24 Νοεμβρίου 2013

Το

cryptoparty είναι μια σύναξη στην οποία πηγαίνει όποιος θέλει με το λάπτοπ του ή την ταμπλέτα του και εκπαιδεύεται από ειδικούς στην ασφαλή και ανώνυμη χρήση του Διαδικτύου.

Έχετε αναρωτηθεί γιατί η τράπεζά σας δεν σας σας στέλνει ποτέ e-mail; Και, επιπλέον, σας προειδοποιεί πως, αν ποτέ σας σταλεί δήθεν e-mail της, τότε μπορείτε να είστε σίγουροι ότι πρόκειται για απάτη;» ρωτάει…τους παρευρισκομένους ο Μάλτε Ντικ, ακτιβιστής για την ηλεκτρονική προστασία δεδομένων. Η ανοιχτή συνάντηση πραγματοποιείται στην Ενωση Ανταποκριτών στο Βερολίνο και ο Ντικ με τον Χάουκε Λάγκινγκ είναι μέλη του κινήματος Cryptoparty, το οποίο ξεκίνησε μέσω του Twitter πριν από περίπου ένα χρόνο.

Το cryptoparty είναι μια σύναξη στην οποία πηγαίνει όποιος θέλει με το λάπτοπ του ή την ταμπλέτα του και εκπαιδεύεται από ειδικούς στην ασφαλή και ανώνυμη χρήση του Διαδικτύου. Το πρώτο έγινε στη Μελβούρνη και μέσα σε λίγους μήνες η ιδέα εξαπλώθηκε. Ειδικά στη Γερμανία, μετά και τις πρόσφατες αποκαλύψεις περί παρακολουθήσεων, το ενδιαφέρον έχει αυξηθεί – ένα cryptoparty διοργανώθηκε, μάλιστα, και στο Κοινοβούλιο. Σκοπός των ακτιβιστών είναι να μυηθούν όσο το δυνατόν περισσότεροι στην κρυπτογράφηση. Μέχρι πριν από λίγο καιρό οι «καλεσμένοι» ήταν άνθρωποι που έχουν σχέση με υπολογιστές ή νέοι με πολιτικές

ανησυχίες. Σιγά-σιγά η σύνθεση αλλάζει, αφού αρκετοί δικηγόροι και δημοσιογράφοι ή επαγγελματίες που διαχειρίζονται ευαίσθητα δεδομένα δείχνουν ενδιαφέρον, ενώ υπάρχουν και άνθρωποι με συγγενείς σε «δύσκολες» χώρες, όπου καταστρατηγείται το απόρρητο των επικοινωνιών.

Οι δύο ακτιβιστές προσπαθούν να εξηγήσουν ότι καμία online συζήτηση δεν είναι ιδιωτική. Η μυστικότητα δεν υφίσταται στον παγκόσμιο ιστό. «Και αν αυτό δεν σας τρομάζει, διότι γράφετε θεατρικές κριτικές και όχι αποκαλυπτικά ρεπορτάζ, δεν πρέπει να ξεχνάτε πως, όπου μπορούν να παρεισφρήσουν οι μυστικές υπηρεσίες μπορούν και οι απατεώνες», επισημαίνει ο Λάγκινγκ. «Ακόμη και αν κανείς νομίζει πως δεν έχει τίποτα να κρύψει, αυτό το οποίο διακυβεύεται είναι η δημοκρατία. Μπορεί τώρα να μη σας ενδιαφέρει, αλλά τα δεδομένα σας είναι άφθαρτα, αποθηκεύονται και μπορούν να χρησιμοποιηθούν εναντίον σας στο μέλλον», προσθέτει. «Μπορούμε να παρομοιάσουμε τις παρακολουθήσεις με το τσιγάρο ή τη ραδιενέργεια. Μέχρι να πεθάνουν μερικές εκατοντάδες χιλιάδες, δεν ξέραμε τίποτα. Επρεπε να βγουν μελέτες, να μιλήσουν οι επιστήμονες, για να καταλάβουμε τι συμβαίνει και να λάβουμε μέτρα προστασίας», παρεμβαίνει ο Ντικ.

