

ICDL Ενότητα 2

Χρήση Υπολογιστή και Διαχείριση Αρχείων με τη χρήση

LINUX

Ubuntu Linux και Επιφάνεια Εργασίας Gnome

4^ο Μέρος: Ιοί

2.4.1 Βασικές έννοιες

2.4.1.1 Τι είναι ο ιός και ποιες μπορεί να είναι οι επιπτώσεις του

Ένας ιός υπολογιστή είναι ένα πρόγραμμα το οποίο είναι εκ προθέσεως δημιουργημένο για να προκαλεί ενοχλήσεις ή να μεταβάλει ή να διαγράφει δεδομένα. Μερικοί ιοί προκαλούν τέτοια επιβράδυνση στο σύστημα του υπολογιστή, σε βαθμό που να μην μπορεί πλέον να χρησιμοποιηθεί. Ένα από τα χαρακτηριστικά των ιών είναι ότι είναι σχεδιασμένοι για να αντιγράφονται και να εξαπλώνονται.

Οι ιοί δεν αποτελούν ακόμα σοβαρό πρόβλημα για τα συστήματα υπολογιστών Linux, ωστόσο αυτό μπορεί να αλλάξει ανά πάσα στιγμή. Κάθε μέρα δημιουργούνται όλο και περισσότεροι νέοι ιοί. Ακόμα κι αν χρησιμοποιείτε Linux, είναι σημαντικό να είστε ενήμεροι για τους κινδύνους και να λάβετε τις απαραίτητες προφυλάξεις.

Trojan: Ο Trojan (ή Trojan horse) είναι ένας ιός ο οποίος κρύβεται μέσα σε ένα άλλο νόμιμο πρόγραμμα. Όταν το πρόγραμμα χρησιμοποιείται, ο ιός απελευθερώνεται και μπορεί να αρχίσει τη δική του δουλειά, της αντιγραφής και ενόχλησης ή καταστροφής.

Worm: Το worm είναι ένα πρόγραμμα που δημιουργεί αντίγραφα του εαυτού του ξανά και ξανά στη μνήμη του υπολογιστή, μέχρι που ο υπολογιστής μόλις που καταφέρνει να λειτουργεί. Ένα από τα σημάδια εισβολής του είναι η βραδύτητα του υπολογιστή.

Time bomb: Μία Time bomb είναι ένας ιός, ο οποίος μένει σε λανθάνουσα κατάσταση μέχρι μια συγκεκριμένη ημερομηνία ή ώρα ή για μια χρονική περίοδο. Τη δεδομένη ημέρα ή ώρα, ο ιός ξαφνικά ενεργοποιείται και εκτελεί το σκοπό για τον οποίο έχει δημιουργηθεί. Αυτό μπορεί να σημαίνει τη διαγραφή όλων των δεδομένων του σκληρού δίσκου.

Logic bombs: Μία Logic bomb είναι παρόμοια με την Time bomb, μόνο που αντί να ενεργοποιείται κάποια δεδομένη χρονική στιγμή, ενεργοποιείται όταν λαμβάνει χώρα μία συγκεκριμένη λειτουργία. Για παράδειγμα, αντί να γίνει διαμόρφωση μιας δισκέτας, ο ιός κάνει διαμόρφωση στο σκληρό δίσκο.

Macro-viruses: Οι Macro-viruses χρησιμοποιούν ένα ειδικό χαρακτηριστικό γνώρισμα προσαρμογής στις εφαρμογές, τις λεγόμενες μακροεντολές (macros). Οι μακροεντολές σας επιτρέπουν να δημιουργήσετε μικρά προγράμματα για να φέρετε εις πέρας συγκεκριμένες εργασίες στις εφαρμογές σας.

2.4.1.2 Τρόποι με τους οποίους μπορεί ένας ιός να μεταφερθεί στον υπολογιστή σας

Οι ιοί εξαπλώνονται με πολλούς τρόπους:

- Με μεταφορτώσεις (downloads) από το διαδίκτυο.
- Με πειρατικό λογισμικό.
- Με ανταλλαγή δισκετών.
- Με επισυνάψεις του ηλεκτρονικού ταχυδρομείου και σε μηνύματα ηλεκτρονικού ταχυδρομείου.

