OWASP - The Open Web Application Security Project

Ελληνική Ομάδα Εργασίας - http://www.owasp.gr

Μηνιαίο Ενημερωτικό Δελτίο – Φεβρουάριος 2007

ΕΛΛΗΝΙΚΗ ΕΠΙΚΑΙΡΟΤΗΤΑ

Καλώς το κι ας άργησε

Το 3ο τεύχος του newsletter της Ελληνικής ομάδας εργασίας του OWASP είναι εδώ, έστω και με μερικές μέρες καθυστέρηση. Όπως είναι γνωστό, όλες οι δραστηριότητες του OWASP βασίζονται στην εθελοντική προσφορά των μελών του. Ο εθελοντισμός όμως, πολλές φορές, καλώς ή κακώς, έρχεται δεύτερος μετά από επαγγελματικές ή άλλες υποχρεώσεις. Έτσι, άλλες φορές το newsletter θα έρχεται στην ώρα του, άλλες λίγο αργότερα και, πιο σπάνια, λίγο νωρίτερα.

Στην ουσία των πραγμάτων, ο Ιανουάριος ήταν ένας μήνας έντονου δημόσιου προβληματισμού για τη λειτουργία των ανεξάρτητων αρχών. Κύρια αφορμή ήταν αφενός ο προβληματισμός για τη δημοσιοποίηση των ονομάτων δημόσιων προσώπων που είχαν παράνομα απαλλαγεί από την υποχρέωση στράτευσης και αφετέρου η επίθεση στην αμερικανική πρεσβεία, η οποία συνέπεσε χρονικά με τη διεξαγωγή σεμιναρίων και ημερίδας από την ΑΠΔΠΧ και την ΑΔΑΕ αντίστοιχα. Τόσο η προστασία των προσωπικών δεδομένων αλλά και των ελευθεριών του ατόμου, όσο και οι ανεξάρτητες αρχές αμφισβητήθηκαν έντονα όχι μόνο από πολιτικούς και δημόσια πρόσωπα, αλλά και από τον κόσμο, μέσα από τις σχετικές δημοσκοπήσεις. Γεγονός είναι ότι οι αρχές επιτελούν αθόρυβα πολύ σημαντικό έργο. Όμως, όλος αυτός ο διάλογος ίσως τελικά εκφράζει μια ανάγκη επαναπροσδιορισμού της λειτουργίας, των αρμοδιοτήτων τους και γενικότερα του νομικού πλαισίου που τις διέπει, έτσι ώστε να μπορούν να προσαρμόζονται πιο εύκολα στις διαρκώς μεταβαλλόμενες απειλές.

Ημερίδα ΑΔΑΕ

Η ΑΔΑΕ διοργάνωσε ημερίδα την Τρίτη 16 Ιανουαρίου με θέμα: «Γενικές αρχές εθνικής στρατηγικής για το απόρρητο και την ασφάλεια δικτύων και πληροφοριών». Το OWASP.gr παρακολούθησε την πολύ ενδιαφέρουσα ημερίδα που χαρακτηρίστηκε από τη μεγάλη προσέλευση του κοινού.

Η ημερίδα ξεκίνησε με την ομιλία του Γενικού Γραμματέα του Υπουργείου Δικαιοσύνης και δικηγόρο παρ' Αρείω Πάγω, Παναγιώτη Πανούρη. Ο κύριος Πανούρης αποκάλυψε ότι προωθείται μια σειρά μέτρων από το Υπουργείο που σκοπό έχουν να αναβαθμίσουν τις διαδικασίες εφαρμογής της δικαιοσύνης σε εθνικό επίπεδο (e-justice στο Ανώτατο Δικαστήριο, ενιαίο μητρώο φυλακισθέντων/αποφυλακισθέντων). Κύριο μέλημα του υπουργείου είναι η

προστασία των δικαιωμάτων του πολίτη και γι' αυτό ακριβώς και έχει προβεί σε μια σειρά συγκεκριμένων ενεργειών με πιο σημαντική αυτή του εναρμονισμού του ελληνικού με το κοινοτικό δίκαιο αναφορικά με το θέμα της παραβίασης των πνευματικών δικαιωμάτων. Η ομιλία ολοκληρώθηκε με το "δυστυχώς, η τεχνολογία ξεπερνά σε ταχύτητα τον νομοθέτη", φράση την οποία επανέλαβε και ο Γενικός Γραμματέας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομίας και Οικονομικών, κ. Δημοσθένης Αναγνωστόπουλος.

