OWASP – The Open Web Application Security Project

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

Μηνιαίο Ενημερωτικό Δελτίο – Ιανουάριος 2008

ΕΙΣΑΓΩΓΙΚΟ ΣΗΜΕΙΩΜΑ

Μετά από πολύμηνη διακοπή επιστρέφουμε με μεγάλη διάθεση να ενημερώσουμε το κοινό του OWASP.gr για τις εξελίξεις στον χώρο μας, δίνοντας ιδιαίτερη έμφαση στην Ελληνική Επικαιρότητα. Καταρχήν θα θέλαμε να απολογηθούμε για αυτή την αισθητή καθυστέρηση, αλλά οφείλεται σε υποχρεώσεις προς την πατρίδα του έως τώρα αρχισυντάκτη του newsletter μας. Έτσι, νέος αρχισυντάκτη ανέλαβε καθήκοντα για όσο διάστημα ο παλιός υπηρετεί την πατρίδα.

Στο συγκεκριμένο newsletter καλύπτουμε συνοπτικά τα σημαντικότερα γεγονότα όλου αυτού του διαστήματος που δεν υπήρχε ενημέρωση. Στόχος μας είναι να κάνουμε το παρόν πιο εύχρηστο και να του δώσουμε καθαρά χαρακτήρα ενημέρωσης. Σύντομα θα επανέλθουμε στους κανονικούς ρυθμούς έκδοσης του newsletter μιας και οι εξελίξεις στην επικαιρότητα είναι πλέον ραγδαίες.

Επί ευκαιρίας θέλουμε να σας ενημερώσουμε για μια νέα στήλη που αποφασίσαμε να υπάρχει στο ενημερωτικό δελτίο του OWASP.gr και που θα αφορά την δημοσίευση σύντομων άρθρων για επίκαιρα θέματα που απασχολούν το διαδίκτυο. Κάθε φορά θα παρουσιάζουμε συνοπτικά ένα άρθρο βγαλμένο μέσα από τις εμπειρίες μας στο διαδίκτυο ή ακόμη και σε γενικότερα θέματα της πληροφορικής. Θεωρούμε ότι θα πρέπει με τον τρόπο μας να συμβάλλουμε ώστε όλοι οι χρήστες του διαδικτύου να είναι πλήρως ενημερωμένοι, ιδιαίτερα όσον αφορά θέματα απειλών στο διαδίκτυο. Φυσικά είμαστε ανοικτοί τόσο σε προτάσεις για θέματα που θα θέλατε να καλύψουμε ή ακόμα και ολόκληρα άρθρα στην κατεύθυνση αυτή.

ΕΛΛΗΝΙΚΗ ΕΠΙΚΑΙΡΟΤΗΤΑ

Παραίτηση Προέδρου Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Την παραίτησή τους υπέβαλαν στον Πρόεδρο της Βουλής και στον υπουργό Δικαιοσύνης, ο Πρόεδρος και τα μέλη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στις 19/11/2007. Η Αρχή προχώρησε σε αυτή την κίνηση καθώς δεν τηρήθηκε απόφασή της και καταγράφηκε η πορεία του Πολυτεχνείου μέσω του κλειστού κυκλώματος C4I, ύστερα από σχετική άδεια που ζήτησε η αστυνομία από τον εισαγγελέα. Αξίζει να σημειωθεί ότι η Αρχή έχει ρητώς απαγορεύσει την λειτουργία του συστήματος C4I, ιδιαίτερα όταν αυτό πρόκειται να χρησιμοποιηθεί για την καταγραφή διαδηλώσεων, ενώ από την άλλη πλευρά ο υπουργός Δημόσιας Τάξης έχει υποβάλλει αίτηση ακυρώσεως όπως δικαιούται από τον νόμο. Η υπόθεση εκκρεμεί ενώπιον της ολομέλειας του Συμβουλίου της Επικρατείας (ΣτΕ).

