ανθρώπους με προσοχή - ο μεγαλύτερος κίνδυνος μπορεί να προέλθει από τους καλύτερους φίλους σας, του πιο έμπιστους υπαλλήλους σας ή ακόμη και από τα μέλη της οικογένειάς σας. Επίσης φυλάξτε τις δισκέτες σας με θρησκευτική ευλάβεια - είναι η πιο κοινή πηγή μολύνσεων.

## ΑΠΑΓΟΡΕΥΣΤΕ ΤΗΝ ΠΡΟΣΠΕΛΑΣΗ ΣΤΟ ΣΥΣΤΗΜΑ ΣΑΣ

Οποιοσδήποτε έχει προσπελάσει στο σύστημά σας θα πρέπει να αποτελεί έναν πιθανόν κίνδυνο. Δοκιμάστε να παραβιάσετε μόνοι σας το σύστημά σας ή αν είστε υπεύθυνος για το σύστημα υπολογιστών σε μια εταιρεία, οργανώστε μια προσομοίωση εισβολής. Πολλές εταιρείες έμαθαν πολλά για την ασφάλεια υπολογιστών χρησιμοποιώντας ειδικές ομάδες εισβολής για τα συστήματά τους.

Η απαγόρευση της προσπέλασης στο σύστημα είναι μια διαδικασία τόσο απλή όσο η τοποθέτηση του υπολογιστή σε ένα κλειδωμένο δωμάτιο. Ετσι δε θα υπάρχει τρόπος μόλυνσης, μόνο στην περίπτωση που κάποιος έχει την ευκαιρία να τρέξει ένα μολυσμένο πρόγραμμα σε αυτόν.

Να επιτρέπετε να χρησιμοποιούν το σύστημά σας μόνο όσοι

το έχουν ανάγκη και μόνο υπό την επίβλεψή σας, ώστε να τηρούνται όλες οι διαδικασίες ασφαλείας.

Εκθέτετε επίσης σε κίνδυνο το σύστημά σας όταν επιτρέπετε στους πωλητές προγραμμάτων, συμβούλους ή άλλους ανθρώπους να προσπελάσουν τον υπολογιστή σας για να τρέξουν διάφορα προγράμματα ή εργασίες. Εαν δε μπορείτε να απαγορεύσετε αυτού του είδους την προσπέλαση στο σύστημά σας, περιορίστε την όσο μπορείτε και όταν δε μπορείτε να την αποφύγετε, θα μπορούσατε να υποχρεώσετε τους διαφόρους να ελέγχουν τις δισκέτες τους πριν περάσουν την πόρτα του γραφείου σας.

Να θυμάστε πάντα ότι όλοι οι υπάλληλοι που προσπελαύνουν ένα "ευαίσθητο", όσον αφορά την ασφάλεια σύστημα, θα μπορούσαν επίσης να το σαμποτάρουν αν έχουν κάποια τέτοια πρόθεση.

Πολλές εταιρείες κάνουν συντονισμένες ενέργειες για να απομονώσουν τα υπολογιστικά τους συστήματα από υπαλλήλους αμφιβόλου ποιότητος που έχουν απολυθεί. Να έχετε όμως υπόψη σας ότι μέχρι να λάβουν κάποια τέτοια μέτρα μπορεί ο ιός να έχει ήδη τοποθετηθεί σε κάποιο σύστημα.

Η χρήση ενός ημερολογίου του συστήματος εντείνει στους υπαλλήλους την ανάγκη για ασφάλεια και μπορεί να παρέχει πολύτιμες πληροφορίες στην περίπτωση που θα εμφανιστεί κάποια μόλυνση.

Βέβαια το ημερολόγιο από μόνο του δε μπορεί να εμποδίσει την ανεπίτρεπτη προσπέλαση. Οι αυτόματες διαδικασίες σύνδεσης με το σύστημα μπορούν να επεκταθούν ώστε να καταγράφουν

τη δραστηριότητα που λαβαίνει χώρα σε όλα τα προγράμματα εφαρμογών που χρησιμοποιούνται στο σύστημα. Οι διαδικασίες αυτές μπορούν να έχουν τη μορφή ενός απλού αρχείου ομαδοποιημένων εντολών (batch file).

Μην αποθηκεύετε τα ημερολόγια μόνο σε ηλεκτρονική μορφή. Θα μπορούσαν να χαθούν και αυτά σε περίπτωση μόλυνσης από ιό. Κρατήστε τα σε χαρτί.

**ΦΥΛΑΞΤΕ ΤΙΣ ΔΙΣΚΕΤΕΣ ΣΑΣ ΚΑΙ ΚΡΑΤΕΙΣΤΕ ΤΟΥ ΞΕΝΟΥΣ ΜΑΚΡΥΑ ΤΟΥΣ**

Οι μολυσμένοι δίσκοι είναι αυτοί που πιθανώς διαδίδουν τους περισσότερους ιούς. Είναι προφανές ότι οι ξένες δισκέτες δε θα πρέπει να χρησιμοποιούνται αν δεν περάσουν από έλεγχο, αλλά και αυτές που χρησιμοποιούνται ήδη σε ένα "καθαρό" σύστημα μπορούν να μολυνθούν χωρίς να το αντιληφθεί κανείς. Μπορεί για παράδειγμα, κάποιος να χρησιμοποιήσει μια δισκέτα σε άλλη μηχανή μέσα στο γραφείο ή στο σπίτι του - η απόσταση δεν παίζει κανένα ρόλο όσον αφορά το ρίσκο μόλυνσης.

Μπορεί να τοποθετήσετε μια δισκέτα σε κάποιον άλλο υπολογιστή είτε μέσα στον ίδιο δωμάτιο είτε κάποιου άλλου για να εκτυπώσετε κάποιο αρχείο σας με έναν εκτυπωτή Laser ή plotter και να μολυνθεί έτσι. Μπορεί επίσης να την πάρετε στο σπίτι για να τελειώσετε μια εργασία το Σαββατοκύριακο με τον προσωπικό σας υπολογιστή, όπου εκεί είναι εκτεθειμένη στον κίνδυνο από πολλές πηγές. Μπορεί ακόμη να τη μετακινή-

σετε από τη μια όψη του γραφείου σας στην άλλη, για να μεταφέρετε δεδομένα ή προγράμματα από τον υπολογιστή σας σε κάποιον άλλον φορητό, όπου και αυτό το τόσο μικρό ταξίδι μπορεί να αποβεί επικίνδυνο.

Ποτέ μη δανείζετε δισκέτες των προγραμμάτων σας σε άλλους - μπορεί να κολλήσουν κάποιο ιό και να τον μεταφέρουν και στο σύστημά σας. Εάν έχετε κάποιο σοβαρό λόγο για να δανείσετε ένα πρόγραμμα, δώστε το σε δισκέτα αντίγραφο, την οποία θα καταστρέψετε και θα ξαναφορτώσετε όταν σας επιστραφεί.

Αυτές και πολλές άλλες περιπτώσεις φυσικής μεταφοράς δισκετών από το ένα σύστημα στο άλλο, προσφέρουν πολλές ευκαιρίες για εξάπλωση ιών, αλλά ουσιαστικά μπορεί να τις έχετε όλες υπό τον έλεγχό σας και να απαιτείτε να λαμβάνονται οι λογικές προφυλάξεις. Το να απαγορεύετε να χρησιμοποιούνται στον υπολογιστή σας ξένες δισκέτες μέχρις ότου σιγουρευτείτε ότι δε φέρουν ιούς είναι πιο δύσκολο. Τέτοιες δισκέτες μπορούν να εισαχθούν στο σύστημά σας με τον πιο αθώο τρόπο.

Είναι προφανές ότι δε θα πρέπει να επιτρέπετε σε κανέναν να χρησιμοποιεί τις δικές σας δισκέτες προγραμμάτων στον υπολογιστή σας. Ούτε και θα πρέπει να τις δέχεστε ως δώρα ή δανεικές δισκέτες με πειρατικά προγράμματα. Τα πειρατικά αντίγραφα προγραμμάτων έχουν τόσο εκτεταμένη χρήση που μπορεί να έχουν περάσει από αναρρίθμητες μηχανές πριν από εσάς, οποιεσδήποτε εκ των οποίων θα μπορούσαν να είναι μολυσμένες.

Να είστε ιδιαίτερα προσεκτικοί με τους ντήλερς οι οποίοι προσπαθούν να σας δελεάσουν με το να σας προσφέρουν μαζί με

τον υπολογιστή σας και αντίγραφο πολλών προγραμμάτων - είτε μέσα στο σκληρό δίσκο που σας πούλησαν, είτε σε δισκέτες. Τα προγράμματα αυτά μπορεί να είναι είτε ελεύθερα προς διανομή (freeware, shaveware), είτε πειρατικά αντίγραφα προγραμμάτων που πωλούνται στο εμπόριο. Ασχετα με την πηγής του όμως, για σας θα πρέπει να θεωρούνται ύποπτα όσον αφορά τους ιούς.

**ΣΗΜΑΝΤΙΚΟ ΓΕΓΟΝΟΣ** : Ορισμένα βοηθητικά προγράμματα έχουν τη δυνατότητα να ελέγχουν την κατάσταση των προγραμμάτων και των δίσκων σας πολύ εύκολα. Καλό είναι να τα χρησιμοποιείτε τακτικά, δημιουργώντας μια ρουτίνα για τον υπολογιστή σας, η οποία πολλά θα σας αποφέρει.

