Τέσσερις μύθοι
για την ασφάλεια των Windows έναντι των Linux

(Νοέμβριος 2004, COMDEX '04 Edition)

1. Τα Windows υφίστανται τόσες πολλές επιθέσεις γιατί υπάρχουν πολύ περισσότερες εγκαταστάσεις Windows απ' ότι Linux

Αυτό δεν ισχύει όσον αφορά τους διακομιστές. Οι πλατφόρμες Linux και BSD με Apache web servers είναι οι πιο διαδεδομένες με ποσοστό 68% σε αντίθεση με το συνδυασμό Windows–IIS Που κατέχει μόνο 21% (σύμφωνα με έρευνα της Netcraft, Σεπτέμβριος 2004). Παρ' όλα αυτά ο IIS είναι ο πιο συχνός στόχος με χειρότερο παράδειγμα το σκουλήκι Code Red που προσέβαλε περί τους 360.000 web servers παγκοσμίως και δεν διαδόθηκε περισσότερο (ούτε και κυκλοφορεί πλέον) μόνο διότι περιλάμβανε στον κώδικά του ημερομηνία λήξεως (σταμάτησε να διαδίδεται μετά από 3 εβδομάδες). Υπήρξαν σκουλήκια που είχαν στόχο συστήματα Linux/Apache με παράδειγμα τον Slapper, ο οποίος δεν εκμεταλλευόταν αδυναμία του ίδιου του Apache αλλά του πρωτοκόλλου SSL στην υλοποίηση OpenSSL. Σε αυτή τη περίπτωση όμως ο καθαρισμός και η επαναφορά του συστήματος ήταν απλούστατη χωρίς να χρειάζεται καν επανεκκίνηση του συστήματος χάρη στη λειτουργική οργάνωση του Linux.

Και άλλες υπηρεσίες διακομιστών της Microsoft δεν υπερέχουν όμως. Παράδειγμα η περίπτωση του σκουληκιού Slammer που, εκμεταλλευόμενος μια αδυναμία του Microsoft SQL Server που βασίζεται στο RPC (δικτυακή υπηρεσία των Windows που δεν είναι δυνατό να απενεργοποιηθεί και πολλές φορές ούτε να περιοριστεί, και συχνός παράγοντας αδυναμιών), κατάφερε σχεδόν να παραλύσει το διαδίκτυο (π.χ. πέταξε τη Νότια Κορέα, ισχυρή στο τομέα της πληροφορικής, εκτός διαδικτύου για πολλές ώρες).

Στη περίπτωση της desktop χρήσης των Windows και Linux, ότι αφορά τους διακομιστές ισχύει παρόμοια και στο desktop: τα Linux είναι πιο ασφαλή από τα Windows. Για παράδειγμα η περσινή επίθεση του σκουληκιού Blaster και η φετινές του Sasser και του Netsky (και οι τρεις εκμεταλλευόμενοι αδυναμίες σχετικές με το RPC) και οι παραλλαγές τους προσέβαλαν ο καθένας εκατοντάδες χιλιάδες συστήματα (μερικοί ανεβάζουν τον αριθμό για τον Blaster σε 1 εκατομμύριο) και ταλανίζουν ακόμα πολλούς χρήστες του διαδικτύου. Ο μέσος χρόνος επιβίωσης ενός ανενημέρωτου και απροστάτευτου Windows XP στο διαδίκτυο παραμένει επί μήνες τώρα κάτω από τα 20 λεπτά (πηγή: SANS Internet Storm Center). Και το χειρότερο; Ο χρήστης δεν χρειάζεται να κάνει τίποτα αφού συνδεθεί στο διαδίκτυο. Σε αντίθεση, η συντριπτική πλειοψηφία των desktop Linux συστημάτων παραμένουν ουσιαστικά απρόσβλητα από τη στιγμή που θα εγκατασταθούν.

Ισχύει όμως το ίδιο και για τις εφαρμογές σε εγκατάσταση desktop; Για την κατ' εξοχήν ευαίσθητη εφαρμογή, τον Internet Explorer, τα πράγματα δεν είναι ρόδινα. Σχεδόν κάθε μήνα υπάρχουν νέες διορθώσεις ασφαλείας για τον Internet Explorer. Ευτυχώς, για τις καθημερινές ανάγκες των χρηστών για πρόσβαση στο internet υπάρχουν άλλοι, πολύ καλοί web browsers διαθέσιμοι ακόμα και δωρεάν, αν και η χρήση λειτουργικών κομματιών του Internet Explorer εσωτερικά από άλλες εφαρμογές σε συνδυασμό με το προβληματικό μοντέλο ασφαλείας του Internet Explorer δεν καθησυχάζουν τους ειδικούς (ο ειδικός σε θέματα ασφαλείας Bruce Schneier σχολιάζει: "Νομίζω πως είναι ανοησία να χρησιμοποιείς τον Internet Explorer. Είναι γεμάτος τρύπες στην ασφάλειά

του και είναι πολύ δύσκολο να τον ρυθμίσεις ώστε να παρέχει ικανοποιητική βαθμό ασφάλειας.").

