ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΡΕΥΝΑΣ & ΤΕΧΝΟΛΟΓΙΑΣ ΦΟΡΕΑΣ: Ινστιτούτο Βιομηχανικών Συστημάτων - ΙΝ.ΒΙ.Σ / Ε.Κ. «Αθηνά»

ΔΙΕΥΘΥΝΣΗ: Κτίριο ΕΠΠ, Οδός Σταδίου, ΤΚ 26504, Πλατάνι ΠΑΤΡΩΝ ΤΗΛΕΦΩΝΟ: 2610 910302 FAX : 2610 910303

Πλατάνι Πατρών, 16/11/2011 Θέμα: Απάντηση επιστολής Ιατρικού Συλλόγου Πατρών

Σε συνέχεια της από 9547/15-11-2011 επείγουσας επιστολής σας διενεργήσαμε προκαταρκτική έρευνα για το παρεχόμενο επίπεδο ασφάλειας των εφαρμογών Ιστού (web applications), οι οποίες λειτουργούν στα URL <http://www.e-svntagografisi.gr/> και <http://www.e-diagnosis.gr/>. Οι διαπιστώσεις μας είναι οι εξής:

1. Η διεπαφή της εφαρμογής “e-diagnosis” (εφεξής «e-diagnosis») δεν παρουσιάζει κάποια ένδειξη ότι αποτελεί δημόσια ή κρατική εφαρμογή (π.χ. εθνόσημο ή λογότυπος). Επιπλέον, η εφαρμογή λειτουργεί σε υποδομή (server) που βρίσκεται εκτός του δικτύου της Δημόσιας Διοίκησης (Greek Public Administration Network) και συγκεκριμένα σε ιδιώτη πάροχο υπηρεσιών Διαδικτύου. Αποτελεί στοιχείο περαιτέρω διερεύνησης το κατά πόσο είναι αποδεκτό να διακινούνται και κυρίως να αποθηκεύονται τα ευαίσθητα δεδομένα της συγκεκριμένης εφαρμογής σε συστήματα ιδιωτών.
2. Η διεπαφή της εφαρμογής παρέχει τη δυνατότητα σύνδεσης με διαπιστευτήρια χρήστη. Η οθόνη σύνδεσης δεν παρέχεται με κρυπτογραφημένη σύνδεση (χρήση πρωτοκόλλου ασφάλειας TLS ή SSL), όπως συμβαίνει κατά την κοινή πρακτική για την υποβολή των διαπιστευτηρίων χρήστη (username/password). Επιπλέον, τα διαπιστευτήρια υποβάλλονται μέσω Διαδικτύου σε μη προστατευμένη (κρυπτογραφημένη) φόρμα, με αποτέλεσμα να είναι δυνατή η υποκλοπή των διαπιστευτηρίων από έναν ενδιάμεσο κακόβουλο κόμβο του Διαδικτύου. Μετά την υποκλοπή, τα διαπιστευτήρια αυτά μπορούν να χρησιμοποιηθούν από οποιοδήποτε άλλο υπολογιστή στο Διαδίκτυο.
3. Η οθόνη σύνδεσης δεν παρέχει κάποιο εμφανή μηχανισμό προστασίας από μαζικές προσπάθειες σύνδεσης (massive authentication). Συνεπώς, είναι εφικτή η χρήση κακόβουλου λογισμικού με σκοπό α) την εύρεση των διαπιστευτηρίων «σύνδεσης χρηστών μέσω αυτοματοποιημένων μαζικών δοκιμών και β) ο καταιγισμός δοκιμών σύνδεσης με σκοπό τη μείωση της ποιότητας της παρεχόμενης υπηρεσίας έως και το σημείο αδυναμίας παροχής σύνδεσης σε όλους τους πιστοποιημένους χρήστες (denial of service attack). Παρόμοιο πρόβλημα, σε μικρότερη όμως κλίμακα, διαπιστώνεται και για τη διεπαφή της ηλεκτρονικής συνταγογράφησης (e-syntagografisi) καθώς η ύπαρξη του μηχανισμού CAPTCHA δύναται να μειώσει το ρυθμό αιτήσεων σύνδεσης. Ωστόσο, κρίνουμε ότι ο βαθμός δυσκολίας για την αυτόματη επίλυση από έναν υπολογιστή των συγκεκριμένων τεστ είναι ιδιαίτερα χαμηλός. Τέλος, παρόμοια έλλειψη μηχανισμού προστασίας διαπιστώθηκε και

στην οθόνη υπενθύμισης κωδικού πρόσβασης[[1]](#footnote-2). Σε αυτήν την περίπτωση, αν κάποιος γνωρίζει το όνομα χρήστη (username) και το κινητό τηλέφωνο του

r 2 ' r

ιατρού , μπορεί να αιτείται διαρκώς την υπενθύμιση του κωδικού πρόσβασης, με αποτέλεσμα να λαμβάνει πληθώρα μηνυμάτων SMS ο ιατρός. Πέραν από την προφανή ενόχληση, η μαζική λήψη μηνυμάτων ενδέχεται να καταλάβει τη διαθέσιμη μνήμη του κινητού τηλεφώνου, με αποτέλεσμα να μην μπορεί να λάβει άλλα, πιθανόν πολύ επείγοντα μηνύματα SMS.

