OWASP – The Open Web Application Security Project

Ελληνική Ομάδα Εργασίας – *http://www.owasp.gr*

Μηνιαίο Ενημερωτικό Δελτίο – Φεβρουάριος 2008

ΕΙΣΑΓΩΓΙΚΟ ΣΗΜΕΙΩΜΑ

Διανύουμε ένα πολύ σημαντικό μήνα για την Ελληνική ομάδα εργασίας του OWASP καθότι σε λίγες μέρες θα παρουσιάσει για πρώτη φορά τη δουλειά της σε ένα ευρύτερο κοινό, στα πλαίσια του 1ου Συνεδρίου Κοινοτήτων Ελεύθερου Λογισμικού και Λογισμικού Ανοιχτού Κώδικα (http://www.fosscomm.gr) . Η παρουσίαση αυτή, που αποτελεί ταυτόχρονα και την πρώτη (αν)επίσημη συνάντηση των μελών του, σημαδεύει μια προσπάθεια που ξεκίνησε από τις αρχές του χρόνου για ένα ανανεωμένο και πιο δραστήριο OWASP.gr. Ήδη, είδατε κάποια δείγματα, όπως το ανανεωμένο newsletter, αλλά και την συμμετοχή στην ομάδα IA4 του E-Business Forum, νεώτερα για την οποία θα διαβάσετε παρακάτω.

Αισιοδοξούμε, ότι οι δραστηριότητες αυτές, σε συνδυασμό με τις πρωτοβουλίες που αναπτύσσουν κυρίως τα νεώτερα μέλη, θα προκαλέσει μεγαλύτερη κινητικότητα και κυρίως το ενδιαφέρον πολλών από εσάς. Σε κάθε περίπτωση, ελπίζουμε να έχουμε την ευκαιρία να δούμε

Στην τρέχουσα επικαιρότητα, ξεχωρίζει η υπόθεση του press-gr και οι προεκτάσεις της, ενώ εξελίξεις είχαμε και στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αφού ανακοινώθηκε η νέα της σύνθεση και σύντομα αναμένεται να αναλάβουν αρμοδιότητες τα νέα της μέλη.

ΕΛΛΗΝΙΚΗ ΕΠΙΚΑΙΡΟΤΗΤΑ

Παρουσίαση Ομάδας Εργασίας IA4 του E-Business Forum στο Moneyshow 2008

Στις 2 Φεβρουαρίου 2008 στο χώρο της Αίγλης στο Ζάππειο η ομάδα εργασίας IA4 του E-business Forum παρουσίασε στο Moneyshow 2008 τα αποτελέσματα των πεπραγμένων της, ολοκληρώνοντας την πορεία της κάτω από την ομπρέλα του E-Business Forum. Η επιτυχημένη εκδήλωση, με τίτλο «Κυβερνοαπειλές: Από την πρόληψη στην άμεση αντιμετώπιση», χαρακτηρίστηκε από μεγαλύτερη από του αναμενόμενου προσέλευση του κοινού (με αρκετά μέλη του OWASP.gr να δίνουν το παρών) και περιλάμβανε εκτός από την παρουσίαση των πεπραγμένων της ομάδας, ομιλίες από φορείς όπως το DART, η Microsoft και το eTEE. Ακολούθησε ενδιαφέρουσα συζήτηση στην οποία τόσο το πάνελ όσο και οι παρευρισκόμενοι επεσήμαναν την έλλειψη ενημέρωσης του κοινού αλλά και εργαλείων και μεθοδολογιών για τον επαγγελματία. Το OWASP.gr επεσήμανε τη συνδρομή του στον τομέα αυτό και επιβεβαίωσε για μια ακόμη φορά τη διαρκή συνεργασία του με τους υπεύθυνους της ομάδας IA4 με απώτερο σκοπό τη δημιουργία ενός «Ελληνικού Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών». Μάλιστα, μέσα από τη συνεργασία αυτή ελπίζουμε να έχουμε σύντομα ενδιαφέροντα νέα για τα μέλη του OWASP.gr.