Οι προσεκτικές εταιρείες ή ακόμη και ιδιώτες χρήστες, υποβάλλουν σε τέτοιου είδους ελέγχους ακόμη και τις αυθεντικές και σφραγισμένες δισκέτες προγραμμάτων που αγοράζουν πριν τις χρησιμοποιήσουν. Αυτές οι προφυλάξεις έχουν καταστεί αναγκαίες τόσο λόγω σκόπιμων όσο και τυχαίων μολύνσεων που μπορούν να συμβούν σε εμπορικά προγράμματα, ακόμη και σε αυτά των μεγαλύτερων εταιρειών κατασκευής προγραμμάτων.

Πολλοί λιανικοί πωλητές δημιουργούν συνεχώς άθελά τους και χωρίς να το ξέρουν νέα θέματα λόγω της γενναιόδωρης πολιτικής των ανταλλαγών και επιστροφών που ακολουθούν. Ενα προιόν που επιστράφηκε μολυσμένο μπορεί να ξαναπουληθεί σε άλλον πελάτη. Ποτέ λοιπόν μην αγοράζετε προγράμματα τα οποία δεν είναι στην αυθεντική, σφραγισμένη συσκευασία. Εντούτοις όμως ούτε και αυτό είναι απόλυτα εγγυημένο, δεδομένου ότι

πολλοί κατασκευαστές προγραμμάτων ξαναπακετάρουν και ξανασφραγίζουν τις δισκέτες που επιστρέφονται για να τις ξαναπουλήσουν. Ας ελπίσουμε ότι αυτή η πρακτική θα παρακμάσει, τουλάχιστον μεταξύ των σοβαρών κατασκευαστών software που έχουν κάποια φήμη να προστατέψουν.

Οπου και όποτε είναι πρακτικό και ταιριάζει με τις ανάγκες σας, αγοράζετε πάντα την τελευταία έκδοση ενός προγράμματος. Μια αξιόλογη εταιρεία κατασκευής προγραμμάτων συνεχώς βελτιώνει τα προιόντα της, οπότε η έκδοση ενός πρροιόντος θα πρέπει να περιέχει πολύ λιγότερα λάθη από όλες τις προηγούμενες.

Οι ιοί θα συνεχίσουν να προσβάλλουν τα προγράμματα των διαφόρων κατασκευαστών οι οποίοι έχουν λάβει ορισμένα μέτρα ώστε να περιορίσουν στο ελάχιστο από τους εισβολείς.

Οι κατασκευαστές προγραμμάτων ξέρουν ότι μπορεί να εκτεθούν με σφραγισμένες δισκέτες της φίρμας τους. Μην περιμένετε όμως να δείτε ταμπελάκια που να αναγράφουν "Εγγυημένα χωρίς ιούς", ακόμα και στα πιο σοβαρά προιόντα.

## ΤΕΧΝΙΚΕΣ ΠΡΟΛΗΨΗΣ ΙΩΝ

Εάν όντως χρησιμοποιήσετε κάποια ξένη διασκέτα που μπορεί να είναι μολυσμένη - ειδικά με ένα νέο πρόγραμμα - και

δεν έχετε ένα αποτελεσματικό πρόγραμμα ανίχνευσης ιών, προσπαθήστε να δείτε τα αρχεία της μέσα από κάποιον επεξεργαστή κειμένων. Ψάξτε για ασυνήθιστες ή χυδαίες εκφράσεις μέσα στον ακατανόητο κατά τα άλλα κώδικα μηχανής που περιέχουν. Τέτοια μηνύματα εμφανίζουν πολλοί ιοί και καλό θα είναι να ψάξετε για φράσεις όπως "WARNING" "VIRUS", "ΚΑ - ΗΑ" ή άλλες κοινές βρισιές. Καταγράψτε το όνομα, τη διεύθυνση και το σήμα του copyright του κατασκευαστή. Εάν λείπουν ή φαίνονται να είναι ψεύτικα, υποπτευθείτε κάποιον hacker. Να έχετε πάντως υπόψη σας ότι ακόμη και η απλή ανάγνωση αυτών των αρχείων μέσα από τον επεξεργαστή κειμένου μπορεί να απελευθερώσει κάποιους ιούς.

Ενα άλλο προληπτικό μέτρο, είναι να διαβάζετε το αρχείο οδηγιών που συνήθως συνοδεύει ένα νέο πρόγραμμα και έχει επέκταση ονόματος η TXT ή DOC. Ενα προσεκτικά κατασκευασμένο πρόγραμμα που μεταφέρει ιό, θα μπορούσε να περιέχει ένα αρχείο README. Εάν όμως οι εκφράσεις και η ποιότητα του κειμένου που περιέχει είναι φτωχή, αυτό είναι μια προειδοποίηση ότι ίσως πρόκειται για ιό.

Τα αυτοκόλλητα προστασίας από την εγγραφή κάνουν σημαντική δουλειά και θα πρέπει να τα χρησιμοποιήσετε σε όλες τις δισκέτες που δεν πρόκειται να γράφετε πάνω τους. Προστατεύοντας τις δισκέτες από εγγραφή τις απομονώνετε από τις επιθέσεις των ιών. Αν δείτε να εμφανίζεται κάποιο ανεξήγητο μήνυμα λάθους προστασίας από εγγραφή (write protect error) όταν έχετε τη δισκέτα μέσα στον οδηγό αλλά δεν κάνετε καμία ενέργεια για να την προσπελάσετε, να το θεωρήσετε σαν

πιθανή δραστηριότητα ιού.

Να έχετε πάντα προστατευόμενη από εγγραφή τη δισκέτα εκκίνησης του λειτουργικού συστήματος και να χρησιμοποιείτε μόνο αυτή αν ο υπολογιστής σας έχει μόνο δυο οδηγούς δισκετών χωρίς σκληρό δίσκο. Εάν έχετε σκληρό δίσκο και φορτώνετε από αυτόν το λειτουργικό σύστημα μπορείτε να επεκτείνετε αυτή τη μέθοδο προστασίας, κάνοντας αναγνώσιμα μόνο (read only) τα αρχεία COM και EXE. Η διαδικασία αυτή έχει διάφορες μορφές ανάλογα με την έκδοση του DOS που χρησιμοποιείτε, ενώ υπάρχουν ειδικά βοηθητικά προγράμματα για τον ίδιο σκοπό.

Εάν έχετε σκληρό δίσκο, ποτέ μην ανάβετε τον υπολογιστή έχοντας δισκέτα σε κάποιο οδηγό. Αυτό για να διασφαλίσετε ότι το λειτουργικό σύστημα εκκινεί πάντα από το σκληρό δίσκο και όχι από κάποια δισκέτα που πιανόν να περιέχει έναν ιό που μολύνει τον τομέα εκκίνησης, ικανό να αποκτήσει άμεσα τον έλεγχο του υπολογιστή σας.

Καλό θα ήταν να αντικαθιστάτε περιοδικά τα πιο ευάλωτα αρχεία του λειτουργικού συστήματος από την αυθεντική δισκέτα, την οποία διατηρείτε "καθαρή" και ξέρετε ότι δεν περιέχει ιούς. Πέρα από τα COM, EXE και SYS αρχεία που είναι οι πιο κοινοί στόχοι των ιών, μη ξεχνάτε και τα αρχεία οδηγών συσκευών (όπως του ποντικιού για παράδειγμα) που φορτώνονται από το αρχείο CONFING.SYS. Να αντικαθιστάτε και αυτά επίσης.

## ΝΑ ΕΙΣΤΕ ΙΔΙΑΙΤΕΡΑ ΠΡΟΣΕΚΤΙΚΟΙ ΟΤΑΝ ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ BULLETIN BOARDS

Δεδομένου ότι δρουν σα μέσο επικοινωνίας για την ανταλλαγή δεδομένων και συχνά προγραμμάτων, τα bulletin boards είναι ιδιαίτερα τρωτά σα μεταφορείς ιών.

Αν και πολλά στοιχεία τους θα σας δελεάσουν, μη φορτώσετε ποτέ προγράμματα από ύποπτα bulletin boards. Επίσης μη χρησιμοποιείτε bulletin boards που διαδίδουν πειρατικά προγράμματα. Εχετε τις ίδιες πιθανότητες να κολλήσει ο υπολογιστής σας με όσες θα είχατε να κολλήσετε οι ίδιοι κάποιον βιολογικό ιό αν χρησιμοποιήσετε κάποια μη ασφαλή δημόσια λουτρά.

Ενας αριθμός χρηστών που βρίσκει τα bulletin boards χρήσιμα αλλά και διασκεδαστικά, χρησιμοποιεί πλέον έναν υπολογιστή αποκλειστικά και μόνο για το σκοπό αυτό. Ετσι αν κολλήσουν κάποιο ιό θα μπορούν εύκολα να τον απομονώσουν και να τον εξαλείψουν, χωρίς να μπορέσει να εισβάλλει στο κανονικό τους σύστημα και να καταστρέψει πολύτιμα αρχεία.