Ο Πρόεδρος της Αρχής κ. Γουργουράκης, δήλωσε ότι «Με τον τρόπο αυτό παραβιάστηκαν ευθέως οι διατάξεις της Αρχής που έχουν προαναφερθεί και εκ των πραγμάτων πλήττεται, κατά τη γνώμη μου, η συνταγματικώς κατοχυρωμένη ανεξαρτησία της και μειώνεται το κύρος της, το οποίο έχω, ως εκ της θέσεώς μου, υποχρέωση να υπερασπίζομαι και να προστατεύω».

Το θέμα πυροδότησε και συντηρεί ακόμα έντονες συζητήσεις στα μέσα, για τη λειτουργία των καμερών αυτή καθεαυτή, το ρόλο της αρχής, την ανεξαρτησία της αλλά και τη σχέση μεταξύ των διαφόρων φορέων.

Νέος ιστοχώρος Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Με την ευκαιρία της παγκόσμιας ημέρας προστασίας προσωπικών δεδομένων η Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα παρουσίασε σε συνέντευξη τύπου στις 28/1/2008 το νέο της ιστοχώρο. Η νέα διαδικτυακή πύλη ήρθε να αντικαταστήσει το παλιό παρωχημένο και όχι ιδιαίτερα λειτουργικό site της Αρχής. Στη νέα υλοποίησή του περιέχονται περισσότερες πληροφορίες σχετικά με τα θέματα της Αρχής ενώ πλέον προβλέπεται και η αλληλεπίδραση με πολίτες και υπεύθυνους επεξεργασίας. Για παράδειγμα ένας πολίτης μπορεί να υποβάλλει μία προσφυγή μέσα από το site και στη συνέχεια να παρακολουθήσει την πορεία της, να γραφεί στη λίστα του Άρθρου 13 και να υποβάλλει ηλεκτρονικά οποιοδήποτε έγγραφο σχετίζεται με τις υποθέσεις του. Αντίστοιχα, οι υπεύθυνοι επεξεργασίας μπορούν πλέον ηλεκτρονικά να υποβάλλουν γνωστοποιήσεις και αιτήσεις για άδειες αλλά και να λαμβάνουν τη λίστα του Άρθρου 13 με ένα πολύ εύκολο και άμεσο τρόπο.

Στη συγκεκριμένη συνέντευξη τύπου ο Πρόεδρος της αρχής αναφέρθηκε και στο θέμα της παραίτησής του και αναπόφευκτα δέχθηκε και αρκετές σχετικές ερωτήσεις. Συγκεκριμένα αιτιολόγησε την απόφαση αυτού και των μελών της αρχής να παραμείνουν υπηρεσιακά στις θέσεις τους για ένα «εύλογο χρονικό διάστημα», όπως ορίζει ο νόμος, εξαιτίας

«επειγόντων ζητημάτων που δεν επιδέχονται αναβολή» (αναφέρθηκε χαρακτηριστικά η περίπτωση Ζαχόπουλου). Το εύλογο αυτό χρονικό διάστημα λήγει στις 19/2/2008, τρεις μήνες μετά την παραίτησή τους, οπότε και η Πολιτεία, αναλαμβάνοντας τις ευθύνες της, οφείλει να έχει ορίσει νέο Πρόεδρο και νέα μέλη. Στη συνέχεια ο Πρόεδρος έκανε μια σύντομη αναδρομή στα πεπραγμένα της Αρχής, αναφέροντας χαρακτηριστικά ότι στη φετινή έκθεση του οργανισμού Privacy International, η χώρα μας πρώτευσε σε πολλά θέματα που αφορούν την προστασία της ιδιωτικότητας του πολίτη (περισσότερα σχετικά στο επόμενο newsletter). Τέλος, δεν θέλησε να πάρει θέση στις πολλές ερωτήσεις που δέχθηκε για την υπόθεση Ζαχόπουλου, αναφέροντας χαρακτηριστικά ότι αποτελεί μέρος δικογραφίας και αρμόδια πλέον είναι τα ποινικά δικαστήρια.