Αναφορικά με τη δημιουργία ενός «Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών» αυτή καθεαυτή, ενδιαφέρον αλλά και προβληματισμό προκάλεσε η διαπίστωση ότι το νέο νομοσχέδιο για τη λειτουργία της ΕΥΠ, αναθέτει το ρόλο αυτό στη συγκεκριμένη υπηρεσία. Πέρα από τα σχόλια και τα ερωτηματικά που προέκυψαν, κυρίως στις συζητήσεις στα πηγαδάκια που δημιουργήθηκαν μετά το τέλος της εκδήλωσης, διαπιστώθηκε κατά γενική ομολογία ότι διαφορετικοί φορείς αναλαμβάνουν τέτοιες αξιόλογες πρωτοβουλίες, χωρίς όμως να υπάρχει συνεργασία μεταξύ τους, που αναμφισβήτητα θα επέφερε και καλύτερα αποτελέσματα. Ο εκπρόσωπος του DART, κ. Βασιλάκος, επεσήμανε τις διαφορετικές αρμοδιότητες τους, με το DART για παράδειγμα να ασχολείται περισσότερο με την ενημέρωση του κοινού και των απλών, μη ειδικών χρηστών. Σίγουρα όμως η ύπαρξη ενός ενιαίου φορέα, ή έστω η αρμονική συνεργασία μεταξύ των υπαρχόντων φορέων, την οποία τόσο το DART όσο και η ομάδα IA4 υποστηρίζει, θα ήταν προτιμότερη. Το OWASP.gr ελπίζει η πολύ καλή προσπάθεια της ομάδας IA4 να βρει άξιους συνεχιστές και κυρίως υποστηρικτές έτσι ώστε να μην πέσει στο κενό μία από τις λίγες ολοκληρωμένες και σωστά μελετημένες πρωτοβουλίες στην Ελλάδα σχετικά με την ψηφιακή ασφάλεια.

Υπόθεση press-gr: αδύνατη η εύρεση χρήστη του δικτύου της Βουλής

Σάλος προκλήθηκε τις τελευταίες μέρες σχετικά με τα γνωστό blog press-gr του οποίου οι «ιδιοκτήτες» φέρονται να εμπλέκονται σε υπόθεση εκβιασμού. Αρκετές συζητήσεις έχουν γίνει με αφορμή το γεγονός αυτό, σχετικά με τα blogs και την αυτορρύθμισή τους, την ανάγκη νομοθέτησης για τον περιορισμό τους, αλλά και την ηθική των bloggers γενικότερα. Το OWASP.gr από τη μεριά του εστιάζει στις τεχνικές λεπτομέρειες του θέματος και μάλιστα

όχι τόσο στα περίεργα που είμαστε πλέον συνηθισμένοι να διαβάζουμε από ημιμαθείς στην καλύτερη περίπτωση δημοσιογράφους (χαρακτηριστικό παράδειγμα το μήνυμα που εστάλη «απέναντι από το Υπουργείο Οικονομικών», δηλαδή από το δωρεάν ασύρματο Internet που παρέχεται στην Πλατεία Συντάγματος). Από νωρίς διαπιστώθηκε ότι κάποιο επίμαχο μήνυμα εστάλη μέσα από το δίκτυο της Βουλής και αναζητήθηκε η ταυτότητα του χρήστη που το έστειλε. Θα περίμενε κανείς ότι το δίκτυο της Βουλής να παρέχει τη δυνατότητα εύρεσης ενός τέτοιου χρήστη, παρέχοντας ταυτόχρονα την απαραίτητη ανωνυμία που απαιτείται από το χαρακτήρα του. Εδώ όμως αρχίζουν τα περίεργα, τα οποία πιθανώς έχουν περισσότερο πολιτικές παρά καθαρά τεχνικές προεκτάσεις. Μέχρι αυτή τη στιγμή το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος, ο φορέας που θα περίμενε κανείς να αναλάβει την υπόθεση, αδυνατεί να κάνει αυτοψία για ασαφείς λόγους (δεν επιθυμεί; δεν του επιτρέπεται;). Αντίθετα η υπόθεση ανατέθηκε στο αρμόδιο τμήμα της Βουλής, για λόγους λεπτότητας το οποίο αποφάνθηκε ότι αδυνατεί να βρει το χρήστη για μια σειρά από λόγων με αποκορύφωμα το γεγονός ότι «λόγω του θεσμικού χαρακτήρα και της αποστολής της Βουλής αλλά και των ιδιοτήτων των χρηστών του δικτύου της, εντός και εκτός Κοινοβουλίου (Βουλευτές, διαπιστευμένοι κοινοβουλευτικοί συντάκτες, γραφεία κομμάτων κ.λπ.) η ύπαρξη διαδικασιών και μέσων καταγραφής και ελέγχου μέχρι φυσικού προσώπου, όσον αφορά την πρόσβαση στο διαδίκτυο, κρίθηκε σκόπιμο να μην εφαρμόζεται από την έναρξη των υπηρεσιών πρόσβασης στο διαδίκτυο τη δεκαετία του 90 και η πρακτική αυτή ουδέποτε διαφοροποιήθηκε από όλες τις Διοικήσεις της Βουλής μέχρι σήμερα».