Το φόρτωμα των προγραμμάτων που έχουν "συμπιεστεί" για να γλυτώσουν τόσο χώρο στον δίσκο όσο και χρόνο εκπομπής τους έχουν γίνει ένα ιδιάζον πρόβλημα. Οι διαδικασίες συμπίεσης και αποσυμπίεσης των αρχείων απαιτούν ειδικά προγράμματα, τα οποία με την σειρά τους είναι ιδανικά μέρη τόσο για να κρυφτεί ένας ιός, όσο και για να ενεργοποιηθεί και να κάνει ζημιά.

Εάν όντως φορτώσετε κάποιο πρόγραμμα από bulletin board ή άλλο δίκτυο κατευθείαν στο σκληρό δίσκο, βάλτε το προσωρινά τουλάχιστον σε απόμόνωση πριν το τρέξετε και διακινδυνεύσετε την απελευθέρωση κάποιου ιού μέσα στα αρχεία σας.

Αυτό μπορείτε να το κάνετε ως εξής :
αντιγράφετε πρώτα τα αρχεία από το δίκτυο σε μια κενή δισκέτα την οποία μόλις φορμάρετε και δεν περιέχει τίποτα. Κατόπιν, σβήστε το πρόγραμμα που φορτώσατε στο σκληρό δίσκο και μην προσπαθήσετε να το τρέξετε αν δεν το ελέγξετε στη δισκέτα. Μόνον όταν αποδειχθεί ότι το πρόγραμμα δεν είναι μολυσμένο, μπορείτε να το ξαναφορτώσετε στο σκληρό σας δίσκο.

Ορισμένα από τα προγράμματα που κυκλοφορούν στα bulletin board ή πωλούνται σε εκθέσεις υπολογιστών, μοιάζουν να προσφέρουν γη και ουρανό, πράγμα που μπορεί να είναι παγίδα. Ενα πραγματικά καλό πρόγραμμα αργά ή γρήγορα γίνεται γνωστό και είναι απίθανο ο δημιουργός του να επιλέξει την ανωνυμία. Ενα άγνωστο πρόγραμμα που ο δημιουργός του δεν έχει δώσει το όνομά του πρέπει να θεωρείται ύποπτο. Ομοια θα πρέπει να αντιμετωπίζονται και τα προγράμματα που είναι μικρά σε μέγεθος και υπόσχονται εκπληκτικά αποτελέσματα. Τέτοια στοιχεία θα πρέπει να σας κάνουν να υποπτεύεστε ότι το πρόγραμμα που φορτώσατε στο δίσκο μπορεί να είναι ιός κρυμμένος σε ένα δούρειο ίππο.

Σε αυτήν την περίπτωση, η καλύτερη ενέργεια αναχαίτησης είναι να σβήσετε το πρόγραμμα από το σκληρό δίσκο ή να ξαναφορμάρετε τη δισκέτα στην οποία βρίσκεται και να μην πάρετε περισσότερο ρίσκο με αυτό.

## ΝΕΑ ΤΕΧΝΟΛΟΓΙΚΑ ΕΠΙΤΕΥΓΜΑΤΑ ΓΙΑ ΤΗΝ ΠΡΟΛΗΨΗ ΙΩΝ

Η καλύτερη και πιο αποδοτική πρόληψη των μολύνσεων θα υπάρξει όταν η αρχιτεκτονική θα αλλάξει δραστικά, ώστε να παρέχει ένα περιβάλλον στο οποίο αυτά τα αναπαραγόμενα προγράμματα δε θα μπορούν να ευδοκιμούν.

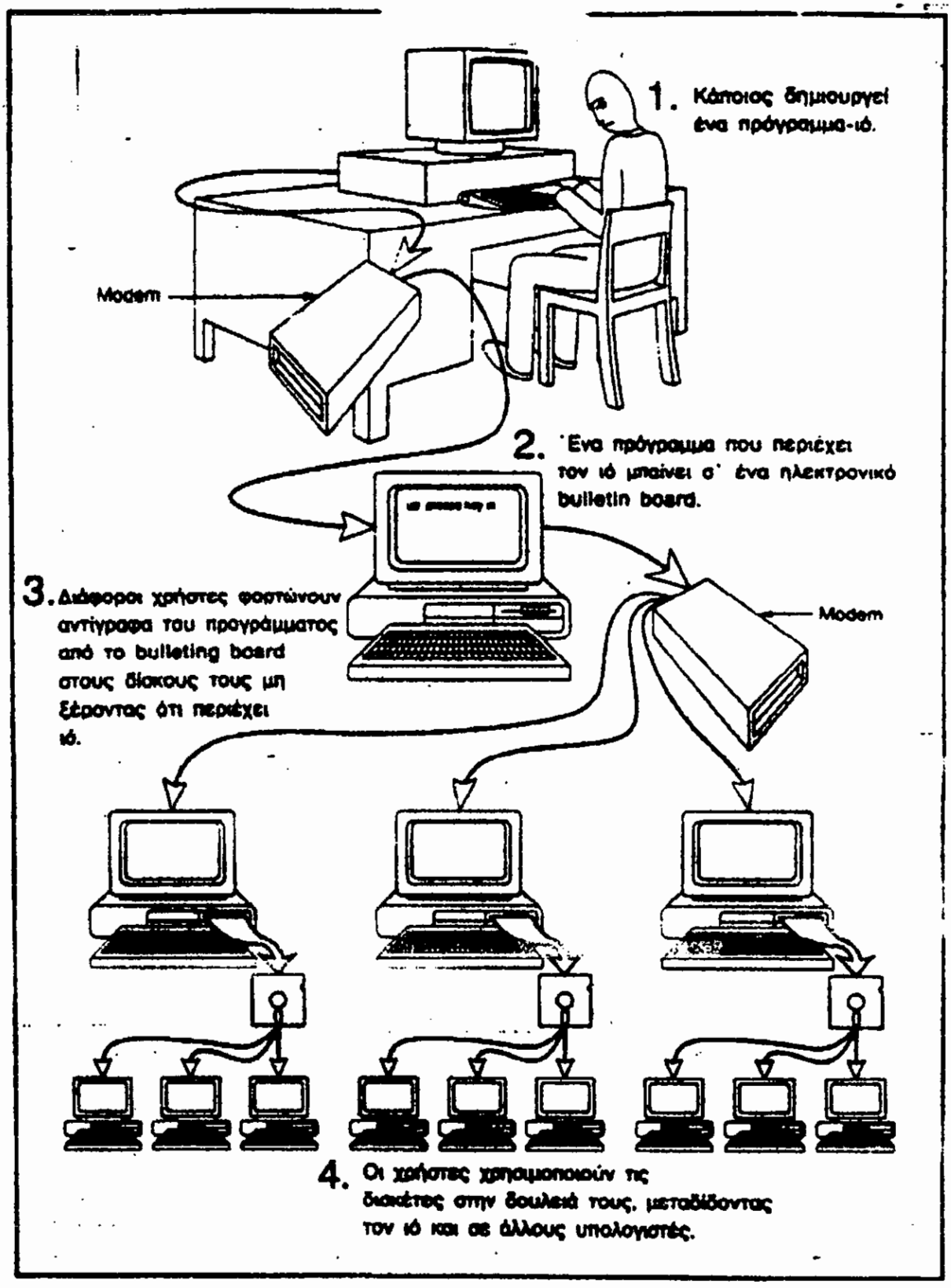
Το λειτουργικό σύστημα OS/2 θα μπορούσε να είναι ένα βήμα προς την κατεύθυνση αυτή, με τις δυνατότητες πολυεπεξεργασίας που διαθέτει. Σε ένα τέτοιο περιβάλλον είναι εύκολο να τρέχετε το αντιβιοτικό σας πρόγραμμα στο υπόβαθρό των κοινωνικών σας δραστηριοτήτων, ώστε να είναι έτοιμο να αναλάβει δράση και να υπερασπιστεί τα δεδομένα σας αν ανιχνεύσει δραστηριότητα ιών.

Το Disk Defender μια συσκευή που δημιουργήθηκε από τον Dennis Director και αποτελεί ένα ακόμη βήμα προς την σωστή κατεύθυνση στο θέμα προστασίας των ήδη υπαρχόντων συστημάτων προσωπικών υπολογιστών και Mac. Ο Director έχει αναπτύξει ένα σχετικά απλό ηλεκτρονικό σύστημα που δρα σα φραγμός για τους ιούς, εμποδίζοντάς τους να εισβάλλουν στο σκληρό δίσκο. Είναι ένα προιόν ελαφρώς πιο μπροστά από την εποχή του, δεδομένου ότι λανσαρίστηκε πριν η επιδημία των ιών πάρει τις τωρινές διαστάσεις και πριν τροποιηθούν τα πιο δημοφιλή προγράμματα εφαρμογών ώστε να λειτουργούν αποδοτικά με μειωμένη προσπέλαση εγγραφών στο δίσκο.

Οπως δείχνει και το διάγραμμα της διαμόρφωσης του Disk

Defender, η τοποθέτηση των αρχείων του λειτουργικού συστήματος και των προγραμμάτων εφαρμογών σε μια ζώνη μόνο ανάγνωσης του σκληρού δίσκου. Τα αρχεία δεδομένων που αποθηκεύονται και αυτά πίσω από το φραγμό που θέτει ο Disk Defender προστατεύονται επίσης. Η συσκευή αυτή είναι το ηλεκτρονικό ισοδύναμο του αυτοκόλλητου προστασίας από εγγραφή για το σκληρό δίσκο, αλλά πιο ευέλικτο, διότι μπορεί να γράφετε σε ένα μέρος του δίσκου και να τροποποιήσετε τα αρχεία του.