1. Κατόπιν δοκιμής και ελέγχου, διαπιστώθηκε ότι η εφαρμογή «e-diagnosis» υποστηρίζει κρυπτογραφημένες συνδέσεις (πρωτόκολλο ασφάλειας TLS). Ωστόσο, η δυνατότητα αυτή δεν είναι ενεργή εξ ορισμού (default). Ειδικότερα, ο σύνδεσμος σύνδεσης (Login) παραπέμπει το χρήστη σε μη κρυπτογραφημένη σύνδεση. Επιπλέον διαπιστώνεται ότι ακόμη και στην περίπτωση όπου ένας χρήστης μπορέσει να ενεργοποιήσει χειροκίνητα την ασφαλή σύνδεση, τα τεχνικά της χαρακτηριστικά υπολείπονται των κοινών πρακτικών που χρησιμοποιούνται ευρέως για την προστασία των δεδομένων που μεταδίδονται στο Διαδίκτυο: γίνεται κρυπτογράφηση με κλειδιά μήκους. 128 bit αντί 256 bit και χρήση των λιγότερο ασφαλών αλγόριθμων ασφαλείας RC4 και MD5 έναντι των ευρέως χρησιμοποιούμενων και αποδεκτών AES και SHA1. Παρόμοια προβλήματα δεν εντοπίζονται στην εφαρμογή e- syntagografisi.
2. Ως αναφέρεται στην ιστοσελίδα «Γενικές πληροφορίες» της εφαρμογής «e- diagnosis», τα διαπιστευτήρια σύνδεσης (usemame/password) είναι ταυτόσημα και για τις δύο εφαρμογές (e-diagnosis και e-syntagografisi). Κατά συνέπεια, η διαρροή των διαπιστευτηρίων σύνδεσης μέσω της εφαρμογής e- diagnosis, εξαιτίας της έλλειψης κρυπτογραφημένης επικοινωνίας, επηρεάζει άμεσα την ασφάλεια της εφαρμογής e-syntagografisi, παρά τη χρήση κρυπτογράφησης στη δεύτερη. Συγκεκριμένα, ένας κακόβουλος χρήστης μπορεί να υποκλέψει τα διαπιστευτήρια από την εφαρμογή e-diagnosis και στη συνέχεια να τα χρησιμοποιήσει για να συνδεθεί στην εφαρμογή e- syntagografisi.
3. Δεδομένου ότι η εφαρμογή e-diagnosis λειτουργεί παραγωγικά ήδη για σημαντικό χρονικό διάστημα, η εκ των υστέρων ενεργοποίηση της δυνατότητας κρυπτογραφημένης επικοινωνίας (HTTP με TLS ή SSL), δεν εξασφαλίζει ότι δεν υπήρξε διαρροή των διαπιστευτηρίων σύνδεσης κατά το παρελθόν. Tg .διαπιστευτήρια αυτά μπορούν να χρησιμοποιηθούν εκ των υστέρων, τόσο στην -εφαρμογή e-diagnosis όσο και στην εφαρμογή e- syntagografisi. Προκειμένου να διασφαλιστεί η εμπιστευτικότητα των διαπιστευτηρίων σύνδεσης, απαιτείται α) ο έλεγχος της υποδομής για τυχόν ίχνη παραβίασής ή/και διαρροής δεδομένων β) η ανάκληση και ακύρωση των υπαρχόντων διαπιστευτηρίων σύνδεσης και για τις δύο εφαρμογές και γ) η διανομή νέων διαπιστευτηρίων σύνδεσης σε όλους τους χρήστες, αφού πρώτα βεβαιωθεί το επίπεδο ασφάλειας της νέας διαμόρφωσης της εφαρμογής.
4. Δεδομένου ότι α) η ενεργοποίηση κρυπτογραφημένης επικοινωνίας (HTTP με TLS ή SSL) επιφέρει αύξηση της απαιτούμενης υπολογιστικής ισχύος από τις υποδομές και β) η εφαρμογή e-diagnosis ήδη λειτουργεί παραγωγικά, θα πρέπει να ληφθεί ιδιαίτερη μέριμνα, ώστε να ανταπεξέλθουν οι υποδομές στο νέο φορτίο και να συνεχιστεί απρόσκοπτα η παροχή υπηρεσίας μετά την ενεργοποίηση κρυπτογράφησης.