Αν εξαιρέσουμε τους Βουλευτές οι οποίοι καλύπτονται από την ασυλία και δικαιούνται λόγω του αξιώματός τους να έχουν την ιδιόμορφη αυτή πρόσβαση στο διαδίκτυο, παρατηρούμε ότι υπάρχει μία ομάδα χρηστών που μπορεί να έχει ουσιαστικά ανεξέλεγκτη πρόσβαση στο διαδίκτυο. Παράλληλα, η ομάδα μηχανογράφησης της Βουλής παραδέχεται εμμέσως ότι από το ’90 και μετά δεν έχουν αλλάξει οι απαιτήσεις ασφάλειας του συστήματος. Παρόλο λοιπόν που εμείς οι κοινοί θνητοί γνωρίζουμε ότι μετά από οδηγία της Ευρωπαϊκής Ένωσης θα καταγράφονται ένα σωρό στοιχεία για εμάς από τους παρόχους υπηρεσιών Internet, υπάρχει μια ομάδα δημοσιογράφων αλλά και υπαλλήλων πολιτικών γραφείων, «κλπ.» που εξαιρούνται από αυτή την ιδιότυπη παρακολούθηση. Η πράξη όχι μόνο αποδεικνύει ότι οι άνθρωποι αυτοί που υποτίθεται ότι τους έχουν δοθεί τα δικαιώματα αυτά μετά από ενδελεχείς ελέγχους, είναι υπεράνω υποψίας, αλλά υποπίπτουν σε αξιόποινες πράξεις. Φυσικά, με αφορμή το γεγονός αυτό, οι περαιτέρω υποθέσεις που μπορεί να κάνει κανείς για την ασφάλεια του δικτύου της Βουλής είναι πάρα πολλές.

Διαδικτυακών δυσφημήσεων και εκβιασμών συνέχεια…

Τελειωμό φαίνεται να μην έχουν οι δυσφημίσεις στο διαδίκτυο. Με αφορμή την υπόθεση του press-gr άνοιξε ο ασκός του Αιόλου αφού έγινε γνωστό ότι εκκρεμούν πάνω από 150 σχετικές υποθέσεις. Συγκεκριμένα, τον Φεβρουάριο ο προϊστάμενός της Δίωξης Ηλεκτρονικού Εγκλήματος, κ. Σφακιανάκης, παρέδωσε στον εισαγγελέα πρωτοδικών πάνω από 150 μηνύσεις που αφορούν το ηλεκτρονικό έγκλημα, η πλειοψηφία των οποίων ασχολείται με δυσφημιστικά μηνύματα σε ιστοσελίδες. Σύμφωνα με την είδηση, ο εισαγγελέας επέστρεψε τις μηνύσεις στον κ. Σφακιανάκη έτσι ώστε να τις "ομαδοποιήσει" η υπηρεσία του και να σχηματιστούν οι αντίστοιχες δικογραφίες.

Το θέμα των δυσφημήσεων και των εκβιασμών μέσω Internet φαίνεται να λαμβάνει πλέον τεράστιες διαστάσεις και στη χώρα μας. Σύμφωνα με δημοσίευμα της Καθημερινής, δεν είναι λίγες οι φορές που έχει απασχοληθεί η Δίωξη Ηλεκτρονικού Εγκλήματος με παρόμοιες υποθέσεις, οι οποίες συχνά έχουν και «ροζ» αποχρώσεις. Υπάρχουν αρκετά παραδείγματα περιπτώσεων που επιτήδειοι απείλησαν να ανεβάσουν φωτογραφίες ή βίντεο με προσωπικές στιγμές είτε με αντάλλαγμα κάποιο χρηματικό ποσό είτε απλά για λόγους εκδίκησης.

