1 Απριλίου 2014

Η «τεχνική του νερόλακκου» και το Ιντερνετ

/ Επιστήμες, Τέχνες & Πολιτισμός

«Στην περίπτωση που υπάρχουν μικρά παιδιά, θα συμβούλευα να χρησιμοποιείται επίσης ένα λογισμικό οικογενειακής ασφάλειας και, ακόμη σημαντικότερο, το PC θα πρέπει να βρίσκεται σε κοινόχρηστο χώρο», συμβουλεύει ο κ. Ηλίας Χάντζος.

Πού θα πήγαινε το μυαλό σας αν ακούγατε κάποιον να μιλάει για την «τεχνική του νερόλακκου»; Ενδεχομένως σε κάποιον αγρότη, ίσως σε έναν γεωπόνο, το μόνο σίγουρο, πάντως, είναι ότι δεν θα φανταζόσασταν ποτέ κάποιον... χάκερ. Κι όμως, αυτήν την ονομασία έδωσαν οι διώκτες του κυβερνοεγκλήματος σε μια τεχνική ηλεκτρονικής εισβολής στα κομπιούτερ μας. Ο λόγος;

Επειδή θυμίζει τον τρόπο που κυνηγούν οι τίγρεις τα θηράματά τους, στην Ινδία και στην Ασία. Τα συγκεκριμένα αιλουροειδή δεν τρέχουν ποτέ κυνηγώντας τις αντιλόπες, αλλά στήνουν «καρτέρι» στις πηγές όπου θα πάνε για να πιουν νερό. «Κάτι ανάλογο κάνουν τον τελευταίο καιρό και αρκετοί κυβερνοεγκληματίες», λέει στην «Κ» ο κ. Ηλίας Χάντζος, ειδικός σε θέματα προστασίας ιδιωτικότητας μεγάλης πολυεθνικής εταιρείας. «Δηλαδή, δεν επιτίθενται απευθείας στα μηχανήματα όσων έχουν βάλει στο στόχαστρο, αλλά παραβιάζουν ιστοσελίδες που γνωρίζουν ότι επισκέπτονται οι συγκεκριμένοι χρήστες, ώστε να τους μολύνουν όταν τις επισκεφθούν. Δηλαδή, τους στήνουν καρτέρι».

Ο κ. Χάντζος βρέθηκε στην Ελλάδα πριν από λίγες ημέρες με αφορμή μια ομιλία του σε συνέδριο για την ασφάλεια στον κυβερνοχώρο, που διοργάνωσε η ελληνική προεδρία της Ε.Ε. Με την ευκαιρία, μίλησε στην «Κ» για το κατά πόσον οι Ελληνες είναι εκτεθειμένοι σε κυβερνοαπειλές –στον βαθμό που συμβαίνει στο εξωτερικό– και ήταν αποκαλυπτικός. «Η αλήθεια», μας είπε «είναι ότι ακόμη τα κρούσματα είναι λιγότερα στη χώρα μας, κάτι που έχει να κάνει με τη συγκριτικά περιορισμένη διείσδυση του Ιντερνετ». Μας βοηθάει όμως και κάτι ακόμη: το γεγονός ότι η γλώσσα μας δεν είναι ευρέως διαδεδομένη και έτσι «βγάζουν μάτι» τα κακόβουλα μηνύματα, που συνήθως είναι κακές μεταφράσεις από «αυτόματα μηχανάκια».

«Ωστόσο, αυτό δεν σημαίνει πως πρέπει να εφησυχάζουμε, αφού έχουν σημειωθεί και εδώ καλά “ενορχηστρωμένες” επιθέσεις». Και θυμάται: «Για παράδειγμα, αν και ξενόφερτος, “ο ιός της Αστυνομίας” ζητούσε “λύτρα” σε άπταιστα ελληνικά».

