Κρυπτογράφηση δεν σημαίνει ιδιωτικότητα: τι λένε τα μεταδεδομένα για εσάς

Το κρυπτογραφημένο περιεχόμενο και τα ορατά μεταδεδομένα είναι δύο διαφορετικά πράγματα. Όταν μια υπηρεσία μιλάει για «κρυπτογράφηση από άκρο σε άκρο», λέει μόνο τη μισή ιστορία.

Το λουκέτο που δεν προστατεύει τα πάντα

Ένα μεγάλο μέρος των σημερινών υπηρεσιών ανταλλαγής μηνυμάτων διαφημίζουν κρυπτογράφηση από άκρο σε άκρο. Και είναι αλήθεια: το περιεχόμενο των μηνυμάτων ταξιδεύει κρυπτογραφημένο, έτσι ώστε κανείς στη διαδρομή – ούτε καν ο πάροχος της υπηρεσίας – να μην μπορεί να διαβάσει το κείμενο ενώ αυτό μεταφέρεται. Μέχρι εδώ, η δήλωση είναι ακριβής.

Το πρόβλημα είναι ότι το περιεχόμενο είναι μόνο ένα μέρος της ιστορίας. Παρόλο που κανείς δεν μπορεί να διαβάσει τι λέτε, η υπηρεσία γνωρίζει άλλα πράγματα με πολύ υψηλή ακρίβεια: με ποιον μιλάτε, τι ώρα, πόσο συχνά, από ποια περίπου τοποθεσία, σε ποια συσκευή, πόσα μηνύματα στέλνετε και πόσα λαμβάνετε, πόσα αρχεία μοιράζεστε. Όλα αυτά ονομάζονται μεταδεδομένα. Και τα μεταδεδομένα, σε πολλές περιπτώσεις, λένε σχεδόν τόσα όσα και το ίδιο το μήνυμα.

Τι αποκαλύπτουν τα μεταδεδομένα

Δεν χρειάζεται να διαβάσει κανείς ένα μήνυμα για να γνωρίζει πολλά πράγματα. Εάν ένα άτομο καλεί ή γράφει σε έναν ογκολόγο κάθε Τρίτη πρωί στις εννέα η ώρα για έξι μήνες, δεν είναι απαραίτητο να ακούσει τη συνομιλία για να υποψιαστεί τι συμβαίνει. Εάν δύο άτομα ανταλλάσσουν εκατό μηνύματα την ημέρα και ξαφνικά σταματήσουν, δεν χρειάζεται να διαβάσετε κανένα για να καταλάβετε τι συνέβη. Εάν ένας φοροτεχνικός λάβει είκοσι μηνύματα στη σειρά από τον ίδιο πελάτη το βράδυ πριν από το κλείσιμο του τριμήνου, το μοτίβο μιλάει από μόνο του.

Τα μεταδεδομένα αποκαλύπτουν μοτίβα συμπεριφοράς: ποιος σχετίζεται με ποιον, ποια είναι τα προγράμματα κάθε ατόμου, πότε είναι ξύπνιο, πότε κοιμάται, πότε ταξιδεύει, ποιοι πελάτες είναι οι πιο ενεργοί, ποιες επαγγελματικές σχέσεις είναι οι πιο έντονες. Ένας διακομιστής που συλλέγει μεταδεδομένα μπορεί να δημιουργήσει ένα λεπτομερές προφίλ της προσωπικής και επαγγελματικής ζωής οποιουδήποτε χρήστη χωρίς να έχει διαβάσει ποτέ ούτε μια λέξη από αυτά που γράφει.

Υπάρχει ένα ιστορικό παράδειγμα που το απεικονίζει αυτό με σκληρότητα. Ο πρώην διευθυντής της NSA, Michael Hayden, το διατύπωσε ευθέως το 2014: *«We kill people based on metadata»*. Η δήλωση αναφερόταν σε αμερικανικές στρατιωτικές επιχειρήσεις εναντίον στόχων που εντοπίστηκαν αποκλειστικά βάσει των επικοινωνιακών τους μοτίβων. Ούτε ένα μήνυμα που διαβάστηκε. Μόνο το γράφημα των επαφών και τα ωράρια.