2. **Το Ανοιχτό Λογισμικό είναι εκ φύσεως λιγότερο ασφαλές επειδή οι κακοήθεις χάκερ μπορούν να βρουν τα ελαττώματα πιο εύκολα**

Τα παραπάνω δεδομένα καταρρίπτουν και αυτό το μύθο. Η πράξη αποδεικνύει ότι η πρόσβαση στον πηγαίο κώδικα δεν εκθέτει το λογισμικό. Ούτε, από την άλλη, η έλλειψη πηγαίου κώδικα προστατεύει το λογισμικό κάνοντας πιο δύσκολη την εξεύρεση αδυναμιών σε αυτά.

3. **Υπάρχουν περισσότεροι συναγερμοί για τα Linux απ' ότι για τα Windows, οπότε τα Linux είναι λιγότερο ασφαλή από τα Windows**
4. **Παίρνει περισσότερο χρόνο από την ανακάλυψη ενός ελαττώματος μέχρι την έκδοση του διορθωτικού του στα Linux απ' ότι στα Windows**

Και οι δύο παραπάνω μύθοι βασίζονται σε μονοδιάστατες μετρήσεις που δεν έχουν κανένα νόημα απλούστατα διότι η σοβαρότητα κάθε αδυναμίας δεν μετριέται από μια μόνο παράμετρο. Οι κυριότερες παράμετροι, σύμφωνα με τον Nicholas Petreley είναι:

1. Η *μέγεθος βλάβης* για κάθε αδυναμία ασφαλείας αφορά τη μέτρηση της δυνατής βλάβης που μπορεί να προκαλέσει. Μια αδυναμία που εκθέτει τους κωδικούς των administrator έχει υψηλό δείκτη μεγέθους βλάβης. Μια αδυναμία που κάνει απλώς την οθόνη να τρεμοπαίζει θα είχε πολύ χαμηλότερο δείκτη, που θα ανέβαινε μόνο αν αυτή η βλάβη ήταν δύσκολο να διορθωθεί.
2. Η *ευκολία εκμετάλλευσης* προσδιορίζει πόσο εύκολο ή δύσκολο είναι να αξιοποιήσει κάποιος την αδυναμία. Απαιτούνται ανώτερες γνώσεις και τεχνικές προγραμματισμού για την αξιοποίηση της αδυναμίας, ή μπορεί σχεδόν οποιοσδήποτε με στοιχειώδεις γνώσεις στους υπολογιστές να την αξιοποιήσει κακόβουλα;
3. Η *δυνατότητα έκθεσης* προσδιορίζει το μέγεθος της πρόσβασης που απαιτείται για την αξιοποίηση κάθε αδυναμίας. Αν ο οποιοσδήποτε επίδοξος χάκερ (κοινώς γνωστοί και ως “script kiddies”) στο διαδίκτυο μπορεί να αξιοποιήσει μια αδυναμία σε ένα διακομιστή που έχεις προστατέψει με firewall, αυτή η αδυναμία έχει υψηλό δείκτη δυνατότητας έκθεσης. Αν η αδυναμία είναι αξιοποιήσιμη μόνο από υπάλληλο της εταιρίας με στοιχειώδη πρόσβαση στο σύστημα και κάνοντας χρήση υπολογιστή εντός της εταιρίας, τότε η δυνατότητα έκθεσης στην αδυναμία είναι σημαντικά χαμηλότερη.

Όλα αυτά προϋποθέτουν πάντα ότι όλα τα στοιχειώδη μέτρα ασφαλείας έχουν παρθεί, όπως π.χ. σωστή χρήση κωδικών πρόσβασης και διαβαθμίσεων ασφαλείας για χρήστες και υπηρεσίες που λειτουργούν στους διακομιστές.

Περισσότερες πληροφορίες:

Μελέτη του Nicholas Petreley από την οποία προέρχονται τα περισσότερα στοιχεία:
http://www.theregister.com/2004/10/22/security_report_windows_vs_linux.pdf

Σχόλια του ειδικού σε θέματα ασφαλείας και συγγραφέα σχετικών βιβλίων Bruce Schneier:
http://www.schneier.com/blog/archives/2004/10/schneier_micros.html

Έρευνα Netrcraft: http://news.netcraft.com/archives/2004/08/31/September_2004_seb_server_survey.html

SANS: www.sans.org