Τρόποι αντιμετώπισης απο τους ιούς των υπολογιστών...

Τρόποι αντιμετώπισης απο τους ιούς των υπολογιστών...

Ομάδα εργασίας:

Ζαχαριουδάκη Δέσποινα B1
Κυριακάκης Μανώλης B2
Ρίζου Μαρία B3
Ρομπογιαννάκη Αγγελική B3
Ρουκουνάκης Γιώργος B3

Επιβλέπων Καθηγητής: Δετοράκης Ιωάννης

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Το διαδίκτυο – ο νέος δίαυλος επικοινωνίας- φιλοξενεί και διακινεί ‘υπερκείμενα’ ‘η ιστοσελίδες. Αποτελεί το σημείο συνάντησης του ιδιώτη με τον ‘δήμο’ και την ‘αγορά’(πληροφοριών), του δημιουργού με τον θεατή ή τον πελάτη. Αποτελεί χώρο εκδήλωσης απόψεων και διαδηλώσεις πολιτών, τόπο συνάθροισης συζητήσεων κλπ. διαδίκτυο αποτελεί πόρο και μέσο. Πόρο γιατί χρησιμοποιείται καθεαυτό για την οργάνωση, την αποθήκευση και την αναζήτηση γνώσης αλλά και μέσο που διαμεσολαβεί στην επικοινωνία των προσώπων μεταξύ τους. Ωστόσο τα διαδίκτυο εκτός από τα απεριόριστα μέσα που διαθέτει δυστυχώς υπηρετεί και ένα πλέγμα εξουσίας στο οποίο επιβάλλονται συμφέροντα διαφόρων πεποιθήσεων όπως τα κακόβουλα προγράμματα οι ιοί. Ο ιός υπολογιστή είναι ένα μικρό πρόγραμμα λογισμικού που εξαπλώνεται από έναν υπολογιστή σε έναν άλλο και παρεμβαίνει στη λειτουργία των υπολογιστών. Ένας ιός υπολογιστή μπορεί να καταστρέψει ή να διαγράψει δεδομένα σε έναν υπολογιστή, να χρησιμοποιήσει ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου για να μεταδώσει τον ιό σε άλλους υπολογιστές ή ακόμα και να διαγράψει όλα τα δεδομένα στο σκληρό δίσκο.

Παρακάτω θα ασχοληθούμε με την τρόπο αντιμετώπισης αλλά και για το πώς θα προλάβουμε την δράση τους.

Προληπτικά μέτρα για την αντιμετώπιση των ιών:

Κατ' αρχήν εγκαταστήστε ένα antivirus λογισμικό και φροντίστε για την καθημερινή ενημέρωσή του για νέους ιούς. Υπάρχουν διαθέσιμα διάφορα εμπορικά και ελεύθερης χρήσης λογισμικά για τον σκοπό αυτό. Το ΚΥΤΠ διανέμει το F-Secure Antivirus (βλέπε παρακάτω για την διαδικασία απόκτησής του). Αυτοματοποιήστε την ενημέρωσή του μέσω του internet (π.χ. κατά την νύχτα). Μη ενημερωμένο antivirus λογισμικό είναι πρακτικά άχρηστο.

Ρυθμίστε το λογισμικό antivirus για αυτόματη ανίχνευση κάθε νέου αρχείου που «κατεβάζετε» από το Internet. (μέσω web/email/ftp, κλπ.).

Ανιχνεύετε σε τακτικά χρονικά διαστήματα (π.χ. εβδομαδιαία) όλους τους σκληρούς δίσκους του υπολογιστή σας. Η διαδικασία αυτή (scanning) παράγει αυτόματα κάποια μηνύματα από τον έλεγχο αυτό (log files). Μην τα αγνοείτε.

Να είστε επιφυλακτικοί όταν επισκέπτεστε μία ιστοσελίδα που σας προτείνει ένας άγνωστος. Μπορεί να περιέχει κώδικα ιού, ο οποίος ΔΕΝ φαίνεται με την πρώτη ματιά. Ελαχιστοποιείστε τις επισκέψεις σας σε ιστοσελίδες αμφίβολης αξιοπιστίας.

Απενεργοποιείστε το άνοιγμα Java ή Activex εφαρμογών στον Internet Browser.

Αποφεύγετε το άμεσο άνοιγμα attached files σε emails.

Επιλέξτε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ σας στον Windows Explorer. Ίσως κάποιος να σας στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχετε την παραπάνω επιλογή ενεργοποιημένη, ίσως να εκτελέσετε το αρχείο, που να περιέχει ιό.

Οι χρήστες πρέπει να θεωρούν ότι τα αρχεία (μέσω cd, δισκετών ή email) που λαμβάνουν από κάποιον άλλον μπορεί να είναι μολυσμένα.

Χρησιμοποιείστε κάποιο προσωπικό τείχος προστασίας (Firewall). Το τείχος προστασίας είναι μια εφαρμογή που ελέγχει και καταγράφει την δικτυακή κίνηση από και προς τον υπολογιστή. Καμιά επικοινωνία δεν καθίσταται δυνατή εάν δεν την αποδεχτεί ο χρήστης. Τυπική χρήση ενός τείχους προστασίας είναι να αφήνονται ανοιχτές μόνο συγκεκριμένες θύρες (π.χ. για τη χρήστη του διαδικτύου και τη χρήση του ηλεκτρονικού ταχυδρομείου), ενώ όλες οι υπόλοιπες διατηρούνται κλειστές. Για παράδειγμα ενεργοποιείστε το Personal Firewall των Windows XP με SP2, το ελεύθερης χρήσης ZoneAlarm ή το F-Secure Client Security που διανέμεται από το ΚΥΤΠ.

Χρησιμοποιείτε τον κεντρικό mail server του ΑΠΘ (mail.auth.gr) για την ηλεκτρονική σας αλληλογραφία που παρέχει φιλτράρισμα από ιούς.

Εγκαταστήστε ένα antispyware / anti-Trojan λογισμικό. Υπάρχουν διάφορα ελεύθερης χρήσης τέτοια λογισμικά (Adaware, Spybot, Microsoft Anti-spyware, κλπ.).

Θεραπευτικά μέτρα σε περιόδους μόλυνσης:

Η μόλυνση από ιό σε μεγάλο ποσοστό ανιχνεύεται από ένα ενημερωμένο πρόγραμμα antivirus. Σε κάποιες περιπτώσεις βέβαια, όταν ο ιός συνήθως πρωτοεμφανίζεται και μέχρι οι εταιρίες να βρουν την λύση απομάκρυνσης του, υπάρχει το ενδεχόμενο μη ανίχνευσής του. Όταν υπάρχουν ενδείξεις ιού (ως σύμπτωμα) ο οποίος δεν είναι ανιχνεύσιμος από το antivirus συνήθως καταφεύγουμε σε τρίτα εργαλεία ανίχνευσης και αφαίρεσης (π.χ. Stinger). Σε αυτές τις περιπτώσεις απευθυνθείτε σε κάποιον έμπειρο τεχνικό του τμήματός σας ή στο ΚΥΤΠ. Το ΚΥΤΠ συνήθως εκδίδει δελτία τύπου μέσω ηλεκτρονικού ταχυδρομείου κατά τις εξάρσεις νέων ιών.

Στην περίπτωση που βρέθηκε ιός από το πρόγραμμα Antivirus υπάρχουν 2 ενδεχόμενα. Να μπορεί το πρόγραμμα Antivirus να αναιρέσει τον ιό (ανοσοποίηση, διαγραφή, κλπ.) ή να μην μπορεί οπότε θα πρέπει να το κάνουμε μόνοι μας ακολουθώντας κάποιες οδηγίες ή χρησιμοποιώντας κάποιο εργαλείο λογισμικού ειδικά για τον σκοπό αυτό. Συνήθως οι ίδιες οι κατασκευάστριες εταιρίες των λογισμικών antivirus παρέχουν τέτοιου είδους εργαλεία και οδηγίες (F-Secure, Symantec, McAfee, κλπ.). Σε κάποιες εξαιρετικές περιπτώσεις οι χρήστες πρέπει να επέμβουν σε αλλαγές του Μητρώου των Windows (Registry). Επειδή πολλές φορές η διαδικασία αυτή είναι μη αναστρέψιμη είναι καλό σ' αυτή την περίπτωση να απευθυνθείτε σε κάποιο έμπειρο τεχνικό του τμήματός σας ή στο ΚΥΤΠ.
Απόκτηση των προγραμμάτων F-Secure Antivirus / Client Security από το ΚΥΤΠ.
Για την αντιμετώπιση των ιών το ΚΥΤΠ διανέμει τα F-Secure AntiVirus και F-Secure Client Security της Datafellows. Η άδεια χρήσης του λογισμικού ισχύει μέχρι τις 10/05/2006. Επισημαίνεται ότι το F-Secure Client Security είναι ένα γενικότερο προϊόν προστασίας προσωπικών υπολογιστών, περιλαμβάνει το F-Secure Antivirus, αλλά επιπρόσθετα διαθέτει και τοίχο προστασίας (firewall), καθώς και προστασία από spyware. Λόγω πολυπλοκότητας στην εγκατάσταση του προϊόντος Client Security, συστήνεται κυρίως σε έμπειρους χρήστες.
Για την απόκτησή του κατεβάστε την αίτηση από την ιστοσελίδα του ΚΥΤΠ . Στείλτε την αίτηση με fax (998302) ή στο email Το ΚΥΤΠ θα σας αποστείλει τον αντίστοιχο κωδικό εγκατάστασης μέσω fax (εφόσον ο αριθμός του fax ανήκει στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης) ή μέσω email (σε email με κατάληξη auth.gr). Κατόπιν διαλέξτε από τον σχετικό πίνακα το λειτουργικό που σας ενδιαφέρει και κατεβάστε το αντίστοιχο αρχείο στον υπολογιστή σας. Εναλλακτικά, για μη δικτυωμένους υπολογιστές μπορείτε να παραλάβετε το σχετικό CD από το ΚΥΤΠ (δίνοντας ένα άδειο CDR με λευκή επιφάνεια εκτύπωσης).

Θέματα λειτουργικών συστημάτων:

Πολλές φορές οι ιοί εκμεταλλεύονται ατέλειες ή αρχικές ρυθμίσεις των λειτουργικών συστημάτων. Οι κατασκευάστριες εταιρίες προβαίνουν κατά διαστήματα σε διορθωτικές κινήσεις για την κάλυψη αυτών των ατελειών (Service Packs και Patches). Οι διορθώσεις αυτές μπορεί να είναι είτε κρίσιμες, απαραίτητες δηλαδή για όλους τους χρήστες, είτε μη κρίσιμες όταν αφορούν ειδικές ομάδες χρηστών οι οποίοι κάνουν χρήση ειδικών εφαρμογών του λογισμικού.

Τα Service Packs δεν κυκλοφορούν τόσο συχνά (3-4 εκδόσεις για κάθε έκδοση λειτουργικού). Τα Patches διατίθενται αρκετά συχνά για διόρθωση συγκεκριμένων προβλημάτων. Τα Service Packs μπορούν να θεωρηθούν ως ένα σύνολο από Patches. Σε κάθε περίπτωση συνιστάται η εγκατάσταση των Service Packs γιατί συνήθως βελτιστοποιούν το λειτουργικό μας σύστημα, την ασφάλεια και την απόδοσή του. Επειδή όμως η προσθήκη τους ενδέχεται να απαιτεί τεχνικές γνώσεις, καλό είναι να απευθύνεστε σε κάποιο έμπειρο τεχνικό ή το ΚΥΤΠ. Επίσης για να αποφευχθεί τυχόν απώλεια δεδομένων είναι καλό να γίνεται backup στον υπολογιστή πριν από την προσθήκη οποιουδήποτε Service Pack ή ενέργειες που μπορούν να διασφαλίσουν την επιστροφή του συστήματος στην προηγούμενη κατάσταση.
Τόσο τα patches όσο και τα Service Packs μπορούμε να τα κατεβάσουμε μέσα από την επιλογή Windows Update των Windows (Start Menu ή από τον Πίνακα Ελέγχου). Προσέξτε ότι σε κάποιες εκδόσεις των Windows δεν επιτρέπεται η διαδικασία Windows Update αν δεν έχει γίνει η προμήθειά τους με νόμιμο τρόπο.
Το ΚΥΤΠ σε συνεργασία με την Microsoft® προσφέρει το πρόγραμμα διανομής λογισμικού MSDN Academic Alliance (MSDNAA). Το λογισμικό περιλαμβάνει το σύνολο του λογισμικού της Microsoft, εκτός του MS Office (περιλαμβάνεται όμως η MS Access) και απευθύνεται σήμερα αποκλειστικά στα μέλη των Τμημάτων (μέλη ΔΕΠ, Ερευνητές και Φοιτητές). Κατά συνέπεια το λογισμικό MSDN AA δεν δύναται να χρησιμοποιηθεί σε Διοικητικές Υπηρεσίες ή εφαρμογές.

Προληπτικά μέτρα σχετικά με την ενημέρωση των λειτουργικών συστημάτων:

Κάντε συχνά update στο λειτουργικό σύστημα του Η/Υ σας ή ακόμα καλύτερα αυτοματοποιήστε την διαδικασία Windows Update, ώστε να καλύπτονται τα όποια κενά ασφαλείας έχουν εντοπιστεί (Πίνακας Ελέγχου > Αυτόματη Ενημέρωση).
Εφαρμόζετε τα Service Packs αφού ρωτήσετε πρώτα κάποιο έμπειρο τεχνικό ή το ΚΥΤΠ.
Αναβαθμίστε άμεσα τις μη υποστηριζόμενες και λιγότερο ασφαλείς εκδόσεις MS Windows 98, MS Windows ME, MS Windows NT στις αντίστοιχες εκδόσεις MS Windows XP και 2003.
Πρόσφατα Service Packs της Microsoft.
MS Windows XP Service Pack 2 (SP2) με ημερομηνία κυκλοφορίας 25 Αυγούστου 2004.
MS Windows 2000 Service Pack 4 με ημερομηνία κυκλοφορίας 26 Ιουνίου 2003.
MS Windows 2003 Service Pack 2 με ημερομηνία κυκλοφορίας 12 Μαρτίου 2007.
Για να εγκαταστήσετε τα παραπάνω Service Packs χρησιμοποιήστε τις Αυτόματες Ενημερώσεις (Automatic Updates) ή το Windows Update ή απευθυνθείτε στο ΚΥΤΠ για τα CDs.