Θύματα phishing οι Έλληνες χρήστες

Με παραπλανητικά μηνύματα ηλεκτρονικής αλληλογραφίας επιτήδειοι προσπαθούν να αποσπάσουν ευαίσθητα προσωπικά δεδομένα του αποδέκτη όπως τραπεζικούς λογαριασμούς, αριθμούς πιστωτικών καρτών, κλπ. Οι επιτήδειοι, που πιθανότατα προέρχονται από το εξωτερικό καθώς το περιεχόμενο των μηνυμάτων υστερεί συντακτικά και δείχνει να προέρχεται από αυτοματοποιημένο μεταφραστικό σύστημα, προσποιούνται ότι επικοινωνούν εκ μέρος της Citibank ή της τράπεζας Πειραιώς με σκοπό να πείσουν τον αποδέκτη να εκτελέσει κάποιο πρόγραμμα ή να ακολουθήσει κάποιο συγκεκριμένο σύνδεσμο στο διαδίκτυο. Χαρακτηριστικό παραμένει το γεγονός ότι τα ελληνικά των επιτήδειων παραμένουν φτωχά με αποτέλεσμα τα σχετικά e-mail να βρύθουν από λάθη. Ουκ ολίγες φορές μας έχουν απασχολήσει περιστατικά phishing στην Ελλάδα, γεγονός που κατατάσσει αυτή την μορφή ηλεκτρονικής απειλής πρώτη και με διαφορά στην λίστα. Τον τελευταίο καιρό πάντως, παρατηρείται έγκυρη αντίδραση των σχετικών αρχών αφού πολύ γρήγορα αντιλαμβάνονται τις επιθέσεις αυτές και καταργούν τα σχετικά κακόβουλα site, αναδρομολογώντας τα στη σωστή διεύθυνση όπου υπάρχει και σχετική ειδοποίηση.

Μπαράζ defacement σε ιστοσελίδες Ελληνικών σχολείων

Ανησυχίες προκαλούν οι συχνές επιθέσεις που δέχονται ελληνικές ιστοσελίδες, αλλά ακόμη περισσότερο όταν στόχος γίνονται δημόσιοι οργανισμοί. Τα defacement έχουν γίνει πλέον της μόδας σε ιστοσελίδες Ελληνικών σχολείων, με το πιο πρόσφατο γεγονός που ιστοσελίδα σχολείου της Πάτρας δέχθηκε επίθεση και το περιεχόμενό της αντικαταστάθηκε με πορνογραφικό υλικό! Η συγκεκριμένη επίθεση εκτιμάται ότι προέρχεται εκτός Ελλάδας, και για μια ακόμη φορά εντοπίζεται η ανάγκη σύστασης Ομάδας Άμεσης Επέμβασης με σκοπό να προλαμβάνει και να αντιμετωπίζει τέτοιου είδους περιστατικά.

Διεθνης Επικαιροτητα

Υπολογιστής του Β' Παγκόσμιου Πολέμου αποκρυπτογραφεί μηνύματα

Στη Μεγάλη Βρετανία μετά από 60 χρόνια απουσίας, πανίσχυρος υπολογιστής μπήκε πάλι σε λειτουργία και άρχισε να αποκρυπτογραφεί μηνύματα. Ο Colossus, όπως ονομάζεται, είχε χρησιμοποιηθεί στον Β' Παγκόσμιο πόλεμο για να προδώσει τις κινήσεις των Γερμανών, ενώ στην συνέχεια καταστράφηκε από τους Βρετανούς για να παραμείνει μυστική η τεχνολογία. Η ανακατασκευή του διήρκεσε 15 χρόνια. Εκτιμάται ότι ο συγκεκριμένος υπολογιστής με τις δυνατότητες που είχε τότε, συντόμευσε τον πόλεμο κατά 1,5 χρόνο.