Ενας από τους μύθους που υπάρχουν όσον αφορά την κυβερνοασφάλεια έχει να κάνει με την ύπαρξη απολύτως «στεγανών» λειτουργικών συστημάτων: «Είναι αφελές να νομίζει κανείς πως δεν διατρέχει καμία απειλή, επειδή χρησιμοποιεί υπολογιστή γνωστής μάρκας», λέει χαρακτηριστικά. Επίσης, παρ’ όλο που ένα λογισμικό ασφάλειας μειώνει κατά πολύ τους κινδύνους, καμία τεχνική λύση δεν θα προστατεύσει τον χρήστη, αν αυτός δεν προσέχει τα προγράμματα που εγκαθιστά, αλλά και τα e-mail ή τις ιστοσελίδες που «ανοίγει».

Η πρώτη γραμμή άμυνας

Επομένως, η ελεγχόμενη online δραστηριότητα είναι και θα παραμείνει πάντοτε η πρώτη γραμμή άμυνας, στην οποία περιλαμβάνεται και η λελογισμένη έκθεση στα κοινωνικά δίκτυα. «Για παράδειγμα, ίσως μοιάζει ακίνδυνο ένας χρήστης να έχει “ανεβάσει” στο Facebook το πότε έχει γενέθλια, ωστόσο η ημερομηνία γέννησης είναι ερώτηση για την πρόσβαση στην πιστωτική κάρτα», αναφέρει. Επειδή η χώρα

μας άργησε να προσαρμοστεί στις τεχνολογικές εξελίξεις, μια σημαντική μερίδα των σημερινών 40ρηδων και 50ρηδων, στην Ελλάδα, αναπόφευκτα δεν έχει μεγάλη εξοικείωση, τόσο ως επαγγελματίες όσο και –κυρίως– ως γονείς. «Νομίζω πως αυτό το έλλειμμα εμπειρίας καλύπτεται αρκετά από το ενημερωτικό υλικό οργανισμών, δημοσίων υπηρεσιών κ.ά.», επισημαίνει. Ολο αυτό το υλικό συγκλίνει πάνω-κάτω στους ίδιους κανόνες προστασίας των υπολογιστών, δηλαδή στη χρήση των πιο πρόσφατων εκδόσεων του λειτουργικού και των προγραμμάτων, στην εγκατάσταση μιας ολοκληρωμένης «σουίτας ασφαλείας» και στη δημιουργία ισχυρών κωδικών και την προστασία τους.

«Στην περίπτωση που υπάρχουν μικρά παιδιά, θα συμβούλευα να χρησιμοποιείται επίσης ένα λογισμικό οικογενειακής ασφάλειας και, ακόμη σημαντικότερο, το PC θα πρέπει να βρίσκεται σε κοινόχρηστο χώρο», τονίζει ο κ. Χάντζος.

Οι ίδιοι κανόνες ισχύουν και για τις «έξυπνες» συσκευές, στις οποίες εξάλλου στρέφουν ολοένα και περισσότερο την προσοχή τους οι κυβερνοεγκληματίες. Παρ’ όλο που για το λειτουργικό Android υπάρχουν περισσότερα κρούσματα, για τον κ. Χάντζο η προσεκτική χρήση και μια σουίτα ασφαλείας εγγυώνται ικανοποιητική ασφάλεια. «Αν και το “οικοσύστημα” των iPhone και iPad περιφρουρείται σαφώς περισσότερο, σε απόλυτο αριθμό το λειτουργικό τους έχει περισσότερες ευπάθειες, επομένως θα συνιστούσα ένα λογισμικό ασφαλείας και σε αυτήν την περίπτωση», συμπληρώνει. Στην πραγματικότητα, οι φορητές συσκευές είναι πιο εύκολο, από κλοπή ή απώλεια, να πέσουν στα χέρια «αδιάκριτων» και, μαζί με αυτές, τυχόν ευαίσθητα αποθηκευμένα δεδομένα.

ΚΩΣΤΑΣ ΔΕΛΗΓΙΑΝΝΗΣ

Πηγή: kathimerini.gr Έντυπη