Το ίδιο βράδυ, ένα ακόμη cryptoparty με περίπου 60 καλεσμένους διοργανώνεται στην περιοχή Νόικελν, στο Βερολίνο. Η Λέντσι, ο Νικολάι και ο Ντικ εξηγούν ότι η ασφάλεια στο Διαδίκτυο δεν μπορεί να επιτευχθεί μόνο με μερικές εφαρμογές, αλλά είναι μια διαδικασία, ένας «αγώνας» ανάμεσα σε εκείνους που παρακολουθούν και σε εκείνους που δεν το δέχονται. Δεν δίνουν απαντήσεις, κυρίως θέτουν ερωτήσεις. «Γιατί είναι σημαντική η ιδιωτικότητα; Διότι τα αρχεία μου, οι επαφές μου, οι αναζητήσεις μου, όλα όσα κάνω ή γράφω στον υπολογιστή μου και στο Διαδίκτυο ανήκουν σ’ εμένα και σε κανέναν άλλο;» Σκέφτομαι τις πρόσφατες αποκαλύψεις των Anonymous για τις αναζητήσεις στο Google προσώπου της ελληνικής επικαιρότητας: «Βότανο για αιμορροΐδες, κρίση στο γάμο, προβλέψεις ζωδίων, μασάζ αισθησιακό βίντεο…». Αμέσως μετά χωριζόμαστε σε ομάδες, ανάλογα με το τι μας ενδιαφέρει να μάθουμε: ανώνυμη περιήγηση στο Διαδίκτυο, κρυπτογράφηση e-mails και συνομιλιών σε chat. Γίνεται φανερή η ανάγκη χρήσης ελεύθερου λογισμικού όπως και ότι όλες οι κρυπτογραφικές λύσεις έχουν κενά. Τα δε προγράμματα κατά των ιών είναι αμφιβόλου αποτελεσματικότητος. «Ωστόσο, όσο περισσότερα εμπόδια βάζεις στους “κακούς”, όποιοι και αν είναι αυτοί, τόσο πιο δύσκολο είναι να τα καταφέρουν».

Ποια είναι η πιο συνηθισμένη μέθοδος παρακολούθησης; «Τα πάντα βασίζονται σε αλγόριθμους: βρες μου όλους όσοι ζουν στο Βερολίνο, είναι Αμερικανοί και γράφουν στα mails τους τις τάδε λέξεις. Οσο πιο καλός ο αλγόριθμος, τόσο καλύτερα τα αποτελέσματα. Βέβαια, αν το τελευταίο διάστημα έχεις

επικοινωνήσει μέσω e-mail με τον Στρέμπελε (σημ.: τον Γερμανό πολιτικό των Πρασίνων που συνάντησε τον Σνόουντεν), τότε τη συγκεκριμένη αλληλογραφία είναι βέβαιο ότι θα τη διαβάσει ανθρώπινο μάτι».

Και πώς τα ξέρουμε όλα αυτά; ξαναρωτάω. «Από τα ντοκουμέντα του Σνόουντεν. Δηλαδή τα ξέραμε και πριν, αλλά τώρα αποδείχτηκαν». Η βραδιά συνεχίζεται με επιτυχία και το ενδιαφέρον παραμένει αμείωτο. Οι εθελοντές ειδικοί τα εξηγούν όλα με απλά λόγια και έχουν μεγάλη υπομονή. Μας γίνεται σαφές ότι, όταν χρησιμοποιείς το Facebook ή παρόμοιες εφαρμογές, αλλά και τον τραπεζικό σου λογαριασμό, είναι αδύνατον να είσαι ανώνυμος. Ωστόσο, για όλα υπάρχουν λύσεις. Αποφασίζω να κατεβάσω ένα πρόγραμμα για να λαμβάνω τα e-mails που διατηρώ στο Google και το Yahoo, χωρίς να είμαι εκτεθειμένη στα κενά ασφαλείας των δύο αυτών παρόχων. Παραπονιέμαι στον εθελοντή ότι λατρεύω το Gmail, πως είναι ό,τι πιο φιλικό για τους χρήστες έχω δοκιμάσει, ότι θα μου λείψει και όλα αυτά που προσφέρει είναι εντελώς δωρεάν. «Φυσικά και είναι δωρεάν, αφού του χαρίζεις όλα σου τα δεδομένα… Να σου ζητήσει και χρήματα από πάνω;» με αποστομώνει.

