Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΥΔΕ ΕΤΑΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

2.1.1 Απαιτήσεις ασφάλειας συστήματος

"**Healthier Doc:** ολοκληρωμένος, ευφυής βοηθός υποστήριξης διαχείρισης υγείας, επικοινωνίας και εξ αποστάσεως παρακολούθησης"
(Τ2ΕΔΚ-04015)

Ομάδα Εργασίας
Δημητρόπουλος Αλέξιος
Δημητράντζου Αναστασία
Σεϊντής Κωνσταντίνος
Φράγκος Κωνσταντίνος

Πίνακας περιεχομένων

Περιγραφή στόχων και περιεχομένου παραδοτέου

Το παρόν έγγραφο αποτελεί το υποπαραδοτέο 2.1.1 " Απαιτήσεις ασφάλειας συστήματος" και συμπληρώνει το παραδοτέο 2.1 «Έγγραφο προδιαγραφής μη λειτουργικών απαιτήσεων. Περιέχει τις τρέχουσες κατευθυντήριες σχετικά με την ασφάλεια του σχεδιαζόμενου συστήματος. Καθώς η εξασφάλιση της ασφαλείας της εφαρμογής και ειδικότερα των δεδομένων των χρηστών αποτελούν κεντρικό θέμα για την εφαρμογή, λόγω και του αντικειμένου της, κρίθηκε απαραίτητο να καταγραφούν ξεχωριστά και να μελετηθούν σε μεγαλύτερο βάθος.

Ο έγκαιρος προσδιορισμός των πιθανών κινδύνων σε σχέση με την ασφάλεια και η ενσωμάτωση πρακτικών αντιμετώπισής τους ήδη από τον αρχικό σχεδιασμό (security by design) αποτελεί καλή πρακτική που θα επιτρέψει την ανάπτυξη ενός προϊόντος που θα καλύπτει τις προσδοκίες των χρηστών μας σε αυτόν τον τομέα. Εξ άλλου η έγκαιρη ενσωμάτωση και ο διαρκής έλεγχος των τεχνικών ασφαλείας της πλατφόρμας αποτελεί κλειδί για τη μείωση των τρωτών σημείων αλλά και ταυτόχρονα τον περιορισμό του χρόνου ανάπτυξης.

Όπως είναι αναμενόμενο, οι απαιτήσεις που θα καταγραφούν εδώ μπορεί να διαφοροποιηθούν κατά την υλοποίηση ανάλογα με τις τεχνολογικές εξελίξεις και τυχόν νέες απειλές που θα εμφανιστούν, καθώς μιλάμε για ένα τομέα με ραγδαία ανάπτυξη και νέες εκδόσεις βασικών εργαλείων και πλατφόρμων μπορεί να αλλάξουν σε σημαντικό βαθμό το τοπίο. Παρ' όλα αυτά οι βασικές αρχές που περιγράφονται, κατά βάση θα μείνουν σταθερές και θα συνεχίσουν να αποτελούν κεντρικό κομμάτι της στρατηγικής του έργου για την αντιμετώπιση απειλών.

Το παρόν έγγραφο δεν θα επικεντρωθεί σε θέματα ιδιωτικότητας και προστασίας δεδομένων που αφορούν ρυθμίσεις και επιλογές που δίνονται στο χρήστη, καθώς αυτές οι παράμετροι έχουν καλυφθεί στα σχετικά παραδοτέα, εκτός από μεμονωμένες αναφορές σε περιπτώσεις που υπάρχει άμεση συσχέτιση με κάποιο συγκεκριμένο θέμα ασφαλείας που εξετάζεται.

Καθιερωμένες πρακτικές και πρότυπα

Σαν πρώτο βήμα για τον καθορισμό των απαιτήσεων ασφαλείας, καθορίζονται διαδεδομένα πρότυπα με τα οποία η πλατφόρμα θα πρέπει επίσημα ή ανεπίσημα να συμμορφώνεται. Αυτά αποτελούν τα:

- IEC 62304
- ISO27001
- SOC2 Type 2

Επίσης, θα υπάρχει ευθυγράμμιση με τις οδηγίες του Open Web Application Security Project (OWASP), το οποίο είναι μια διαδικτυακή κοινότητα που παράγει ελεύθερα διαθέσιμα άρθρα, μεθοδολογίες, τεκμηρίωση, εργαλεία και τεχνολογίες στον τομέα της ασφάλειας εφαρμογών Ιστού.