Γενικότερες καλές πρακτικές:

Λειτουργικά συστήματα τα οποία δεν παρέχουν το απαραίτητο επίπεδο ασφάλειας ή δεν υποστηρίζονται πλέον από τις κατασκευάστριες εταιρίες (όπως Windows 95/98/ME/NT), πρέπει να αποφεύγονται σε θέσεις εργασίας και ακόμα περισσότερο σε εξυπηρετητές. Πρέπει να ληφθεί μέριμνα για την άμεση αναβάθμισή τους αν υπάρχουν. Ακόμα και τα Windows 2000 είναι καλό να αναβαθμιστούν αν και συνεχίζεται η υποστήριξή τους επί του παρόντος.

Είναι επίσης καλό να αναβαθμιστούν και οι εκδόσεις των MS Office 95/97/2000 σε MS Office XP ή 2003. Αν τυχόν είχατε προμηθευτεί την έκδοση του MS Office με Software Assurance (SA) δικαιούστε για το προβλεπόμενο χρονικό διάστημα την αναβάθμιση αυτή δωρεάν από τον προμηθευτή σας.

Δεν πρέπει να εγκαθίσταται λογισμικό πέραν του απαραίτητου ώστε να αποφεύγονται προβλήματα λόγω αυξημένης πολυπλοκότητας ή κακής αλληλεπίδρασης (conflicts).

Επιβάλλεται η αποφυγή εγκατάστασης προγραμμάτων τύπου P2P (kazaa, emule, edonkey, κ.ά.) μέσα από τα οποία συνήθως διακινείται παράνομο λογισμικό, πορνογραφικό περιεχόμενο και γενικότερα παράνομα αρχεία, με αποτέλεσμα να θέτουν προ νομικών ευθυνών την εκάστοτε διοίκηση ή να μειώνουν την ασφάλεια του πληροφοριακού συστήματος των Υπηρεσιών. Γενικότερα συνιστάται ο διαχωρισμός των σταθμών εργασίας των Διοικητικών/ Ακαδημαϊκών Υπηρεσιών σε σταθμούς αποκλειστικής πρόσβασης για υπηρεσίες και σε σταθμούς γενικής χρήσης (πρόσβασης στο διαδίκτυο, στο ηλεκτρονικό ταχυδρομείο, κλπ).

Οι χρήστες είναι υπεύθυνοι για την επιλογή και διαφύλαξη «ασφαλούς» συνθηματικού (password) για την πρόσβαση στο λογαριασμό τους. Ασφαλές συνθηματικό είναι αυτό που δεν μπορεί κάποιος να υποθέσει εύκολα, συνεπώς πρέπει να αποφεύγονται αυτούσιες λέξεις, ονόματα συγγενικών προσώπων, ημερομηνίες γέννησης, κλπ. Επίσης το συνθηματικό δεν θα πρέπει να είναι μέρος του ονόματος χρήστη (username). Το συνθηματικό πρέπει να αλλάζει τακτικά (π.χ. μία φορά το τρίμηνο ή αμέσως μετά από υποψία παραβίασης). Καλό είναι να περιέχει παραπάνω από 7 χαρακτήρες κάποιων εκ των οποίων να είναι αριθμοί και special characters (%$!*&, κλπ.).

Τα συνθηματικά είναι αυστηρώς προσωπικά, απαγορεύονται να δίδονται σε τρίτους, δεν πρέπει να γράφονται σε χαρτί ή να φυλάσσονται σε οποιαδήποτε μορφή (ηλεκτρονική ή μη). Πρέπει να αποφεύγονται οι κοινοί λογαριασμοί οι οποίοι αντιστοιχούν σε περισσότερα από ένα φυσικά πρόσωπα (π.χ. user1, user2, κλπ.).

Όταν επισκεπτόμαστε σελίδες στο internet οι οποίες απαιτούν registration, ΔΕΝ χρησιμοποιούμε το ίδιο password με αυτό που έχουμε για την πρόσβαση στον υπολογιστή μας.

Για λόγους ασφάλειας οι χρήστες υποχρεούνται να κάνουν πλήρη έξοδο από το σύστημα (logoff) μετά το πέρας της εργασίας τους.

Οι χρήστες πρέπει να φροντίζουν για την λήψη αντιγράφων ασφαλείας των δεδομένων τους (backup). Το backup μπορεί να γίνεται είτε τοπικά σε περιφερειακές μονάδες Η/Υ της Υπηρεσίας (CDRW, DAT, κλπ.), είτε κεντρικά μέσω του κεντρικού συστήματος Backup ΑΠΘ (βλέπε παρακάτω). Τα μέσα στα οποία παίρνονται τα αντίγραφα ασφάλειας (μαγνητικά μέσα όπως ταινίες, DLTs, DAT, zip

drives, σκληροί δίσκοι, CDRW, WORM, κλπ.) φυλάσσονται κατά ένα μέρος σε ασφαλές σημείο εντός της Υπηρεσίας σε χώρους μακριά από ηλεκτρομαγνητικά πεδία, ακτινοβολία, υγρασία, υψηλή θερμοκρασία, κλπ. και κατά ένα μέρος σε διαφορετικό σημείο, κατά προτίμηση εκτός κτιρίου Υπηρεσίας.
Για την ευκολότερη διαχείριση των υπολογιστών σας σημειώστε με αυτοκόλλητη ταμπέλα πάνω σε κάθε PC την ημερομηνία κτήσης, τον χρόνο εγγύησης, το προμηθευτή και τα χαρακτηριστικά του PC (CPU, μνήμη, δίσκος, κλπ.) το όνομα και το IP address του για γρήγορη αναφορά.
Σε pop-up παράθυρα και ερωτήσεις (π.χ. σας ενδιαφέρει κάτι ή όχι) κατά την πλοήγησή μας στο internet μην επιλέγετε ποτέ ΝΑΙ ή ΟΧΙ. Μην κλείνετε τα παράθυρα αυτά πάνω δεξιά από το "Χ". Πολλές φορές όλες αυτές οι επιλογές εκτελούν τον ίδιο κώδικα στέλνοντας πληροφορίες σχετικά με τον υπολογιστή σας, ή εκτελώντας κακόβουλο λογισμικό. Κλείστε τα κατευθείαν από τα Windows (Γραμμή Εργαλείων, δεξί κλικ, Κλείσιμο).
Μην εκτελείτε καθημερινές λειτουργίες στον υπολογιστή σας ως Διαχειριστής (Administrator), εκτός αν είναι απαραίτητο.
Η επιβάρυνση του Desktop σας με File/Directory Shortcuts, add-ons, Internet Explorer toolbars, εντυπωσιακά ποντίκια/κλεψύδρες , Screen Savers, κλπ. αφαιρεί μνήμη από τον υπολογιστή σας και μειώνει γενικότερα την απόδοσή του.
Σε τακτικά χρονικά διαστήματα (τουλάχιστον μία φορά το 6μηνο) επιλέγετε (Accessories>System Tools> Disk Defragmenter και Disk Cleanup) που βελτιώνουν την απόδοση του υπολογιστή σας.
Για να χρησιμοποιήσετε τη δυνατότητα των Windows "System-Restore" (επαναφορά του συστήματος σε προηγούμενη κατάσταση) θα πρέπει να έχετε ενεργοποιημένο το "System-Restore" από τον Πίνακα Ελέγχου. Έτσι μπορούμε να επαναφέρουμε το σύστημά μας σε παλαιότερη «υγιή» κατάσταση (πριν π.χ. την μόλυνση από κάποιο ιό).

Υπηρεσία κεντρικού Backup:

Το Κεντρικό BACKUP είναι μία δικτυακή υπηρεσία λήψης αντιγράφων δεδομένων με σκοπό την χρησιμοποίησή τους σε περίπτωση βλάβης του υπολογιστή, του σκληρού δίσκου, συγκεκριμένων αρχείων, ή λανθασμένων ενεργειών χρήστη. Τα backups λαμβάνονται κάθε νύχτα (incremental) το δε Σαββατοκύριακο λαμβάνεται συνολικό (full). Τα δεδομένα σας είναι διαθέσιμα (ανακτήσιμα) για διάστημα μέχρι και ενός μήνα από την ημερομηνία λήψης του backup. Ο διαθέσιμος αποθηκευτικός χώρος για κάθε μηχάνημα είναι 20GB uncompressed ή 40 GB compressed (full backup). Όσον αφορά την ασφάλεια των δεδομένων, το λογισμικό δίνει την δυνατότητα:
Password protection
Encryption
Password protection and Encryption
Έτσι η διαδικασία ανάκτησης των δεδομένων δεν είναι εφικτή από οποιοδήποτε άλλο χρήστη πέραν του κατόχου. Για την ενεργοποίηση του κεντρικού backup στον υπολογιστή σας επικοινωνήστε με το ΚΥΤΠ.

Πρόσθετες υπηρεσίες διαχείρισης και παρακολούθησης υπολογιστικών συστημάτων:

Για σημαντικά υπολογιστικά συστήματα και εξυπηρετητές, το ΚΥΤΠ προσφέρει 2 πρόσθετες υπηρεσίες:

- Κεντρικό Performance Monitoring
- Έλεγχος Ασφάλειας Υπολογιστικών Συστημάτων

Το Κεντρικό Performance Monitoring είναι ένα σύστημα παρακολούθησης της κατάστασης υπολογιστικών συστημάτων. Το σύστημα ελέγχει πάνω από το δίκτυο:
Διασύνδεση του συστήματος με το δίκτυο (έμμεσα υπονοεί και την λειτουργία του συστήματος)
Φόρτος CPU
Χωρητικότητα δίσκων
Μηνύματα του συστήματος που αφορούν την απόδοση και την ασφάλεια
Λειτουργία συγκεκριμένων services που κρίνεται σκόπιμο να παρακολουθούνται (ftp, http, smtp services, License Managers, databases, κλπ.).
Οι εκάστοτε διαχειριστές ειδοποιούνται για την κατάσταση των υπολογιστικών τους συστημάτων με δύο τρόπους:

1. Μέσω του Internet σε συνεχή βάση όπου απεικονίζεται αναλυτικά η τρέχουσα κατάσταση των συστημάτων που είναι ενταγμένα στο σύστημα (ΠΡΑΣΙΝΟ: σύστημα ok, ΚΙΤΡΙΝΟ: υπενθύμιση, ΚΟΚΚΙΝΟ: πρόβλημα). Το σύστημα επίσης παρέχει ιστορικά δεδομένα σχετικά με την κατάσταση των συστημάτων.
2. Μεσω email σε περιπτώσεις προβλημάτων ή υπενθυμίσεων.

Η υπηρεσία Ελέγχου Ασφάλειας Υπολογιστικών Συστημάτων (Nessus Security Scanning) απευθύνεται αποκλειστικά σε διαχειριστές συστημάτων. Το Nessus διαπιστώνει την ύπαρξη τρωτών σημείων, από τα οποία θα μπορούσε κάποιος τρίτος να εισβάλει ή γενικά να προκαλέσει προβλήματα στην ομαλή λειτουργία των μηχανημάτων. Το Nessus περιέχει περισσότερα από 1200 δοκιμές ασφάλειας όπως Backdoors, CGI abuses, Denial Of Service, Remote file access, Shell access, κλπ.
Η ενημέρωση των διαχειριστών συστημάτων για τα αποτελέσματα γίνεται μέσω του internet (NessusPHP web interface – με πρωτόκολλο HTTPS) και σε περιοδική βάση ανάλογα με την επιλογή του χρήστη (εβδομαδιαίως, μηνιαίως, κλπ). Τα αποτελέσματα του security scanning δεν περιέχουν μόνο λίστα με τα προβλήματα ασφαλείας, αλλά αναλυτικές πληροφορίες για το πως να διορθωθούν αυτά τα προβλήματα καθώς και δείκτη επικινδυνότητας ή ρίσκου για κάθε πρόβλημα. Η βάση δεδομένων με τις δοκιμές που εφαρμόζονται από το Nessus, ανανεώνεται διαρκώς και σε καθημερινή βάση, για να συμπεριλάβει security checks για τελευταία και πρόσφατα προβλήματα ασφαλείας.
Όλα τα μηχανήματα ανεξαρτήτως λειτουργικού συστήματος που είναι ενταγμένα στο δίκτυο του ΑΠΘ μπορούν να κάνουν χρήση της υπηρεσίας. Για την ενεργοποίηση της υπηρεσίας επικοινωνήστε με το ΚΥΤΠ.

Τεχνική υποστήριξη:

Υπηρεσίες τεχνικής υποστήριξης περί των θεμάτων που αναπτύσσονται στο παρόν κείμενο, παρέχονται για όλους τους χρήστες του ΑΠΘ, είτε στο τηλέφωνο 2310992000 κατά τις ώρες 09:00 έως 14:30 τις εργάσιμες ημέρες, είτε μέσω email.
Παρακαλείσθε όταν επικοινωνείτε με το ΚΥΤΠ να αναφέρετε το ονοματεπώνυμό σας, την ιδιότητά σας στο ΑΠΘ και το email σας (XXX@XXX.auth.gr), ώστε να γίνεται καταχώρηση της κλήσης στο Helpdesk του ΚΥΤΠ. Επίσης αν επικοινωνείτε τηλεφωνικά είναι καλό να συγκρατείτε το όνομα του τεχνικού που ανέλαβε την κλήση σας.