Ακολούθως, ο πρόεδρος της ΑΔΑΕ κ. Ανδρέας Λαμπρινόπουλος, επεσήμανε την ανάγκη για δημιουργία ενός Συστήματος Παρακολούθησης Νέων Κινδύνων για τις Επικοινωνίες, που θα λειτουργεί σε επίπεδο κράτους και θα διαχειρίζεται ανεξάρτητος φορέας. Κύριος σκοπός του νέου οργάνου θα είναι η ανάλυση επικινδυνότητας και η πρόταση βέλτιστων πρακτικών σε επιχειρήσεις και οργανισμούς που επιθυμούν να προστατέψουν τις δικτυακές και υπολογιστικές τους υποδομές. Πρόσθεσε ότι αυτό δεν μπορεί να το αναλάβει η ΑΔΑΕ ελέω ένδειας τόσο σε ανθρώπινο δυναμικό όσο και σε υλικοτεχνικό εξοπλισμό.

Στην πρώτη ενότητα, για την ασφάλεια των κρίσιμων υποδομών, το πάνελ περιελάμβανε ομιλητές από τον ENISA, την ΕΥΠ, το ΓΕΕΘΑ, τη ΔΕΗ, το ΣΥΖΕΥΞΙΣ, την Τράπεζα της Ελλάδος και άλλους φορείς. Αρχικά, ο κ. Βασίλειος Ανδρονόπουλος, Γενικός Γραμματέας Δημόσιας Διοίκησης, αναφέρθηκε στο τρίπτυχο που παγιώνει την αγαστή σχέση του ελληνικού δημοσίου και του Internet, δηλαδή την υιοθέτηση Εθνικού Συστήματος Αυθεντικοποίησης, την εναρμόνιση των επισήμων ιστοτόπων των υπηρεσιών με συγκεκριμένα πρότυπα πρόσβασης/χρήσης και την ύπαρξη θεσμοθετημένου πλαισίου διαλειτουργικότητας μεταξύ των δημοσίων φορέων με παράλληλη χρήση ψηφιακών πιστοποιητικών. Στη συνέχεια, ο προβληματισμός για την ασφάλεια εναλλασσόταν με διαπιστώσεις προόδου, όπως το γεγονός ότι πλέον απουσιάζουν χαρτάκια με συνθηματικά από τις οθόνες των υπολογιστών στα γραφεία της ΔΕΗ. Τελειώνοντας, ο κ. Στέλιος Μαϊστρος, υπεύθυνος για την ομάδα GRNET-CERT του Ε.Δ.Ε.Τ, παρατήρησε ότι αυξάνεται το ελληνικό spam αλλά και η χρήση δικτύων p2p για ανταλλαγή υλικού που καταπατά τα πνευματικά δικαιώματα των δημιουργών του μέσα στο δίκτυο του ΕΔΕΤ, αποτέλεσμα, κατά τον ομιλητή, της υλοποίησης του «φοιτητικού DSL».

Στη δεύτερη ενότητα, ιδιαίτερο ενδιαφέρον παρουσίασαν τα «Νομικά Θέματα Διασφάλισης Απορρήτου Επικοινωνιών». Αρχικά μίλησε ο κ. Γεώργιος Παπαδημητρίου, Καθηγητής Συνταγματικού Δικαίου του Πανεπιστημίου Αθηνών, κάνοντας μια μικρή αναδρομή στον "βιολογικό κύκλο" των Ανεξαρτήτων Αρχών και εστιάζοντας την προσοχή του στο δημόσιο χαρακτήρα του ελέγχου της ορθής λειτουργίας των Αρχών από τα συντεταγμένα θεσμικά όργανα. Χαρακτήρισε αρχικά πεπλανημένη την επιλογή του κοινοβουλευτικού ελέγχου, μιας και ο τελευταίος ασκείται από την Βουλή προς την εκάστοτε κυβέρνηση και όχι προς τις Ανεξάρτητες Αρχές. Συνέχισε, όμως, σημειώνοντας ότι η απόφαση αυτή ευστοχεί στο ότι υπαγάγει τις Αρχές σε κάποιου είδους έλεγχο. Το έργο αυτό επιτελεί η Επιτροπή Θεσμών και Διαφάνειας της Βουλής αλλά δυστυχώς ο έλεγχος λαμβάνει χώρα περιστασιακά και συνήθως βάση επικαιρότητας και μόνο. Παράλληλα, ο καθηγητής παρατήρησε την απουσία πρόβλεψης για έναν ετήσιο απολογισμού έργου και ενεργειών των Ανεξαρτήτων Αρχών. Αναφερόμενος στους φορείς εξουσίας έθιξε το λυπηρό φαινόμενο της αδιαφορίας αυτών προς τις Αρχές και υποστήριξε ότι ο θεσμικός σεβασμός των ανεξαρτήτων οργάνων είναι εχέγγυο του σύγχρονου δημοκρατικού πολιτισμού. Ολοκλήρωσε την ομιλία του χαρακτηρίζοντας προηγμένο το Σύνταγμα του ελληνικού κράτους αλλά ανώριμες ακόμα τις Ανεξάρτητες Αρχές του.

