

Ελεύθερο Λογισμικό / Λογισμικό Ανοικτού Κώδικα

Ασφάλεια μέσω της διαφάνειας



Εμπιστοσύνη στην κοινότητα

Ο πηγαίος κώδικας των εφαρμογών και των βιβλιοθηκών στις οποίες στηρίζονται είναι ελεύθερα διαθέσιμος στο διαδίκτυο. Είναι δύσκολο να μην γίνει αντιληπτή από τις κοινότητες προγραμματιστών και χρηστών κάποια κακόβουλη λειτουργία “κρυμμένη” σε ελεύθερα διαθέσιμο κώδικα. Ακόμα και αν δεν έχεις τις τεχνικές γνώσεις ή το χρόνο να εξετάσεις τον κώδικα κάποια από τα εκατομμύρια μέλη της κοινότητας το έχουν κάνει.

Λιγότερα σφάλματα και κενά ασφαλείας

Όσο μεγαλύτερη είναι η βάση ανθρώπων που δοκιμάζουν, ελέγχουν, μελετούν και συν-αναπτύσσουν τον κώδικα του λογισμικού, τόσο πιο γρήγορα εντοπίζονται και λύνονται τα προβλήματα.

"given enough eyeballs, all bugs are shallow" (Linus's law)

Τα σφάλματα δεν αποκρύπτονται. Διορθώνονται γρήγορα.

Ο ελεύθερος κώδικας ελέγχεται από ανοικτές κοινότητες ανθρώπων και όχι από κάποια εταιρία που ανησυχεί για τη βλάβη που μπορεί να προκαλέσει στην δημόσια εικόνα της και στις πωλήσεις της η δημοσιοποίηση ενός σοβαρού σφάλματος ή κενού ασφαλείας στα προϊόντα της, και συνεπώς έχει όφελος να αποκρύψει ένα τέτοιο γεγονός. Τα κενά ασφαλείας και τα σφάλματα που ανακαλύπτονται στο ελεύθερο λογισμικό γίνονται άμεσα γνωστά στα μέλη της κοινότητας και διορθώνονται το ίδιο γρήγορα. Δεν υπάρχουν καθυστερήσεις στην δημιουργία και την διανομή των διορθώσεων ασφαλείας, όπως στο κλειστό λογισμικό λόγω της πολιτικής, ή των περιορισμένων πόρων της κατασκευάστριας εταιρίας.

“Είναι απλά ουτοπικό να βασίζεις στη μυστικότητα την ασφάλεια του λογισμικού ηλ. υπολογιστών. Μπορεί να καταφέρεις να κρατήσεις τον τρόπο λειτουργίας ενός προγράμματος μακριά από τα μάτια του κοινού, αλλά μπορείς να αποτρέψεις την εφαρμογή αντίστροφης μηχανικής πάνω σε αυτό από τους αντιπάλους σου; Πιθανότατα όχι.” (Whitfield Diffie, co-inventor of public-key cryptography)

FREE SOFTWARE

FREE SOCIETY

JOIN FSF

Σύγχρονες διανομές Linux

Ασφάλεια μέσω διαφάνειας

- Ανοικτός κώδικας

Ασφάλεια μέσω σχεδιασμού

- Αρχιτεκτονική Unix
- Προστασία μνήμης διεργασιών
- Προσωπικοί λογαριασμοί χρηστών
- Προσωπικοί χώροι αποθήκευσης αρχείων
- Προσωπικές ρυθμίσεις εφαρμογών
- Άδειες πρόσβασης αρχείων
- Αρθρωτός σχεδιασμός
- Firewall στον πυρήνα
- Chroot/Sandbox

Ασφάλεια μέσω της ποικιλομορφίας

- Ποικιλία διανομών
- Χρήση πολλαπλών προγραμμάτων για την ίδια εργασία
- Ποικιλία τρόπων ρύθμισης και παραμετροποίησης

Ασφάλεια μέσω κρυπτογραφίας

- Ευαίσθητα δεδομένα κρυπτογραφούνται
- Υποστήριξη κρυπτογραφημένων συστημάτων αρχείων
- ssh για ασφαλή απομακρυσμένη πρόσβαση
- scp/sftp για ασφαλή μεταφορά αρχείων
- Αυτόματος έλεγχος ψηφιακών υπογραφών md5sum κατά τη λήψη ενημερώσεων ή νέου λογισμικού από τα αποθετήρια της διανομής

Ασφάλεια μέσω των χρηστών

- Καθημερινή χρήση μέσω προσωπικού λογαριασμού περιορισμένων δικαιωμάτων
- Λήψη δικαιωμάτων υπερχρήστη μόνο όταν είναι απαραίτητο
- Συχνή ενημέρωση του λειτουργικού και του συνόλου των εφαρμογών
- Εγκατάσταση προγραμμάτων μόνο από έμπιστες πηγές