Προγράμματα προστασίας από ιούς:

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη - ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους αναδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντίκα είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν.

Κάθε αντιιό έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο, τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιιό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα). Θα πρέπει να σημειωθεί ότι οι δημιουργοί ιών λαμβάνουν σοβαρά υπόψη τους τις μεθόδους εντοπισμού του "προϊόντος" τους και δημιουργούν ιούς, οι οποίοι προσπαθούν να αποφύγουν τον εντοπισμό, ακόμη και με απενεργοποίηση του αντιϊκού. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει τακτικότατα το λογισμικό του αλλά και να δημιουργεί τις ειδικές δισκέτες, που τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους, ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.

Προγράμματα Προστασίας:

- Avira AntiVir Personal Edition

Το Avira AntiVir είναι ένα λογισμικό προστασίας από ιούς, spyware, malware και rootkit και διατίθεται δωρεάν για προσωπική χρήση. Είναι πολύ ελαφρύ στους πόρους και το ποσοστό ανίχνευσης malware είναι εξαιρετικό. Το AntiVir δεν περιλαμβάνει δυνατότητες σάρωσης web ή e-mail που είναι διαθέσιμο μόνο στην πληρωμένη έκδοση. Αυτό σημαίνει ότι το AntiVir δεν θα σας προειδοποιήσει για τα μολυσμένα e-mail πριν τα ανοίξετε αλλά θα σας προστατεύσει μόλις ανοίξετε κάποιο μολυσμένο e-mail.

- Microsoft Security Essentials

Το Microsoft Security Essentials είναι ένα λογισμικό προστασίας από ιούς, spyware, malware και rootkit. Είναι πολύ ελαφρύ στους πόρους με καλό ποσοστό ανίχνευσης, ιδιαίτερα για rootkits και είναι πολύ καλό στην αφαίρεση malware που ήδη υπάρχουν στον υπολογιστή σας. Το Security Essentials είναι η καλύτερη επιλογή για τους μέσους χρήστες, λόγω της ελάχιστης απαιτούμενης αλληλεπίδρασης του χρήστη. Θα ενημερώνετε και θα αφαιρεί τις απειλές αυτόματα. Διατίθεται δωρεάν από τη Microsoft αλλά απατεί την ύπαρξη γνήσιου λειτουργικού Windows.

- Avast! Free Antivirus

Το Avast! Free Antivirus είναι επίσης ένα εξαιρετικό δωρεάν λογισμικό προστασίας από ιούς, spyware, malware και rootkit. Είναι ελαφρύ στους πόρους και έχει καλό ποσοστό ανίχνευσης. Το Avast έχει πολλά χαρακτηριστικά, με πλήρεις δυνατότητες σε πραγματικό χρόνο, που συμπεριλαμβάνουν ανίχνευση των ιστοσελίδων, e-mail, IM, P2P και ασπίδες δικτύου καθώς και σάρωση κατά την εκκίνηση. Χρειάζεται εγγραφή η οποία είναι δωρεάν για τη λήψη ενημερώσεων για νέους ιούς.

- AVG Anti-Virus Free Edition

Το AVG Anti-Virus Free Edition είναι ένα δημοφιλές δωρεάν λογισμικό προστασίας από ιούς, spyware, malware. Στις νέες του εκδόσεις προσφέρει ένα υψηλό επίπεδο προστασίας και σε πραγματικό χρόνο καθώς σερφάρετε στο Internet.

- SuperAntiSpyware

Το SuperAntiSpyware είναι ένα δημοφιλές δωρεάν λογισμικό προστασίας από κακόβουλο λογισμικό όπως spyware, adware και malware. Η δωρεάν έκδοση δεν έχει την προστασία συνεχώς ενεργοποιημένη αλλά προστατεύεστε κάνοντας χειροκίνητα σάρωση του υπολογιστή σας.

- Malwarebytes Anti-Malware

Το Malwarebytes Anti-Malware είναι ακόμα ένα δημοφιλές λογισμικό προστασίας από κακόβουλο λογισμικό όπως worms, trojans, rootkits, dialers, spyware, adware και malware. Η δωρεάν έκδοση δεν έχει ενεργοποιημένη την προστασία σε πραγματικό χρόνο ούτε και την προγραμματισμένη σάρωση και την προγραμματισμένη ενημέρωση αλλά θα πρέπει να κάνετε χειροκίνητα και σε τακτά χρονικά διαστήματα ενημέρωση και σάρωση του υπολογιστή σας.

- Comodo Firewall

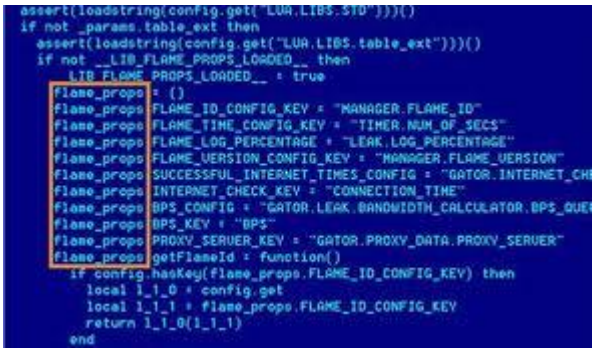
Το Comodo Firewall είναι η καλύτερη επιλογή για χρήστες που αναζητούν μια δωρεάν σουίτα ασφαλείας με πλήρη χαρακτηριστικά. Έχει μια ισχυρή και μια πολύ δραστήρια HIPS ή την δυνατότητα επιτήρησης εφαρμογών με τίτλο "Defense +", η οποία φτάνει ή υπερβαίνει τις επιδόσεις ασφαλείας αντίστοιχων επι πληρωμή προϊόντων. Η νέα έκδοση περιέχει πολλά νέα χαρακτηριστικά, επιτρέποντας ταυτόχρονα έμπειρους χρήστες να διατηρούν τον απόλυτο έλεγχο του συστήματός τους, ελέγχοντας τα ports, τα πρωτόκολλα και πλήρη έλεγχο της διαμόρφωσης. Κατά την εγκατάσταση, σας δίνει τη δυνατότητα επιλογής ανάμεσα σε δύο επίπεδα ασφάλειας. Το "τείχος προστασίας μόνο" mode και το Comodo Internet Security που περιλαμβάνει antivirus, antimalware, και επιπλέον χαρακτηριστικά.

- Online Armor Free

Το Online Armor Free είναι ένα δωρεάν τείχος προστασίας. Σας προστατεύει από επιθέσεις hacker, από κακόβουλα προγράμματα και προστατεύει την ταυτότητά σας. Έχει μια ισχυρή και μια πολύ δραστήρια HIPS ή την δυνατότητα επιτήρησης εφαρμογών με τίτλο "Program Guard" που ελέγχει την συμπεριφορά των προγραμμάτων σας. Η πρόσθετη έκδοση (επι πληρωμή) διευρύνει την προστασία με αυτόματες ενημερώσεις και περιλαμβάνει Antivirus και Antispyware δυνατότητες καθώς και προστασία στις online τραπεζικές σας συναλλαγές.

- Zone Alarm Free Firewall

Το ZoneAlarm® Free Firewall είναι ένα τείχος προστασίας. Σας προστατεύει από εισβολείς (hacker) και λογισμικό υποκλοπής spyware. Οι χρήστες μπορούν να προσαρμόσουν τις ρυθμίσεις ασφαλείας ανάλογα με τις ανάγκες τους. Τα αναδυόμενα παράθυρα δίνουν πληροφορίες, παραθέτοντας το όνομα του προγράμματος ή το όνομα του εκτελέσιμου αρχείου που ζητεί την πρόσβαση ώστε ο χρήστης να αποφασίσει τι θα γίνει. Το Zone Alarm Free προσφέρει προστασία εισερχόμενων / εξερχόμενων, Stealth mode που σας κάνει αόρατους, Anti-phishing προστασία και προστασία κλοπής ταυτότητας. Διατίθεται δωρεάν και επί πληρωμή.



Πολλοί από μας έχουμε αναρωτηθεί ποιο λογισμικό ασφαλείας να εγκαταστήσουμε στον υπολογιστή μας και τις περισσότερες φορές αναζητούμε κάποιο δωρεάν πρόγραμμα.
Για να σας βοηθήσουμε στο θέμα αυτό σας παραθέτουμε παρακάτω μία συγκριτική ανάλυση των 3 δημοφιλέστερων δωρεάν antivirus, του AVG, του Avira και του Avast!. Κατά την αξιολόγηση του λογισμικού ασφάλειας, υπάρχουν δύο κύριοι τομείς τους οποίους θα πρέπει να εξετάσουμε: χαρακτηριστικά και επιδόσεις.

1. **Χαρακτηριστικά**:

Όσον αφορά στις δυνατότητες, όπως φαίνεται και στον παραπάνω πίνακα, και τα τρία προϊόντα παρέχουν την αναγκαία προστασία. Ωστόσο, το avast! είναι το μόνο που προσφέρει το «κάτι παραπάνω» λόγω των έξτρα χαρακτηριστικών.
Αποδοτικότητα\Επιδόσεις:
Αποτελέσματα σε τεστ κατ' απαίτηση του χρήστη:

2. **Προστασία Real time**:

Με βάση τα παραπάνω γραφήματα οι γενικές ενδείξεις είναι σαφείς, το Avira ανιχνεύει τα περισσότερα κακόβουλα προγράμματα, με το avast! να έρχεται δεύτερο, και το AVG τρίτο. Ωστόσο, αξίζει να σημειωθεί ότι το Avira αναφέρει λανθασμένα ως κακόβουλα κάποια προγράμματα (false positives), ενώ τα avast! και AVG έχουν πολύ μικρότερο αριθμό τέτοιων λαθών.
Ταχύτητα και χρήση πόρων υπολογιστή:

3. **Χρόνος εκκίνησης υπολογιστή:**

4. **Χρόνος εκτέλεσης εφαρμογής (Firefox):**

5. **Σκανάρισμα σκληρού δίσκου (13GB):**

6. **Χρήση ελεύθερης μνήμης**

7. **Χρήση ελεύθερης μνήμης (μέγιστο):**

Όπως μπορείτε να δείτε, τα αποτελέσματα χρήσης RAM και ταχύτητας είναι κάπως συγκεχυμένα. Σε κάθε τεστ τα καλύτερα αποτελέσματα τα δίνει διαφορετικό λογισμικό. Ωστόσο, κάτι που αξίζει να σημειώσουμε είναι το πόσο δυσανάλογα μεγάλο χρόνο πήρε για το avast! να κάνει ένα πλήρες σκανάρισμα (19 λεπτά). Η διαφορά είναι μεγάλη, ιδίως αν ληφθεί υπόψη το γεγονός ότι στα άλλα τεστ το avast! σημείωσε παρόμοια αποτελέσματα με τα άλλα δύο, κυρίως στο θέμα χρήσης της RAM.

- ***Συμπέρασμα***

Όπως ήταν αναμενόμενο, δεν υπάρχει κανείς νικητής. Ωστόσο, εάν υπάρχει μία διαχωριστική γραμμή θα ήταν μεταξύ AVG και avast!/Avira. Το AVG είναι ίσως το πιο δημοφιλές, ωστόσο, λαμβάνοντας υπόψη τα παραπάνω τεστ (ιδίως τα τεστ ανίχνευσης ιών), ίσως δεν είναι καλύτερο από τα άλλα δύο. Αυτό βέβαια δεν σημαίνει ότι το AVG είναι κακό, απλά δεν παρέχει κανένα πλεονέκτημα έναντι των άλλων. Το avast! έχει τα περισσότερα πρόσθετα χαρακτηριστικά και χρησιμοποιεί την λιγότερη μνήμη RAM όσο είναι σε αδράνεια, όμως παίρνει πολύ χρόνο για να κάνει μια πλήρη σάρωση. Το Avira είναι ό,τι καλύτερο όσον αφορά την ανίχνευση κακόβουλου λογισμικού, αλλά και έχει πολλά false positives. Οπότε για να απαντήσουμε στην ερώτηση – ποιο να χρησιμοποιήσω; Εξαρτάται. Αν ψάχνετε για την καλύτερη προστασία, Avira. Αν θέλετε ένα πιο ολοκληρωμένο, αλλά όχι με το καλύτερο ποσοστό ανίχνευσης, τότε avast!