Η καθιέρωση καλών πρακτικών και κυρίως ενός συστήματος διασφάλισης ποιότητας και ελέγχου θα βοηθήσει την αποφυγή κινδύνων που προκύπτουν λόγω κακής διαμόρφωσης/ υλοποίησης του

συστήματος ασφαλείας, που αποτελεί μια από τις πιο διαδεδομένες αιτίες κενών ασφαλείας. Κάθε συστατικό μέρος του συστήματος θα πρέπει να έχει ελεγχθεί σε βάθος και να έχει υλοποιηθεί και παραμετροποιηθεί σωστά, αλλά και να υπάρχει συντονισμός στην υλοποίηση, επικοινωνία και συντήρηση των επιμέρους μερών, προκειμένου να μην προκληθούν τεχνικές αστοχίες λόγω μη συμβατών εκδόσεων, ρυθμίσεων κτλ. Σε αυτή την κατεύθυνση σημαντικό επίσης είναι να διατηρούνται στο ελάχιστο τα συστατικά μέρη της πλατφόρμας και κυρίως στοιχεία όπως βιβλιοθήκες που χρησιμοποιούνται, 3rd party platforms κτλ. Η λιτότητα στο σχεδιασμό και την υλοποίηση αποτελεί καλή πρακτική σε ότι αφορά την ασφάλεια. Καθώς στοιχεία όπως libraries, frameworks κτλ έχουν σε πολλές περιπτώσεις ουσιαστικά τα ίδια δικαιώματα με την εφαρμογή κενά ασφαλείας σε αυτά αποτελούν κίνδυνο για την ακεραιότητα της ίδιας της εφαρμογής. Σε αυτή την κατεύθυνση θα γίνεται τακτική επαναξιολόγηση της ασφάλειας των στοιχείων αυτών και του βαθμού κατά τον οποίο παραμένουν up to date και συντηρούνται αποτελεσματικά.

Η κρυπτογράφηση, το κλείδωμα αρχείων και αρχείων, η ακεραιότητα, οι μηχανισμοί κωδικών πρόσβασης καθώς και η ιχνηλασιμότητα των συστημάτων απόκτησης δεδομένων θα πρέπει να ενημερώνεται συνεχώς ώστε να αποτρέπεται η δυνατότητα αποκωδικοποίησης του συστήματος διαχείρισης δεδομένων σε οποιοδήποτε επίπεδο και διάδοσης προσωπικών πληροφοριών.

Τα διάφορα μέρη της εφαρμογής, θα πρέπει να είναι κατά κανόνα ανεξάρτητα και να επικοινωνούν μόνο με προκαθορισμένους και καλά ορισμένους και προστατευμένους τρόπους (πχ ασφαλές API).

Για καλύτερο έλεγχο οι διαφορετικές εκδόσεις της πλατφόρμας (development, testing, production) θα πρέπει να έχουν πανομοιότυπες ρυθμίσεις. Τέλος, το σύνολο των σφαλμάτων και εξαιρέσεων θα αναγνωρίζονται και θα γίνονται handled από το σύστημα στο σημείο που προέκυψαν.

Τέλος θα καθορισθούν διαδικασίες διαρκούς ελέγχου ασφαλείας και αναβάθμισης των σχετικών μεθόδων, κατά τη διάρκεια. αλλά και μετά το τέλος του έργου.

Κίνδυνοι που συνδέονται με τα δεδομένα και την ιδιωτικότητα

Είναι σύνηθες εφαρμογές και APIs να μην προστατεύουν σωστά ευαίσθητα δεδομένα μα αποτέλεσμα αυτά να τεθούν σε κίνδυνο καθώς δεν έχουν χωρίς πρόσθετη προστασία, όπως κρυπτογράφηση κατά την αποθήκευση ή κατά τη μεταφορά. Η πλατφόρμα θα σχεδιαστεί ώστε να προστατεύει τα δεδομένα κατά τόσο στον server όσο και κατά την ανταλλαγή παίρνοντας ειδικές προφυλάξεις ανάλογα και με το κάθε χρησιμοποιούμενο πρόγραμμα περιήγησης.

Τα ευαίσθητα δεδομένα θα πρέπει να είναι κρυπτογραφημένα τόσο στον server όσο και κατά τη μεταφορά τους και θα υπάρχει αυστηρός έλεγχος μέσα από το σύστημα ταυτοποίησης σε σχέση με το ποιος θα έχει το δικαίωμα πρόσβασης σε αυτά. Επίσης, δεν θα αποθηκεύονται τοπικά στον browser και θα σβήνονται από τη μνήμη αμέσως μετά τη χρήση τους (πχ απενεργοποίηση δυνατότητας caching). Κατά τη μεταφορά θα χρησιμοποιηθούν ασφαλή πρωτόκολλα όπως το TLS και το HTTPs

Η ακεραιότητα των βάσεων δεδομένων θα διασφαλίζεται με περιοδική – αυτοματοποιημένη - επαλήθευση των δεδομένων που υπάρχουν σε αυτές.