Στη συνέχεια μίλησε ο κ. Χρήστος Ντουχάνης, Πάρεδρος του Συμβουλίου της Επικρατείας. Τέσσερα ήταν τα βασικά μέρη της ομιλίας. Το πρώτο είχε να κάνει με τις νομοθετικές διατάξεις που ορίζουν το καθεστώς λειτουργίας της ΑΔΑΕ. Ανέφερε

χαρακτηριστικά ότι οι δια ζώσης επικοινωνίες δεν εμπίπτουν στην δικαιοδοσία της ΑΔΑΕ. Στο δεύτερο μέρος παρουσιάστηκαν συνοπτικά οι αρμοδιότητες της ΑΔΑΕ με την υποσημείωση ότι ο νομοθέτης έχει δείξει υπερβολική σχολαστικότητα στην θέσπιση των κανόνων και ότι δεν είναι σώφρον να αντιμετωπίζεται η συγκεκριμένη Αρχή σαν μια οποιαδήποτε διοικητική υπηρεσία, όπου ορίζεται σαφώς ποιος και πότε θα σηκώνει τα τηλέφωνα. Στη συνέχεια έγινε αναφορά στη φύση της ΑΔΑΕ και στη δυνατότητα προσβολής των αποφάσεών της από φυσικά ή νομικά πρόσωπα. Έπειτα ειπώθηκαν κάποια γενικά πράγματα αναφορικά με το ποιόν των μελών της ΑΔΑΕ, τον τρόπο επιλογής τους και τις αρμοδιότητες που τους ανατίθενται.
Ο δικηγόρος κ. Αλκιβιάδης Ψάρρας, διέκρινε τα προσωπικά δεδομένα σε απόρρητα και μη απόρρητα (χαρακτηριστικά ανέφερε ότι «υπάρχει και ο τηλεφωνικός κατάλογος») ενώ διαπίστωσε ότι στην ελληνική πραγματικότητα μπορεί να υπάρξει παραβίαση απορρήτου χωρίς όμως να παραβιαστούν προσωπικά δεδομένα. Τέλος, ο δικηγόρος κ. Μαρίνος Παπαδόπουλος ξεκίνησε αναφερόμενος στην περίπτωση ενός ISP που χωρίς να συμβουλευτεί την ΑΔΑΕ προχώρησε σε αποκάλυψη στον θιγόμενο των προσωπικών στοιχείων (ονοματεπώνυμο) συνδρομητή του ISP που με βάση τη μηνυτήρια αναφορά είχε αποστείλει στον ενάγοντα υβριστικό e-mail. Τελικά, αποδείχτηκε ότι κάποιος κακόβουλος είχε εισβάλλει στον υπολογιστή του εναγόμενου και τελικά ο ISP τιμωρήθηκε με πρόστιμο. Ολοκληρώνοντας, επιτέθηκε στην ΑΠΔΠΧ και την αδιαφορία που δείχνει ως προς τον θεσμικό ρόλο της ΑΔΑΕ και το θεσμικό πλαίσιο που διέπει το απόρρητο των επικοινωνιών.
Ακολούθησε συζήτηση, κατά την οποία ο κ. Παπαδημητρίου πρότεινε στον Υπουργό να καλέσει σε διαβούλευση τις δύο Αρχές και ολοκλήρωσε την δευτερολογία του διατυπώνοντας την άποψη ότι οι Αρχές είναι η «τρυφερή έκφραση της Πολιτείας» και ότι η Δημοκρατία «ζει απ' τη διαβούλευση, η οποία οδηγεί στην συναίνεση». Στη συνέχεια, ο κ. Ντουχάνης επανήλθε στο θέμα του κατά πόσο οι Αρχές είναι διοικητικές (υπάγονται στην εκτελεστική εξουσία) ή είναι αυτόνομες ενώ η ημερίδα έκλεισε με μια τοποθέτηση του κ. Παπαδόπουλου, ο οποίος εκμυστηρεύτηκε στο κοινό ότι αν και σπούδασε νομικά σε Ελλάδα και Αμερική και τεχνολογία επικοινωνιών στην Αμερική, δεν συνάντησε πουθενά τόση αλαζονεία όση στην Ελλάδα.

Ευχαριστούμε θερμά τον tnu από το post του οποίου στο group dit.comp.security του news server testnews.di.uoa.gr διαμορφώθηκε το παραπάνω άρθρο.