Τρόποι Προστασίας από τους Ιούς:

Γνήσιο Λειτουργικό Σύστημα (πχ Windows) και Ενημερώσεις (updates) του Λειτουργικού που διορθώνουν τα σφάλματα ασφαλείας (critical updates).
Εγκατάσταση Λογισμικού Antivirus συνεχή ενημέρωσή του (συνήθως αναβαθμίζονται όταν κάθε φορά που συνδεόμαστε στο Internet) να έχει οπωσδήποτε αυτόματη λειτουργία ανίχνευσης σε κάθε λειτουργία του Υπολογιστή και βεβαίως να το βάζουμε να ψάχνει τον υπολογιστή μας κατά τακτά χρονικά διαστήματα. (Προσοχή στον υπολογιστή μας ΔΕΝ ΠΡΕΠΕΙ ΝΑ ΕΙΝΑΙ ΕΓΚΑΤΕΣΤΗΜΕΝΑ ΠΑΡΑΠΑΝΩ ΑΠΟ ΕΝΑ ANTIVIRUS).
Εγκατάσταση προγράμματος Antimalware-antispyware το οποίο να ενημερώνεται (αυτόματα ή χειροκίνητα) και συχνό ψάξιμο του υπολογιστή μας. (τέτοιου είδους προγράμματα σε αντίθεση με τα antivirus μπορούμε να εγκαταστήσουμε περισσότερα του ενός).
Να ελέγχουμε αν είναι ενεργοποιημένο το FIREWALL (ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ) των Windows ή να χρησιμοποιήσουμε κάποιο άλλο πρόγραμμα αντ' αυτού.
Μην σερφάρετε σε αμφίβολης προέλευσης Ιστοσελίδες και να είστε πάρα πολύ προσεκτικοί με πίνακες που σας ζητάνε να κατεβάσουν κάτι στον υπολογιστή σας (ΠΑΝΤΑ ΝΟ, ΠΟΤΕ YES!!!).
Μεγάλη προσοχή σε Δωρεάν προγράμματα ή σε Free Versions που προσφέρονται από αναξιόπιστες πηγές.
Συνήθως μέσα στην άδεια χρήσης σας προτρέπουν να συμφωνήσετε στην εγκατάσταση διαφημιστικών προγραμμάτων (CD ΠΕΡΙΟΔΙΚΩΝ κλπ).
Αν και κάνει κακό στις διαπροσωπικές σχέσεις γενικά είναι καλό να μην ξέρει κανείς τα user name και τα password σας.
Προστατευθείτε από τους Ιούς (Viruses)

- Γενικά
- Τρόποι Προστασίας από τους Ιούς
- Οι Πρώτοι Εκτελέσιμοι Ιοί
- Οι Ιοί του Boot Sector
- Οι Ιοί των e-mails
- Τα προγράμματα Dialers
- Τα σκουλήκια (Worms)
- Οι Κερκόπορτες (Backdoors)
- Οι Επιθέσεις DoS (Denial of Service)
- Οι Επιθέσεις DDoS (Distributed Denial of Service)
- Οι Φάρσες Ιών (Virus Hoaxes)
- Τα προγράμματα Spyware
- Οι Δούρειοι Ίπποι (Trojan Horses)
- Τα Spam e-mails
- Τα Cookies
- Τα Προγράμματα Spyware και Adware
- Το Web Tracking
- Τα Internet Passports

Τρόποι Προστασίας από τους Ιούς:
Ο βασικός τρόπος προστασίας από τους ιούς των υπολογιστών είναι η εγκατάσταση, η σωστή ρύθμιση και η συνεχής ενημέρωση ή επικαιροποίηση (update) μέσω του Internet ενός έγκυρου προγράμματος προστασίας από ιούς, που είναι γνωστά με τον όρο Antivirus ή αντιικά προγράμματα. Υπάρχουν ακόμη ειδικά προγράμματα για προστασία από ιούς τύπου spyware, adware αλλά και από dialers και από τη μάστιγα των spam e-mails.
Η χρήση ενός ψηφιακού τείχους προστασίας (firewall), με τη μορφή software ή hardware, είναι χρήσιμη αλλά θα πρέπει να γίνεται με προσοχή και με την προϋπόθεση ότι υπάρχει καλή γνώση του τρόπου ρύθμισης και λειτουργίας του. Οι γενικοί κανόνες προστασίας είναι ότι θα πρέπει να προσέχουμε τι προγράμματα εκτελούμε στον υπολογιστή μας, τι αρχεία κατεβάζουμε από το Internet, ποιος μας στέλνει e-mail καθώς και ποιος έχει το δικαίωμα να χρησιμοποιήσει τον υπολογιστή μας όταν εμείς απουσιάζουμε. Προσοχή πρέπει να δίνουμε και στα προγράμματα που διαφημίζονται και διανέμονται δωρεάν καθώς και στα προγράμματα που χρησιμοποιούμε για να κάνουμε chat.
Μια πολύ καλή λύση είναι να εγκαταστήσουμε και να εκτελέσουμε μια από τις εφαρμογές που αναλαμβάνουν να ανιχνεύσουν στο σύστημά μας τα τυχόν υπάρχοντα ευαίσθητα σημεία (vulnerabilities) και να μας τα παρουσιάσουν με παραστατικό τρόπο. Τέλος, μια πολύ καλή συμβουλή είναι να λαμβάνουμε πολύ τακτικά, ίσως και καθημερινά, εφεδρικά αντίγραφα ασφαλείας των αρχείων μας, σε CD, σε DVD ή σε εξωτερικό σκληρό δίσκο, μια διαδικασία που είναι γνωστή με τον όρο back-up, έτσι ώστε ακόμα και στην ακραία περίπτωση που χάσουμε σημαντικά αρχεία από την επίθεση κάποιου ιού, να μπορέσουμε να τα ανακτήσουμε άμεσα.

Από τα πιο γνωστά αντιικά προγράμματα είναι το Norton Antivirus της εταιρείας Symantec, το McAfee της εταιρείας Network Associates, το Kaspersky, το Panda, το Sophos, το F-Prot της εταιρείας Frisk, το F-Secure καθώς και το AntiVir και το AVG της εταιρείας Grisoft που διατίθενται δωρεάν για προσωπική χρήση. Όλα έχουν τη δυνατότητα αυτόματης ενημέρωσης (update) μέσω του Internet.
Απλές Οδηγίες Προστασίας από τους Ιούς. Μπορείτε να προστατευθείτε από τους ιούς με μερικά απλά βήματα :

- Αν ανησυχείτε πολύ για τους παραδοσιακούς ιούς, θα πρέπει να δουλεύετε μ' ένα πιο ασφαλές λειτουργικό σύστημα όπως είναι το UNIX ή το Linux.
- Αν χρησιμοποιείτε ένα μη ασφαλές λειτουργικό σύστημα, τότε θα πρέπει να προμηθευθείτε ειδικό λογισμικό προστασίας από ιούς.
- Θα πρέπει να βεβαιωθείτε ότι είναι ενεργό το Macro Virus Protection σ' όλες τις εφαρμογές της Microsoft και ΠΟΤΕ δεν θα πρέπει να εκτελείτε μακροεντολές (macros) σ' ένα έγγραφο εκτός κι αν είστε σίγουροι για το τι ακριβώς κάνουν.
- Δεν θα πρέπει ποτέ να κάνετε διπλό κλικ σ' ένα συνημμένο που περιέχει ένα εκτελέσιμο αρχείο που έχει φθάσει μέσω e-mail. Τα συνημμένα που έρχονται ως αρχεία του Word (.DOC), ως φύλλα εργασίας (.XLS), ως εικόνες (.GIF και .JPG) κ.ά. είναι αρχεία δεδομένων και δεν μπορούν να κάνουν ζημιά εκτός από το πρόβλημα που αναφέρθηκε προηγουμένως με τις μακροεντολές στα έγγραφα του Word και του Excel. Ένα αρχείο που έχει επέκταση EXE, COM ή VBS είναι εκτελέσιμο και μπορεί να κάνει ό,τι ζημιά θελήσει στον υπολογιστή μας.

Τα περισσότερα e-mails που κυκλοφορούν στο Internet και "ενημερώνουν" τους χρήστες για την ύπαρξη ενός νέου ιού είναι ψεύτικα και περιέχουν ιούς. Αν το e-mail που λάβατε σας "ενημερώνει" για την ύπαρξη ενός νέου ιού και σας παροτρύνει να το στείλετε και σ' άλλους χρήστες τότε είναι βέβαιο ότι περιέχει ιό. Μπορείτε να δείτε βιβλιοθήκες με πληροφορίες για ιούς που υπάρχουν στο δίκτυο. Στις βιβλιοθήκες αυτές αναφέρονται και τα e-mail που είναι φάρσες (hoaxes).
Αν βάλετε μια μολυσμένη δισκέτα ή ένα μολυσμένο CD στα drives σας, δεν θα κολλήσετε τον ιό που περιέχει η δισκέτα ή το CD αλλά μόνο αν εκτελέσετε το μολυσμένο αρχείο. Εάν έχετε κάποιο antivirus στον υπολογιστή σας θα δείτε ότι κατευθείαν θα σας εμφανίσει μήνυμα ότι το CD ή η δισκέτα περιέχει κάποιον ιό. Αυτό βέβαια προϋποθέτει ότι το antivirus είναι ενημερωμένο (updated) και μπορεί να αναγνωρίσει τον ιό.
Αν έχετε κολλήσει κάποιον ιό, δεν είναι πάντα σίγουρο ότι θα προκαλέσει κάποια ζημιά. Όπως προανέφερα υπάρχουν ιοί που απλά αντιγράφονται μέσα στον υπολογιστή με αποτέλεσμα να βαραίνουν το σύστημα και να απασχολούν χώρο από την μνήμη του υπολογιστή. Ευτυχώς οι ιοί που κάνουν ζημιά στους υπολογιστές είναι λίγοι. Μπορεί να διαγράφουν αρχεία ή να εμφανίζουν διάφορα ενοχλητικά μηνύματα με αποτέλεσμα να βαραίνουν την RAM ή να προκαλούν διαρροή εγγράφων.
Χαρακτηριστικά Παραδείγματα Ιών Υπολογιστών. Ο πρώτος ιός υπολογιστών εμφανίσθηκε στα μέσα της δεκαετίας του 1980 και ήταν δημιούργημα δύο Πακιστανών ονόματι Basit και Amjad Alvi, οι οποίοι όταν ανακάλυψαν ότι το πρόγραμμα για υπολογιστή (λογισμικό) που είχαν δημιουργήσει αντιγραφόταν παράνομα από κάποιους άλλους, αποφάσισαν να δημιουργήσουν ένα μικρό προγραμματάκι το οποίο αντέγραφε τον εαυτό του και εμφάνιζε ένα προειδοποιητικό μήνυμα copyright σε κάθε παράνομο αντίγραφο που έκαναν οι πελάτες τους. Για την ιστορία, ο ιός έμεινε γνωστός με το όνομα Brain.
Γνωστοί ιοί υπολογιστών που άφησαν εποχή ήταν ο Melissa, ο Michelangelo (διέγραφε τον σκληρό δίσκο όταν η ημερομηνία του υπολογιστή έδειχνε 6 Μαρτίου), ο I Love You, ο Slammer, ο Chernobyl (διέγραφε το BIOS όταν η ημερομηνία του υπολογιστή έδειχνε 26 Απριλίου), ο Blaster, ο MyDoom, ο Jerk, ο Yankee, ο LoveLet-A, ο NightShade (κλείδωνε με κωδικό τα αρχεία που δουλεύουμε όταν η ημερομηνία του υπολογιστή έδειχνε Παρασκευή και 13) κ.ά.
Το 1988 ο φοιτητής Robert Morris δημιούργησε το πρώτο worm, που έφερε το όνομά του, και κατάφερε να μολύνει σχεδόν το 10% των συνδεδεμένων στο Internet υπολογιστών. Ο ιός Michelangelo έκανε την εμφάνισή του το 1992, ήταν ο πρώτος ιός που απέκτησε μεγάλη δημοσιότητα και ανάγκασε τις εταιρείες να δημιουργήσουν προγράμματα antivirus.
Το 2002 αμερικανικό δικαστήριο καταδίκασε σε φυλάκιση 20 μηνών τον David Smith, τον δημιουργό του ιού Melissa. Ήταν από τους πρώτους ιούς που μεταδιδόταν μέσω μηνυμάτων e-mail με τη μορφή ενός συνημμένου αρχείου Word και προξένησε ζημιές εκατομμυρίων δολαρίων. Ο ιός δημιουργήθηκε το έτος 1999. Αν ο χρήστης έκανε το λάθος να ανοίξει το επισυναπτόμενο αρχείο, ο ιός ενεργοποιείτο, αναπαρήγαγε τον εαυτό του και έστελνε ένα ανάλογο μήνυμα στους πρώτους 50 παραλήπτες που έβρισκε στο βιβλίο διευθύνσεων (address book) του θύματος. Η ποινή θεωρήθηκε ελαστική καθώς συνεκτιμήθηκε η προσφορά του δράστη στην ανίχνευση και τον εντοπισμό άλλων ιών.
Ο ιός I Love You εξαπλώθηκε ταχύτατα το έτος 2000 σ" όλον τον κόσμο και προκάλεσε μεγάλη αναστάτωση και κινητοποίηση. Ως δράστης συνελήφθη ένας 23χρονος από τις Φιλιππίνες, ο οποίος ισχυρίσθηκε ότι δεν δημιούργησε τον ιό αλλά ότι απλά τον βελτίωσε. Ο ιός αυτός έδειξε μια ιδιαίτερη προτίμηση σε αρχεία

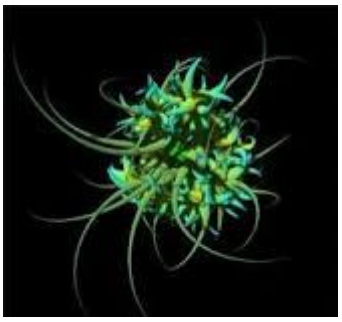
πολυμέσων τύπου .jpg, .mpeg και .mp3 και εκτιμάται ότι προκάλεσε ζημιές ύψους 8-10 δισ. δολαρίων σ" ολόκληρο τον κόσμο.
Ο Ολλανδός Jan De Witt σκέφθηκε ένα πολύ έξυπνο κόλπο το έτος 2001 για να μπορέσει να μολύνει τους υπολογιστές ανυποψίαστων χρηστών. Δημιούργησε έναν ιό με το όνομα της διάσημης Ρωσίδας τενίστριας Αννας Κουρνίκοβα και με δόλωμα ένα συνημμένο αρχείο που περιείχε δήθεν μια γυμνή φωτογραφία της, ο ιός εγκαθίστατο στον υπολογιστή του χρήστη με τις γνωστές συνέπειες. Ο Jan De Witt συνελήφθη και καταδικάστηκε σε 150 ώρες κοινωνικής εργασίας.
Ο ιός Bugbear άλλαξε κάπως τα δεδομένα στον χώρο του underground των υπολογιστών καθώς ήταν ένας από τους πρώτους που δεν έκανε φανερή ζημιά στους υπολογιστές που μόλυνε αλλά είχε ως αποστολή να κλέβει αριθμούς πιστωτικών καρτών και τραπεζικά δεδομένα, χωρίς να αφήνει ίχνη και να γίνεται έτσι αντιληπτός, και έστελνε μετά αυτές τις πληροφορίες στον δημιουργό του. Από σχετικές έρευνες που έγιναν προέκυψε ότι με τη βοήθεια αυτού του ιού υποκλάπησαν στοιχεία από 1.300 τράπεζες, οικονομικούς οργανισμούς και μεγάλες εταιρείες.

