Τα προσωπικά σου δεδομένα κινδυνεύουν!

Με αφορμή την κυκλοφορία των Windows 10 αλλά και τις συνεχείς διαρροές κυβερνητικών εγγράφων μυστικών υπηρεσιών διαφόρων χωρών (βλ. υπόθεση Snowden), γεννιέται η ανάγκη να ανοίξει ο διάλογος γύρω από τη σημερινή κατάσταση της ιδιωτικότητας και της ασφάλειας των επικοινωνιών και των δεδομένων μας. Φαίνεται πως οι μηχανισμοί που χρησιμοποιούνται στην κυβερνοπαρακολούθηση αγγίζουν ολοένα και μεγαλύτερο ποσοστό του κόσμου που χρησιμοποιεί τις ψηφιακές επικοινωνίες, ενώ έχει καταρρεύσει οποιαδήποτε υπόνοια εμπιστοσύνης στις εταιρείες που διαχειρίζονται τα δεδομένα μας για εμάς.

Το παράδειγμα των Windows 10 είναι ιδιαίτερα διαφωτιστικό για την φύση των προσωπικών δεδομένων που συλλέγονται από τις διάφορες εταιρείες, αλλά και το πώς γίνεται αυτό. Τα δεδομένα αυτά περιλαμβάνουν από το όνομα, το email, και τις προτιμήσεις του χρήστη μέχρι και τις αναζητήσεις του στο internet, στο τοπικό του σύστημα, την τοποθεσία που βρίσκεται ανά πάσα στιγμή αλλά και ακόμα πιο προσωπικές πληροφορίες, όπως τα αρχεία πολυμέσων που άνοιξε, και το τι έχει πει στο μικρόφωνο. Το πιο ενδιαφέρον κομμάτι στην διαδικασία αυτή, είναι ότι ο χρήστης συναινεί σε αυτήν μέσω μιας συμφωνίας (terms & conditions) όπου αναφερεται ότι ουσιαστικά σαν ανταλλαγμα, η microsoft θέλει να γνωρίζει τι σκεφτόμαστε, και μάλιστα να έχει την κυριότητα επί των δεδομένων αυτών.

Υπάρχουν 2 πτυχές στην εκμετάλλευση των προσωπικών μας δεδομένων:
Η πρώτη έχει να κάνει με την εμπορική τους χρήση, δηλαδή την κατασκευή ενός εξατομικευμένου προφίλ για κάθε χρήστη βάσει του οποίου χτίζονται στοχευμένα διαφημιστικά μοντέλα (π.χ. google ads), αλλά και την αξιοποίησή τους για την φαινομενική βελτίωση των παρεχόμενων υπηρεσιών. Το άτομο και οι προσωπικές του προτιμήσεις έχουν μετασχηματιστεί στο πλέον επικερδές εμπόρευμα του 21ου αιώνα. Το εμπόρευμα αυτό, δε, είτε διακινείται μεταξύ εταιρειών είτε τελικά γίνεται διαθέσιμο στις υπηρεσίες παρακολούθησης διαφόρων κρατών, αφού ένα συνεχώς μεταβαλλόμενο νομικό περιβάλλον υποχρεώνει τις εταιρείες να διαθέτουν τα δεδομένα τους όποτε μια κρατική υπηρεσία τα ζητήσει, με όλο και λιγότερους περιορισμούς.

Εδώ εισέρχεται και η δεύτερη πτυχή, η οποία κρίνεται και ως η σημαντικότερη. Είναι, πλέον, ευρέως γνωστό ότι καθένας απο εμάς έχει "φακελωθεί" στις εν λόγω υπηρεσίες. Η συλλογή δεδομένων και η κατασκευή αυτού του φακέλου γίνεται ανεξαρτήτως από την θέληση του χρήστη, είτε αυτός κρίνεται επικίνδυνος για το καθεστώς είτε όχι. Έτσι, υπάρχουν τεράστιες βάσεις δεδομένων στις οποίες έχουν αποθηκευτεί πληροφορίες για όλους μας, χωρίς να έχουμε τη δυνατότητα να ξέρουμε πού καταλήγουν αλλά και το πώς αξιοποιούνται. Ταυτόχρονα, οι εντεινόμενες προσπάθειες του κόσμου να έχει μια στοιχειώδη προστασία με τρόπους όπως η κρυπτογραφία έρχονται σε σύγκρουση με τους τεχνολογικούς περιορισμούς των υπηρεσιών πληροφοριών, ανοίγοντας το δρόμο για την ποινικοποίησή της.

Μπορεί με την ανάπτυξη της τεχνολογίας να έχουν πολλαπλασιαστεί οι μέθοδοι και οι τρόποι με τους οποίους εταιρείες/κράτη παρακολουθούν τον κόσμο, όμως παράλληλα έχουμε πιο πολλά (και πιο εύχρηστα) εργαλεία στα χέρια μας για να κρύβουμε τα δεδομένα μας και να διατηρούμε την ιδιωτικότητά μας.