Ενημερωτικά σεμινάρια Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Στα πλαίσια του εορτασμού της Ημέρας Προστασίας Δεδομένων, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διεξήγαγε από τις 29 ως τις 31 Ιανουαρίου σεμινάρια με σκοπό την ενημέρωση των πολιτών σχετικά με τα δικαιώματά τους, τις υποχρεώσεις των υπευθύνων επεξεργασίας και τους κινδύνους που είναι δυνατόν να προκύψουν από τη μη νόμιμη επεξεργασία των προσωπικών δεδομένων. Το πρόγραμμα των σεμιναρίων περιελάμβανε παρουσιάσεις στις εξής θεματικές περιοχές: προστασία δεδομένων και εργασιακές σχέσεις, CCTVs, spam, βιομετρικά δεδομένα, τραπεζικός/χρηματοπιστωτικός τομέας, υγεία, μέτρα ασφάλειας στην επεξεργασία των προσωπικών δεδομένων, πρόσβαση στη δημόσια πληροφορία, παιδιά και προστασία δεδομένων. Το OWASP.gr παρακολούθησε τις δύο πρώτες ημέρες των σεμιναρίων, που χαρακτηρίστηκαν από τις υψηλού επιπέδου παρουσιάσεις αλλά και τη σχετικά χαμηλή προσέλευση του κοινού, την οποία κάποιοι απέδωσαν στη περιορισμένη προβολή τους από τη πλευρά της Αρχής.
Το πρώτο μέρος των σεμιναρίων και τις δύο μέρες αναφερόταν στο θεσμικό πλαίσιο προστασίας προσωπικών δεδομένων και τα μέτρα ασφάλειας στην επεξεργασία

προσωπικών δεδομένων. Κατά την παρουσίαση του θεσμικού πλαισίου αναλύθηκε συνοπτικά το υπάρχον νομικό καθεστώς που διέπει την Αρχή. Αν και η παρουσίαση γινόταν από νομικούς, χρησιμοποιήθηκε αργή και κατανοητή γλώσσα, χωρίς πολλούς νομικούς όρους και εκφράσεις. Βέβαια ο όγκος της πληροφορίας που παρουσιάστηκε ήταν μεγάλος για να μπορέσει να τον απορροφήσει το κοινό, αλλά σίγουρα δόθηκε η γενική ιδέα και το πνεύμα λειτουργίας της Αρχής. Έτσι, αρχικά ορίστηκαν οι έννοιες των προσωπικών και ευαίσθητων προσωπικών δεδομένων, του υπεύθυνου, του εκτελούντος, του αποδέκτη και του υποκειμένου. Στη συνέχεια αναλύθηκαν οι διάφορες προϋποθέσεις επεξεργασίας των δεδομένων ενώ στο τέλος παρουσιάστηκαν ορισμένες ενδεικτικές αποφάσεις της Αρχής. Η παρουσίαση των μέτρων ασφάλειας στην επεξεργασία προσωπικών δεδομένων έγινε από πληροφορικούς ελεγκτές της αρχής, οι οποίοι συνοπτικά ανέπτυξαν τα βασικά σημεία που πρέπει να προσέχει ο πολίτης για να προστατεύει τα δεδομένα του. Αυτά περιελάμβαναν συμβουλές για την ασφάλεια τόσο στο επίπεδο του Internet (antivirus, firewall, κλπ.) όσο και σε τηλεφωνικές ή δια ζώσης επικοινωνίες.

Οι τελευταίες δύο παρουσιάσεις της πρώτης μέρας αφορούσαν στην προστασία των προσωπικών δεδομένων στον τραπεζικό τομέα και τις εργασιακές σχέσεις. Στον τραπεζικό τομέα η έμφαση δόθηκε σε προβλήματα που υπάρχουν με την ΤΕΙΡΕΣΙΑΣ ΑΕ αλλά και με προ-εγκρίσεις πιστωτικών καρτών και δανείων. Η αίσθηση που δημιουργήθηκε μετά τις παρεμβάσεις και τις ερωτήσεις του ακροατηρίου είναι αφενός ότι οι τράπεζες μετά από μία περίοδο ασυδοσίας έχουν περιορίσει τις αυθαιρεσίες και αφετέρου έχουν ήδη γίνει σημαντικά βήματα για να αποφεύγονται τα συχνά παρουσιαζόμενα προβλήματα συνωνυμιών στην ΤΕΙΡΕΣΙΑΣ. Αναφορικά με τις εργασιακές σχέσεις, τονίστηκε ότι οι εργαζόμενοι έχουν τη δυνατότητα να χρησιμοποιούν υποδομές του εργοδότη για τηλεφωνική και ηλεκτρονική επικοινωνία για προσωπικούς λόγους, χωρίς να παρακολουθούνται. Επίσης τονίστηκε ότι οι εργαζόμενοι δε μπορούν να παραιτηθούν των δικαιωμάτων τους, ενώ στο τέλος παρουσιάστηκαν σχετικές αποφάσεις της Αρχής. Η αίσθηση που δημιουργήθηκε από τη συζήτηση που ακολούθησε είναι ότι το υπάρχον νομικό πλαίσιο για τα προσωπικά δεδομένα, τις νέες τεχνολογίας και το χώρο εργασίας είναι αρκετά ισχυρό αλλά είτε έχει ατονήσει είτε διατάξεις του δεν έχουν ενεργοποιηθεί ποτέ.