Ο Disk Defender είναι ένας καλός δρόμος που αξίζει να τον ψάχνετε, είτε είστε υπεύθυνοι πολλών συστημάτων, είτε απλοί χρήστες. Η συσκευή αυτή μπορεί να διαμορφωθεί ως μια ποικιλία περιστάσεων τόσο σε προσωπικούς υπολογιστές όσο και σε Mac.


1. Κάποιος δημιουργεί ένα πρόγραμμα-ιό.
Modem
2. Ένα πρόγραμμα που περιέχει τον ιό μπαίνει σ' ένα ηλεκτρονικό bulletin board.
3. Διάφοροι χρήστες φορτώνουν αντίγραφα του προγράμματος από το bulleting board στους δίσκους τους μη ξέροντας ότι περιέχει ιό.
Modem
4. Οι χρήστες χρησιμοποιούν τις δισκέτες στην δουλειά τους, μεταδίδοντας τον ιό και σε άλλους υπολογιστές.

## Η ΤΕΛΙΚΗ ΠΡΟΣΤΑΣΙΑ - ΤΑ ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ ΣΑΣ

Εχοντας μια αποτελεσματική πολιτική τήρησης αντιγράφων ασφαλείας δε θα εμποδίσετε την μόλυνση από ιούς, αλλά παραμένει το καλύτερο μέσο άμυνας διότι διατηρεί τα δεδομένα σας και καθιστά δυνατή την πλήρη ανάκτηση του συστήματος. Επειδή οι ιοί μπορούν να εξαπλωθούν και στα αντίγραφα ασφαλείας, αυτά θα πρέπει να περιέχουν μόνο δεδομένα, καθώς επίσης θα πρέπει να υπάρχουν δυο ή περισσότερες εκδόσεις τους, ώστε να ελαχιστοποιείται το ρίσκο να χάσετε όλα τα δεδομένα σας διότι έχετε πάρει αντίγραφο και για κάποιο μολυσμένο πρόγραμμα.

Εάν έχετε δεδομένα τα οποία πρέπει να διατηρήσετε, π.χ ζωτικής σημασίας προγράμματα για την εταιρεία σας ή το χειρόγραφο κάποιου βιβλίου, θα πρέπει να έχετε εκτός από ηλεκτρονικά αντίγραφα και αντίγραφα από χαρ#ί. Μη χρησιμοποιείτε πολύπλοκα γράμματα και μορφοποίηση αλλά τέτοια ώστε να μπορούν να αναγνωσθούν εύκολα από κάποια συσκευή ηλεκτρονικής ανάγνωσης (SCANNER) που κυκλοφορούν. Φυλάξτε με ασφάλεια τα αντίγραφα αυτά. Αν ποτέ χαθούν όλα τα ηλεκτρονικά δεδομένα σας από μόλυνση ιού ή από οποιαδήποτε άλλη αιτία, μπορείτε να χρησιμοποιείτε έναν Scanner για να διαβάσετε τα αντίγραφα που κρατάτε σε χαρτί.

## ΟΙ ΠΙΟ ΦΗΜΙΣΜΕΝΟΙ ΑΝΑ ΤΟΝ ΚΟΣΜΟ ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ

Υπάρχουν εκατοντάδες τύποι διαφορετικών ιών που κυκλοφορούν στον κόσμο. Κάθε μέρα βγαίνουν και νέες εκδόσεις των ογδόντα και πάνω διαφορετικών ιών που έχουν καταγραφεί μόνο στο περιβάλλον DOS.

Η δεκαετία του ενενήντα άρχισε με μια τρομερή αύξηση στο ποσοστό μολύνσεων των υπολογιστών Mac. Νέοι και πιο ισχυροί κυκλοφόρησαν και ενσωματώθηκαν στο σύνολο των ήδη υπαρχόντων. Ο ιός η VIR που πρώτος άρχισε να εισβάλλει σε υπολογιστές Mancintosh στη Δυτική Γερμανία το 1987, έχει εξελειχθεί σε περισσότερες από 30 μορφές ιών για τους Mac οι οποίες έχουν εξαπλωθεί ανά τον κόσμο.

Ορισμένοι ιοί που ξεκίνησαν σαν αθώες φάρσες, έχουν πλέον μεταμορφωθεί σε καταστροφείς αρχείων. Ο ιός Christmas που γράφτηκε από κάποιον γερμανό φοιτητή για να διασκεδάσει τους φίλους του, παρέλυσε όλο το διεθνές δίκτυο της IBM, προσβάλλοντας συστήματα σε πολλές χώρες. Ιοί που προορίζονταν για συγκεκριμένους στόχους στην Ευρώπη, εξαπλώθηκαν σε όλον τον κόσμο μέσω δορυφόρων και προκάλεσαν χάος σε συστήματα στην Αυστραλία, τον Καναδά και την Ιαπωνία.

Τα λάθη των προγραμμάτων κοστίζουν μόνο στις Ηνωμένες Πολιτείες της Αμερικής πάνω από ένα δισεκατομμύριο δολλάρια ετησίως. Σε όλον τον κόσμο ο αριθμός αυτός είναι σίγουρα διπλάσιος, ενώ ταυτόχρονα ο ρυθμός αποτυχίας των προγραμμάτων

αυξάνετε συνεχώς, καθώς δημιουργούνται όλο και περισσότεροι. Ιοί θα συνεχίσουν να αναπαράγονται και θα προστίθενται σε αυτούς και νέα είδη που θα πυροδοτούν την εξάπλωση των μολύνσεων.

Η εξαρτώμενη από τους υπολογιστές κοινωνία δέχετε επίθεση από εχθρούς που δε μπορούμε να τους προσδιορίσουμε και τα κίνητρα των οποίων αδυνατούμε να τα καταλάβουμε : Οι εχθροί αυτοί είναι πολλοί και δρουν με τυχαίο ή ασυντόνιστο τρόπο, χρησιμοποιώντας για κάλυψη την ίδια την τεχνολογία.

Πολλή σύγχιση προέρχεται επίσης και από το γεγονός ότι ορισμένοι ιοί εμφανίζονται να είναι νέοι, ενώ δεν είναι. Δεδομένου ότι είναι λιγότερος κόπος για έναν κατασκευαστή ιών να μετατρέψει έναν ήδη υπάρχοντα ιό από ότι να γράψει έναν νέο, οι προγραμματιστές αυτοί τείνουν να ανακυκλώνουν τον κώδικα ενός υπάρχοντος ιού και προσθέτουν νέο κώδικα μόνο, όταν είναι αναγκαίο να επιτευχθούν συγκεκριμένοι σκοποί. Μπορεί να φαίνεται νέος σε κάποιον που συναντά την τροποποιημένη έκδοση για πρώτη φορά και έτσι του δίνει νέο όνομα.

Σε άλλες περιπτώσεις, συγχωνεύονται στοιχεία δυο ή περισσοτέρων ιών και σχηματίζουν μια νέα μορφή υβριδικού προγράμματος που διατηρεί τα πιο αποτελεσματικά χαρακτηριστικά των πατρικών ιών. Τέτοιοι ιοί μπορούν να περιέχουν πολύ αποτελεσματικό μηχανισμό διάδοσης, τον καλύτερο κώδικα αναπαραγωγής που υπάρχει και έχουν τη δυνατότητα να κρύβονται σχετικά εύκολα.

**ΣΗΜΑΝΤΙΚΟ ΓΕΓΟΝΟΣ** : Τα επίσημα προγράμματα των κατασκευαστών

που είναι σφραγισμένα είναι σχεδόν απόλυτα ασφαλή. Αν και περιστασιακά έχουν μολυνθεί και επίσημα προγράμματα από ιούς, οι περισσότεροι κατασκευαστές λαμβάνουν τα κατάλληλα μέτρα, ώστε να κάνουν όσο το δυνατόν μικρότερο τον κίνδυνο (είναι σίγουρα μικρότερος από τον κίνδυνο των πειρατικών προγραμμάτων ή των προγραμμάτων που διανέμονται ελεύθερα). Αλλά οι κατασκευαστές προγραμμάτων ξέρουν ότι μπορούν να εκτεθούν σε νομικές περιπέτειες αν μπορέσει κάποιος να αποδείξει ότι έχουν διαδώσει ιό μέσα από σφραγισμένο πρόγραμμα.

Αυτός είναι και ο λόγος που δε βλέπετε ετικέτες με τη σήμανση "Εγγυημένα ελεύθερες από ιούς" στις δισκέτες των επισήμων προγραμμάτων, ακόμη και σε προϊόντα που είναι σχεδόν απόλυτα καθαρά.