Το βασικότερο εργαλείο είναι λογισμικό το οποίο μπορεί να εμπιστευεί ο χρήστης, όχι σε βάση μιας υπόσχεσης από τον παραγωγό του αλλά στη βάση της δυνατότητάς του να το ελέγξει ο ίδιος αν πραγματικά κάνει αυτό που υπόσχεται· σε αυτό βασίζεται η ιδέα του ελεύθερου λογισμικού (foss). Το foss είναι ένα σύνολο κανόνων που δεσμεύουν τους συγγραφείς κώδικα ώστε (εκτός των άλλων) να αναγκάζονται να διανείμουν τον πηγαίο κώδικα του προγράμματος τους μαζί με αυτό· έτσι ο χρήστης μπορεί να ελέγχει τι κάνει το κάθε πρόγραμμα που τρέχει στον υπολογιστή του. Αυτό είναι πολύ σημαντικό, καθώς ακόμα και αν πχ τα Windows σου δίνουν τη δυνατότητα να απενεργοποιήσεις κάποιες λειτουργίες που εισβάλλουν στην ιδιωτικότητά σου δεν έχεις κάποια εγγύηση ότι όντως το κάνουν. Παρέα με το ελεύθερο λογισμικό έρχονται και τα ανοικτά πρότυπα, των οποίων οι προδιαγραφές είναι ελεύθερα διαθέσιμες (πχ ogg αντί για mpeg, 7z αντί για rar).

Ακόμα όμως κι αν εμπιστευόμαστε το λογισμικό που τρέχουμε, δεν μπορούμε να εμπιστευτούμε το λογισμικό που τρέχουν άλλοι. Τέτοιοι "άλλοι" είναι εταιρείες όπως η google, το facebook, το dropbox, οι τηλεπικοινωνιακοί πάροχοι κλπ. Για να τους εμποδίσουμε λοιπόν να έχουν πρόσβαση στα δεδομένα μας πρέπει να τα κρυπτογραφούμε. Παρότι αυτό μπορεί να ακούγεται βγαλμένο από ταινία με hackers, η αλήθεια είναι ότι πλέον έχουμε όλα τα απαραίτητα εργαλεία στα χέρια μας:

-- GPG για να στέλνουμε mail.
-- OTR για chatting
-- SSL/TLS enabled εφαρμογές για πλοήγηση στο διαδίκτυο

Ακόμα όμως και αν δεν μπορούν να διαβάσουν τα δεδομένα μας, μπορεί να μη θέλουμε να έχουν τη δυνατότητα να τα συσχετίσουν με εμάς· μπορεί για παράδειγμα να μη θέλουμε να φαίνεται ποιες ιστοσελίδες επισκεφτήκαμε. Κι εδώ υπάρχουν αρκετά foss εργαλεία με το κυριότερο να είναι το TOR το οποίο χρησιμοποιεί ένα δίκτυο ενδιάμεσων κόμβων ώστε να κρύβει (σε ικανοποιητικό για το μέσο χρήστη βαθμό) τη δραστηριότητά μας.

Τα παραπάνω είναι τα βασικά για να έχουμε ασφάλεια στο διαδίκτυο. Μαζί με αυτά όμως καλό θα ήταν και οι ίδιοι να αλλάξουμε τη συμπεριφορά μας στο internet: να μη δίνουμε οι ίδιοι τα δεδομένα μας χωρίς σκέψη, να έχουμε ασφαλή (και μοναδικά για το κάθε site) passwords, να γνωρίζουμε ικανοποιητικά και να μην υπερεκτιμούμε τις δυνατότητες των εργαλείων μας, να προσπαθούμε να διαδίδουμε τη χρήση αυτών των εργαλείων. Είναι επίσης απαραίτητο να αγωνιστούμε και στην πραγματική ζωή για να διασφαλίσουμε το δικαίωμα στην ιδιωτικότητα, απαιτώντας η χρήση των εργαλείων ανωνυμίας/κρυπτογράφησης να είναι ελεύθερη και να μην ελέγχεται, αλλά κυρίαρχα να σταματήσει το καθεστώς της παγκόσμιας και συνεχούς παρακολούθησης.

<u>Τετάρτη 21/10:</u>

13:30 – Κατειλημμένος Παπασωτηρίου (στην κεντρική πλατεία)
Συζήτηση για το ελεύθερο λογισμικό και installfest

<u>Πέμπτη 22/10:</u>

13:30 - Νέα κτίρια ΗΜΜΥ, αίθουσα 003
Προβολή του CitizenFour

Θα ακολουθήσει cryptoparty στην **αίθουσα της Κοινότητας Ελεύθερου Λογισμικού ΕΜΠ** (στο υπόγειο παρκινγκ)

[Σε περίπτωση απεργίας, θα ανακοινωθούν νέες ημερομηνίες/ώρες στα site μας]

[*] Installfest & Cryptoparty: συλλογικές διαδικασίες στις οποίες εγκαθιστούμε διανομές ελεύθερου λογισμικού και εφαρμόζουμε τρόπους προστασίας της ιδιωτικότητάς μας αντίστοιχα, ανταλλάσσοντας γνώση και αμφισβητώντας τη σχέση μαθητή-δέκτη / καθηγητή-πομπού

https://kpapasotiriou.espivblogs.net/

https://foss.ntua.gr/

Κοινότητα Ελεύθερου Λογισμικού ΕΜΠ

Κατειλημμένος Παπασωτηρίου