Τη δεύτερη μέρα, πέρα από τις εισαγωγικές διαλέξεις, δόθηκαν παρουσιάσεις σχετικά με το spam, τα κλειστά κυκλώματα τηλεόρασης και τα βιομετρικά δεδομένα. Σχετικά με το spam, έμφαση δόθηκε στις διατάξεις του νόμου 3471/2006 περί ηλεκτρονικών επικοινωνιών, ο οποίος ορίζει ότι απαιτείται η ρητή συγκατάθεση του υποκειμένου για την αποστολή μηνυμάτων προώθησης, εκτός και αν υπάρχει πρότερη συναλλαγή. Επίσης, στο μήνυμα πρέπει να αναφέρεται ρητά η ταυτότητα του αποστολέα και η διεύθυνση στην οποία κανείς μπορεί να ζητήσει τον τερματισμό της αποστολής τέτοιων μηνυμάτων. Σχετικά με τα κλειστά κυκλώματα τηλεόρασης πέρα από το υπάρχον νομικό πλαίσιο, αναλύθηκαν περιπτώσεις που έχει απαγορευθεί η εγκατάσταση τέτοιων κυκλωμάτων. Τέλος, κατά την παρουσίαση των βιομετρικών δεδομένων αναλύθηκαν σχετικές αποφάσεις της αρχής. Χαρακτηριστικό είναι ότι αναφέρθηκε πως αν και κατά την εγκατάσταση συστημάτων αυθεντικοποίησης με χρήση βιομετρικών δεδομένων απαιτείται απλή γνωστοποίηση στην Αρχή, εντούτοις συνηθίζεται να ελέγχονται όλες οι περιπτώσεις εξαιτίας του ιδιαίτερα ευαίσθητου χαρακτήρα τους.

Η τρίτη ημέρα περιελάμβανε ομιλίες για την πρόσβαση στη δημόσια πληροφορία, για τα προσωπικά δεδομένα των παιδιών και του χώρου της υγείας. Τα σεμινάρια αυτά ήταν μία από τις πρώτες προσπάθειες της Αρχής να αποκτήσει ένα πιο εξωστρεφή χαρακτήρα. Οι πολύ καλές παρουσιάσεις αλλά και οι συζητήσεις που ακολούθησαν ενημέρωσαν και έδωσαν απαντήσεις σε ερωτήματα που προβλημάτιζαν όσους παρακολούθησαν. Όπως δήλωσαν τα μέλη της Αρχής, σκοπός τους είναι κυρίως η

ενημέρωση των πολιτών, έτσι ώστε να είναι αρκετά υποψιασμένοι για να μπορούν να διαφυλάξουν τα προσωπικά τους δεδομένα από κακόβουλες χρήσεις και να καταγγέλλουν στην Αρχή τέτοιες προσπάθειες. Οι προθέσεις της Αρχής πάντως είναι πολλές και καλές. Υστερεί όμως ακόμα σε έμψυχο δυναμικό, όπως η ίδια παρεδέχεται.

Ναι στις κάμερες!
Με αφορμή το τρομοκρατικό χτύπημα κατά της αμερικανικής πρεσβείας, η εταιρία VPRC έκανε δημοσκόπηση σχετικά με τη χρήση των καμερών. Σύμφωνα με τα στοιχεία που δόθηκαν στη δημοσιότητα, 57% των πολιτών πιστεύουν ότι οι κάμερες προστατεύουν παρά παραβιάζουν τα πολιτικά δικαιώματα ενώ 61% των πολιτών συμφωνούν με την τηλεοπτική αστυνόμευση του δημόσιου χώρου, που λειτούργησε στους Ολυμπιακούς Αγώνες. Είναι μάλλον λυπηρό ότι η πλειοψηφία του ελληνικού λαού τάσσεται υπέρ της λειτουργίας των καμερών στους δρόμους παρότι πιστεύει ότι οι κάμερες χρησιμοποιούνται και για την παρακολούθηση πολιτών. Βέβαια, ενδιαφέρον θα είχε να διεξαχθεί η ίδια έρευνα μερικούς μήνες μετά, και όχι εν θερμώ, λίγες ώρες μετά το τρομοκρατικό χτύπημα.