Ευτυχώς, είτε έχουν ακριβή ονόματα, είτε όχι, οι περισσότεροι ιοί μπορούν να ταξινομηθούν. Οπως έχουμε δει νωρίτερα, ουσιαστικά όλοι οι ιοί μπορούν να ταξινομηθούν σε τρεις κατηγορίες, ανάλογα με τα χαρακτηριστικά που εμφανίζουν όταν προσβάλλουν ένα σύστημα :

* Οι εισβολείς του συστήματος εκκίνησης δισκετών ταξιδεύουν μέσο των δισκετών και αποκτούν τον έλεγχο του λειτουργικού συστήματος προσκολλώμενοι στον τομέα εκκίνησης των δισκίων.
* Οι εισβολείς του συστήματος διεισδύουν στα αρχεία του λειτουργικού συστήματος, όπου αναπαράγονται αλλά και ελέγχουν τη λειτουργία του συστήματος.
* Οι εισβολείς των εφαρμογών γενικού σκοπού κρύβονται στα προγράμματα εφαρμογών όλων των ειδών

και ενεργοποιούνται όταν αυτά τρέχουν, αναζητώντας νέες ευκαιρίες για να αναπαραχθούν, να καταστρέψουν δεδομένα ή να αλλάξουν την συμπεριφορά του προγράμματος.

## ΙΟΙ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ DOS

Ας αρχίσουμε με τους ιούς που δρουν σε περιβάλλον DOS, οι οποίοι είναι και οι πλέον πολυάριθμοι, λόγω της μεγάλης δυναμικότητας του DOS.

Ο Disk Killer είναι ένας ιός που προσβάλλει τον τομέα εκκίνησης δίσκων και αποτελεί μια από τις πιο καταστροφικές μορφές ιών που εμφανίστηκαν από τα τέλη του 1989. Οταν ενεργοποιείται εμφανίζει το ακόλουθο μήνυμα :

Disk killer Εκδοση 1.0

της Orge Computers

Εξολοθρεύω το δίσκο. Παρακαλώ μη σβήνετε το σύστημά σας

Δέκα δευτερόλεπτα πριν εμφανιστεί το παραπάνω μήνυμα, ο ιός αυτός έχει αρχίσει να εκτελεί μια χαμηλού επιπέδου μορφοποίηση του δίσκου. Το να σβήσετε τον υπολογιστή σας μόλις δείτε το μήνυμα δε θα φέρει κανένα αποτέλεσμα, καθώς τα δεδομένα του δίσκου σας έχουν αρχίσει να καταστρέφονται πριν προλάβετε να αντιδράσετε.

Ο Disk Killer έχει διαδοθεί ταχύτατα και έχει ακόμη

προσβάλλει μια από τις μεγαλύτερες φίρμες κατασκευαστών προγραμμάτων, η οποία μάλιστα δεσμεύτηκε με ένα εξαιρετικά ακριβό πρόγραμμα επανόρθωσης και πήρε όλα τα απαραίτητα βήματα που μπορούσε για να προστατέψει τους πελάτες της.

Ο Dock Avenger είναι ένας ιός που εισβάλλει στα προγράμματα τύπου COM και EXE και αποτελεί ένα διαρκές πρόβλημα, διότι είναι πολύ μεταδοτικός και καταστροφικός ταυτόχρονα. Ο ιός Dock Avenger αναζητά νέα προγράμματα - θύματα σε οποιαδήποτε χρονική στιγμή δραστηριοποίησης μιάς εφαρμογής κατά τη φορτωσή της, την εκτέλεσή της ή ακόμη κατά τη μεταφορά δεδομένων μεταξύ συστημάτων.

Για παράδειγμα, εάν φορτώσετε ένα μολυσμένο πρόγραμμα από μια δισκέτα στον "καθαρό" σκληρό δίσκο, ο ιός Dock Avenger μπορεί να ενεργοποιηθεί άμεσα. Ακόμη και η εξέταση της δισκέτας από ένα πρόγραμμα ανίχνευσης ιών μπορεί να προκαλέσει την ενεργοποίησή του και κατά συνέπεια τη μόλυνση του συστήματος.

Ο Zerobug είναι άλλος ένας ιός που εισβάλλει στα προγράμματα τύπου COM και προέρχεται από την Ευρώπη. Μεταδίδεται και καταστρέφει τα δεδομένα γρήγορα και αποτελεσματικά. Θα πρέπει να είστε ιδιαίτερα προσεκτικοί με τον ιό αυτό, διότι έχει ενσωματωμένη μια νέα μέθοδο για να ξεγελάσει τα προγράμματα ανίχνευσης ιών που κυκλοφορούν στην αγορά. Ο ιός Zerobug κρύβεται στα προγράμματα εφαρμογών, αλλά δεν κάνει φανερή την παρουσία του διότι διατηρεί τις λεπτομέρειες της ταυτότητας των προγραμμάτων όμοιες με αυτές που δίνει ο κατασκευαστής του. Αυτά είναι μια από τις πιο εμφανείς και

αποτελεσματικές μεθόδους απόκρυψης ιών που έχουν μέχρι στιγμής βρεθεί, καθώς καθιστά άχρηστα τα προγράμματα ανίχνευσης που βασίζονται σε μετρήσεις μεγεθών, στιγμιαίες εικόνες τους ή άλλα τεχνάσματα για να συγκρίνουν την τρέχουσα κατάσταση των προγραμμάτων με αυτή που δίνει ο κατασκευαστής τους.

Ο Alabame είναι ένας ιός που εισβάλλει στα αρχεία του τύπου COM και EXE ο οποίος επίσης εισήγαγε ένα νέο τέχνασμα. Οποτεδήποτε αντιγράφονται αρχεία ή ενεργοποιείται για κάποιον άλλον λόγο ο ιός, αλλάζει το όνομα των αρχείων δίνοντάς τους ονόματα άλλων αρχείων των μολυσμένων συστημάτων.

Σύντομα, όλος ο κατάλογος αρχείων του μολυσμένου συστήματος γίνεται άνω - κάτω, καθώς τα δεδομένα υπάρχουν αλλά δε μπορείτε να τα προσπελάσετε διότι δε ξέρετε τα ονόματα των αρχείων στα οποία βρίσκονται.

Τέτοιου είδους δραστηριότητες των ιών προκαλούν άγχος και σύγχυση στους χρήστες και ιδίως σε αυτούς που δεν είναι εξοικειωμένοι με τη χρήση του υπολογιστή. Ο συντελεστής του άγχους είναι ιδιαίτερα υπολογίσιμος όταν τέτοιου είδους επιθετικές και απρόβλεπτες δραστηριότητες συμβαίνουν όταν είστε κουρασμένοι ή όταν βλέπετε ότι έχει καταστραφεί μεγάλο μέρος της δουλειά σας, σαν κάποιος να πάτησε πίσω από την πλάτη σας το πλήκτρο διαγραφής (Delete) και να τα εξαφάνισε όλα.

Η αντίδρασή σας θα είναι στεναχώρια, εχθρότητα και επιθυμία αντεκδίκησης αν η πράξη αυτή γινόταν από κάποιο άλλο ανθρώπινο ιό. Τα ίδια συναισθήματα κυριαρχούν και όταν η μηχανή που την έχεις εμπιστευθεί ότι φέρεται λογικά και

ενεργεί αξιόπιστα σύμφωνα με τις οδηγίες που τις έχεις δώσει, καταστρέφει όλα τα δεδομένα.

Ο Yankee Doodle είναι ευτυχώς ένας αθώος ιός στην αρχική του τουλάχιστον μορφή. Ενεργοποιείται από το εσωτερικό ρολόι των υπολογιστών. Στις πέντε η ώρα το απόγευμα αρχίζει να παίζει το σκοπό του τραγουδιού "Yankee Doodle Dandy" από το μεγάφωνο του υπολογιστή. Αρχικά - τουλάχιστον - ο ιός αυτός δεν κατάστρεφε τα δεδομένα, ούτε υπερφόρτωνε τα προγράμματα στα οποία εισέβαλλε με τις συνεχείς αναπαραγωγές του.

Ο Do Nothing ξεκίνησε σαν αθώος ιός που πρόσβαλλε τα αρχεία τύπου COM και EXE χωρίς να καταστρέφει δεδομένα ή να υπερφορτώνει τα συστήματα, δρώντας περίπου σαν ένα τουφέκι χωρίς σφαίρες. Το γεγονός ότι δεν έκανε τίποτε άλλο από το να προσκολλάται αποτελεσματικά πάνω στα COM και EXE αρχεία τον έκανε ιδανικό φορέα για τη δημιουργία κακών κενών.

Ο ιός Jerusalem η αλλιώς Israeli, και αυτός που ορισμένες φορές αποκαλείτε Παρασκευή και 13 (το πιθανότερο και αυτό να είναι κάποιο παρακλάδι του Jerusalem). Επειδή, ακριβώς είναι τόσο διαδεδομένος και υπάρχει για πολύ καιρό, τα περισσότερα αντιβιοτικά προγράμματα μπορούν να βρουν τουλάχιστον τις πιο κοινές εκδόσεις του : τα αντιβιοτικά που δε μπορούν να "πιάσουν" τον ιό Jerusalem δε θα πρέπει να θεωρούνται αποτελεσματικά.

Ο ιός Jerusalem έκανε την επίσημη πρώτη εμφάνισή του στο Εβραικό Πανεπιστήμιο της Ιερουσαλήμ και πολύ σύντομα υπήρξαν και άλλες αναφορές μολύνσεων από άλλα συστήματα στο Ισραήλ, συμπεριλαμβανομένου και ενός υπολογιστή που χρησιμοποιούνταν

για στρατιωτικούς σκοπούς.

Το γεγονός αυτό έδωσε λαβή στους ισχυρισμούς ότι ο ιός αυτός δημιουργήθηκε από Παλαιστίνιους σαμποτέρ και ότι θα ενεργοποιούνταν την Παρασκευή 13 Μαίου του 1988 ημέρα της επετείου του διαχωρισμού της Παλαιστίνης από το Ισραήλ.