Ιδιαίτερα στον κλάδο του mHealth υπάρχει αυξημένη ανησυχία σχετικά με σχετικά με την κατάλληλη επεξεργασία των δεδομένων που συλλέγονται μέσω των εφαρμογών. Στη συγκεκριμένη περίπτωση πρέπει να δοθεί προσοχή και στο σκέλος που αφορά τη σύνδεση με 3rd party εφαρμογές και συσκευές. Και εδώ όλες οι επικοινωνίες θα πρέπει να είναι end-to-end κρυπτογραφημένες. Επίσης, σαν γενικός κανόνας, τα όποια προσωπικά δεδομένα θα πρέπει να εμφανίζονται στην οθόνη του χρήστη μόνο ύστερα από εντολή του (να μην εμφανίζονται περισσότερα ή διαφορετικά δεδομένα από αυτά που ζήτησε, προκειμένου να αποφευχθεί να γίνουν ορατά σε τρίτους ακούσια).

Επίσης, δεν θα πρέπει να αποθηκεύονται by default τοπικά στις συσκευές ιατρών και ασθενών από όπου μπορούν πιο εύκολα να ανακτηθούν από τρίτους που τυχόν έχουν πρόσβαση στη συσκευή. Σαν αρχή όλα τα δεδομένα πρέπει να αποθηκεύονται μόνο για το διάστημα που είναι απολύτως απαραίτητα και μόνο μέχρι να ολοκληρωθεί ο σκοπός για τον οποίο εγγράφηκαν. Σκοπός δεν είναι απλά να καλυφθούν οι νομικές απαιτήσεις ιδιωτικότητας και ασφάλειας (πχ GDPR) αλλά να προσφέρουμε ένα απόλυτα ασφαλές σύστημα, με πλήρη διαφάνεια και έλεγχο από τον χρήστη σε σχέση με τα δεδομένα του, το οποίο θα βοηθήσει στην εμπέδωση εμπιστοσύνης κατά τη χρήση της πλατφόρμας.

Προφύλαξη δεδομένων

Θα πρέπει να υπάρχει αυτοματοποιημένη διαδικασία τακτικής λήψης backup και φύλαξής του σε ασφαλή τοποθεσία έτσι ώστε να είναι πάντα δυνατή η ανάκτηση των δεδομένων του χρήστη. Επίσης, ο χρήστης θα πρέπει να μπορεί μετά από αίτημά του να λάβει το σύνολο των δεδομένων του σε κατανοητή μορφή (προτείνεται αρχείο JSON).

Σε αυτή την κατεύθυνση, διαγραφή δεδομένων/ λογαριασμού από την πλευρά του ασθενή θα πρέπει να εξασφαλίζει και την αφαίρεση των σχετικών δεδομένων από τα αρχεία του ιατρού, εκτός αν ο ίδιος δώσει ρητή διαφορετική εντολή.

Ασφάλεια server και βάσης δεδομένων

Θα προτιμηθεί εγκατάσταση σε ασφαλές γνωστό Cloud Service σε αυτόνομο μηχάνημα. Η πρόσβαση θα περιορίζεται αποκλειστικά σε γνωστή προκαθορισμένη IP από τις εγκαταστάσεις της επιχείρησης. Θα χρησιμοποιηθεί SSL σύνδεση μεταξύ των υπηρεσιών, ενώ το σύνολο της βάσης θα είναι κρυπτογραφημένη. Υπάρχει καταγραφή (logging) όλων των λαθών/ εξαιρέσεων που προκύπτουν κατά τη χρήση του συστήματος και ενημερώνεται ο υπεύθυνος ασφαλείας. Το API δέχεται κλήσεις μόνο μέσω πρωτοκόλλου https. Η βάση δεδομένων στο σύνολό της γίνεται backed up περιοδικά σε διαφορετικό server στον οποίο απαγορεύεται οποιαδήποτε άλλη πρόσβαση μέσω διαδικτύου.