Ο Blaster θεωρείται από τους πιο καταστροφικούς ιούς καθώς έχει τη δυνατότητα να μπλοκάρει ολόκληρα δίκτυα υπολογιστών. Δημιουργήθηκε το έτος 2003. Το ίδιο έτος έκανε την εμφάνισή του και ο ιός Slammer, που μόλυνε δεκάδες χιλιάδες υπολογιστές και servers. Το 2003, επίσης, ο ιός Sobig μόλυνε ένα εκατομμύριο υπολογιστές και δημιούργησε προβλήματα δισεκατομμυρίων δολαρίων καθώς μπλόκαρε την κίνηση στο Διαδίκτυο, απενεργοποίησε δεκάδες servers και αναστάτωσε αεροπορικές και σιδηροδρομικές εταιρείες.
Ο ιός MyDoom (Η καταδίκη μου), που έμεινε γνωστός και ως Novarg, κατόρθωσε να μολύνει περισσότερα από 100 εκατομμύρια e-mail μέσα σε ελάχιστες ημέρες, στις αρχές του 2004. Μέσω ενός συνημμένου εγγράφου που εστέλνετο με e-mail και ενός προγράμματος ηλεκτρονικής ανταλλαγής αρχείων (peer-to-peer) κατάφερε να κερδίσει τον τίτλο ενός από τους πιο καταστροφικούς ιούς όλων των εποχών. Ο ιός αυτός δημιουργεί μια κερκόπορτα σε κάθε υπολογιστή που μολύνει και δίνει έτσι τη δυνατότητα σε επίδοξους hackers να αποκτούν πλήρη έλεγχο του μολυσμένου μηχανήματος.
Ένας 18χρονος Γερμανός ήταν ο δημιουργός των ιών Sasser και Netski, που κατάφερε το έτος 2004 και σε διάστημα μερικών εβδομάδων να μολύνει εκατομμύρια υπολογιστές σ' όλον τον κόσμο. Ο ιός προκαλούσε συνεχείς επανεκκινήσεις των μολυσμένων υπολογιστών.
Το 2004 έκανε την εμφάνισή του ένας ιός «νέας γενιάς», ο Scob, ο οποίος λειτουργούσε ύπουλα και σκοπός τους ήταν να συλλέγει αριθμούς πιστωτικών καρτών, απόρρητους κωδικούς και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές μέσω του Διαδικτύου. Ο ιός έστελνε μετά αυτά τα στοιχεία σε οργανωμένες συμμορίες στη Ρωσία, με στόχο ίσως την μεταπώλησή τους.
Ανάλογη δουλειά με τον ιό Scob έκανε και ο ιός Mimail, ο οποίος εμφάνιζε μια φόρμα καταχώρησης στοιχείων, όπως αριθμούς πιστωτικών καρτών, και στη συνέχεια έστελνε αυτά τα δεδομένα με e-mail σε κάποιους χρήστες στη Ρωσία.

Πρόσφατα, μεγάλη βρετανική εταιρεία που δραστηριοποιείται στα στοιχήματα μέσω του Διαδικτύου έπεσε θύμα εκβιασμού από σπείρα δημιουργίας ιών υπολογιστών, οι οποίοι της ζήτησαν να καταθέτει τακτικά ένα μεγάλο χρηματικό ποσό σ' έναν τραπεζικό λογαριασμό στην Λετονία, προκειμένου να μην γίνονται επιθέσεις ιών στους υπολογιστές της.

Τα Προγράμματα Spyware, Adware και Hijack.Όπως ήδη γνωρίζουμε, με τα cookies ένας δικτυακός τόπος μπορεί να εξάγει χρήσιμα στατιστικά συμπεράσματα σ' ό,τι έχει να κάνει μόνο με τις δικές του ιστοσελίδες. Ποια εταιρεία, όμως, δεν θα ήθελε να γνωρίζει ποιους δικτυακούς τόπους προτιμούν να επισκέπτονται οι χρήστες και τι ακριβώς βλέπουν; Οι πληροφορίες αυτές είναι πολύτιμες στις εταιρείες ώστε να μπορέσουν να προωθήσουν σωστά τα προϊόντα τους, να δημιουργήσουν καινούργια προϊόντα ή υπηρεσίες, να στήσουν ηλεκτρονικά καταστήματα (e-shops) κ.ά.

Προς τον σκοπό αυτό δημιουργήθηκαν διάφορα προγράμματα, τα αποκαλούμενα spyware, τα οποία εγκαθίστανται αυτόκλητα στον υπολογιστή μας, δηλ. χωρίς εμείς να έχουμε ζητήσει κάτι τέτοιο, και παρακολουθούν συνεχώς και αδιαλείπτως όλες τις κινήσεις και τις προτιμήσεις μας στο Internet, ενημερώνοντας κατάλληλα τους δημιουργούς τους. Η βασική αποστολή τους μ' άλλα λόγια είναι να μας κατασκοπεύουν, εν αγνοία μας φυσικά. Εκτός, όμως, από την κατασκοπεία μπορεί να εμφανίζουν διάφορα διαφημιστικά μηνύματα, συνήθως σε ανεξάρτητα παράθυρα, τα λεγόμενα pop-ups, όπου το περιεχόμενο της διαφήμισης προσαρμόζεται αυτόματα στις προτιμήσεις του χρήστη-καταναλωτή. Αυτά τα προγράμματα αποκαλούνται πιο συγκεκριμένα adware.



Τα προγράμματα spyware και adware εγκαθίστανται συνήθως μαζί μ' άλλα προγράμματα που προσφέρονται δωρεάν (freeware). Στην πράξη πάντως δεν υπάρχει σαφής διαχωρισμός μεταξύ των προγραμμάτων spyware και adware. Έτσι λοιπόν, ένα πρόγραμμα spyware μπορεί να εμφανίζει και διαφημιστικά μηνύματα, ενώ ένα πρόγραμμα adware μπορεί να παρακολουθεί τις κινήσεις μας και να στέλνει προσωπικά μας στοιχεία σε τρίτους. Συνήθως, τα προγράμματα αυτού του τύπου εξυπηρετούν διαφημιστικούς σκοπούς είτε από τις ίδιες τις ενδιαφερόμενες εταιρείες είτε από εταιρείες που εξυπηρετούν άλλες εταιρείες στις οποίες πωλούν τις πληροφορίες που συγκεντρώνουν.

Επειδή δεν μπορούμε να γνωρίζουμε αν τα προγράμματα αυτά απλά καταγράφουν τις κινήσεις μας στο Διαδίκτυο και αλιεύουν έτσι τις καταναλωτικές μας συνήθειες ή μεταδίδουν προσωπικά μας δεδομένα, όπως είναι οι αριθμοί τραπεζικών λογαριασμών και πιστωτικών καρτών, καλό θα ήταν να φροντίσουμε να απαλλαγούμε απ' αυτά. Η Αμερικανική Επιτροπή Ομοσπονδιακού Εμπορίου επενέβη και ζήτησε από το αρμόδιο δικαστήριο να εμποδίσει την πώληση του προγράμματος με το όνομα Spyware Assassin, το οποίο διαφημιζόταν σε banners ιστοσελίδων και εμφάνιζε απατηλές προειδοποιήσεις για δήθεν ύπαρξη προγραμμάτων spyware στον υπολογιστή του χρήστη.

Στην πραγματικότητα και τα προειδοποιητικά μηνύματα ήταν ψευδή και το πρόγραμμα ανίκανο να απαλλάξει τους χρήστες από κατασκοπευτικά προγράμματα spyware. Τελευταία έχουν κάνει την εμφάνισή τους και προγράμματα που αλλάζουν την αρχική σελίδα (Home Page) του φυλλομετρητή Internet Explorer ενός υπολογιστή, χωρίς φυσικά την συγκατάθεση του χρήστη. Τα προγράμματα αυτά είναι γνωστά με τον όρο Hijack και ο απώτερος στόχος τους είναι να κάνουν γνωστές συγκεκριμένες ιστοσελίδες ή να διαφημίσουν προϊόντα και υπηρεσίες.

Υπάρχει και το ενδεχόμενο με τις ενέργειές τους αυτές να αυξάνουν τον αριθμό των επισκέψεων συγκεκριμένων ιστοσελίδων, ούτως ώστε οι κάτοχοι των ιστοσελίδων αυτών να μπορούν να προσελκύσουν περισσότερες και καλύτερα αμειβόμενες διαφημίσεις.
Έλαβαν το όνομα hijack (αεροπειρατεία) καθώς εγκαθίστανται στον υπολογιστή μας χωρίς να τα πάρουμε είδηση και υποχρεώνουν το πρόγραμμα πλοήγησης που χρησιμοποιούμε να μεταβεί στις ιστοσελίδες που αυτά θέλουν. Τα προγράμματα hijack συνήθως δεν προκαλούν ζημιές, απλά είναι ενοχλητικές οι ενέργειές τους. Η απεγκατάστασή τους είναι συνήθως μια χρονοβόρα διαδικασία καθώς δημιουργούν πολλές φορές καταχωρήσεις και στο Μητρώο (Registry) των Windows.

Τρόποι αντιμετώπισης:

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη - ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νεοδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν.
Κάθε αντιϊκό έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο, τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα). Θα πρέπει να σημειωθεί ότι οι δημιουργοί ιών λαμβάνουν σοβαρά υπόψη τους τις μεθόδους εντοπισμού του "προϊόντος" τους και δημιουργούν ιούς, οι οποίοι προσπαθούν να αποφύγουν τον εντοπισμό, ακόμη και με απενεργοποίηση του αντιϊκού. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει τακτικότατα το λογισμικό του αλλά και να δημιουργεί τις ειδικές δισκέτες, που τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους, ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.

- ***Γενικές οδηγίες πρόληψης:***

Συχνή αλλαγή των κωδικών πρόσβασής σας σε κάθε email account, που χρησιμοποιείτε. Αποφυγή της διατήρησης ιστορικού και μνήμης στις ρυθμίσεις του browser σας (μετά την έξοδό σας από αυτόν). Τακτικός έλεγχος του συστήματός σας με εφαρμογές για τον εντοπισμό spyware, keyloggers κτλ. Μη γνωστοποιείτε τα στοιχεία πρόσβασης του email account σας σε τρίτους. Να θυμάστε ότι το ίδιο ισχύει και για τον κωδικό πρόσβασης της σύνδεσής σας, ο οποίος όσον αφορά την ηλεκτρονική σας διεύθυνση στο δίκτυο του ΟΤΕ είναι ίδιος.
Οι ενέργειες αυτές μπορούν να γίνουν είτε προληπτικά είτε εφόσον ήδη έχετε εντοπίσει τα συγκεκριμένα κακόβουλα προγράμματα στο σύστημά σας. Αναφέρονται συνοπτικά αλλά οι ειδικές παραπομπές είναι πολύ κατατοπιστικές για τις ενέργειες που πρέπει να γίνουν σε κάθε περίπτωση από εσάς ή τον τεχνικό σας.

Σχέδιο προστασίας.

Τρόποι Προστασίας από τους Ιούς:

Ο βασικός τρόπος προστασίας από τους ιούς των υπολογιστών είναι η εγκατάσταση, η σωστή ρύθμιση και η συνεχής ενημέρωση ή επικαιροποίηση (update) μέσω του Internet ενός έγκυρου προγράμματος προστασίας από ιούς, που είναι γνωστά με τον όρο Antivirus ή αντιικά προγράμματα. Υπάρχουν ακόμη ειδικά προγράμματα για προστασία από ιούς τύπου spyware, adware αλλά και από dialers και από τη μάστιγα των spam e-mails.

Η χρήση ενός ψηφιακού τείχους προστασίας (firewall), με τη μορφή software ή hardware, είναι χρήσιμη αλλά θα πρέπει να γίνεται με προσοχή και με την προϋπόθεση ότι υπάρχει καλή γνώση του τρόπου ρύθμισης και λειτουργίας του. Οι γενικοί κανόνες προστασίας είναι ότι θα πρέπει να προσέχουμε τι προγράμματα εκτελούμε στον υπολογιστή μας, τι αρχεία κατεβάζουμε από το Internet, ποιος μας στέλνει e-mail καθώς και ποιος έχει το δικαίωμα να χρησιμοποιήσει τον υπολογιστή μας όταν εμείς απουσιάζουμε. Προσοχή πρέπει να δίνουμε και στα προγράμματα που διαφημίζονται και διανέμονται δωρεάν καθώς και στα προγράμματα που χρησιμοποιούμε για να κάνουμε chat.
Μια πολύ καλή λύση είναι να εγκαταστήσουμε και να εκτελέσουμε μια από τις εφαρμογές που αναλαμβάνουν να ανιχνεύσουν στο σύστημά μας τα τυχόν υπάρχοντα ευαίσθητα σημεία (vulnerabilities) και να μας τα παρουσιάσουν με παραστατικό τρόπο. Τέλος, μια πολύ καλή συμβουλή είναι να λαμβάνουμε πολύ τακτικά, ίσως και καθημερινά, εφεδρικά αντίγραφα ασφαλείας των αρχείων μας, σε CD, σε DVD ή σε εξωτερικό σκληρό δίσκο, μια διαδικασία που είναι γνωστή με τον όρο back-up, έτσι ώστε ακόμα και στην ακραία περίπτωση που χάσουμε σημαντικά αρχεία από την επίθεση κάποιου ιού, να μπορέσουμε να τα ανακτήσουμε άμεσα.
Από τα πιο γνωστά αντιικά προγράμματα είναι το Norton Antivirus της εταιρείας Symantec, το McAfee της εταιρείας Network Associates, το Kaspersky, το Panda, το Sophos, το F-Prot της εταιρείας Frisk, το F-Secure καθώς και το AntiVir και το AVG της εταιρείας Grisoft που διατίθενται δωρεάν για προσωπική χρήση. Όλα έχουν τη δυνατότητα αυτόματης ενημέρωσης (update) μέσω του Internet.