Από Linux μέχρι «κλειδιά» για chat

Γενικός κανόνας: Αποκτάμε συνείδηση ότι ο ηλεκτρονικός κόσμος δεν είναι τόσο ασφαλής όσο παρουσιάζεται. Καλό είναι να ενημερωνόμαστε και να μην εμπιστευόμαστε άκριτα τις ευκολίες που μας παρέχονται: δεν νοείται να είμαστε απλώς πελάτες, οι οποίοι αγοράζουν και καταναλώνουν. Λύσεις υπάρχουν, ακόμη και για αρχάριους, και μάλιστα δωρεάν.

Στο τέλος του πάρτι έχω ανακαλύψει ότι ο υπολογιστής μου είναι γεμάτος ιούς που γνωρίζουν τα passwords μου. Η μόνη λύση είναι να βγάλω τα Windows και να εγκαταστήσω το Linux, το πλέον ασφαλές λογισμικό. «Το χρησιμοποιεί το γερμανικό υπουργείο Εξωτερικών σε όλους τους υπολογιστές που διαχειρίζονται ευαίσθητα δεδομένα», μου εξηγούν. Ξαφνικά μου έχει κοπεί εντελώς η όρεξη να χρησιμοποιήσω το λάπτοπ. Νιώθω σαν να μπήκαν κλέφτες στο σπίτι μου. «Και γιατί δεν έχουν ήδη καταχραστεί τον τραπεζικό μου λογαριασμό;» θέλω να μάθω. «Ετυχε… Υπάρχουν πολλών ειδών απατεώνες», με διαφωτίζει ο Νικολάι, φοιτητής Ανθρωπολογίας. «Ισως να θέλουν απλώς τη μνήμη του υπολογιστή σου για να ανεβάζουν πορνό ή τη σύνδεσή σου στο Ιντερνετ, για να στέλνουν spam. Ποιος ξέρει τι γίνεται εκεί έξω, στον αχανή παγκόσμιο ιστό;»

1. Εγκαθιστούμε ελεύθερο λειτουργικό Linux. Το κατεβάζουμε από το Διαδίκτυο και, αν είμαστε στοιχειωδώς εξοικειωμένοι, μπορούμε εύκολα να κάνουμε την εγκατάσταση. Δεν έχει «τρύπες», από τις οποίες κάποιος θα εισέλθει στον υπολογιστή μας. Οι ιοί που το απειλούν είναι ελάχιστοι. Το περιβάλλον του, για

έναν συνηθισμένο χρήστη, είναι οικείο. Κατόπιν, μπορούμε να κατεβάσουμε ελεύθερα προγράμματα, όπως επεξεργαστές κειμένου ή εικόνας. Συνήθως όλα διατίθενται και στα Ελληνικά. Δοκιμάζουμε το Linux Xubuntu, το οποίο είναι αρκετά εύκολο για αρχάριους.