Το γεγονός ότι μια υπηρεσία συλλέγει μεταδεδομένα δεν σημαίνει απαραίτητα ότι θα τα χρησιμοποιήσει εναντίον των χρηστών της. Σημαίνει ότι έχει την ικανότητα να το κάνει και ότι ένας τρίτος με πρόσβαση σε αυτά

τα δεδομένα – μέσω δικαστικής εντολής, μέσω παραβίασης ασφάλειας ή μέσω πώλησης σε τρίτους, εάν το επιτρέπουν οι όροι της υπηρεσίας – την έχει επίσης.

Η πρόσβαση στο βιβλίο επαφών

Ένα άλλο διάνυσμα που περνά σχεδόν απαρατήρητο: η λίστα επαφών. Ένα μεγάλο μέρος των υπηρεσιών ανταλλαγής μηνυμάτων ζητά πρόσβαση στο βιβλίο επαφών του τηλεφώνου κατά την εγγραφή. Ανεβάζουν όλους τους αριθμούς στον διακομιστή τους για να δείξουν ποιος άλλος χρησιμοποιεί την υπηρεσία. Από εκείνη τη στιγμή, η εταιρεία έχει έναν πλήρη χάρτη των σχέσεων του χρήστη, ακόμη και αν αυτός δεν έχει γράψει ποτέ ούτε ένα μήνυμα σε κανέναν.

Για έναν επαγγελματία που δεσμεύεται από το επαγγελματικό απόρρητο – δικηγόρο, γιατρό, ψυχολόγο, σύμβουλο – αυτό το βιβλίο επαφών περιέχει πελάτες. Εάν το βιβλίο επαφών έχει μεταφορτωθεί σε διακομιστή τρίτου μέρους, τα ονόματα των πελατών βρίσκονται σε μια υποδομή της οποίας τη δικαιοδοσία και τις πολιτικές ο επαγγελματίας δεν ελέγχει. Το επαγγελματικό απόρρητο δεν παραβιάζεται την ημέρα που κάποιος διαρρέει μια συνομιλία: παραβιάστηκε πολύ νωρίτερα, τη στιγμή της συναίνεσης για τη μεταφόρτωση.

Η διαφορά μεταξύ κρυπτογράφησης και μη συλλογής

Κρυπτογράφηση σημαίνει προστασία του περιεχομένου. Ιδιωτικότητα σημαίνει να μην συλλέγεις ό,τι δεν είναι απαραίτητο. Είναι διαφορετικά πράγματα και η διαφορά είναι λειτουργικά καθοριστική. Μια υπηρεσία μπορεί να κρυπτογραφεί τέλεια όλα τα μηνύματα και ταυτόχρονα να γνωρίζει σχεδόν τα πάντα για τους χρήστες της μέσω των μεταδεδομένων. Και τα δύο είναι απόλυτα συμβατά. Στην πραγματικότητα, είναι το κυρίαρχο επιχειρηματικό μοντέλο στον κλάδο.

Η σωστή ερώτηση για την αξιολόγηση της πραγματικής ιδιωτικότητας μιας υπηρεσίας δεν είναι *«κρυπτογραφεί το περιεχόμενο;»*. Αυτή η ερώτηση έχει απαντηθεί εδώ και χρόνια. Η σωστή ερώτηση είναι: *«ποια μεταδεδομένα παράγει και πού αποθηκεύονται;»*. Και πάνω απ' όλα: *«ποια μεταδεδομένα δεν χρειάζεται να παράγει;»*.