- Με έγγραφα. Οι Macro-viruses που περιγράφονται παραπάνω, μπορεί να κρύβονται σε καθημερινά έγγραφα κειμένου, υπολογιστικά φύλλα και παρουσιάσεις.

Οι ιοί μπορεί να εμπεριέχονται σε τέτοιες εφαρμογές. Μόλις μεταφορτωθούν και εκτελεστούν οι εφαρμογές, ο ιός φορτώνεται στη μνήμη του υπολογιστή και μολύνει άλλα προγράμματα στον υπολογιστή σας. Αυτοί οι ιοί μπορούν να κάνουν πολύ ανεπιθύμητες λειτουργίες όπως η αποστολή μολυσμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε διευθύνσεις που βρίσκονται στο βιβλίο διευθύνσεών σας. Μερικοί ιοί μπορούν ακόμα και να κλείσουν τον υπολογιστή σας και να εμποδίζουν την επανεκκίνηση του λειτουργικού σας συστήματος.

Γι' αυτό είναι πολύ σημαντικό να εγκαθιστάτε λογισμικό και ανοικτά αρχεία από αξιόπιστες πηγές. Αν δεν είστε σίγουρος για κάτι που κατεβάσατε από το διαδίκτυο ή λάβατε μέσω ηλεκτρονικού ταχυδρομείου, θα είναι καλύτερο να μην το ανοίξετε ή να μην το εκτελέσετε.

2.4.1.3 Τα πλεονεκτήματα της χρήσης μιας αντι-ιικής εφαρμογής

Αντι-ιικό λογισμικό

Το λογισμικό αυτό σαρώνει τα αρχεία για να εντοπίσει τμήματα κώδικα, που ονομάζονται υπογραφές (signatures), τα οποία τα αναγνωρίζει ως μέρη ενός ιού. Μία υπογραφή είναι μια διακριτική σειρά εντολών, οι οποίες βρίσκονται μόνο στο σχετικό ιό. Γι' αυτό το σάρωμα εμπλέκει και την ανάλυση του κώδικα των προγραμμάτων στην έρευνα για υπογραφές που εμπεριέχονται σε νόμιμα προγράμματα.

Η ενημέρωση του αντι-ιικού λογισμικού περιλαμβάνει κυρίως την ενημέρωση των αρχείων των υπογραφών. Αυτό θα πρέπει να γίνεται τακτικά, όσο το δυνατόν. Πολύ περισσότερο μάλιστα, όταν λαμβάνετε συχνά αρχεία από εξωτερικές πηγές. Αυτό καθεαυτό το αντι-ιικό πρόγραμμα θα ενημερώνεται κατά καιρούς. Αυτές οι ενημερώσεις θα περιλαμβάνουν πρόσθετα χαρακτηριστικά και βελτιωμένες μεθόδους σάρωσης.

Η ενημέρωση του αντι-ιικού και η σάρωση των περιεχομένων ενός υπολογιστή σε τακτά διαστήματα, θα σας παρέχουν ένα καλό μέτρο προστασίας, σε περίπτωση που ο υπολογιστής σας μολυνθεί. Καλό αντι-ιικό λογισμικό μπορεί επίσης να μπλοκάρει την είσοδο ιών στο σύστημά σας.

Άλλα μέτρα προστασίας

Υπάρχει πλήθος προστατευτικών μέτρων που μπορείτε να λάβετε προκειμένου να προστατευτείτε από ιούς:

- Να εγκαταστήσετε ένα καλό αντι-ιικό λογισμικό και να το ενημερώνετε τακτικά, για παράδειγμα τουλάχιστον μια φορά το μήνα ή καλύτερα μία φορά την εβδομάδα. Πάντα όμως να θυμάστε, ότι ένα αντι-ιικό λογισμικό δεν είναι τέλειο. Δεν μπορεί να είναι το μοναδικό μέτρο προστασίας.
- Να ελέγχετε όλες τις δισκέτες προτού τις διαβάσετε.
- Ενεργοποιήστε τη λειτουργία αυτόματης προστασίας του αντι-ιικού λογισμικού, για να ελέγχονται όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου.
- Να είστε επιφυλακτικοί με μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς, ιδίως αν περιέχουν επισυναπτόμενα. Ορισμένοι πολύ προσεκτικοί χρήστες διαγράφουν μηνύματα ηλεκτρονικού ταχυδρομείου για τα οποία δεν είναι

σίγουροι, χωρίς να τα ανοίξουν.