Ηλεκτρονική Βιομηχανική Κατασκοπεία στην Ελλάδα

Εντύπωση προκάλεσαν στις αρχές του χρόνου δημοσιεύματα σε γνωστά ειδησεογραφικά διαδικτυακά sites, Ελληνικά αλλά και του εξωτερικού, που ενέπλεκαν Έλληνα μαθηματικό και προγραμματιστή σε υπόθεση βιομηχανικής κατασκοπίας που αφορούσε στη γαλλική εταιρία Dassault. Δυο εβδομάδες νωρίτερα η εφημερίδα Καθημερινή είχε αναφέρει το συμβάν σε άρθρο της, χωρίς να δίνει συγκεκριμένες λεπτομέρειες. Μάλιστα, στο ίδιο άρθρο αναφέρθηκαν και άλλες παρόμοιες περιπτώσεις με εταιρίες που οδηγήθηκαν ακόμα και στην πτώχευση. Χαρακτηριστικό είναι, όπως έχουμε αναφέρει και στο παρελθόν, ότι τα συμβάντα αυτά δεν έρχονται στη δημοσιότητα με το φόβο της αρνητικής διαφήμισης των εμπλεκόμενων εταιριών. Βέβαια, η πρακτική αυτή έχει οδηγήσει αρκετούς, ειδήμονες και μη, να θεωρούν ότι «στην Ελλάδα δε συμβαίνουν αυτά που ακούμε στην Αμερική». Την ίδια ώρα οι διωκτικές αρχές εκφράζουν αδυναμία να μας προστατέψουν διαπιστώνοντας σε αρκετές περιπτώσεις κενά στη σχετική νομοθεσία.

Defacements σε κρατικές ιστοσελίδες

Για άλλη μία φορά κρατικά site αποδεικνύονται ευάλωτα σε επιθέσεις. Συγκεκριμένα, εισβολέας με το ψευδώνυμο r0ukZ0uk άλλαξε τις αρχικές σελίδες των www.neagenia.gr και foundation.parliament.gr τοποθετώντας κείμενα για την παιδεία και τη δημοκρατία αλλά και προσωπικές του απόψεις σχετικά με τα θέματα αυτά. Αν και οι σελίδες επανήλθαν πολύ γρήγορα στη κανονική τους μορφή, οι αλλαγές έγιναν αντιληπτές από αρκετούς με αποτέλεσμα το θέμα να αναφερθεί στα διαδικτυακά μέσα ενημέρωσης (κυρίως blogs) άλλα όχι και στα συμβατικά.

OWASP.GR

Συμμετοχή OWASP.gr στο 1ο Συνέδριο Κοινοτήτων ΕΛ/ΛΑΚ

Η Ελληνική ομάδα εργασίας του OWASP θα συμμετάσχει στο 1ο Συνέδριο Κοινοτήτων Ελεύθερου Λογισμικού/Λογισμικού Ανοιχτού Κώδικα που διοργανώνεται στις 21 και 22 Μαρτίου στο Εθνικό Μετσόβιο Πολυτεχνείο (http://www.fosscomm.gr/). Το Συνέδριο αυτό θα αποτελέσει και την πρώτη επίσημη συγκέντρωση των μελών του OWASP.gr. Έτσι, σας περιμένουμε όλους εκεί, για να γνωριστούμε αλλά και να γνωρίσετε από κοντά τις προσπάθειες που κάνουμε.

Στόχος του OWASP.gr θα είναι να παρουσιάσει στο ευρύ κοινό που υποστηρίζει τις πρωτοβουλίες ΕΛ/ΛΑΚ τις προσπάθειές του για την αφύπνιση της Ελληνικής κοινότητας, απλούς χρήστες αλλά και επαγγελματίες, προγραμματιστές και στελέχη οργανισμών, σχετικά με θέματα ασφάλειας στο Διαδίκτυο. Στα πλαίσια αυτά θα παρουσιαστεί η Ελληνική μετάφραση του OWASP Top 10 2007 αλλά και ένα εργαλείο εύρεσης ευπαθειών σε εφαρμογές διαδικτύου που αυτό τον καιρό αναπτύσσεται.

Πέρα από τη συμμετοχή σας, σας καλούμε να στείλετε τις προτάσεις σας έτσι ώστε η παρουσία του OWASP.gr στο συνέδριο αυτό να γίνει όσο πιο επιτυχημένη γίνεται.

Η παρουσίαση του OWASP.gr θα λάβει χώρα το Σάββατο, 21 Μαρτίου στις 17:50 σύμφωνα με το πρόγραμμα που υπάρχει εδώ: http://www.fosscomm.gr/xoops20171/htdocs/uploads/programma_synedriou.html ενώ πληροφορίες για την πρόσβαση στο χώρο του συνεδρίου θα βρείτε στο site του συνεδρίου: http://www.fosscomm.gr/