Ανάλυση · 16 Μαΐου 2026

← Προηγούμενο·Επόμενο →

Όταν δεν υπάρχει κανείς στη μέση

Η κρυπτογράφηση αυτού που περνάει από έναν διακομιστή προστατεύει το περιεχόμενο. Η απουσία διακομιστή στη μέση εξαλείφει το ερώτημα. Δεν είναι το ίδιο.

Δύο άτομα, μία συζήτηση

Όταν δύο άνθρωποι μιλούν πρόσωπο με πρόσωπο σε ένα δωμάτιο, κανείς δεν χρειάζεται να υποσχεθεί ότι δεν άκουσε τίποτα. Δεν άκουσε επειδή δεν ήταν εκεί. Όταν δύο άτομα περνούν ένα χαρτί από το ένα χέρι στο άλλο, κανείς στη μέση δεν χρειάζεται να ορκιστεί ότι δεν το διάβασε. Δεν υπάρχει κανείς στη μέση.

Τα περισσότερα πράγματα στην καθημερινή ζωή λειτουργούν έτσι. Δεν υπογράφουμε συμφωνίες εμπιστευτικότητας με τον αέρα που μεταδίδει τη φωνή μας, ούτε με το χαρτί που κρατάμε. Η ιδιωτικότητα της συζήτησης δεν στηρίζεται στην υπόσχεση ενός μεσάζοντα, επειδή δεν υπάρχει μεσάζων. Αυτός είναι ένας από τους ισχυρότερους τρόπους για να είσαι ιδιωτικός: όχι επειδή κάτι ή κάποιος συμπεριφέρεται καλά, αλλά επειδή δεν υπάρχει κάτι ή κάποιος.

Όταν η συζήτηση μεταφέρεται σε ένα ψηφιακό κανάλι, αυτό αλλάζει από προεπιλογή. Το συνηθισμένο μοντέλο είναι το εξής: δύο άτομα συνδέονται σε έναν διακομιστή, ο διακομιστής λαμβάνει το μήνυμα, το κρυπτογραφεί ή το αποθηκεύει κρυπτογραφημένο και το παραδίδει στον παραλήπτη. Ο διακομιστής είναι στη μέση. Ο διακομιστής μπορεί να είναι ειλικρινής. Μπορεί να ελέγχεται. Μπορεί να λειτουργεί σε ευνοϊκή δικαιοδοσία και υπό αυστηρή πολιτική απορρήτου. Όλα αυτά μπορεί να είναι αληθινά. Αλλά ο διακομιστής είναι στη μέση.

Η διαφορά μεταξύ κρυπτογράφησης και μη συλλογής (δεύτερο μέρος)

Σε προηγούμενο άρθρο αυτής της ίδιας σειράς υποστηρίζουμε ότι η κρυπτογράφηση του περιεχομένου και η μη συλλογή μεταδεδομένων δεν είναι το ίδιο. Υπάρχει ένα ακόμη βήμα που πρέπει να διατυπωθεί με σαφήνεια: η κρυπτογράφηση αυτού που περνάει από έναν διακομιστή και η απουσία διακομιστή επίσης δεν είναι το ίδιο.

Το πρώτο μοντέλο —διακομιστής στη μέση, κρυπτογραφημένο περιεχόμενο— προστατεύει το περιεχόμενο από τον διαχειριστή του διακομιστή, από το προσωπικό συντήρησής του, από έναν εξωτερικό επιτιθέμενο που παραβιάζει το σύστημα. Και αυτό είναι σημαντικό. Αλλά δεν εξαλείφει τον διακομιστή. Ο διακομιστής είναι ακόμα εκεί. Εξακολουθεί να επεξεργάζεται μεταδεδομένα. Εξακολουθεί να είναι ένα σημείο που μπορεί να δεχθεί δικαστική εντολή, νόμιμη παρέμβαση, πολιτική πίεση ή παραβίαση ασφαλείας. Εξακολουθεί να είναι ένα σημείο που απαιτεί την εναπόθεση εμπιστοσύνης σε κάποιον.

Το δεύτερο μοντέλο —να μην υπάρχει διακομιστής μεταξύ των δύο άκρων— δεν προστατεύει καλύτερα το κρυπτογραφημένο περιεχόμενο: αν η κρυπτογραφία είναι ισχυρή, το περιεχόμενο είναι προστατευμένο και στις δύο περιπτώσεις. Αυτό που αλλάζει δεν είναι το περιεχόμενο. Αυτό που αλλάζει είναι ότι η ερώτηση *«τι γίνεται με τον διακομιστή;»* παύει να έχει αντικείμενο, επειδή δεν υπάρχει διακομιστής για να ρωτήσουμε.