- Χρησιμοποιήστε έναν ISP που ελέγχει μηνύματα ηλεκτρονικού ταχυδρομείου πριν αυτά φτάσουν στον παραλήπτη.
- Μη μεταφορτώνετε λογισμικό από άγνωστους ιστοτόπους.
- Προσέχετε όταν χρησιμοποιείτε δισκέτες από άγνωστες πηγές.
- Μην εγκαθιστάτε πειρατικό λογισμικό.

2.4.1.4 Η σημασία της «απολύμανσης» αρχείων

Όταν εντοπιστεί ένας ιός, το λογισμικό θα επιχειρήσει να τον απομακρύνει. Αυτό ονομάζεται **καθαρισμός ή απολύμανση**. Η απολύμανση περιλαμβάνει απομάκρυνση του κώδικα του ιού από το αρχείο στο οποίο είναι επισύναψη.

Μερικές φορές συμβαίνει το σύστημα να εντοπίζει ιούς αλλά να μην μπορεί να τους αποβάλει. Σε αυτή την περίπτωση, συχνά θα δίνεται η επιλογή της **διαγραφής ή της απομόνωσης** του μολυσμένου αρχείου. Μία μελλοντική ενημέρωση του λογισμικού μπορεί να είναι ικανή να απομακρύνει τον ιό. Αν μπορεί να γίνει αυτό, παύει η απομόνωση.

2.4.2 Χειρισμός ιών

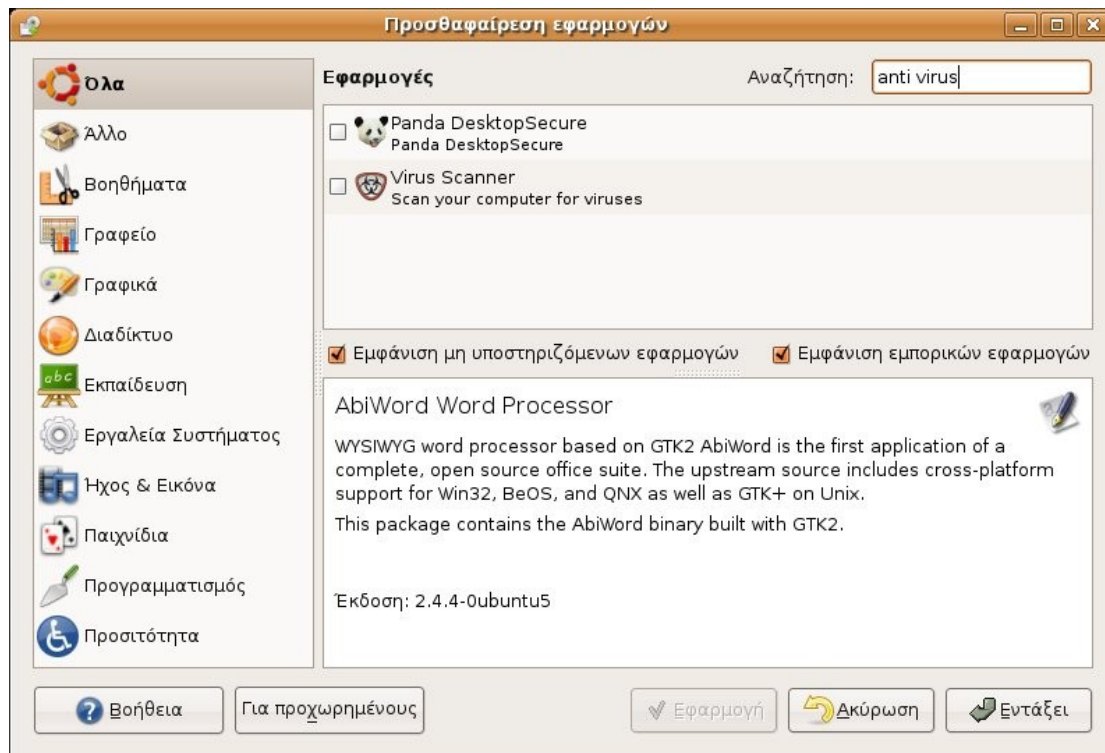
2.4.2.1 Χρήση αντι-ιικής εφαρμογής για τον έλεγχο συγκεκριμένων οδηγών, φακέλων, αρχείων