Απλές Οδηγίες Προστασίας από τους Ιούς:

- Μπορείτε να προστατευθείτε από τους ιούς με μερικά απλά βήματα :

Αν ανησυχείτε πολύ για τους παραδοσιακούς ιούς, θα πρέπει να δουλεύετε μ' ένα πιο ασφαλές λειτουργικό σύστημα όπως είναι το UNIX ή το Linux.
Αν χρησιμοποιείτε ένα μη ασφαλές λειτουργικό σύστημα, τότε θα πρέπει να προμηθευθείτε ειδικό λογισμικό προστασίας από ιούς.
Θα πρέπει να βεβαιωθείτε ότι είναι ενεργό το Macro Virus Protection σ' όλες τις εφαρμογές της Microsoft και ΠΟΤΕ δεν θα πρέπει να εκτελείτε μακροεντολές (macros) σ' ένα έγγραφο εκτός κι αν είστε σίγουροι για το τι ακριβώς κάνουν.
Δεν θα πρέπει ποτέ να κάνετε διπλό κλικ σ' ένα συνημμένο που περιέχει ένα εκτελέσιμο αρχείο που έχει φθάσει μέσω e-mail. Τα συνημμένα που έρχονται ως αρχεία του Word (.DOC), ως φύλλα εργασίας (.XLS), ως εικόνες (.GIF και .JPG) κ.ά. είναι αρχεία δεδομένων και δεν μπορούν να κάνουν ζημιά εκτός από το πρόβλημα που αναφέρθηκε προηγουμένως με τις μακροεντολές στα έγγραφα του Word και του Excel. Ένα αρχείο που έχει επέκταση EXE, COM ή VBS είναι εκτελέσιμο και μπορεί να κάνει ό,τι ζημιά θελήσει στον υπολογιστή μας.

Διαδικασία λήψης αντιγράφων ασφαλείας.

Τι είναι το αντίγραφο ασφαλείας:

Το αντίγραφο ασφαλείας ενός αρχείου είναι ένα αντίγραφο του αρχείου που αποθηκεύεται σε διαφορετική θέση από το πρωτότυπο. Εάν θέλετε να παρακολουθείτε τις αλλαγές σε ένα αρχείο τότε μπορείτε να έχετε πολλά αντίγραφα ασφαλείας αυτού του αρχείου.

Γιατί πρέπει να δημιουργώ αντίγραφα ασφαλείας;

Ο σκοπός της δημιουργίας αντιγράφων ασφαλείας για να βεβαιωθείτε ότι τα ψηφιακά δεδομένα σας μπορεί να επιβιώσει οποιοδήποτε από τους κινδύνους που περιμένουν. Κατ 'αρχήν, αυτή είναι μια απλή διαδικασία. Αντιγράψτε όλα τα αρχεία σας σε κάποιο άλλο (-α), να κρατήσει το αντίγραφο ασφαλείας σε ασφαλές μέρος, και να το χρησιμοποιήσετε για να επαναφέρετε τα δεδομένα σε περίπτωση προβλήματος. Αν είστε ένα υπολογιστή του χρήστη και όλα όσα θέλετε να διατηρήσετε μπορούν να χωρέσουν σε ένα σκληρό δίσκο, μπορεί να είναι σχεδόν τόσο απλό όσο αυτό.
Για πολλούς από τους αναγνώστες, όμως, τα πράγματα δεν είναι τόσο απλά. Οι εικόνες και τα βίντεο που θέλετε να δημιουργήσετε αντίγραφα ασφαλείας δεν μπορεί να είναι σε έναν υπολογιστή, πολύ λιγότερο σε έναν σκληρό δίσκο. Πιθανόν να έχετε πολλαπλές εκδόσεις των εικόνων. Για τα έργα βίντεο που έχετε πιθανώς πολλές πρόσθετα αρχεία έργου και τα περιουσιακά στοιχεία (όπως γραφικά και μουσική). Ποια αυτά κρατάς και πώς θα κρατήσει ότι ευθεία; Πώς μπορείτε να ενημερώσετε αντίγραφα ασφαλείας καθώς εργάζεστε σε αρχεία; Πώς μπορείτε να επικυρώνουν τα αντίγραφα ασφαλείας, έτσι ώστε να μπορούν να έχουν τη βεβαιότητα ότι το αρχείο μπορεί να αποκατασταθεί σωστά σε περίπτωση προβλήματος; Ας περιγράψει τα εργαλεία που χρησιμοποιούνται στην δημιουργία αντιγράφων ασφαλείας για να δούμε πώς μπορούμε να βάλουμε όλα μαζί με ασφάλεια και αποτελεσματικά.

Για ποια αρχεία πρέπει να δημιουργώ αντίγραφα ασφαλείας;

Πρέπει να δημιουργείτε αντίγραφα ασφαλείας για οποιοδήποτε αρχείο είναι δύσκολη ή αδύνατη η αντικατάστασή του, ενώ θα πρέπει να δημιουργείτε αντίγραφα ασφαλείας για τα αρχεία που αλλάζετε συχνά. Εικόνες, βίντεο, μουσική, έργα και οικονομικά στοιχεία είναι μερικά παραδείγματα αρχείων για τα οποία πρέπει να δημιουργείτε αντίγραφα ασφαλείας. Δεν χρειάζεται να δημιουργείτε αντίγραφα ασφαλείας για προγράμματα διότι μπορείτε να χρησιμοποιήσετε τους δίσκους των αρχικών προϊόντων για να κάνετε επανεγκατάστασή τους, ενώ παράλληλα τα προγράμματα καταλαμβάνουν πολύ χώρο στο δίσκο.

Πόσο συχνά πρέπει να δημιουργώ αντίγραφα ασφαλείας;

Εξαρτάται από τον αριθμό των αρχείων που δημιουργείτε και τη συχνότητα δημιουργίας τους. Εάν δημιουργείτε νέα αρχεία κάθε μέρα, τότε ίσως πρέπει να δημιουργείτε αντίγραφα ασφαλείας κάθε εβδομάδα ή και κάθε μέρα. Εάν δημιουργείτε πολλά αρχεία περιστασιακά, για παράδειγμα, όταν αποθηκεύετε πολλές ψηφιακές φωτογραφίες από ένα πάρτι γενεθλίων ή μια αποφοίτηση, τότε δημιουργήστε τα αντίγραφα ασφαλείας αμέσως. Καλύτερα είναι να προγραμματίσετε τακτική, αυτόματη δημιουργία αντιγράφων ασφαλείας έτσι ώστε να μην χρειάζεται καν να το σκεφτείτε. Μπορείτε να επιλέξετε την καθημερινή, εβδομαδιαία ή μηνιαία δημιουργία αντιγράφων ασφαλείας. Μπορείτε επίσης να δημιουργείτε αντίγραφα ασφαλείας με μη αυτόματο τρόπο, μεταξύ των αυτόματων αντιγράφων ασφαλείας.

- ***Σημείωση***
  - Η δυνατότητα ρύθμισης αυτόματης δημιουργίας αντιγράφων ασφαλείας δεν περιλαμβάνεται στα Windows Vista Home Basic. Ωστόσο, τα Windows θα σας θυμίζουν κατά περιόδους να δημιουργείτε αντίγραφα ασφαλείας.

Ποιοι τύποι αρχείων δεν περιλαμβάνονται στη δημιουργία αντιγράφων ασφαλείας;

Ο Οδηγός δημιουργίας αντιγράφων ασφαλείας αντιγράφει τους περισσότερους συνηθισμένους τύπους αρχείων. Δεν περιλαμβάνονται τα παρακάτω αρχεία:

- Αρχεία που έχουν κρυπτογραφηθεί με χρήση του συστήματος αρχείων κρυπτογράφησης (EFS)
- Αρχεία συστήματος (τα αρχεία που χρειάζονται τα Windows για την εκτέλεσή τους)
- Αρχεία προγραμμάτων
- Αρχεία που έχουν αποθηκευτεί σε σκληρούς δίσκους με διαμόρφωση συστήματος αρχείων FAT
- Ηλεκτρονικό ταχυδρομείο με βάση το Web που δεν είναι αποθηκευμένο στο σκληρό σας δίσκο
- Αρχεία που βρίσκονται στον Κάδο Ανακύκλωσης
- Προσωρινά αρχεία
- Ρυθμίσεις προφίλ χρήστη

- ***Σημείωση***

Αν εκτελείτε το Windows Vista Service Pack 1, τα κρυπτογραφημένα αρχεία EFS περιλαμβάνονται στα αντίγραφα ασφαλείας. Το σύστημα EFS δεν περιλαμβάνεται στα Windows Vista Starter, τα Windows Vista Home Basic και τα Windows Vista Home Premium.

Πόσο αποθηκευτικό χώρο χρειάζομαι για τα αντίγραφα ασφαλείας;

Αυτό εξαρτάται από το μέγεθος των αρχείων για τα οποία δημιουργείτε αντίγραφα ασφαλείας. Τα Windows παρακολουθούν τα αρχεία που έχουν προστεθεί ή τροποποιηθεί από την τελευταία δημιουργία αντιγράφων ασφαλείας έτσι, ώστε το μόνο που χρειάζεται είναι να κάνετε ενημέρωση των υπαρχόντων αντιγράφων ασφαλείας, γεγονός που εξοικονομεί χώρο στο δίσκο.

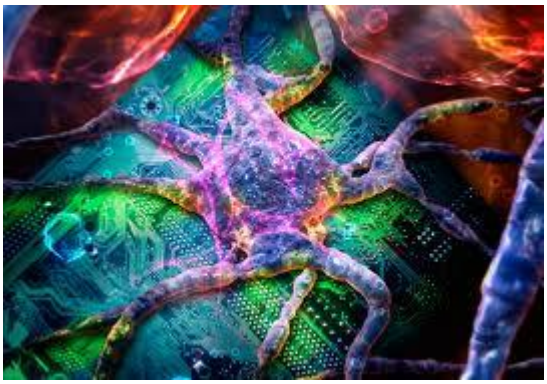
Όταν επιλέγετε μια θέση για να αποθηκεύσετε τα αντίγραφα ασφαλείας, ο οδηγός κάνει αναζήτηση στον υπολογιστή σας και εμφανίζει όλες τις θέσεις όπου μπορείτε να κάνετε αποθήκευση. Εάν η θέση που θέλετε δεν εμφανίζεται στη λίστα, τότε ενδέχεται να υπάρχει ένα από τα εξής προβλήματα:

Η θέση είναι μια μονάδα μαγνητοταινίας. Δεν μπορείτε να αποθηκεύσετε αντίγραφα ασφαλείας σε μαγνητοταινίες.

Η θέση είναι ο ίδιος ο δίσκος για τον οποίο θέλετε να δημιουργήσετε αντίγραφο ασφαλείας. Δεν μπορείτε να δημιουργήσετε αντίγραφο ασφαλείας ενός δίσκου μέσα στον ίδιο δίσκο. Για παράδειγμα, δεν μπορείτε να δημιουργήσετε αντίγραφα ασφαλείας του περιεχομένου της μονάδας δίσκου E στο δίσκο E.

Η θέση είναι μια μονάδα CD-ROM. Δεν μπορείτε να χρησιμοποιήσετε μια μονάδα CD-ROM για να δημιουργήσετε αντίγραφα ασφαλείας. Θα πρέπει να χρησιμοποιήσετε συσκευή εγγραφής CD, γνωστή και ως μονάδα CD-R ή CD-RW.

Η θέση είναι μια μονάδα flash USB. Δεν μπορείτε να αποθηκεύσετε αντίγραφα ασφαλείας σε μια μονάδα flash.



Η θέση δεν είναι μορφοποιημένη ως NTFS, FAT, ή Universal Disk Format (UDF) (καλείται επίσης Live File System). Τα αντίγραφα ασφαλείας μπορούν να αποθηκευτούν μόνο σε δίσκους που έχουν μορφοποιηθεί χρησιμοποιώντας τα συστήματα αρχείων NTFS, FAT ή UDF. Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα Σύγκριση συστημάτων αρχείων NTFS και FAT.

Η θέση είναι είτε ο δίσκος του συστήματος (ο δίσκος όπου έχουν εγκατασταθεί τα Windows, γνωστός και ως μονάδα δίσκου C), είτε η δισκέτα εκκίνησης (ο δίσκος που χρησιμοποιούν τα Windows για την εκκίνηση του υπολογιστή σας, γνωστός και ως δίσκος εκκίνησης).

Η θέση είναι ένα κοινόχρηστο στοιχείο δικτύου σε έναν υπολογιστή που εκτελεί τα Windows XP Home Edition. Δεν μπορείτε να αποθηκεύσετε εφεδρικά αντίγραφα σε αυτά τα κοινόχρηστα στοιχεία επειδή η ρύθμιση αδειών σε κοινόχρηστα στοιχεία δικτύου και ο έλεγχος ταυτότητας μέσω δικτύου δεν υποστηρίζονται από τα Windows XP Home Edition.