Η εφαρμογή «e-syntagograflsi» παρέχει οδηγίες χρήσης προς ιατρούς και φαρμακεία μέσα από το URL <http://www.e-syntagografisi.gr/7page> id=T52. Η μελέτη των οδηγιών κατέληξε στις εξής επιπλέον διαπιστώσεις:

1. Σύμφωνα με τη σελίδα 9 των οδηγιών για Φαρμακεία[[2]](#footnote-3), ο φαρμακοποιός έχει τη δυνατότητα ηλεκτρονικής καταχώρισης μίας χειρόγραφης συνταγής. Με βάση τις παρεχόμενες οδηγίες, η ταυτοποίηση του ιατρού που εκδίδει τη συνταγή γίνεται αποκλειστικά με βάση τον Α.Μ.Κ.Α. του ιατρού. Ωστόσο ο Α.Μ.Κ.Α. είναι ευρέως διαθέσιμη πληροφορία και δυνητικά μπορεί να το χρησιμοποιήσει οποιοσδήποτε φαρμακοποιός. Με βάση το υπόδειγμα της σελίδας 8, δε διευκρινίζεται στο υπόδειγμα εκτύπωσης μίας συνταγής αν αποτελεί πρωτογενή καταχώριση του ιατρού ή του φαρμακοποιού. Επιπλέον, δεν περιγράφεται κάποια διαδικασία για την ειδοποίηση ή εκ των υστέρων ενημέρωση του ιατρού για την καταχώριση μίας συνταγής εκ μέρους του από έναν φαρμακοποιό (π.χ. αποστολή SMS ή email). Συνεπώς, σε περίπτωση κακόβουλων ενεργειών εκ μέρους ενός φαρμακοποιού, δημιουργείται ένα διαχειριστικό κόστος για τον ιατρό, προκειμένου να αποδείξει ποιος καταχώρισε μία συνταγή.
2. Σύμφωνα με τη σελίδα 19 των οδηγιών για Φαρμακεία, ένας φαρμακοποιός γνωρίζοντας μόνο το Α.Μ.Κ.Α. ενός ασθενούς (τρίτη οθόνη στη σελίδα) μπορεί να αναζητήσει και να λάβει μία πλήρη λίστα των συνταγών που αφορούν το συγκεκριμένο ασθενή. Συνεπώς, το πλήρες ιστορικό συνταγογράφησης ενός ασθενούς είναι διαθέσιμο σε ένα φαρμακοποιό μέσα από τη συγκεκριμένη λειτουργία. Αποτελεί στοιχείο περαιτέρω διερεύνησης κατά πόσο μία τέτοια πληροφορία παραβιάζει το ιατρικό απόρρητο και την προστασία των (ευαίσθητων) προσωπικών δεδομένων του ασθενούς.
3. Σύμφωνα με τη σελίδα 22 των οδηγιών για Φαρμακεία, η εμφάνιση της συνταγής ενός ασθενούς αποκαλύπτει και τον Α.Μ.Κ.Α. του ιατρού. Συνεπώς, ακόμη και αν δεν είναι με κάποιο άλλο τρόπο ήδη γνωστό, μπορεί να χρησιμοποιηθεί η συγκεκριμένη φόρμα για την άντληση αυτή της πληροφορίας για την' περαιτέρω αξιοποίησή της όπως αναλύεται στην παρατήρηση 8 παραπάνω.
4. Σύμφωνα με τη σελίδα 22 των οδηγιών για Φαρμακεία, η εμφάνιση της

r *^* r

συνταγής ενός ασθενούς αποκαλύπτει και τον αριθμό κλήσης του κινητού τηλεφώνου του ιατρού. Η πληροφορία αυτή μπορεί περαιτέρω να αξιοποιήθεί όπως αναλύεται στην παρατήρηση 3 παραπάνω.

Παραμένουμε στη διάθεσή σας για οποιαδήποτε περαιτέρω διευκρίνιση τυχόν χρειαστείτε.

Δρ Αρτέμιος Γ. Βογιατζής Εντεταλμένος ερευνητής

2 Χάριν οικονομίας κειμένου, χρησιμοποιούμε το αρσενικό γένος στην όποια αναφορά στο τρίτο ενικό πρόσωπο, αλλά σε κάθε περίπτωση εννοούνται όλα τα γένη.

1. <http://register.e-syntagografisi.gr/Common/ForgotPassword.aspx> [↑](#footnote-ref-2)
2. Αρχείο «Farmakeio.pdf» διαθέσιμο στο <http://www.e-svntagografisi.gr/files/Farmakeio.pdf>, [τελευταία επίσκεψη 16 Νοεμβρίου 2011 ώρα 08:50], [↑](#footnote-ref-3)