Εμπλοκή της ΕΕΤΤ στο θέμα με τους dialers
Στο περασμένο newsletter είχαμε αναφερθεί σε μία απάτη με dialers που είχε δει το φως της δημοσιότητας. Λίγες μέρες αργότερα, η ΕΕΤΤ εξέδωσε προσωρινή διάταξη υποχρεώνοντας την εταιρία ΜΑΚΝΑΝ να απενεργοποιήσει όλες τις γραμμές 901 που της είχαν εκχωρηθεί, αλλά και τον ΟΤΕ να μην εισπράξει τα ποσά που αντιστοιχούν σε κλήσεις σε αυτούς τους αριθμούς. Ο ΟΤΕ από τη μεριά του, έσπευσε να ενημερώσει το κοινό ότι ναι μεν θα τηρήσει τη διαταγή της ΕΕΤΤ αλλά αυτός από τη μεριά του απλά κάνει… τη δουλειά του, αφού και υποχρεούται να εκχωρεί τέτοιες γραμμές και δεν μπορεί να ελέγχει τις χρεώσεις και το περιεχόμενό τους. Αντίθετα, όπως επισημαίνει ο ΟΤΕ σε δελτίο τύπου, δρα σα μεσολαβητής, εισπράττοντας από τον καταναλωτή το αντίστοιχο ποσό και δίνοντας το μεγαλύτερο μέρος του στις εταιρίες που παρέχουν αυτές τις υπηρεσίες. Σε κάθε περίπτωση, ελπίζουμε ότι η απόφαση αυτή, που ομολογουμένως είναι αρκετά πρωτοποριακή για τα ελληνικά δεδομένα, θα αποτελέσει τη βάση για την αντιμετώπιση μελλοντικών αντίστοιχων περιπτώσεων.

Απάτη μέσω Internet από 3 απόστρατους αξιωματικούς
Τρεις απόστρατοι αξιωματικοί συνελήφθησαν στις αρχές του μήνα από το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος για απάτη μέσω internet. Συγκεκριμένα, οι αξιωματικοί προσέγγιζαν μέσω e-mail επαγγελματίες με σκοπό να τους πουλήσουν διάφορα εμπορεύματα. Στη συνέχεια εισέπρατταν μεγάλες προκαταβολές τις οποίες και «ξέπλεναν» μέσω 15 offshore εταιριών που είχαν ιδρύσει για το σκοπό αυτό και εξαφανίζονταν χωρίς φυσικά να παραδίδουν ποτέ τα εμπορεύματα. Η περίπτωση αυτή μάλλον θυμίζει mail που λίγο πολύ όλοι έχουμε λάβει, από έκπτωτους πρίγκιπες της Αφρικής που θέλουν να τους βοηθήσουμε (με το αζημίωτο πάντα) να μεταφέρουν π.χ. ένα μεγάλο χρηματικό ποσό.

Και βιομηχανική κατασκοπία μέσω Internet
Την πρώτη υπόθεση βιομηχανικής κατασκοπίας εξιχνίασε το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος. Ειδικότερα, ιδιοκτήτης ναυτιλιακής εταιρίας κατήγγειλε ότι πρώην υπάλληλός του είχε εγκαταστήσει στον φορητό ηλεκτρονικό υπολογιστή του, εν αγνοία του φυσικά, λογισμικό το οποίο είχε τη δυνατότητα να συλλαμβάνει ήχο από τον περιβάλλοντα χώρο και στη συνέχεια να τον αποστέλλει μέσω Internet σε ιστοσελίδα της Ρωσίας. Στη συνέχεια προσέγγιζε ο ίδιος τους πελάτες και έδινε

καλύτερες προσφορές με αποτέλεσμα να έχει καταφέρει να κερδίσει πολλές αναθέσεις. Ο ουκρανικής καταγωγής 27χρονος που συνελήφθη αποδέχθηκε τις κατηγορίες, οι οποίες ουσιαστικά αφορούν υποκλοπή συνομιλιών μέσω Internet.

OWASP.gr

OWASP Projects

Μία από τις δραστηριότητες του OWASP είναι η ανάπτυξη projects. Στόχος των projects είναι η συντονισμένη υλοποίηση εργαλείων και η συγγραφή κειμένων σχετικά με θέματα της ασφάλειας των διαδικτυακών εφαρμογών. Περισσότερες πληροφορίες μπορείτε να βρείτε στη σελίδα: http://www.owasp.org/index.php/Category:OWASP_Project ενώ τα projects που χρειάζονται άμεσα τη συνδρομή εθελοντών περιλαμβάνουν τα: Java project, .NET project, OWASP Testing Project v2.0 και άλλα. Παράλληλα, υπάρχει η ειδική κατηγορία OWASP Student Projects (http://www.owasp.org/index.php/OWASP_student_projects) με projects που απευθύνονται σε φοιτητές. Για περισσότερες πληροφορίες μπορείτε να ανατρέξετε στα αντίστοιχα URLs ή στο 3ο newsletter του OWASP.