Μπορώ να δημιουργήσω αντίγραφα ασφαλείας σε CD ή σε DVD εάν δεν είμαι εκεί για να τοποθετήσω το δίσκο. Τα αντίγραφα ασφαλείας χωράνε σε ένα δίσκο και ο δίσκος βρίσκεται ήδη μέσα στον υπολογιστή κατά την έναρξη της δημιουργίας των

αντιγράφων ασφαλείας. Διαφορετικά, προγραμματίστε τη δημιουργία αντιγράφων ασφαλείας για κάποια στιγμή που θα μπορείτε να τοποθετήσετε τους δίσκους. Τα Windows θα σας ειδοποιήσουν αργότερα ότι η δημιουργία αντιγράφων ασφαλείας δεν ολοκληρώθηκε και τότε θα μπορείτε να τοποθετήσετε το δίσκο για να συνεχίσετε τη δημιουργία αντιγράφων ασφαλείας.
Εάν σας τελειώσουν οι δίσκοι κατά τη δημιουργία αντιγράφων ασφαλείας, τότε μπορείτε να ολοκληρώσετε τη διαδικασία αργότερα.
Επιπλέον τα αντίγραφα ασφαλείας δημιουργούνται για την τελευταία αποθηκευμένη έκδοση του κάθε αρχείου. Επομένως, για τα αρχεία που αλλάξατε κατά τη δημιουργία αντιγράφων ασφαλείας πρέπει να δημιουργήσετε αντίγραφα ασφαλείας την επόμενη φορά. Μπορείτε να προγραμματίσετε την αυτόματη δημιουργία αντιγράφων ασφαλείας κατά τη διάρκεια της νύχτας ή όταν δεν εργάζεστε στα αρχεία. Κατά την εξέλιξη της δημιουργίας αντιγράφων ασφαλείας μπορείτε να κάνετε διάφορες εργασίες, όπως ανάγνωση ηλεκτρονικού ταχυδρομείου ή χρήση του Internet.
Δεν είναι δυνατόν να ληφθούν αντίγραφα από ένα δίσκο που έχει χαθεί. Ωστόσο, μπορείτε να επαναφέρετε τα αρχεία από τους δίσκους που δημιουργήσατε πριν από αυτούς που χάσατε. Εάν δεν γνωρίζετε ακριβώς τι υπήρχε στους δίσκους που χάθηκαν, τότε μπορείτε να δείτε τη λίστα με τα αρχεία για τα οποία δημιουργήσατε αντίγραφα ασφαλείας. Εάν εκτελείτε τα Windows Vista Business, τα Windows Vista Enterprise ή τα Windows Vista Ultimate, τότε μπορείτε να χρησιμοποιήσετε σκιώδη αντίγραφα για να ανακτήσετε προηγούμενες εκδόσεις των αρχείων κατευθείαν από το σκληρό δίσκο και όχι από τα αντίγραφα ασφαλείας.

Ο τρόπος για προβολή μιας λίστας με τα αρχεία για τα οποία έχετε δημιουργήσει αντίγραφα ασφαλείας γίνεται ως εξής:

1. Ανοίξτε το Κέντρο αντιγράφων ασφαλείας και επαναφοράς κάνοντας κλικ στο κουμπί Έναρξη και στις επιλογές Πίνακας Ελέγχου, Σύστημα και συντήρηση και Κέντρο αντιγράφων ασφαλείας και επαναφοράς.
2. Κάντε κλικ στο κουμπί Επαναφορά αρχείων.

Μπορείτε να περιηγηθείτε ή να πραγματοποιήσετε αναζήτηση στα περιεχόμενα των αντιγράφων ασφαλείας.

Η διαφορά χρησιμοποίησης του οδηγού δημιουργίας αντιγράφων ασφαλείας μεταξύ δημιουργίας αντίγραφων ασφαλείας μόνος μου.

Εάν κάνετε εγγραφή των αντιγράφων των αρχείων σας σε δίσκο CD ή DVD ή αποθηκεύετε ένα αντίγραφο σε εξωτερικό σκληρό δίσκο, τότε κάθε φορά που θέλετε να δημιουργήσετε ένα αντίγραφο ασφαλείας θα πρέπει να επιλέξετε με μη αυτόματο τρόπο το κάθε αρχείο και φάκελο που θέλετε. Επίσης θα πρέπει να θυμάστε να δημιουργείτε αντίγραφα ασφαλείας των νέων ή τροποποιημένων αρχείων και φακέλων. Κάτι τέτοιο ενδέχεται να είναι χρονοβόρο και κοπιαστικό. Όταν χρησιμοποιείτε τον Οδηγό δημιουργίας αντιγράφων ασφαλείας, τα Windows παρακολουθούν τα νέα ή τροποποιημένα αρχεία και φακέλους. Στη συνέχεια, όταν δημιουργείτε νέα αντίγραφα ασφαλείας, μπορείτε να επιλέξετε όλα τα δεδομένα στον υπολογιστή σας ή μόνο τα αρχεία που έχουν αλλάξει μετά την τελευταία δημιουργία αντιγράφων ασφαλείας. Εάν επιλέξετε την αυτόματη δημιουργία αντιγράφων ασφαλείας, τότε τα Windows θα δημιουργούν τακτικά αντίγραφα ασφαλείας των αρχείων και των φακέλων σας έτσι ώστε να μην χρειάζεται να το θυμάστε εσείς.

Οταν ο υπολογιστής σας είναι απενεργοποιημένος κατά την προγραμματισμένη δημιουργία αντιγράφων ασφαλείας, τότε δεν θα εκτελεστεί η αυτόματη δημιουργία αντιγράφων ασφαλείας. Ωστόσο, την επόμενη φορά που θα ανοίξετε τον υπολογιστή σας, θα μπορείτε να δημιουργήσετε αντίγραφα ασφαλείας των αρχείων σας και να επαναφέρετε το κανονικό πρόγραμμα δημιουργίας αντιγράφων ασφαλείας.

Η διαγραφή ενός αντιγράφου ασφαλείας.

Εάν τα αντίγραφα ασφαλείας είναι αποθηκευμένα σε δίσκους CD ή DVD, τότε μπορείτε να απορρίψετε τους δίσκους που περιέχουν παλαιότερα αντίγραφα ασφαλείας. Φροντίστε όμως να κρατήσετε αυτούς που περιέχουν τα πιο πρόσφατα αντίγραφα ασφαλείας. Εάν τα αντίγραφα ασφαλείας είναι αποθηκευμένα σε έναν εξωτερικό ή εσωτερικό σκληρό δίσκο, τότε μπορείτε να διαγράψετε ένα αντίγραφο ασφαλείας ακολουθώντας τα εξής βήματα:

1. Ανοίξτε τη θέση όπου αποθηκεύτηκε το αντίγραφο ασφαλείας.

Για παράδειγμα, εάν τα αντίγραφα ασφαλείας βρίσκονται στον εξωτερικό σκληρό δίσκο με την ετικέτα "E," τότε συνδέστε τον εξωτερικό σκληρό δίσκο στον υπολογιστή σας και κατόπιν ανοίξτε τη μονάδα E.

2. Κάντε δεξιό κλικ στο φάκελο που περιέχει το αντίγραφο ασφαλείας που θέλετε να διαγράψετε και μετά κάντε κλικ στο κουμπί Διαγραφή.

- ***Σημειώσεις***

Τα αντίγραφα ασφαλείας αποθηκεύονται στην εξής μορφή: <θέση αντιγράφων ασφαλείας>\<όνομα υπολογιστή>\Backup Set <έτος-μήνας-ημέρα> <ώρα>. Για παράδειγμα, εάν το όνομα του υπολογιστή σας είναι Υπολογιστής, η θέση των αντιγράφων ασφαλείας είναι η E και δημιουργήσατε τα αντίγραφα στις 2 Απριλίου 2006, στις 16:32:00, τότε το αντίγραφο ασφαλείας θα βρίσκεται στη θέση E:\Υπολογιστής\Backup Set 2006-02-04 163200. Για να διαγράψετε αυτό το αντίγραφο ασφαλείας πρέπει να κάνετε δεξιό κλικ στο φάκελο με το όνομα Backup Set 2006-02-04 163200.

Εάν κάνετε πλήρη δημιουργία αντιγράφων ασφαλείας, τότε δημιουργείται ένα φάκελος και ονομάζεται σύμφωνα με την ημερομηνία εκείνης της ημέρας. Όταν θα προσθέτετε ενημερωμένες εκδόσεις, η ημερομηνία θα παραμένει η ίδια, θα γίνεται όμως ενημέρωση των αντιγράφων ασφαλείας σας. Την επόμενη φορά που θα κάνετε πλήρη δημιουργία αντιγράφων ασφαλείας, θα δημιουργηθεί ένας νέος φάκελος αντιγράφων ασφαλείας και θα ονομαστεί με την ημερομηνία εκείνης της ημέρας. Στη συνέχεια, οι τυχόν ενημερωμένες εκδόσεις θα προστίθενται σε αυτόν το νέο φάκελο. Δεν πρέπει να διαγράψετε τον τρέχοντα φάκελο αντιγράφων ασφαλείας.

Δημιουργία αντιγράφου ασφαλείας.

Για να δημιουργήσετε αντίγραφα ασφάλειας των αρχείων σας
Βήμα 1:
Ξεκινήστε το Βοηθητικό πρόγραμμα δημιουργίας αντιγράφων ασφαλείας
Κάντε κλικ στο κουμπί Έναρξη και στη συνέχεια κάντε κλικ στην επιλογή Εκτέλεση. Πληκτρολογήστε ntbackup.exe στο πλαίσιο Άνοιγμα και έπειτα κάντε κλικ στο OK.
Βήμα 2:
Επιλέξτε στοιχεία για δημιουργία αντιγράφων ασφάλειας αυτών και επιλέξτε την τοποθεσία για αυτά τα αντίγραφα ασφάλειας.

- ***Σημείωση*** Εάν ξεκινήσει ο Οδηγός δημιουργίας αντιγράφων ασφάλειας και επαναφοράς, το βοηθητικό πρόγραμμα εκτελείται σε λειτουργία Οδηγού. Μπορείτε να κάνετε κλικ για να καταργήσετε την επιλογή του πλαισίου ελέγχου Πάντα εκκίνηση με λειτουργία οδηγού και έπειτα επανεκκινήστε το Βοηθητικό πρόγραμμα δημιουργίας αντιγράφων ασφάλειας. Εάν συνεχίσετε τη χρήση του Οδηγού δημιουργίας αντιγράφων ασφάλειας και επαναφοράς, τα βήματα θα είναι λίγο διαφορετικά

Κάντε κλικ στην καρτέλα Αντίγραφα ασφαλείας. εκείνων που αναφέρονται στην παρακάτω ενότητα. Για να δημιουργήσετε αντίγραφα ασφάλειας των αρχείων σας
Βήμα 1: Ξεκινήστε το Βοηθητικό πρόγραμμα δημιουργίας αντιγράφων ασφαλείας Κάντε κλικ στο κουμπί Έναρξη και στη συνέχεια κάντε κλικ στην επιλογή Εκτέλεση. Πληκτρολογήστε ntbackup.exe στο πλαίσιο Άνοιγμα και έπειτα κάντε κλικ στο OK. Βήμα 2: Επιλέξτε στοιχεία για δημιουργία αντιγράφων ασφάλειας αυτών και επιλέξτε την τοποθεσία για αυτά τα αντίγραφα ασφάλειας:

1. Κάντε κλικ στην επιλογή Λειτουργία για προχωρημένους.

   - ***Σημείωση*** Εάν ξεκινήσει ο Οδηγός δημιουργίας αντιγράφων ασφάλειας και επαναφοράς, το βοηθητικό πρόγραμμα εκτελείται σε λειτουργία Οδηγού. Μπορείτε να κάνετε κλικ για να καταργήσετε την επιλογή του πλαισίου ελέγχου Πάντα εκκίνηση με λειτουργία οδηγού και έπειτα επανεκκινήστε το Βοηθητικό πρόγραμμα δημιουργίας αντιγράφων ασφάλειας. Εάν συνεχίσετε τη χρήση του Οδηγού δημιουργίας αντιγράφων ασφάλειας και επαναφοράς, τα βήματα θα είναι λίγο διαφορετικά εκείνων που αναφέρονται στην παρακάτω ενότητα.

2. Κάντε κλικ στην καρτέλα Αντίγραφα ασφαλείας.

3. Στο μενού Εργασία, κάντε κλικ στην επιλογή Νέα.

4. Επιλέξτε τα πλαίσια ελέγχου δίπλα στις μονάδες δίσκου για τις οποίες θέλετε να δημιουργήσετε αντίγραφα ασφάλειας. Εάν επιλέξετε συγκεκριμένα αρχεία ή φακέλους, αναπτύξτε το στοιχείο μονάδας δίσκου όπου βρίσκονται αυτά τα αρχεία ή φάκελοι. Έπειτα, επιλέξτε τα πλαίσια ελέγχου για τα αρχεία ή τους φακέλους για τα οποία επιθυμείτε να δημιουργήσετε αντίγραφα ασφάλειας.

5. Επιλέξτε το πλαίσιο ελέγχου Κατάσταση συστήματος που βρίσκεται στην περιοχή Ο Υπολογιστής μου στο παράθυρο πλοήγησης.

- ***Σημείωση*** Εάν επιθυμείτε να δημιουργήσετε αντίγραφα ασφάλειας των ρυθμίσεων συστήματος και αρχείων δεδομένων, δημιουργήστε αντίγραφα ασφάλειας όλων των δεδομένων στον υπολογιστή σας και των δεδομένων Κατάστασης συστήματος. Τα δεδομένα Κατάστασης συστήματος περιλαμβάνουν το μητρώο, τη βάση δεδομένων καταχώρησης κλάσης COM+, αρχεία που βρίσκονται στην περιοχή Προστασία αρχείων των Windows, αρχεία εκκίνησης και άλλα αρχεία συστήματος.

