11 Μαρτίου 2017

Μελέτη της RAND: Δεν είμαστε ποτέ ασφαλείς με τα προγράμματα λογισμικού που… λιμπίζονται οι χάκερς

/ Γενικά Θέματα

Εκατοντάδες σοβαρά κενά ασφαλείας παραμένουν στο λογισμικό, χωρίς να διορθώνονται από τους προγραμματιστές τους και χωρίς καν να γίνονται αντιληπτά από τον πολύ κόσμο, με συνέπεια να αποτελούν κατ’ εξοχήν δέλεαρ για τους απανταχού χάκερ.

Αυτό προειδοποιεί μελέτη της αμερικανικής RAND, σύμφωνα με την οποία κατά μέσο όρο μεσολαβούν σχεδόν επτά χρόνια ανάμεσα στην αρχική ιδιωτική ανακάλυψη κάποιου τέτοιου κενού και στη δημόσια αποκάλυψή του, οπότε γίνεται πια γνωστό ευρέως στο κοινό.

Οι συγκεκριμένες «τρύπες» ασφαλείας χαρακτηρίζονται «zero-day», επειδή όταν πια γνωστοποιούνται, οι δημιουργοί προγραμματιστές τους έχουν σχεδόν μηδενικό χρόνο στη διάθεσή τους για να τις κλείσουν με τις κατάλληλες επεμβάσεις, με αποτέλεσμα όχι σπάνια οι χάκερ να τους προλαβαίνουν. Εκτιμάται ότι χρειάζονται κατά μέσο όρο 22 μέρες για να αναπτυχθεί από έναν χάκερ το κατάλληλο πρόγραμμα πλήρους εκμετάλλευσης ενός κενού, αλλά κάλλιστα θα μπορούσε να το κάνει πολύ πιο γρήγορα.

Οι ερευνητές της RAND Corporation, με επικεφαλής την ειδική στην ασφάλεια πληροφοριών Λίλιαν Άμπλον, έκαναν την πρώτη δημόσια μελέτη που εστιάζει στα ουκ ολίγα κενά ασφαλείας τα οποία παραμένουν ακόμη άγνωστα στο ευρύ κοινό.

Ανέλυσαν πάνω από 200 περιπτώσεις τέτοιων ευάλωτων περιοχών στα διάφορα προγράμματα λογισμικού και, όπως αναφέρουν, σχεδόν το 40% από αυτές παραμένουν ακόμη άγνωστες στο ευρύ κοινό.

Σύμφωνα με τη RAND, στην πράξη περνάνε κατά μέσο όρο 6,9 χρόνια, εωσότου το πρόβλημα δημοσιοποιηθεί, μια καθυστέρηση που οφείλεται είτε σε σκοπιμότητα, είτε σε άγνοια. Το 25% των “zero day” κενών ασφαλείας παραμένουν άγνωστα και αδιόρθωτα επί ενάμισι έτος, ενώ ένα άλλο 25% για πάνω από 9,5 χρόνια!

Κάποιες περιπτώσεις θεωρούνται «αθάνατες», επειδή το κενό ασφαλείας θεωρείται ότι θα παραμείνει… αιώνια, καθώς ο δημιουργός του λογισμικού δεν διαθέτει πια τον σχετικό κώδικα προγραμματισμού ή αδυνατεί να κάνει ανανεώσεις του προϊόντος του με νέα «μπαλώματα» ασφάλειας. Μερικά κενά λέγονται «ζόμπι», επειδή λόγω αναθεώρησης του κώδικα προγραμματισμού, η εκμετάλλευσή τους μπορεί να γίνει μόνο σε παλαιότερες εκδόσεις του λογισμικού.

Ένα αιωρούμενο ερώτημα μέχρι σήμερα είναι κατά πόσο οι κυβερνήσεις και οι εταιρείες πρέπει να αποκαλύπτουν δημοσίως ή να σιωπούν, όταν ανακαλύπτουν κρίσιμες «τρύπες» στην κυβερνοασφάλεια, οι οποίες θα μπορούσαν να αξιοποιηθούν για κακόβουλους σκοπούς.

Η μελέτη εκτιμά ότι έχει όντως μια λογική η αποφυγή αποκάλυψης αρκετών κενών ασφαλείας, λόγω της επιθυμίας αυτοπροστασίας από τις δημόσιες υπηρεσίες ή τις εταιρείες που θέλουν να προστατεύσουν τα κυβερνοσυστήματά τους. Από την άλλη, οι λεγόμενοι «λευκοί» (καλοπροαίρετοι) χάκερ έχουν περισσότερα κίνητρα να προβούν σε αποκαλύψεις, μόλις ανακαλύψουν μια «τρύπα».

Βέβαια, μόλις μαθευτεί το νέο, κάποιοι «μαύροι» (κακοπροαίρετοι) χάκερ μπορεί να σπεύσουν αμέσως να εκμεταλλευθούν την «τρύπα», προκειμένου να αποκτήσουν πρόσβαση σε συστήματα και δίκτυα-στόχους, είτε πρόκειται για κυβερνο-έγκλημα είτε για κυβερνο-κατασκοπία.

Πηγή: koolnews.gr