ΕΠΙΣΤΗΜΟΝΙΚΑ

Πρωτότυπο βιομετρικό κλειδί με βάση την εγκεφαλική λειτουργία:

Ένα ηλεκτρονικό σύστημα ασφαλείας που χρησιμοποιεί τα ηλεκτρικά σήματα του εγκεφάλου για την παραγωγή βιομετρικών δεδομένων είναι αυτό τον καιρό σε περίοδο δοκιμών. Το σύστημα αναπτύχθηκε από τον Δημήτριο Τζοβάρα και τους συναδέλφους του, στο Εθνικό Κέντρο Έρευνας και Τεχνολογικής Ανάπτυξης. Το πρωτότυπο βιομετρικό σύστημα αναμένεται να είναι ιδιαίτερα ασφαλές, και συνεπώς κατάλληλο για ευαίσθητες εφαρμογές με υψηλές απαιτήσεις, σύμφωνα με τους ερευνητές που το ανέπτυξαν. Χρησιμοποιεί μία δημοφιλή μέθοδο για τη μέτρηση της εγκεφαλικής δραστηριότητας, γνωστή ως Ηλεκτροεγκεφαλογραφία (EEG).

Εφόσον η εγκεφαλική δραστηριότητα ενός ατόμου καθορίζεται από το νευρωνικό χάρτη του εγκεφάλου, η ίδια τεχνική μπορεί να χρησιμοποιηθεί για να αναγνωρίσει μοναδικά κάποιον. Το σύστημα απαιτεί από τον χρήστη να παρέχει EEG μετρήσεις εκ των προτέρων, καθώς και μετά από κάθε χρήση. Κάτι τέτοιο γίνεται εφικτό χρησιμοποιώντας ένα «καπέλο» που επικοινωνεί ασύρματα με έναν υπολογιστή, όπου και συλλέγονται τα δεδομένα. Το βιομετρικό σύστημα αυτό είναι κομμάτι ενός σημαντικού Ευρωπαϊκού έργου με τον τίτλο Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis (HUMABIO).

ΣΧΟΛΙΟ

Με αφορμή (και όχι αιτία) την επίθεση με ρουκέτα κατά της Αμερικανικής Πρεσβείας πολλοί ζητούν να αλλάξει η απόφαση της ΑΠΔΠΧ και να επιτραπεί η χρήση των καμερών παρακολούθησης της κυκλοφορίας και για την πρόληψη κακουργηματικών ενεργειών. Ας δούμε τι συμβαίνει ως τώρα και εάν εφαρμόζεται ορθά η απόφαση της Αρχής.

[Video με ατυχήματα σε ελληνικούς δρόμους έχουν] περάσει mail-με-mail (κατά το χέρι-με-χέρι) από σχεδόν κάθε Ελληνικό mailbox. Αν πάει κανείς στο Youtube και ψάξει για "Greek traffic accident" θα δει video που δεν είναι καθόλου μα καθόλου