Ασφάλεια μέσω χαμηλού κόστους κτήσης και συντήρησης

- Δωρεάν πρόσβαση σε ενημερώσεις τόσο του λειτουργικού όσο και των εφαρμογών. (Οι χρήστες μπορούν να κρατούν συνεχώς ενημερωμένο το λογισμικό χωρίς κόστος.)
- Δωρεάν πρόσβαση σε πληθώρα εφαρμογών ελεύθερου κώδικα για σχεδόν κάθε εργασία μέσα από την ίδια τη διανομή. (Οι χρήστες δεν έχουν ανάγκη να προστρέχουν σε αμφιβόλου αξιοπιστίας πηγές freeware ή παράνομα τροποποιημένου κλειστού κώδικα λογισμικού)

Βασικές πρακτικές προστασίας ενός συστήματος Linux

Το Linux (ως ένα UNIX λειτουργικό σύστημα) δεν μπορεί να προσβληθεί από ιούς με τον ίδιο τρόπο που προσβάλλεται ένα Dos/Windows σύστημα. Στο UNIX, οι μηχανισμοί ασφάλειας αποτελούν βασικό στοιχείο του λειτουργικού συστήματος (πχ. οι απλοί χρήστες δεν έχουν δικαίωμα να γράφουν ελεύθερα σε όλες τις περιοχές του σκληρού δίσκου ή να εκτελούν κάποιες εφαρμογές και εντολές). Κακόβουλο λογισμικό (ιοί, worms, trojan horses) για UNIX υπάρχει, αλλά δεν αποτελεί (μέχρι σήμερα τουλάχιστον) πραγματικό πρόβλημα για οικιακούς χρήστες.

Για να προστατευθείτε αρκεί να ακολουθείτε κάποιους βασικούς κανόνες ασφάλειας:

- Χρησιμοποιείτε ισχυρούς κωδικούς πρόσβασης. Μην χρησιμοποιείτε τον ίδιο κωδικό για πρόσβαση σε πολλούς λογαριασμούς/συστήματα/υπηρεσίες. Αλλάζετε συχνά τον κωδικό σας.
- Μην τρέχετε εφαρμογές και προγράμματα με δικαιώματα υπερχρήστη (root/sudo) αν δεν είναι απαραίτητο. Να συνδέεστε με τον λογαριασμό απλού χρήστη για καθημερινή χρήση.
- Εγκαθιστάτε πακέτα λογισμικού μόνο από έμπιστες πηγές.
- Ελέγχετε τις PGP υπογραφές όταν κατεβάζετε πακέτα από εναλλακτικές τοποθεσίες (mirrors).
- Εάν δεν ξέρετε τι κάνει ένα εκτελέσιμο αρχείο, ή δεν εμπιστεύεστε την πηγή προέλευσής του, αποφύγετε να το εκτελέσετε ή εκτελέστε το σε κάποιον δοκιμαστικό λογαριασμό με περιορισμένα δικαιώματα και όχι με δικαιώματα υπερχρήστη (root/sudo).
- Διατηρείτε το σύστημά σας ενημερωμένο.
- Χρησιμοποιείτε το firewall του πυρήνα (iptables).
- Μην τρέχετε και μην κάνετε πρόσβασιμες από το διαδίκτυο υπηρεσίες (services) που δεν είναι απαραίτητες.
- Χρησιμοποιείτε κρυπτογραφημένα πρωτόκολλα για απομακρυσμένη πρόσβαση και μεταφορά αρχείων (ssh, https, sftp).

Γενικά δεν χρειάζεται να αγοράσετε ή να χρησιμοποιείτε κάποιο ειδικό λογισμικό προστασίας από ιούς (anti-virus). Παρά ταύτα, υπάρχουν τόσο κλειστού κώδικα, όσο και ελεύθερα προγράμματα ανίχνευσης κακόβουλου λογισμικού για linux, τα οποία στοχεύουν κυρίως στην ανίχνευση και εξουδετέρωση κακόβουλου λογισμικού για windows, πριν τα προσβεβλημένα αρχεία φτάσουν σε κάποιο ευπαθές σύστημα.

Και μην ξεχνάτε:

Ο πιο αδύναμος κρίκος στην ασφάλεια ενός συστήματος είναι ο χρήστης. Όσες δικλίδες ασφαλείας και να παρέχει ένα σύστημα (είτε σε επίπεδο λογισμικού, είτε σε επίπεδο hardware) μπορούν εύκολα να ακρωθούν από μια απρόσεκτη ενέργεια ή κακή συνήθεια του χρήστη. Απόλυτα ασφαλές λογισμικό δεν υπάρχει.

The only secure computer is one that's unplugged, locked in a safe, and buried 20 feet under the ground in a secret location...and i'm not even too sure about that one -- Dennis Huges, FBI.

Σχετικές πηγές:

<http://www.linuxsecurity.com/>

<http://www.linuxtopia.org/LinuxSecurity/>

<http://www.nic.com/~dave/SecurityAdminGuide/SecurityAdminGuide.html>

<http://www.itc.virginia.edu/unixsys/sec/>