Εμπιστοσύνη, απουσία, και η διαφορά μεταξύ τους

Η εμπιστοσύνη μπορεί να είναι καλά τοποθετημένη. Τίμιες εταιρείες υπάρχουν. Αυστηροί ελεγκτές υπάρχουν. Νομοθεσίες ευνοϊκές προς τον χρήστη υπάρχουν. Σοβαρές υπηρεσίες που συμμορφώνονται σχολαστικά με όλα τα παραπάνω υπάρχουν. Η εμπιστοσύνη, όταν παραχωρείται σε έναν πάροχο που την αξίζει, δεν είναι κακή διευθέτηση.

Αλλά η εμπιστοσύνη, όσο ισχυρή κι αν είναι, παραμένει εμπιστοσύνη. Είναι μια κοινωνική λύση, όχι μια τεχνική λύση. Μια εταιρεία μπορεί να αλλάξει χέρια. Μια δικαιοδοσία μπορεί να αλλάξει κυβέρνηση. Μια δικαστική εντολή μπορεί να έρθει αύριο. Μια νέα ευπάθεια μπορεί να ανακαλυφθεί τον επόμενο μήνα. Τίποτα από αυτά δεν συμβαίνει από κακή πίστη. Συμβαίνει επειδή ο πάροχος υπάρχει, και ό,τι υπάρχει υπόκειται στα ενδεχόμενα του κόσμου.

Η απουσία ενός παρόχου δεν υπόκειται σε αυτά τα ίδια ενδεχόμενα. Μια δικαστική εντολή δεν μπορεί να ζητήσει δεδομένα από έναν διακομιστή που δεν υπάρχει. Ένας επιτιθέμενος δεν μπορεί να παραβιάσει έναν διακομιστή που δεν υπάρχει. Μια αλλαγή στην πολιτική μιας εταιρείας δεν μπορεί να επηρεάσει δεδομένα που αυτή η εταιρεία δεν είχε ποτέ. Η φράση κλειδί είναι απλή: τα δεδομένα που δεν υπάρχουν δεν μπορούν να χαθούν.

Σχετικά με το θεμιτό επιχείρημα από την πλευρά του διακομιστή

Όποιος προσφέρει μια υπηρεσία επαγγελματικών μηνυμάτων με διακομιστή στη μέση συνήθως διατυπώνει τρία απολύτως έγκυρα επιχειρήματα. Πρώτον, ότι ο διακομιστής είναι απαραίτητος για να εγγυηθεί την παράδοση όταν ο παραλήπτης είναι εκτός σύνδεσης. Δεύτερον, ότι η κρυπτογράφηση του περιεχομένου είναι ισχυρή και επομένως ο πάροχος δεν μπορεί να το διαβάσει. Τρίτον, ότι η υπηρεσία συμμορφώνεται με την ευρωπαϊκή νομοθεσία και ότι τα δεδομένα προστατεύονται από τον νόμο.

Και τα τρία επιχειρήματα είναι αληθινά. Κανένα δεν αλλάζει τη φύση του ζητήματος. Είναι αλήθεια ότι ένας διακομιστής επιτρέπει την αποθήκευση μηνυμάτων για ετεροχρονισμένη παράδοση· είναι επίσης αλήθεια ότι η ετεροχρονισμένη παράδοση μπορεί να λυθεί με άλλον τρόπο, μέσω πρωτοκόλλων άμεσης επικοινωνίας μεταξύ συσκευών, βελτιωμένων εδώ και δεκαετίες και λειτουργικών σήμερα. Είναι αλήθεια ότι η κρυπτογράφηση του περιεχομένου κατά τη μεταφορά είναι ισχυρή στις σοβαρές υπηρεσίες. Και είναι αλήθεια ότι η ευρωπαϊκή νομοθεσία προστατεύει τους χρήστες περισσότερο από εκείνη πολλών άλλων τόπων.

Το ζήτημα δεν είναι αν οι υπηρεσίες με διακομιστή στη μέση είναι νόμιμες, ούτε αν είναι ασφαλείς, ούτε αν προστατεύουν το περιεχόμενο. Μπορεί να είναι, είναι νόμιμες, και είναι συνήθως ασφαλείς. Το ζήτημα είναι ότι το να έχεις έναν διακομιστή στη μέση είναι μια αρχιτεκτονική επιλογή, όχι μια τεχνική επιβολή. Και κάθε επιλογή έχει συνέπειες. Μια αρχιτεκτονική με διακομιστή στη μέση δημιουργεί απαραίτητα έναν παράγοντα στον οποίο πρέπει να δείξουμε εμπιστοσύνη. Μια αρχιτεκτονική χωρίς διακομιστή στη μέση όχι.

Τι λέει ο νόμος και τι κάνει η αρχιτεκτονική

Ο ΓΚΠΔ δεν απαιτεί ένα συγκεκριμένο αρχιτεκτονικό μοντέλο. Απαιτεί αποτελέσματα: ελαχιστοποίηση δεδομένων, περιορισμό σκοπού, προστασία από τον σχεδιασμό και εξ ορισμού, ικανότητα απόδειξης συμμόρφωσης. Μια υπηρεσία με διακομιστή στη μέση μπορεί να πληροί όλες αυτές τις απαιτήσεις. Μια υπηρεσία χωρίς διακομιστή στη μέση πληροί αρκετές από αυτές εκ κατασκευής, όχι κατόπιν δήλωσης. Η απόλυτη ελαχιστοποίηση —να μην συλλέγεται τίποτα που δεν είναι απολύτως απαραίτητο για την παράδοση του μηνύματος— είναι τετριμμένη όταν δεν υπάρχει διακομιστής που να μπορεί να συλλέξει κάτι.