Επειδή οι ιοί είναι ακόμα άγνωστοι στα συστήματα Linux, δεν υπάρχει μεγάλη ανάπτυξη αντι-ιικών λογισμικών. Ωστόσο μπορείτε εύκολα να εγκαταστήσετε και να χρησιμοποιήσετε κάποιο αντι-ιικό λογισμικό.

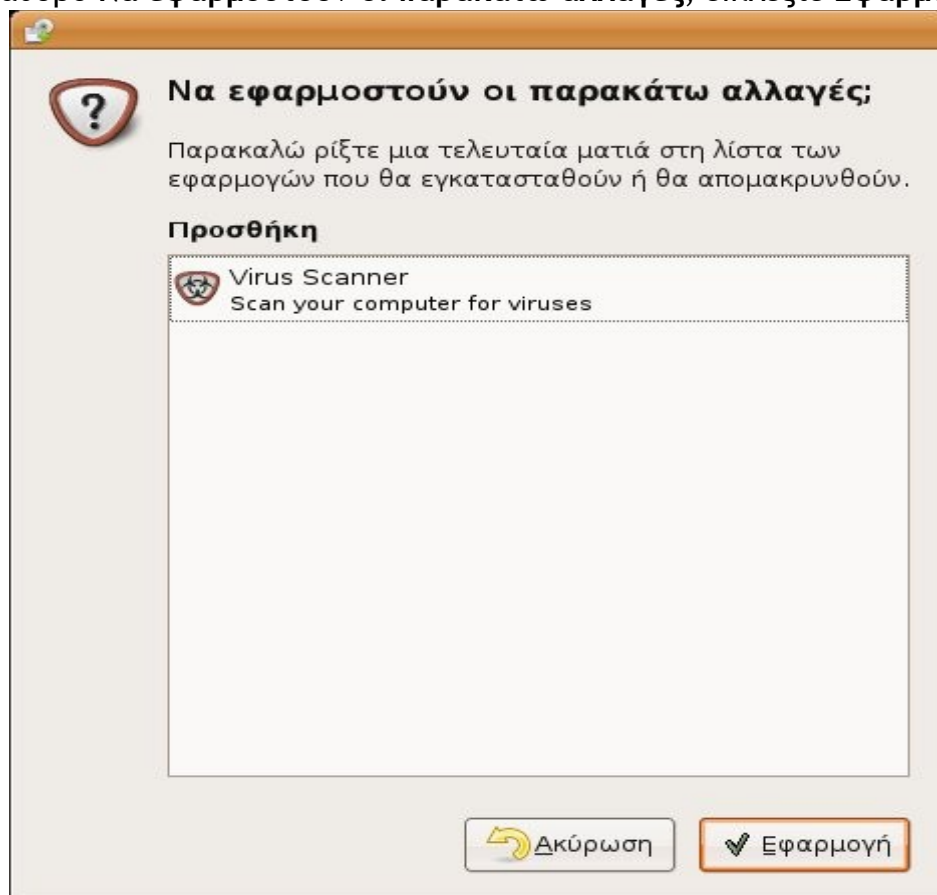
Εγκατάσταση αντι-ιικού

- Εφαρμογές -> Προσθαφαίρεση...