Ο ιός αυτός εισβάλλει σε αρχεία COM και EXE. Η έκδοση Jerusalem - C του ιού αυτού δεν έχει πλέον το λάθος της αρχικής και μπορεί να προσδιορίζει τα EXE αρχεία που δεν έχουν ακόμα μολυνθεί. Η έκδοση Jerusalem - C δε ξεφεύγει εύκολα από τον έλεγχο ενώ ταυτόχρονα κάνει φανερή την παρουσία της μέσω των δραστηριοτήτων αναπαραγωγής. Η βελτίωση αυτή κάνει πιο επικίνδυνο τον ιό, δεδομένου ότι έχει μεγαλύτερο χρόνο επώασης και μπορεί να μολύνει εύκολα τα συστήματα.

Υπάρχει επίσης ο New Jerusalem - Jerusalem D ιός, ο οποίος δεν έχει τους χρονικούς περιορισμούς του αρχικού. Η έκδοση αυτή αρχίζει να καταστρέφει τα δεδομένα του συστήματος αμέσως μόλις αυτό μολυνθεί, χωρίς να δίνει κάποιο άλλο σημείο της ύπαρξής του.

Ο ιός Sunday είναι άλλη μια έκδοση του ιού Jerusalem, η οποία χρησιμοποιεί πολύ αποτελεσματικά τον κώδικα μόλυνσης και αναπαραγωγής του πρωτότυπου. Ομως φανερώνει το όνομά του και ενεργοποιείται όταν το εσωτερικό ρολόι του υπολογιστή δείξει ημέρα Κυριακή. Οταν ο ιός αυτός ενεργοποιείται ο χρήστης βλέπει στην οθόνη το ακόλουθο μήνυμα :

Today is Sunday. Why are you working?
All work and no play make you a dull boy

Σήμερα είναι Κυριακή. Γιατί εργάζεστε;

Συνέχεια δουλειά και καθόλου διασκέδαση σε κάνουν βαρετό.

Και άλλα άσχημα νέα για τον Jerusalem : Μπορεί ακόμη να μην έχουμε δει τα χειρότερα, με ακόμη πιο καταστροφικές εκδόσεις του ιού, προγραμματισμένες να ενεργοποιηθούν σε ημερομηνίες μέσα στη δεκαετία του 1990.

Υπάρχει μια θεωρία μεταξύ ορισμένων δημιουργών ιών ότι ο "σούπερ - ιός" είναι αυτός που θα μπορεί να μολύνει μυστικά όσο περισσότερα συστήματα μπορεί, πριν αρχίσει να κάνει οποιαδήποτε ζημιά. Ο χρονοδιακόπτης του θα έχει τεθεί να ενεργοποιηθεί μερικά χρόνια αργότερα, έτσι ώστε να έχει αρκετό καιρό να εξασπλωθεί σε εκατομμύρια μηχανές.

Ο ιός Παρασκευή και 13 συγχέεται συχνά με τον Jerusalem διότι και αυτός ενεργοποιείται κάθε Παρασκευή που τυχαίνει να έχει ο μήνας 13. Καταστρέφει βέβαια τα προγράμματα όταν ενεργοποιηθεί, αλλά δεν συνεχίζει να αναπαράγεται ανεξέλεγκτα όπως ο Jerusalem.

Ο ιός Ping Pong που είναι επίσης γνωστός και με τα ονόματα Bouncing Ball, Italian, Vera Cruz, μολύνει τον τομέα εκκίνησης των δίσκων και συνεχίζει να ευδοκιμεί σε πολλά συστήματα σήμερα. Η μόνη εμφανής συνέχεια της μόλυνσης είναι μια μικρή μπάλα που εμφανίζεται να χοροπηδάει στην οθόνη. Ορισμένες όμως εκδόσεις του έχουν ένα προγραμματιστικό λάθος το οποίο έχει σαν αποτέλεσμα ο ιός να γράφει πάνω στον πίνακα κατανομής αρχείων με συχνότητα μια στις κάθε οκτώ μολύνσεις που συμβαίνουν, προκαλώντας την κατάρευση του συστήματος και

την απώλεια των δεδομένων.

Η επανεκκίνηση του συστήματος είναι συνήθως επαρκής ενέργεια για να απαλλαγείτε από τον ιό Ping Pong. Οι παλιότερες εκδόσεις του μόλυναν μόνο δισκέτες, αλλά οι πιο νέες μπορούν να προκαλέσουν ζημιά και σε σκληρούς δίσκους.

Ο ιός Ghost που πρωτοεμφανίστηκε το 1990, συγχέεται πολύ συχνά με τον Ping Pong διότι και αυτός εμφανίζει μια μπάλα που τρέχει στην οθόνη. Αλλά ο ιός Ghost μολύνει μόνο τους τομείς εκκίνησης και τα αρχεία τύπου COM σε σκληρούς δίσκους και δισκέτες. Ετσι εκτός από τη χρήση της εντολής SYS με την οποία θα θεραπεύσετε τον τομέα εκκίνησης, θα πρέπει να διαγράψετε και όλα τα μολυσμένα COM αρχεία.

Ο ιός Colombus Day, ο οποίος είναι γνωστός και με τα ονόματα October 13 ή Datacrime, στην πραγματικότητα πρόσφερε μια μεγάλη εξυπηρέτηση στην κοινωνία των υπολογιστών τον Οκτώβριο του 1989. Προκάλεσε τόσο μεγάλη δημοσιότητα και προβολή από τα μέσα μαζικής ενημέρωσης, ώστε αρκετοί άνθρωποι άρχισαν να παίρνουν στα σοβαρά για πρώτη φορά την επιδημία των ιών.

Υπήρξε μια άνθιση του διεθνούς ενδιαφέροντος για να βρεθεί και να εξολοθρευτεί ο ιός αυτός από τα σημαντικά υπολογιστικά συστήματα. Ειδικοί πάνω στην καταπολέμηση ιών κατάφεραν να σώσουν τα δεδομένα σε σημαντικά κυβερνητικά υπολογιστικά συστήματα της Σουηδίας που είχε μολυνθεί και επίσης η απώλεια δεδομένων είτε εκμηδενίστηκε, είτε ελαχιστοποιήθηκε σε άλλα συστήματα, πανεπιστημιακά, συγκοινωνιών, τραπεζών σχεδόν σε όλο τον κόσμο, από τη Γαλλία στην

Αυστραλία.

Η 13η Οκτωβρίου του 1989 ξεθύμανε σαν αστείο πυροτέχνημα, χωρίς να συμβεί το ολοκαύτωμα των υπολογιστών που ορισμένα από τα μέσα μαζικής ενημέρωσης πρέβλεπαν, επιφέροντας έτσι αρνητικό αντίκτυπο. Ορισμένοι θεώρησαν ότι ήταν απλώς ένας ψεύτικος συναγερμός και υποτίμησαν τους πραγματικούς κινδύνους που αντιπροσωπεύουν οι ιοί.

Εντούτοις, ο ιός Jerusalem συνέχισε την άνετη επέλασή του στα υπολογιστικά συστήματα, προκαλώντας συνεχώς νέες μολύνσεις, αρκετές για να αποζημιώσουν εν μέρει την αποτυχία του Colombus Day να επιδείξει πλήρως την υπεροχή του μέσα στο 1989. Ακόμη και τώρα ο ιός Colombus Day συνεχίζει να πολλαπλασιάζεται αποδεικνύοντας έτσι ότι με κανέναν τρόπο, δεν είναι ξοφλημένος. Μπορεί να ενεργοποιηθεί οποιαδήποτε μέρα μετά την 13η Οκτωβρίου, σε οποιαδήποτε χρονιά και συνεπώς θα πρέπει να συνεχίσουμε να παρακολουθούμε τα ίχνη του.

Το μέγεθος των προγραμμάτων που μολύνονται από τον ιό αυτό, αυξάνεται κατά 1168 χαρακτήρες με επακόλουθες συνέπειες, την καθυστέρηση στην εκτέλεση των προγραμμάτων, την απώλεια δεδομένων και το ξαναφορμάρισμα του σκληρού δίσκου.

Ο ιός Cascade βρίσκεται στην κυκλοφορία αρκετό καιρό και αποτελεί τη βάση για ένα πλήθος άλλων ιών οι οποίοι φέρουν είτε το ίδιο όνομα, είτε το όνομα 1701 ή 1704.

Ο ιός 1701 ονομάστηκε κατ'αυτόν τον τρόπο διότι είναι ένα μόνιμο στη μνήμη πρόγραμμα το οποίο αυξάνει το μέγεθος οποιουδήποτε COM αρχείου κατά 1701 χαρακτήρες, ενώ ο 1704 συμπεριφέρεται ελαφρώς διαφορετικά και προσθέτει στα μολυσ-

μένα αρχεία 1704 χαρακτήρες. Ονομάζεται δε Blackjack.

Οι ιοί αυτοί περιέχουν εξελιγμένες τεχνικές απόρριψης, οι οποίες τους βοηθούν να ξεφεύγουν από τα προγράμματα ανίχνευσης και κάνουν δύσκολη τη διάσπασή τους. Ο κώδικάς τους μπερδεύει τα προγράμματα ανίχνευσης προκαλώντας την τυχαία ενεργοποίηση του ιού, έτσι ώστε δυο εκδόσεις του να μην είναι ποτέ ίδιες.