Για μη ευαίσθητες καθημερινές χρήσεις, μια αρχιτεκτονική με διακομιστή είναι απολύτως λογική και η εμπιστοσύνη σε έναν σοβαρό πάροχο είναι μια έγκυρη διευθέτηση. Για τις άλλες χρήσεις —αυτές που φέρουν θεσμοθετημένο επαγγελματικό απόρρητο, αυτές που συνεπάγονται δεοντολογική ευθύνη, αυτές που αγγίζουν ιδιαίτερα ευαίσθητες πληροφορίες— η απουσία ενός σημείου εμπιστοσύνης δεν είναι πολυτέλεια, είναι δομικό πλεονέκτημα.

Για τον επαγγελματία αναγνώστη

Τα ερωτήματα που πρέπει να θέσουμε μπροστά σε μια επαγγελματική υπηρεσία επικοινωνίας, ήδη γνωστά από προηγούμενα άρθρα αυτής της ίδιας σειράς, ολοκληρώνονται με ένα μόνο ακόμη αρχιτεκτονικό ερώτημα:

1. Κρυπτογραφεί το περιεχόμενο κατά τη μεταφορά; (Πιθανότατα ναι.)
2. Δημιουργεί και αποθηκεύει μεταδεδομένα σχετικά με το σε ποιον μιλάω και πότε; (Πιθανότατα ναι.)
3. Υπάρχει διακομιστής στη διαδρομή μεταξύ της συσκευής μου και του παραλήπτη;
4. Αν υπάρχει: ποιος τον διαχειρίζεται, σε ποια δικαιοδοσία, και τι θα έπρεπε να συμβεί για να παραδώσει δεδομένα για μένα;
5. Αν δεν υπάρχει: τα προηγούμενα ερωτήματα δεν έχουν αντικείμενο.

Η διαφορά μεταξύ των δύο κατηγοριών δεν είναι διαφορά βαθμού, αλλά είδους. Όταν έρθει η ώρα να το εξηγήσετε σε έναν πελάτη, σε έναν ασθενή ή σε έναν συνάδελφο, η πιο ειλικρινής διατύπωση είναι και η πιο απλή: στη μία υπάρχει κάποιος στη μέση· στην άλλη, όχι.

Αυτό το άρθρο κλείνει τον αρχικό κύκλο του Cuadernos Lacre. Μετά τη συζήτηση για την κρυπτογράφηση, τα μεταδεδομένα και το επαγγελματικό απόρρητο, ολοκληρώνουμε την αρχιτεκτονική εικόνα: η κρυπτογράφηση του περιεχομένου και η απουσία διακομιστή στη μέση είναι διαφορετικά πράγματα. Και τα δύο μπορεί να είναι νόμιμα· μόνο το ένα εξαλείφει το σημείο εμπιστοσύνης.

Πηγές και περαιτέρω μελέτη

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Θεμελιώδες κείμενο της αρχής σύμφωνα με την οποία οι εγγυήσεις ενός συστήματος πρέπει να υλοποιούνται στα άκρα, όχι στο ενδιάμεσο κανάλι.
- Κανονισμός (ΕΕ) 2016/679, άρθ. 25 — προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού.
- Κανονισμός (ΕΕ) 2016/679, άρθ. 5.1.γ — αρχή της ελαχιστοποίησης των δεδομένων.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Κεφάλαια για αρχιτεκτονικές που ελαχιστοποιούν τη συλλογή εκ κατασκευής.

← ΠροηγούμενοGDPR και επαγγελματική ανταλλαγή μηνυμάτων: γιατί οι περισσότεροι παραβιάζουν τους κανόνες χωρίς να το γνωρίζουνΕπόμενο →CUADERNOS_LIST_SCHREMS_TITLE

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
b1464b8363191ce447e4cd4951559f9ea3ce3410c8468d28a75e721238674d90

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

Αυτός ο ιστότοπος δεν χρησιμοποιεί cookies και δεν φορτώνει πόρους από τρίτους. Χρησιμοποιεί έναν ανώνυμο μετρητή επισκέψεων με δική μας φιλοξενία (Umami, στον ευρωπαϊκό μας διακομιστή) και το ελάχιστο JavaScript που απαιτείται για την προτίμησή σας σε φωτεινό/σκοτεινό θέμα. Χωρίς ιχνηλάτες, χωρίς προφίλ, χωρίς κοινή χρήση δεδομένων. Αν θέλετε να μας ακολουθήσετε: RSS.