Ηλεκτρονικο εγκλημα – τα δικαιωματα μας απεναντι στο spamming

Η συνεχής ανάπτυξη της πληροφορικής και του διαδικτύου, έχει επιφέρει σημαντικές αλλαγές στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Το γεγονός αυτό έχει δημιουργήσει μια εικονική κοινωνία, που μέσα σε αυτή δραστηριοποιούνται διαφόρων ειδών χρήστες με διαφορετικούς σκοπούς και φιλοδοξίες, καθώς και επιχειρήσεις που αποσκοπούν στο κέρδος. Όπως σε κάθε οργανωμένη κοινωνία, έτσι και σε κάθε «ανοργάνωτη» εικονική κοινωνία, υπάρχουν οι συνθήκες για την ανάπτυξη οποιασδήποτε μορφής εγκλήματος που συνοψίζονται στον όρο **Ηλεκτρονικό Έγκλημα**. Μέσω του μηνιαίου newsletter και κάτω από τις αρχές και την φιλοσοφία του OWASP, αποφασίσαμε να αναπτύξουμε συνοπτικά τα δικαιώματα του Έλληνα Χρήστη απέναντι στην πιο διαδεδομένη μορφή ηλεκτρονικού εγκλήματος, το **Spamming**. Η ανάγκη μου αυτή πηγάζει στην πρόσφατη ενημέρωσή μας ότι και Ελληνικές μικρομεσαίες επιχειρήσεις επιλέγουν αυτή την μορφή προώθησής τους.

*«Αυτό το e-mail δεν μπορεί να θεωρηθεί spam εφόσον αναγράφονται τα στοιχεία του αποστολέα και διαδικασίες διαγραφής από την λίστα παραληπτών. Αν είσαστε σε αυτή τη λίστα κατά λάθος ή για οποιονδήποτε άλλο λόγο θέλετε να διαγραφεί το e-mail σας από αυτή τη λίστα παραληπτών e-mail άπλα απαντήστε σε αυτό το e-mail με θέμα "UNSUBSCRIBE" στην ηλεκτρονική διευθυνση ******@******.gr Αυτό το μήνυμα πληρεί τις προυποθέσεις της Ευρωπαικής νομοθεσίας περί διαφημιστικών μηνυμάτων. Κάθε μήνυμα θα πρέπει να φέρει τα πλήρη στοιχεία του αποστολέα ευκρινώς και θα πρέπει να δίνει στον δέκτη τη δυνατότητα διαγραφής. (Directiva 2002/31/CE του Ευρωπαικού Κοινοβουλίου Relative as A5-270/2001 του Ευρωπαικού Κοινοβουλίου).»*

Το παραπάνω κείμενο συνοδεύεται σε σχεδόν όλα τα Spam email από Ελληνικές επιχειρήσεις, αλλά ποιές είναι οι αλήθειες και ποιά τα ψέματα πίσω από αυτό το κείμενο;

Δυστυχώς πολλές επιχειρήσεις εκμεταλλεύονται το γεγονός ότι οι χρήστες είναι ανενημέρωτοι σχετικά με τα δικαιώματά τους στο διαδίκτυο και έτσι ανενόχλητες προχωρούν σε διαφόρων ειδών αθέμιτες διαφημίσεις, πολλές φορές παρερμηνεύοντας έντεχνα την υπάρχουσα νομοθεσία. Παρακάτω θα προσπαθήσω να αναλύσω συνοπτικά τα βασικά σημεία όσον αφορά την αλληλογραφία spam και τις διαφόρων ειδών παρερμηνείες που μπορούν να γίνουν.

Το πρώτο σημείο που θα πρέπει να εστιάσουμε την προσοχή μας, ανεξάρτητα με το περιεχόμενο του παραπάνω κειμένου, είναι η εύλογη ερώτηση για το πώς βρέθηκε η ηλεκτρονική μας διεύθυνση στην λίστα μαζικής αποστολής της επιχείρησης. Η επιχείρηση οφείλει να τηρεί τις προϋποθέσεις του Δικαίου Προστασίας των Δεδομένων Προσωπικού Χαρακτήρα για την συλλογή ηλεκτρονικών διευθύνσεων, κάτι που δεν συμβαίνει στις περισσότερες περιπτώσεις. Σκόπιμα στα spam email που λαμβάνουμε δεν αναφέρεται άμεσα που ή ποιος πρόσθεσε την διεύθυνση ηλεκτρονικού μας ταχυδρομείου σε αυτή την λίστα και ακόμη περισσότερο που βρήκαν την ηλεκτρονική μας διεύθυνση. Σε σύγκριση με το παραπάνω κείμενο, ως άλλοθι αναφέρεται *«Αν είσαστε σε αυτή τη λίστα κατά λάθος..»*, κάτι που θεωρητικά δίνει «άφεση αμαρτιών» στον αποστολέα.