Οι περισσότεροι ενεργοποιούνται μόνο τους τρεις τελευταίους μήνες του χρόνου. Ορισμένοι άλλοι ενεργοποιούνται μόνο την πρώτη Δεκεμβρίου, φορμάροντας τους σκληρούς δίσκους και κατατρέφοντας τα περιεχόμενά τους.

Ο ιός Cascade και τα παρακλάδια του συνεχίζουν να αναπαράγονται καθ'όλη τη διάρκεια του χρόνου και όταν ενεργοποιηθούν, συμπεριφέρονται με μια ποικιλία τρόπων, καθώς οι κατασκευαστές τους προσαρμόζουν κατ'επιθυμίαν. Ορισμένες εκδόσεις εισβάλλουν μόνο σε συγκεκριμένους τύπους έγχρωμων οθονών, ενώ άλλες δημιουργούν ένα προειδοποιητικό μήνυμα του DOS, προσπαθώντας να προσπελάσουν κάποιον προστατευμένο από εγγραφή δίσκο.

Ο New Zealand έγινε σύντομα ο πιο διαδεδομένος από τους ιούς που εμφανίζουν κοινωνικοπολιτικά μηνύματα. Ξεκίνησε αρκετά αθώα, εμφανίζοντας απλά το ακόλουθο μήνυμα :

> Legalize marijuana. Your computer iw now stoned
>
> Νομιμοποίησε τη μαριχουάνα. Ο υπολογιστής είναι τώρα μαστουρωμένος.

Ο ιός αυτός που προσβάλλει τον τομέα εκκίνησης του δίσκου πρωτοεμφανίστηκε στη Νέα Ζηλανδία και απέκτησε το

παρατσούκλι (STONED, μαστουρωμένος) όταν έφθασε στις ΗΠΑ με πιο επιθετική μορφή που είχε τη δυνατότητα να μολύνει και δισκέτες και σκληρούς δίσκους και να προκαλεί απώλειες δεδομένων και στα δυο.

Ο ιός Alameda και οι ποικίλες μορφές του αποτελούν πλέον τη μάστιγα των εκπαιδευτικών ιδρυμάτων. Οι φοιτητές - hachers έχουν χρησιμοποιήσει τον ιό αυτό για να κάνουν άσχημες φάρσες με τους υπολογιστές ή σαν όπλο ενάντια στη διοίκηση. Καθ'όλη τη διάρκεια της ύπαρξής του, ο ιός αυτός έχει αποκτήσει πολλά ονόματα. Στα ονόματα αυτά συμπεριλαμβάνονται τα Merritt, yale, Peehing, Seoul, Sacramento, SF, Soo, Golden Gate και mazatlan.

Η αρχική έκδοση του Alameda είναι αρκετά αθώα και ακόμη περιέχει και ενσωματωμένο ένα μηχανισμό αυτοκαταστροφής. Μπορεί να προσβάλλει τον τομέα εκκίνησης ενός περιορισμένου αριθμού δισκετών - μέχρι 360, ενώ ο κωδικός του περιέχει και εντολές με επεξεργαστή 80286. Αυτοί οι ενσωματωμένοι περιορισμοί έχουν εξαλειφθεί από τις επόμενες εκδόσεις. Τώρα πια οι τελευταίες μορφές του μολύνουν όλα τα συστήματα ανεξέλεκτα, ενεργοποιούνται αμέσως και κάνουν σοβαρές ζημιές τόσο σε δισκέτες όσο και σε σκληρούς δίσκους.

Μέχρι την άφιξη του Alameda, ο Lehigh φαινόταν να είναι διαδεδομένος ιός στις πανεπιστημιακές κοινότητες της Βορείου Αμερικής. Πρωτοανακαλύφθηκε στο Πανεπιστήμιο Lehigh. Από τότε ξεκίνησε μια φρενιώδης δραστηριότητα, επιδεικνύοντας το πόσο γρήγορα και πόσο μακριά μπορεί να εξαπλωθεί μια μόλυνση με την ανταλλαγή δισκετών μεταξύ φοιτητών ή άλλων μελών της

ακαδημαικής κοινότητας.

Η αρχική έκδοση του Lehigh αυξάνει το μέγεθος του αρχείου COMMAND.COM κατά 20 χαρακτήρες και αλλάζει την ώρα και την ημερομηνία του υπολογιστή, έτσι ώστε η παρουσία του μπορεί να εντοπιστεί από κάποιον προσεκτικό χρήστη πριν ενεργοποιηθεί, και αφού κάνει 4 επιπλέον μολύνσεις. Η στάνταρ αντιμετώπιση του ιού αυτού (ο οποίος είναι και ο πιο μελετημένος) είναι απλά η διαγραφή του μολυσμένου αρχείου COMMAND.COM και η αντικατάστασή του από ένα "καθαρό" από τις αρχικές δισκέτες του λειτουργικού συστήματος. Εντούτοις όμως, δε θα πρέπει να περιμένετε ότι και οι τελευταίες τροποποιημένες εκδόσεις του θα συμπεριφέρονται με τον ίδιο τρόπο.

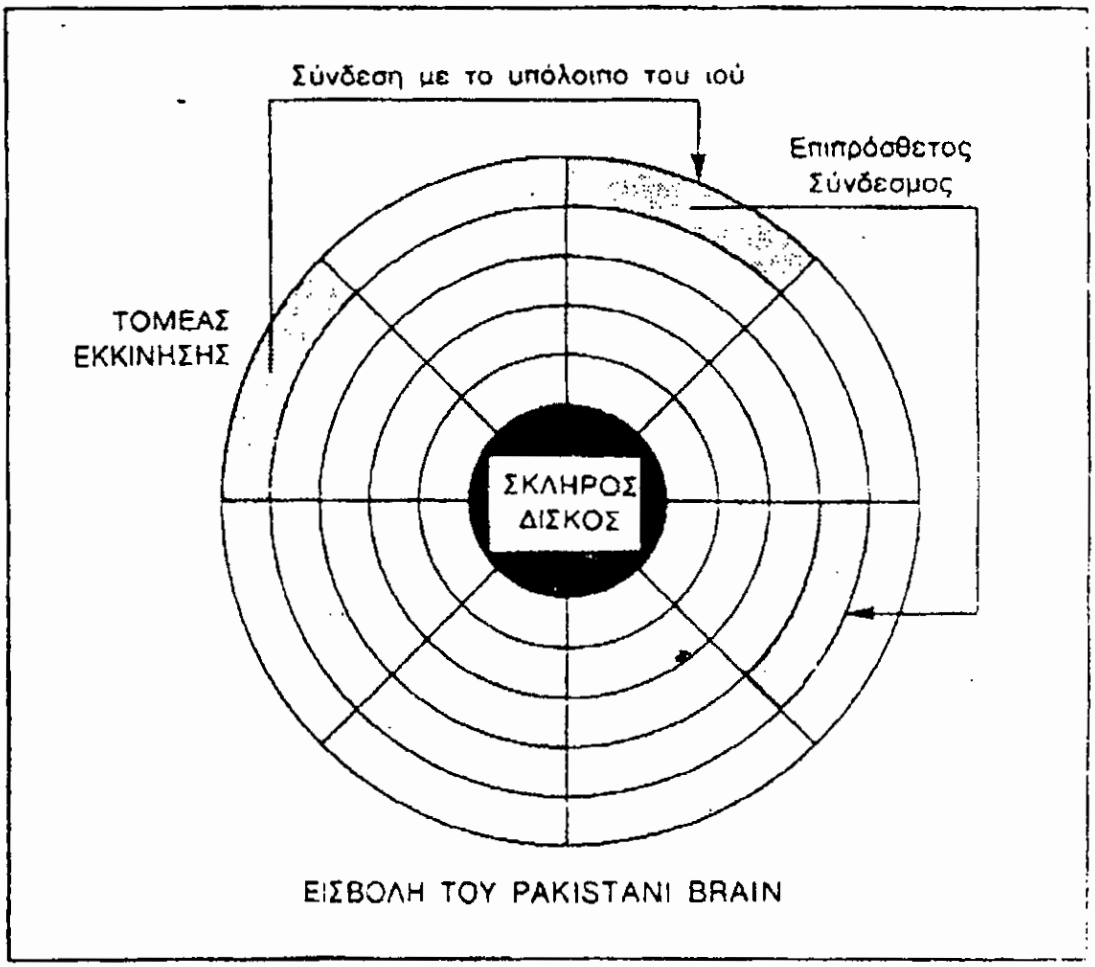
Υπάρχουν αρκετές ομοιότητες μεταξύ του Alamed και του BRAIN, ενός άλλου ιού που προσβάλλει τον τομέα εκκίνησης του δίσκου, ο οποίος φέρει τα ονόματα Fakistani, Brain ή Basit (από τους δημιουργούς του οι οποίοι ήταν οι μόνοι που έβαλαν ποτέ τα ονόματά τους, τις διευθύνσεις και τα τηλέφωνά τους σε σήμα copyright του ιού). Αλλά αυτό έγινε το 1986, όταν οι ιοί δε θεωρούνταν σημαντική απειλή που θα μπορούσε να εκθέσει τους δημιουργούς τους με κυρώσεις - αν συλλαμβάνονταν.