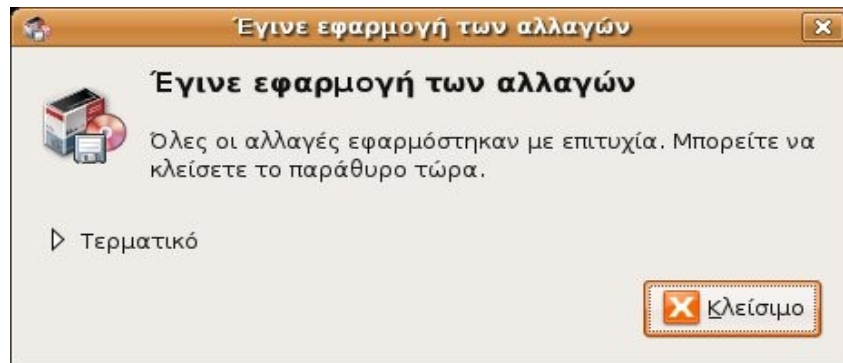
Στο παράθυρο Προσθαφαίρεση εφαρμογών πληκτρολογήστε στο πλαίσιο Αναζήτηση τον όρο anti-virus, για να εντοπίσετε τις διαθέσιμες προς εγκατάσταση αντι-ιικές εφαρμογές.



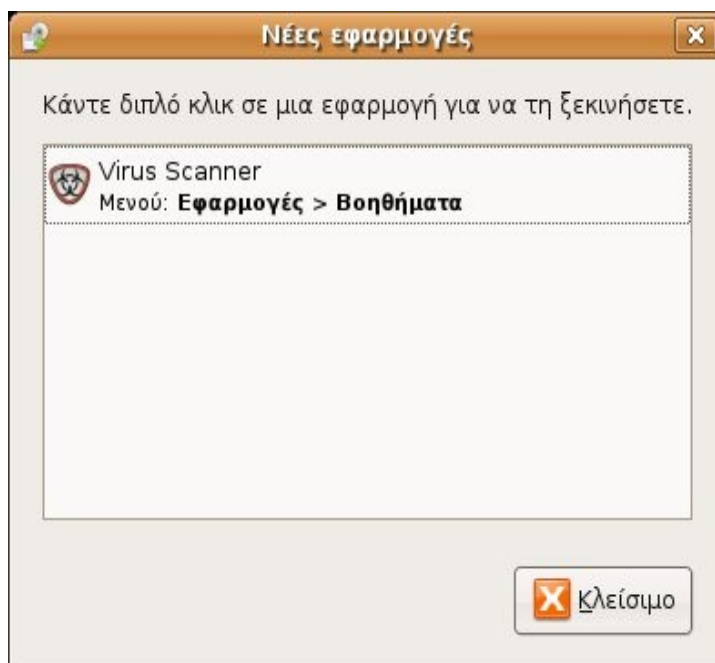
- Επιλέξτε **Virus Scanner** -> **Εφαρμογή**
- Στο παράθυρο **Να εφαρμοστούν οι παρακάτω αλλαγές**, επιλέξτε **Εφαρμογή**.



- Δώστε το κωδικό σας όταν σας ζητηθεί.
- Στο παράθυρο **Έγινε εφαρμογή των αλλαγών**, επιλέξτε **Κλείσιμο**.



Θα ακολουθήσει ο έλεγχος των εγκατεστημένων και διαθέσιμων εφαρμογών.