6. Εάν ο Προορισμός αντιγράφων ασφάλειας είναι διαθέσιμος, κάντε κλικ στον προορισμό αντιγράφων ασφάλειας που επιθυμείτε να χρησιμοποιήσετε.

- ***Σημείωση*** Εάν επιλέξατε Αρχείο σε αυτό το βήμα, πληκτρολογήστε την πλήρη διαδρομή και το όνομα αρχείου για το οποίο επιθυμείτε να δημιουργήσετε αντίγραφα ασφάλειας δεδομένων στο πλαίσιο Μέσο αποθήκευσης αντιγράφων ασφάλειας ή ονόματος αρχείου. Μπορείτε να καθορίσετε μια κοινόχρηστη θέση δικτύου, ως προορισμό για το αρχείο αντιγράφου ασφαλείας. Συνήθως, τα αντίγραφα ασφάλειας αρχείων φέρουν επέκταση ονόματος αρχείου .bkf. Ωστόσο, μπορείτε να χρησιμοποιήσετε οποιαδήποτε επέκταση ονόματος αρχείου που θέλετε.

Βήμα 3: Ξεκινήστε τη δημιουργία αντιγράφων ασφάλειας

1. Κάντε κλικ στην επιλογή Έναρξη δημιουργίας αντιγράφων ασφάλειας για να ανοίξετε το παράθυρο διαλόγου Πληροφορίες για την εργασία δημιουργίας αντιγράφων ασφάλειας.

2. Στην περιοχή Εάν στο μέσο περιέχονται ήδη αντίγραφα ασφάλειας, πραγματοποιήστε οποιοδήποτε από τα εξής:

Εάν θέλετε να προσαρτήσετε αυτό το αρχείο αντιγράφου ασφαλείας σε προηγούμενα αρχεία αντιγράφων ασφαλείας, κάντε κλικ στο κουμπί Προσάρτηση αυτού του αντιγράφου ασφαλείας στο μέσο. Αυτή η επιλογή προσθέτει το νέο αντίγραφο ασφάλειας στο υπάρχον αντίγραφο ασφάλειας ώστε να μπορείτε να διατηρήσετε όλα τα προηγούμενα αντίγραφα ασφάλειας σε ένα αρχείο. Αυτή η επιλογή είναι χρήσιμη εάν επιθυμείτε να επαναφέρετε ένα αντίγραφο ασφάλειας από μια συγκεκριμένη ημέρα. Να γνωρίζετε πως το μέγεθος του αντίγραφου ασφάλειας θα μεγαλώνει με κάθε νέο αντίγραφο ασφάλειας. Μπορεί να επιθυμείτε να παρακολουθήσετε το μέγεθος αρχείου για να βεβαιωθείτε πως δεν θα γεμίσει εν τέλει το σκληρό δίσκο σας. Εάν το αρχείο γίνει πολύ μεγάλο, μπορεί να εξετάσετε την αποθήκευση του αρχείου σε εξωτερικό σκληρό δίσκο. Διαφορετικά, εάν σας απασχολεί εάν το αρχείο χρησιμοποιεί μεγάλη ποσότητα από το χώρο του σκληρού δίσκου, επιλέξτε Αντικατάστασή τους στο μέσο με αυτό το αντίγραφο. Εάν θέλετε να αντικαταστήσετε προηγούμενα αρχεία αντιγράφων ασφαλείας με αυτό το αρχείο αντιγράφου ασφαλείας, κάντε κλικ στο στοιχείο Αντικατάσταση των δεδομένων του μέσου με αυτό το αντίγραφο ασφαλείας. Αυτή η επιλογή είναι χρήσιμη εάν επιθυμείτε μόνο να διατηρείτε το τρέχον αντίγραφο ασφάλειας και δεν σας απασχολεί η διατήρηση των προηγούμενων αντιγράφων ασφάλειας. Διαφορετικά, χρησιμοποιήστε αυτήν την επιλογή εάν σας απασχολεί εάν το αρχείο χρησιμοποιεί μεγάλη ποσότητα του σκληρού δίσκου στον υπολογιστή σας.

3. Κάντε κλικ στο κουμπί Για προχωρημένους.

4. Επιλέξτε το πλαίσιο ελέγχου Επαλήθευση δεδομένων μετά τη δημιουργία αντιγράφων.

5. Στο πλαίσιο Τύπος αντιγράφων ασφάλειας, κάντε κλικ στο είδος αντιγράφου ασφάλειας που επιθυμείτε να δημιουργήσετε. Για μια περιγραφή κάθε τύπου αντιγράφου ασφάλειας, κάντε κλικ στον τύπο αντιγράφου ασφάλειας και η περιγραφή εμφανίζεται στην περιοχή "Περιγραφή." Έχετε τη δυνατότητα να επιλέξετε οποιονδήποτε από τους ακόλουθους τύπους αντιγράφων ασφαλείας:

- Κανονική
- Αντιγραφή
- Επαυξητικός
- Διαφορικός
- Καθημερινά

6. Κάντε κλικ στο κουμπί OK και έπειτα κάντε κλικ στην επιλογή Έναρξη δημιουργίας αντιγράφων ασφάλειας. Εμφανίζεται ένα παράθυρο διαλόγου Πρόοδος δημιουργίας αντιγράφων ασφάλειας και η δημιουργία αντιγράφων ασφάλειας ξεκινά.

Βήμα 4*:* Έξοδος από το βοηθητικό πρόγραμμα δημιουργίας αντιγράφων ασφαλείας

1. Μόλις ολοκληρωθεί η διαδικασία δημιουργίας αντιγράφων ασφαλείας, κάντε κλικ στο κουμπί Κλείσιμο.

2. Στο μενού Εργασία, κάντε κλικ στην επιλογή Έξοδος.
3. Στο μενού Εργασία, κάντε κλικ στην επιλογή Νέα.
4. Επιλέξτε τα πλαίσια ελέγχου δίπλα στις μονάδες δίσκου για τις οποίες θέλετε να δημιουργήσετε αντίγραφα ασφάλειας. Εάν επιλέξετε συγκεκριμένα αρχεία ή φακέλους, αναπτύξτε το στοιχείο μονάδας δίσκου όπου βρίσκονται αυτά τα αρχεία ή φάκελοι. Έπειτα, επιλέξτε τα πλαίσια ελέγχου για τα αρχεία ή τους φακέλους για τα οποία επιθυμείτε να δημιουργήσετε αντίγραφα ασφάλειας.
Επιλέξτε το πλαίσιο ελέγχου Κατάσταση συστήματος που βρίσκεται στην περιοχή Ο Υπολογιστής μου στο παράθυρο πλοήγησης.

- ***Σημείωση*** Εάν επιθυμείτε να δημιουργήσετε αντίγραφα ασφάλειας των ρυθμίσεων συστήματος και αρχείων δεδομένων, δημιουργήστε αντίγραφα ασφάλειας όλων των δεδομένων στον υπολογιστή σας και των δεδομένων Κατάστασης συστήματος. Τα δεδομένα Κατάστασης συστήματος περιλαμβάνουν το μητρώο, τη βάση δεδομένων καταχώρησης κλάσης COM+, αρχεία που βρίσκονται στην περιοχή Προστασία αρχείων των Windows, αρχεία εκκίνησης και άλλα αρχεία συστήματος.

Εάν ο Προορισμός αντιγράφων ασφάλειας είναι διαθέσιμος, κάντε κλικ στον προορισμό αντιγράφων ασφάλειας που επιθυμείτε να χρησιμοποιήσετε.
Εάν επιλέξατε Αρχείο σε αυτό το βήμα, πληκτρολογήστε την πλήρη διαδρομή και το όνομα αρχείου για το οποίο επιθυμείτε να δημιουργήσετε αντίγραφα ασφάλειας δεδομένων στο πλαίσιο Μέσο αποθήκευσης αντιγράφων ασφάλειας ή ονόματος αρχείου.
Μπορείτε να καθορίσετε μια κοινόχρηστη θέση δικτύου, ως προορισμό για το αρχείο

αντιγράφου ασφαλείας. Συνήθως, τα αντίγραφα ασφάλειας αρχείων φέρουν επέκταση ονόματος αρχείου .bkf. Ωστόσο, μπορείτε να χρησιμοποιήσετε οποιαδήποτε επέκταση ονόματος αρχείου που θέλετε.

Βήμα 3: Ξεκινήστε τη δημιουργία αντιγράφων ασφάλειας

1. Κάντε κλικ στην επιλογή Έναρξη δημιουργίας αντιγράφων ασφάλειας για να ανοίξετε το παράθυρο διαλόγου Πληροφορίες για την εργασία δημιουργίας αντιγράφων ασφάλειας.
2. Στην περιοχή Εάν στο μέσο περιέχονται ήδη αντίγραφα ασφάλειας, πραγματοποιήστε οποιοδήποτε από τα εξής:

Εάν θέλετε να προσαρτήσετε αυτό το αρχείο αντιγράφου ασφαλείας σε προηγούμενα αρχεία αντιγράφων ασφαλείας, κάντε κλικ στο κουμπί Προσάρτηση αυτού του αντιγράφου ασφαλείας στο μέσο. Αυτή η επιλογή προσθέτει το νέο αντίγραφο ασφάλειας στο υπάρχον αντίγραφο ασφάλειας ώστε να μπορείτε να διατηρήσετε όλα τα προηγούμενα αντίγραφα ασφάλειας σε ένα αρχείο. Αυτή η επιλογή είναι χρήσιμη εάν επιθυμείτε να επαναφέρετε ένα αντίγραφο ασφάλειας από μια συγκεκριμένη ημέρα. Να γνωρίζετε πως το μέγεθος του αντίγραφου ασφάλειας θα μεγαλώνει με κάθε νέο αντίγραφο ασφάλειας. Μπορεί να επιθυμείτε να παρακολουθήσετε το μέγεθος αρχείου για να βεβαιωθείτε πως δεν θα γεμίσει εν τέλει το σκληρό δίσκο σας. Εάν το αρχείο γίνει πολύ μεγάλο, μπορεί να εξετάσετε την αποθήκευση του αρχείου σε εξωτερικό σκληρό δίσκο. Διαφορετικά, εάν σας απασχολεί εάν το αρχείο χρησιμοποιεί μεγάλη ποσότητα από το χώρο του σκληρού δίσκου, επιλέξτε Αντικατάστασή τους στο μέσο με αυτό το αντίγραφο.

Εάν θέλετε να αντικαταστήσετε προηγούμενα αρχεία αντιγράφων ασφαλείας με αυτό το αρχείο αντιγράφου ασφαλείας, κάντε κλικ στο στοιχείο Αντικατάσταση των δεδομένων του μέσου με αυτό το αντίγραφο ασφαλείας. Αυτή η επιλογή είναι χρήσιμη εάν επιθυμείτε μόνο να διατηρείτε το τρέχον αντίγραφο ασφάλειας και δεν σας απασχολεί η διατήρηση των προηγούμενων αντιγράφων ασφάλειας. Διαφορετικά, χρησιμοποιήστε αυτήν την επιλογή εάν σας απασχολεί εάν το αρχείο χρησιμοποιεί μεγάλη ποσότητα του σκληρού δίσκου στον υπολογιστή σας.

3. Κάντε κλικ στο κουμπί Για προχωρημένους.
4. Επιλέξτε το πλαίσιο ελέγχου Επαλήθευση δεδομένων μετά τη δημιουργία αντιγράφων.
5. Στο πλαίσιο Τύπος αντιγράφων ασφάλειας, κάντε κλικ στο είδος αντιγράφου ασφάλειας που επιθυμείτε να δημιουργήσετε. Για μια περιγραφή κάθε τύπου αντιγράφου ασφάλειας, κάντε κλικ στον τύπο αντιγράφου ασφάλειας και η περιγραφή εμφανίζεται στην περιοχή “Περιγραφή.” Έχετε τη δυνατότητα να επιλέξετε οποιονδήποτε από τους ακόλουθους τύπους αντιγράφων ασφαλείας:

- Κανονική
- Αντιγραφή
- Επαυξητικός
- Διαφορικός
- Καθημερινά

6. Κάντε κλικ στο κουμπί OK και έπειτα κάντε κλικ στην επιλογή Έναρξη δημιουργίας αντιγράφων ασφάλειας. Εμφανίζεται ένα παράθυρο διαλόγου Πρόοδος δημιουργίας αντιγράφων ασφάλειας και η δημιουργία αντιγράφων ασφάλειας ξεκινά.

Βήμα 4: Έξοδος από το βοηθητικό πρόγραμμα δημιουργίας αντιγράφων ασφαλείας

1. Μόλις ολοκληρωθεί η διαδικασία δημιουργίας αντιγράφων ασφαλείας, κάντε κλικ στο κουμπί Κλείσιμο.
2. Στο μενού Εργασία, κάντε κλικ στην επιλογή Έξοδος.

Πηγές:

- http://www.pi-schools.gr/programs/ktp/previous_version/book2/06_p1.pdf
- http://el.wikipedia.org/wiki/
- http://www.bratnet.gr/downloads/category/3-prostasia-apo-ioys-antivirus-adware-spyware.html
- http://pinnokio.gr/arthro/sygkrish-twn-pio-gnwstwn-dwrean-antivirus-avg-vs-avira-vs-avast
- greek.ruvr.ru
- pemptousia.gr
- sigmalive.com
- mpetskas.gr
- tovima.gr
- κοινωνικές επιπτώσεις της πληροφορικής.
- http://pinnokio.gr/arthro/sygkrish-twn-pio-gnwstwn-dwrean-antivirus-avg-vs-avira-vs-avast.
- http://vil.nai.com
- www.computercare.gr
- http://web.itc.auth.gr/portal/content/view/67/238/
- drteddy.gr
- gadget-akia.blogspot.com
- groupon.gr
- datalabs.edu.gr
- siteseeing.gr
- apneagr.blogspot.com
- deals247.gr