Ολες οι εκδόσεις του Brain διατηρούν τις ευφυείς τεχνικές της αρχικής έκδοσης για ταχεία αναπαραγωγή τους οπουδήποτε βρίσκουν κατάλληλο περιβάλλον και αποτελεσματική απόκρυψή τους, ώστε να μην ανιχνεύονται. Ο ιός Brain λαμβάνει άμεσα τον έλεγχο του συστήματος μολύνοντας τον τομέα εκκίνησης του δίσκου και κατόπιν επεκτείνει αυτόν τον έλεγχο διασκορπίζοντας τον εαυτό του σε τμήματα κώδικα τα οποία

κρύβονται σε διάφορα τμήματα του δίσκου και τα οποία επισημαίνονται σαν κακοί τομείς (bad sectors) και συνεπώς δε μπορούν να διαβαστούν από το χρήστη.

Ο ιός Brain εντοπίζει όλα τα προγράμματα τα οποία ελέγχουν τον τομέα εκκίνησης ενός δίσκου για συνομιλίες, και τα επανακατευθύνει στην αρχική έκδοση του τομέα εκκίνησης, εξασφαλίζοντας ότι αυτά ανιχνεύουν την κανονική τους κατάσταση και όχι την πραγματική, δηλαδή τη μολυσμένη.

**Τεχνικές Προστασίας από τους Ιους Υπολογιστών**




ΕΙΣΒΟΛΗ ΤΟΥ PAKISTANI BRAIN

## ΙΟΙ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ MACINTOSH

Η κατάσταση για τους χρήστες υπολογιστών Macintosh χειροτέρεψε γρήγορα στις αρχές του '90, με μια κατακόρυφη αύξηση των μολύνσεων, κυρίως σε συστήματα επιχειρήσεων που επικοινωνούσαν μέσω δικτύου. Μέχρι τότε οι πιο γνωστοί ιοί εκτός του περιβάλλοντος του DOS ήταν οι McMag, Scores και η V.I.R για τους Macintosh και ο Amiga για παλιότερους υπολογιστές Amiga.

Ο ιός VIR εισβάλλει γενικά σε εφαρμογές και υπάρχει εδώ και πολύ καιρό. Πρωτοανακαλύφθηκε στη Γερμανία το 1987 και από τότε μεταλλάχθηκε σε 30 διαφορετικές μορφές οι οποίες μόλυναν πολλούς Macintosh σε όλον τον κόσμο.

Ο ιός Scores μολύνει επίσης τα προγράμματα εφαρμογών και είναι πολύ διαδεδομένος - υπολογιστές στη NASA, στο Κονγκρέσο και σε διάφορους δημόσιους οργανισμούς, έχουν μολυνθεί από τον ιό αυτό. Το διακριτικό του σύμπτωμα το οποίο στη συνέχεια εμφανίστηκε και σε άλλους ιούς είναι η τροποποίηση των εικονιδίων του υπολογιστή. Δίνει στα εικονίδια δυο λειτουργιών εμφάνιση σκυλιού.

Ο ιός Scores ήταν το πρώτο παράδειγμα του πως ένας ιός δημιουργημένος για να χτυπήσει ένα συγκεκριμένο αρχείο - από κίνητρο εκδίκησης - μπορεί να ξεφύγει από τον έλεγχο και να απειλήσει όλη την κοινότητα των υπολογιστών. Από ότι ξέρουμε πρέπει να έχει γραφεί από κάποιο δυσαρεστημένο υπάλληλο, και

στόχευε αποκλειστικά σε δεδομένα που σχετίζονται με την EDS, τη γιγαντιαία επιχείρηση Electronic Data System. Οταν πρωτοανακαλύφθηκε στην EDS το 1987 ήταν ήδη εκτός ελέγχου, προσβάλλοντας όλους τους Macintosh που συναντούσε χωρίς διάκριση.

## ΠΩΣ ΘΑ ΧΡΗΣΙΜΟΠΟΙΗΣΕΤΕ ΤΟ ΑΝΤΙΒΙΟΤΙΚΟ ΠΡΟΓΡΑΜΜΑ

Το αντιβιοτικό πρόγραμμα το οποίο θα σας μιλήσουμε δεν είναι τίποτε άλλο από το ViruScan, το πιο διαδεδομένο πρόγραμμα καταπολέμησης ιών, το οποίο σε συνδυασμό με την τήρηση ορισμένων κανόνων ασφαλείας είναι η καλύτερη μέχρι στιγμή καταπολέμηση των μολύνσεων.

## ΤΙ ΕΙΝΑΙ ΤΟ VIRUSCAN

Το πρόγραμμα Viruscan λειτουργεί ως εξής : ψάχνει το σύστημά σας για να βρει τυπικές δραστηριότητες ιών, και αν βρει κάποια τη συγκρίνει με αυτά που έχει στη βάση δεδομένων του με τα χαρακτηριστικά των ιών.

Η προγραμματιστική εργασία πάνω στο πρόγραμμα Viruscan συντονίστηκε από τον John McAfee, ο οποίος είναι πρόεδρος του Ινστιτούτου CVIA.

Η εξέλιξη και ενημέρωση του προγράμματος έχει γίνει

υπόθεση μια διεθνούς ομάδας ανθρώπων που διευθύνεται από τα γραφεία της CVIA.

## ΠΩΣ ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΤΟ VIRUSCAN

Πριν χρησιμοποιήσετε το Viruscan, αντιγράψτε το σε μια προστατευόμενη από εγγραφή δισκέτα, αφού εκκινήσετε τον υπολογιστή σας με την αρχική προστατευόμενη από την εγγραφή δισκέτα του λειτουργικού συστήματος.

Εισάγετε την προστατευόμενη από την εγγραφή δισκέτα του προγράμματος Viruscan στον οδηγό A : του υπολογιστή σας και πληκτρολογείται SCAN. Εάν θέλετε να ελέγξετε το σκληρό σας δίσκο SCAN C ή SCAN A για τις δισκέτες. Αμέσως μετά, το Viruscan αρχίζει να ελέγχει τις περιοχές και τα αρχεία του συστήματός σας που είναι τρωτά σε μολύνσεις. Σε αυτά συμπεριλαμβάνονται ο πίνακας περιοχών του σκληρού δίσκου ή των δισκετών και τα εκτελέσιμα αρχεία που υπάρχουν.

Εάν βρεθεί κάποιος ιός, το Viruscan θα σας δείξει και το όνομα του και το που βρέθηκε (περιοχή ή αρχείο). Εάν έχουν μολυνθεί πολλά αρχεία το Viruscan θα τα εμφανίσει όλα.

# ΕΠΙΛΟΓΟΣ

Ακολουθώντας τις ανακατατάξεις που συντελούνται λόγω της εξέλιξης της Τεχνολογίας της πληροφορικής, σημαντική πρόοδο έχει παρουσιάσει και ο τομέας : Ασφάλεια Πληροφοριακών συστημάτων.

Οπως ήταν φυσικό ,λοιπόν, μειώνονται τα κενά που προϋπήρχαν και αυξάνονται με γοργούς ρυθμούς οι μέθοδοι βελτίωσης της ασφάλειας των πληροφοριακών συστημάτων.

Αυτό όμως δε σημαίνει ότι δεν υπάρχουν ακόμη περιθώρια βελτίωσης στον τομέα αυτό και ότι δε γίνονται λάθη.

Η συνεχής τεχνολογική εξέλιξη σε όλους τους τομείς και ιδιαίτερα στον τομέα της πληροφορικής, που τα τελευταία χρόνια βρίσκεται σε έξαρση, δεν αφήνει περιθώρια στασιμότητας σε κανέναν τομέα αλλά τον παρασύρει σε "δρόμους" βελτίωσης και ανάπτυξης.

**Οσον αφορά τους ιούς**

Οι υπολογιστές είναι πάρα πολύ ευάλωτοι. Στην πραγματικότητα, γίνονται όλο και πιο ευπρόσβλητοι, όσο αυξάνονται οι δυνατότητες επικοινωνίας μεταξύ τους, ο μεγάλος χρόνος "επώασης", που απαιτείται για να διασπαρθούν οι ιοί, και η μεγάλη ευκολία με την οποία αντιγράφονται και τροποποιούνται τα

προγράμματα των ιών.

Δεδομένου δε, ότι πολλές από τις μορφές της σύγχρονης ζωής εξαρτώνται από τα προγράμματα των υπολογιστών - μηχανική, σχεδίαση, ιατρικές διαγνώσεις, οικονομικά συστήματα κ.ά- το μέγεθος της κατατροφής γίνεται όλο και μεγαλύτερο. Ορισμένοι από τους νέους ιούς θα είναι ιδιαίτερα καταστροφικοί αν εισαχθούν σε τράπεζες δεδομένων, όπου βρίσκεται η "Πληροφορική ευημερία" μας. Οι ηλεκτρονικές πληροφορίες είναι πλέον και αυτές θνητές.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

**Γκριτζάλης Δημήτρης,** "Ασφάλεια Πληροφοριακών Συστημάτων" Ελληνική Εταιρεία Επιστημών, Αθήνα 1989

**Colin Haynes,** "Τεχνικές προστασίας από τους Ιούς των υπολογιστών", Αθήνα 1991 Εκδόσεις Γκιούρδας