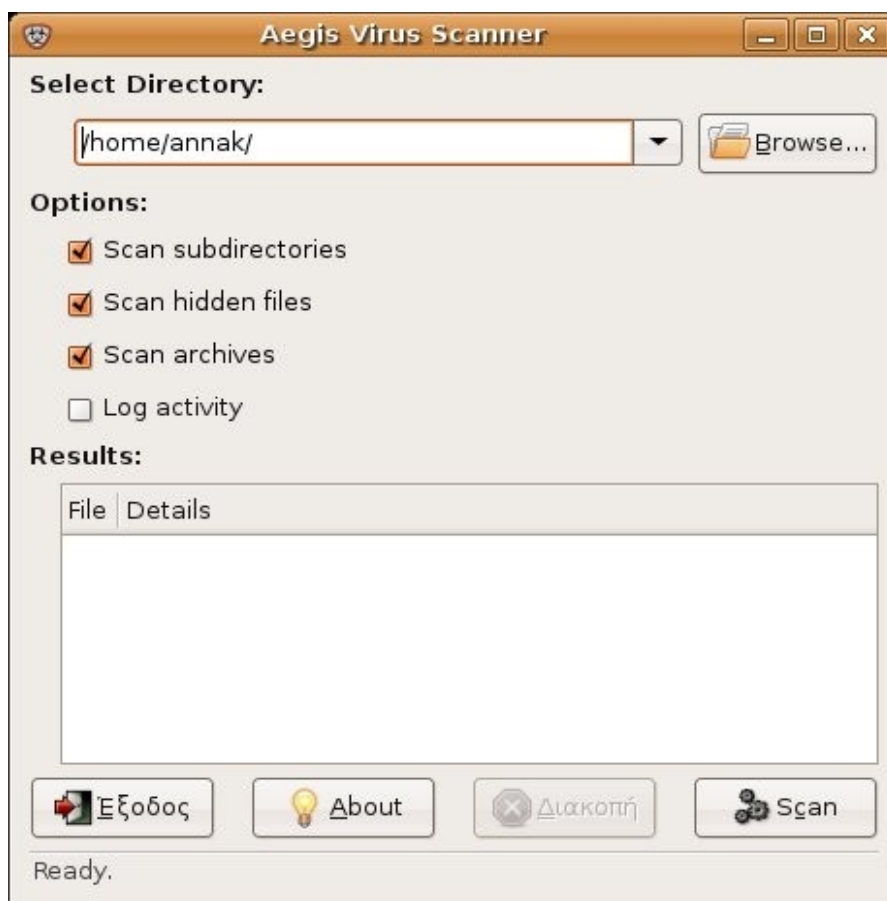


- Στο παράθυρο **Νέες εφαρμογές**, κάντε διπλό κλικ στην εφαρμογή **Virus Scanner**.

Έλεγχος για ιούς

Κάνοντας στο προηγούμενο παράθυρο διπλό κλικ στη εφαρμογή Aegis Virus Scanner, θα ανοίξει η εφαρμογή. Σε περίπτωση που εμφανιστεί παράθυρο διαλόγου για ενημέρωση του αντι-ικού, επιλέξτε **Ναι** (δώστε τον κωδικό σας όταν σας ζητηθεί και μετά την ολοκλήρωση της ενημέρωσης επιλέξτε **Κλείσιμο**).

- Επιλέξτε τον κατάλογο ή τα αρχεία που θέλετε να ελέγξετε, επιλέγοντας το **Browse...**
- Επιλέξτε όποιες από τις παρακάτω επιλογές (**Options**) επιθυμείτε.
- Κάντε κλικ στο **Scan**



Όταν ολοκληρωθεί ο έλεγχος των ιών θα εμφανιστεί σχετικό μήνυμα στη γραμμή κατάστασης του παραθύρου (Scan of complete), όπως φαίνεται και στην εικόνα που ακολουθεί.

2.4.2.2 Η σημασία της τακτικής ανανέωσης του αντι-ιικού λογισμικού

Καινούριοι ιοί δημιουργούνται ολοένα κι αυτό πρέπει να αναλύεται συνεχώς από τους υπεύθυνους για την ανάπτυξη αντι-ιικών λογισμικών. Οι προγραμματιστές αυτοί όχι μόνο πρέπει να είναι σε θέση να εξάγουν την υπογραφή του ιού, αλλά και να αναλύσουν το πώς ο ιός λειτουργεί και πώς μπορεί να απομακρυνθεί από το πρόγραμμα. Αυτές οι αλλαγές θα πρέπει ενσωματωθούν σε ένα αντι-ιικό λογισμικό.

Από τη μεριά τους οι χρήστες πρέπει να μεταφορτώσουν τις αλλαγές και να ενημερώνουν το λογισμικό τους. Όσο μεγαλύτερο χρονικό διάστημα μεσολαβεί μεταξύ των ενημερώσεων, τόσο πιο ευάλωτο είναι το σύστημα του υπολογιστή σας σε νέους ιούς. Συχνά ενημερώσεις διατίθενται σε καθημερινή βάση.