2. Για να σερφάρουμε ανώνυμα, μπορούμε να κατεβάσουμε το TorProjekt, το οποίο διαθέτει τον Tor browser. Με τον συγκεκριμένο browser, κανείς δεν γνωρίζει το IP μας. Ενα τεστ: Ανοίγουμε τον κανονικό μας browser (π.χ. Explorer, Chrome, Firefox) και πληκτρολογούμε τη διεύθυνση www.wieistmeineip.de. Θα εμφανιστεί το IP και η χώρα μας. Αν ανοίξουμε τον Tor browser και κάνουμε την ίδια διαδικασία, θα δούμε ένα ωραιότατο anonymous. Είναι εξαιρετικά χρήσιμο αν δεν θέλουμε να αποθηκεύονται οι αναζητήσεις μας και όσα διαβάζουμε. Μια άλλη λύση, για να κάνουμε αναζητήσεις ως ανώνυμοι, είναι να χρησιμοποιούμε τις σελίδες https://startpage.com ή https://duckduckgo.com.

3. Τα passwords είναι σαν το κλειδί του σπιτιού μας. Δεν το ξεχνάμε, δεν δίνουμε αντίγραφα, δεν έχουμε το ίδιο για το εξοχικό, το σπίτι, το γραφείο, το αυτοκίνητο, τη θυρίδα. Είναι εξαιρετικά επικίνδυνο να χρησιμοποιούμε το ίδιο password ή δύο-τρία ίδια παντού. Πρόσφατα, χάκερ έκλεψαν από την Adobe περίπου 150 εκατομμύρια συνθηματικά. Οι χρήστες δεν αρκεί να αλλάξουν τον κωδικό τους μόνο στην Adobe. Αν χρησιμοποιούν τον ίδιο και σε άλλα sites και εφαρμογές, τότε οι υποκλοπείς μπορούν να μπουν και εκεί. Passwords όπως τα ονόματα των παιδιών μας ή η ημερομηνία γέννησής μας ή ένα απλό 12345 είναι εξαιρετικά επισφαλή. Κάλλιστα μπορούμε να προσθέσουμε μερικά σύμβολα, όπως &,*,), !.

4. Οι τραπεζικές συναλλαγές είναι πολύ ασφαλείς. Πρόβλημα δημιουργείται όταν έχουμε ιούς οι οποίοι «χρησιμοποιούν» ένα key logger και διαβάζουν τα passwords. Με το Linux, σύμφωνα με τους ακτιβιστές, η πιθανότητα αυτή σχεδόν μηδενίζεται. Μετά την εγκατάστασή του, λοιπόν, καλό θα ήταν να αλλάξουμε όλα τα passwords.

5. Για ακόμη πιο αναβαθμισμένη αυτοπροστασία, μπορείτε να κρυπτογραφείτε τα e-mails και τις συνομιλίες σας στα chat-rooms (προϋποθέτει να κάνει το ίδιο και ο συνομιλητής σας). Κατεβάζετε το Mozilla Thunderbird και το λογισμικό κρυπτογράφησης PGP (Pretty Good Privacy). Η πρόταση των ακτιβιστών είναι να κατεβάσει κανείς το GnuPG (www.gnupg.org) με το οποίο δημιουργείτε τα δικά σας «κλειδιά» και «κλειδώνετε» τα mails σας. Πληροφορίες στο www.cryptography.org/getpgp.htm και -για instant messaging- στο www.jabbim.com. Τέλος, η συμβουλή των ειδικών είναι να έχουμε τον δικό μας e-mail server, δηλαδή να διατηρούμε διευθύνσεις e-mail σε ένα δικό μας domain. Κοστίζει ελάχιστα, πολλές φορές λιγότερο και από 1 ευρώ το μήνα.

6. Βάζουμε όρια! Αντί να πετάξουμε το παλιό μας λάπτοπ, το διαμορφώνουμε μόνοι ή με τη βοήθεια ειδικού και κατόπιν το χρησιμοποιούμε μόνο για συναλλαγές και αγορές. Ετσι, δεν θα στερηθούμε από τον «κανονικό» υπολογιστή μας τα διαδεδομένα εμπορικά λογισμικά και θα έχουμε και έναν εφεδρικό για αγορές και τραπεζικές συναλλαγές.

Της Άντζης Σαλταμπάση

Δημοσιεύτηκε στο περιοδικό Κ (τεύχος 546).

Πηγές:pentapostagma.gr – kathimerini.gr