Στην συνέχεια επιβάλλεται από τον νόμο ο αποστολέας της αλληλογραφίας spam, να έχει συμβουλευτεί πρώτα διαφόρων ειδών καταλόγους με πρόσωπα που ρητά έχουν ζητήσει να

εξαιρούνται από τέτοιες ενέργειες, όπως για παράδειγμα η λίστα Robinson. Αυτό το βήμα τις περισσότερες φορές παραβλέπεται είτε λόγω άγνοιας από την πλευρά της επιχείρησης, είτε σκόπιμα για εμπλουτισμό της λίστας με ακόμη περισσότερους παραλήπτες.

Τέλος, οι παρακάτω προϋποθέσεις ορίζονται όσον αφορά το περιεχόμενο των spam email, προϋποθέσεις που πολλές φορές δεν τηρούνται, ή τηρούνται επιλεκτικά ανάλογα κάθε φορά με τα συμφέροντα και τις προθέσεις της επιχείρησης.

Αποφυγή παραπλανητικού τίτλου (subject)

Ο τίτλος σε καμία περίπτωση δεν θα πρέπει να είναι παραπλανητικός σε σχέση με την επιχείρηση καθώς και τίτλος που ελκύει τον αποδέκτη να το διαβάσει.

Αληθινά στοιχεία του αποστολέα

Τα αληθινά στοιχεία της επιχείρησης θα πρέπει να αναφέρονται ρητώς ώστε ο παραλήπτης να γνωρίζει κάθε λεπτομέρεια για το μήνυμα ηλεκτρονικής αλληλογραφίας και τον αποστολέα του.

Αναφορά για το αν η αποστολή έχει ζητηθεί

Θα πρέπει ρητώς να δηλώνεται εάν η συγκεκριμένη αποστολή έχει ζητηθεί από τον παραλήπτη ή αν πρόκειται καθαρά για πρωτοβουλία του αποστολέα.

Εύκολο τρόπο διαγραφής από την λίστα

Τέλος θα πρέπει να προβλέπεται εύκολος και άμεσος τρόπος διαγραφής από την λίστα παραληπτών.

Τι συμβαίνει όμως όταν κάτι από τα παραπάνω δεν έχει τηρηθεί..; Προβλέπεται από την ελληνική νομοθεσία ενδεχόμενη δίωξη της επιχείρησης για παράνομη μαζική ηλεκτρονική αλληλογραφία spam..; Πολλοί μύθοι υπάρχουν εδώ, μεταξύ των οποίων ότι ακόμη δεν υπάρχει νομοθεσία όσον αφορά το ηλεκτρονικό έγκλημα στην χώρα μας.

Η αλήθεια είναι πως όχι μόνο προβλέπεται στην ελληνική νομοθεσία, αλλά ήδη στην χώρα μας έχουν δικαστεί επιχειρήσεις που έχουν διαπράξει ηλεκτρονικό έγκλημα, κυρίως βάση του Προεδρικού Διατάγματος υπ' Αριθ. 131/2003 που πρόκειται για προσαρμογή στην οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου.

Ελπίζουμε η συγκεκριμένη αναφορά να έλυσε πολλές από τις απορίες σας όσον αφορά την ελληνική νομοθεσία γύρω από την ανεπιθύμητη ηλεκτρονική αλληλογραφία, που δυστυχώς έχει αρχίσει να υιοθετείται και από επιχειρήσεις της χώρας μας, χωρίς όμως να υπολογίζουν ότι με αυτό τον τρόπο το μόνο που καταφέρνουν είναι να δυσαρεστήσουν τον παραλήπτη, δηλαδή τον μελλοντικό πελάτη της επιχείρησης.