Μια αρχιτεκτονική που ελαχιστοποιεί τα μεταδεδομένα μέσω του σχεδιασμού (privacy by design) – όχι μέσω υπόσχεσης, όχι μέσω εσωτερικής πολιτικής – είναι δομικά πιο ιδιωτική από μια αρχιτεκτονική που τα συλλέγει και τα κρυπτογραφεί. Επειδή τα δεδομένα που δεν υπάρχουν δεν μπορούν να διαρρεύσουν, ούτε να πωληθούν, ούτε να παραδοθούν σε δικαστική εντολή ούτε να χαθούν σε μια παραβίαση ασφάλειας.

Για τον επαγγελματία αναγνώστη

Εάν η επαγγελματική σας δραστηριότητα περιλαμβάνει απόρρητο, εμπιστευτικότητα ή απλώς σεβασμό στις πληροφορίες τρίτων, αξίζει να θέσετε τις ερωτήσεις με αυτή τη σειρά:

1. Η εφαρμογή που χρησιμοποιώ για την επικοινωνία κρυπτογραφεί το περιεχόμενο; (Πιθανώς ναι.)
2. Κρυπτογραφεί τα μεταδεδομένα; (Πιθανώς όχι.)
3. Παράγει μεταδεδομένα που *δεν χρειάζεται* για να λειτουργήσει; (Σχεδόν σίγουρα ναι.)
4. Πού αποθηκεύονται αυτά τα μεταδεδομένα και υπό ποια δικαιοδοσία; (Πιθανώς εκτός του Ευρωπαϊκού Οικονομικού Χώρου.)
5. Γνωρίζει ο πελάτης ή ο ασθενής μου ότι τα δεδομένα του βρίσκονται εκεί;

Η τελευταία ερώτηση είναι η δυσάρεστη. Γιατί η ειλικρινής απάντηση στις περισσότερες περιπτώσεις είναι: όχι.

Αυτό το άρθρο είναι το πρώτο μιας σειράς για την πραγματική λειτουργία των επαγγελματικών εργαλείων επικοινωνίας. Τα επόμενα τεύχη θα εξετάσουν τη συμμόρφωση με το GDPR στα μηνύματα και την έννοια του επαγγελματικού απορρήτου στην ψηφιακή εποχή.

Πηγές και περαιτέρω μελέτη

- Hayden, M. – Δήλωση στο Πανεπιστήμιο Johns Hopkins, 2014 («We kill people based on metadata»). Διαθέσιμα δημόσια απομαγνητοφωνημένα κείμενα.
- GDPR (Κανονισμός ΕΕ 2016/679), άρθρα 4 και 5 – ορισμός προσωπικών δεδομένων και αρχές επεξεργασίας (τα μεταδεδομένα είναι προσωπικά δεδομένα).
- ΕΕΠΔ και ΕΣΠΔ – γνωμοδοτήσεις σχετικά με την επεξεργασία δεδομένων κίνησης και μεταδεδομένων στις ηλεκτρονικές επικοινωνίες (οδηγία ePrivacy).

← ΠροηγούμενοΜια σύντομη ιστορία του βουλοκέριουΕπόμενο →Το επαγγελματικό απόρρητο στην ψηφιακή εποχή

Πρόσφατα αναγνώσματα

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Πάρτε αυτό το άρθρο μαζί σας όπου το χρειάζεστε.

↓ Markdown ↓ Απλό κείμενο ↓ PDF

Το αρχείο θα ληφθεί στη συσκευή σας. Από εκεί μπορείτε να το αποθηκεύσετε, να το εισαγάγετε στο Solo2 ή να το μοιραστείτε όπου θέλετε. Το Cuadernos δεν αποφασίζει τον προορισμό για εσάς.

Σφραγίδα από βουλοκέρι · SHA-256
cafb75bc09f9e090989902797c83be6d673572bdb18881e45e2c59cad082b901

Cuadernos Lacre · Μια έκδοση της Menzuri Gestión S.L. ·
γραμμένη από τον R.Eugenio · επιμελημένη από την ομάδα του Solo2.