αστεία. Και ρωτάω: [Υπήρξε καμία κύρωση]; Με ποια τεκμηρίωση ζητάτε να επεκταθεί η χρήση των καμερών τη στιγμή που δεν μπορείτε να περιορίσετε τη διοχέτευση των video στο Internet;
Το βασικό επιχείρημα είναι πως "όποιος δεν έχει κάνει κάτι κακό, δεν έχει τίποτε να φοβηθεί". Αλήθεια; "As governments widen their definitions of just who is a potential threat it makes increasing sense for citizens engaged in previous innocuous activities (especially political and financial privacy) to protect their data from being useful if seized." (Steve Schear) Και ναι το παραπάνω απόσπασμα αναφέρεται σε δεδομένα που ο χρήστης κρυπτογραφεί για να μην είναι εύκολα προσβάσιμα από οποιονδήποτε τρίτο, αλλά οι λόγοι είναι οι ίδιοι.
Στις 17/1/2006 ο Βουλευτής κ. Γεωργιάδης στη NET 105.8 υποστήριξε πως εφόσον είναι σε δημόσιο χώρο κάποιος, διατρέχει τον ίδιο κίνδυνο να γίνει γνωστό το "μυστικό" του, όσο κι αν τον δει μια γειτόνισσα. Γι' αυτό όποιος έχει μυστικά καλύτερα να τα διαχειρίζεται σπίτι ή στο γραφείο του. Ενδιαφέρουσα επιχειρηματολογία, αστήρικτη όμως. Την κουτσομπόλα γειτόνισσα την ξέρω και μπορώ να την αποφύγω. Τις (πάμπολλες) κάμερες όμως δε μπορώ. Όπου κι αν στρίψω είναι πάντα μπροστά μου. Στη γειτόνισσα πετάω κι ένα μπινελίκι και εξαφανίζεται. Άμα βρίσω μια κάμερα θα κλείσει;
Όλοι αυτοί που πιέζουν για την αύξηση των καταγραφόμενων δεδομένων ονειροβατούν, κυρίως γιατί δεν έχουν hands-on experience από συστήματα καταγραφής. Όπως λέει και ο John Gilmore: "If you're watching everybody, you're watching nobody". Ένα τέτοιο σύστημα μαζικής καταγραφής είναι αποτυχημένο εν τη γεννέση του. Προάγει τους πάντες σε πιθανούς ύποπτους.
«Ποιο το πρόβλημα λοιπόν;» Αυτό δε μπορεί να ισχυριστεί ένας υποστηρικτής των καταγραφέων; Εκτός από τα χαμένα χρήματα; Μα η παράνομη στόχευση σε πολίτες. Με τι απόδειξη; Μα τα [προαναφερθέντα] video που έχουν διαρρεύσει σαν αστείο στο Youtube αυτό δείχνουν. Σήμερα είναι ένα αστείο, αύριο θα είναι η επί πληρωμή παρακολούθηση του πολίτη στον δρόμο από κάποιο τρίτο.
Δεν αμφισβητώ εγώ την ηθική των χειριστών των καμερών -το έκαναν μόνοι τους, με τα video που έχουν διαρρεύσει. Αλλά τα προβλήματα που υπάρχουν είναι πολλά και δεν δείχνει να τα έχει αντιληφθεί κανείς. Ποιές είναι οι μισθολογικές απολαβές των χειριστών; Είναι τέτοιες που να τους αποτρέπουν από την ιδέα και μόνο του χρηματισμού; Πως μπορούν να προστατευτούν από εκβιαστές; Γιατί ένα παλιό ανέκδοτο της ασφάλειας υπολογιστών λέει: «Μπορείς να σπαταλήσεις εκατοντάδες χιλιάδες δολάρια σε εξοπλισμό για να "σπάσεις" ένα σύστημα, ενώ μπορείς να δώσεις χίλια και να πάρεις τα κλειδιά από την καθαρίστρια». (Μερικές φορές πάλι αρκεί να φτάσεις μέχρι τη ποδιά της καθαρίστριας για να πάρεις τα κλειδιά)
Πως ελέγχεται ο χειριστής της κάμερας; Έχει μελετήσει ποτέ κανείς περιπτώσεις stalking; Τα άλλα προβλήματα; Και εάν ναι, ποιες είναι οι προβλεπόμενες αντιδράσεις; Γιατί μέχρι σήμερα δε φαίνεται να υπάρχει κάτι.
Δε θα μου αλλάξει τον τρόπο ζωής κανένας τρομοκράτης. Αποδείξτε πως μπορείτε να διασφαλίσετε σωστά τις υπάρχουσες κάμερες από διαρροές και να μας προστατεύσετε από τους χειριστές τους και μετά το ξανασυζητάμε για την πλήρη ενεργοποίησή τους, ώστε στοχευμένα και μετά την εντολή εισαγγελέα να μας προστατεύουν από κακόβουλες ενέργειες.

Το σχόλιο αυτό δημοσιεύτηκε για πρώτη φορά στο blog του Γιώργου Αδαμόπουλου (http://blog.postmaster.gr). Τον ευχαριστούμε θερμά για την παραχώρηση.

ΗΣΥΧΙΑ, ΤΑΞΗ ΚΑΙ… ΑΣΦΑΛΕΙΑ

- Πολύς καβγάς για τις Αρχές…
- Μέχρι και μεταξύ τους κόντεψαν να τσακωθούν.
- Δικηγόροι… Συνηθίζουν να περιπλέκουν πράγματα που για τεχνοκράτες είναι μάλλον απλά, χάνοντας πολλές φορές την ουσία.
- Ας ελπίσουμε τουλάχιστον ότι αυτό θα είναι μια καινούρια… αρχή για τις Αρχές και όχι τέλος
- Γιατί κινδυνεύουμε να βρεθούμε με κάμερες παντού ύστερα από… λαϊκή απαίτηση
- Η ασφάλεια πάντως είναι παραίσθηση, η ανασφάλεια γεγονός.
- Μήνυμα προς ΟΤΕ : grep -r '901' /users/dialup/outbound_calls. Δεν είναι δύσκολο!