User authorization

Κεντρικό κομμάτι της ασφάλειας της εφαρμογής αποτελεί το σύστημα αναγνώρισης και εξουσιοδότησης των χρηστών. Θα πρέπει να δίνεται η δυνατότητα για διαφορετικούς τύπους χρηστών με περισσότερα ή λιγότερα δικαιώματα. Κάθε σελίδα θα πρέπει να λειτουργεί έχοντας ως default state την άρνηση ανάκτησης δεδομένων και μόνο όταν επιτυγχάνεται η διαδικασία του user authentication να επιτρέπει την πρόσβαση στα αντίστοιχα δεδομένα. Δύο κίνδυνοι που εμφανίζονται συχνά σε σχέση με την ταυτοποίηση χρηστών αποτελούν η κακή υλοποίηση/ παραμετροποίηση των δικαιωμάτων πρόσβασης που απολαμβάνουν οι διαφορετικές κατηγορίες χρηστών και τα λάθη/ παραλείψεις σε ότι αφορά το σύστημα πιστοποίησης χρηστών.

Για τη σύνδεση του ιατρού στην εφαρμογή ιατρού θα χρησιμοποιείται 2 factor authentication με OTP authentication. Τα στοιχεία για τη σύνδεση με την ΗΔΙΚΑ θα πρέπει να κρυπτογραφούνται. Για κανένα τύπο χρηστών δεν θα χρησιμοποιούνται default ή αρχικοποιημένα credentials. Κατά τη δημιουργία password θα υλοποιηθούν κανόνες προκειμένου να εξασφαλιστεί η καταλληλότητα του κωδικού. Πολλαπλές αποτυχημένες προσπάθειες σύνδεσης θα οδηγούν σε προσωρινή ή και (σε δεύτερο στάδιο) μόνιμο αποκλεισμό του χρήστη από την είσοδο στην εφαρμογή. Μετά την ολοκλήρωση ενός session θα απενεργοποιούνται τα σχετικά στοιχεία ελέγχου ταυτοποίησης (πχ JWT tokens) στον server. Session ή λοιπά IDs που αφορούν την ταυτοποίηση του χρήστη δεν θα πρέπει να είναι ορατά στο url.

Ασφάλεια μεταξύ των μερών της εφαρμογής

Τα διαφορετικά μέρη της εφαρμογής επικοινωνούν μεταξύ τους ανταλλάσσοντας ευαίσθητα δεδομένα των χρηστών προκειμένου να επιτευχθούν οι σκοποί του έργου. Κάθε βήμα αυτής της σύνδεσης θα πρέπει να είναι ασφαλές και απολύτως ελεγχόμενο. Η επικοινωνία θα γίνεται μέσα από RESTful interfaces που θα είναι ευθυγραμμισμένη με το μηχανισμό πιστοποίησης χρηστών. Σε αυτή τη διαδικασία θα υιοθετηθεί το πρωτόκολλο TLS για τη διασφάλιση κρυπτογραφημένης επικοινωνίας μεταξύ πιστοποιημένων μερών. Τα δεδομένα θα περιέχονται σε JWT tokens. Κατά την κρυπτογράφηση θα γίνει χρήση του αλγόριθμου AES-256 (256-bit Advanced Encryption Standard) ο οποίος αποτελεί έναν από τους ευρύτερα χρησιμοποιούμενους στον κλάδο.

Λοιπές προφυλάξεις

Θα ληφθούν μέτρα για την αποφυγή:

α) SQL Injection

Η εισαγωγή δεδομένων στη βάση γίνεται μόνο μέσω API, το οποίο θα χρησιμοποιεί μεθόδους για το validation και τον καθαρισμό/ κανονικοποίηση των δεδομένων που δέχεται.

β) Insecure Deserialization

Το σύστημα δεν θα δέχεται serialized objects από εξωτερικές πηγές

γ) Server-Side Request Forgery (SSRF)

Τα σφάλματα SSRF εμφανίζονται κάθε φορά που ένα web application ανακτά έναν απομακρυσμένο πόρο χωρίς να επικυρώνει τη διεύθυνση URL που παρέχεται από τον χρήστη. Για την αντιμετώπιση του προβλήματος θα γίνεται:

- Επιβολή πολιτικών τείχους προστασίας «άρνησης από προεπιλογή» ή κανόνων ελέγχου πρόσβασης στο δίκτυο για να τον αποκλεισμό κάθε περιττής κίνησης στο intranet
- Sanitization και επικύρωση όλων των δεδομένα εισόδου που παρέχονται από το χρήστη
- Μη αποστολή RAW απαντήσεων σε χρήστες
- Απενεργοποίηση όλων των ανακατευθύνσεων HTTP’