OWASP - The Open Web Application Security Project

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

Μηνιαίο Ενημερωτικό Δελτίο – Ιανουάριος 2007

ΕΛΛΗΝΙΚΗ ΕΠΙΚΑΙΡΟΤΗΤΑ

2007

Το 2007 είναι ήδη εδώ και οι προσδοκίες, όπως άλλωστε κάθε χρόνο είναι πολλές. Πολύ περισσότερο όταν το 2006 ήταν για την Ελλάδα μία χρονιά με σημαντικά γεγονότα στο χώρο της ασφάλειας πληροφοριών. Ειδικότερα, τόσο η πολύκροτη υπόθεση των υποκλοπών, όσο και η διοργάνωση του 1ου Συνεδρίου για τη Διακυβέρνηση του Internet, ένας βασικός άξονας του οποίου ήταν η ασφάλεια, αν μη τι άλλο προβλημάτισαν την ελληνική κοινή γνώμη και την ευαισθητοποίησαν σε θέματα ασφάλειας, ιδιωτικότητας και προσωπικών ελευθεριών.
Εμείς, από τη μεριά μας, να ευχηθούμε το 2007 να είναι μία χρονιά με περισσότερη συνειδητοποίηση και προβληματισμό σε θέματα ασφάλειας.

Ημερίδα e-Passports Security

Στις 8 Δεκεμβρίου πραγματοποιήθηκε στις εγκαταστάσεις του Athens Information Technology στην Παιανία σεμινάριο με θέμα «e-Passports: How secure are they?», ομιλητής του οποίου ήταν ο καθηγητής Τάσος Δημητρίου. Στην ομιλία του ο κ. Δημητρίου παρουσίασε τη μορφή των νέων διαβατηρίων, αναφέρθηκε στα χαρακτηριστικά της τεχνολογίας RFID που χρησιμοποιείται σε αυτά, στα προβλήματα ασφαλείας και συνεπώς στις απειλές που υπάρχουν ως προς την ιδιωτικότητα. Παράλληλα, παρουσιάστηκαν μέθοδοι αντιμετώπισης πιθανόν επιθέσεων που έχουν προταθεί από διεθνείς οργανισμούς.
Χαρακτηριστικό είναι ότι το σεμινάριο πραγματοποιήθηκε σε μία περίοδο που υπάρχει έντονος προβληματισμός για τα νέα διαβατήρια, την ασφάλειά τους και το κατά πόσο διασφαλίζουν την ιδιωτικότητα των πολιτών. Ειδικότερα, τους τελευταίους δύο μήνες είδαμε ερευνητές να προτείνουν αλλαγές στις προδιαγραφές ασφαλείας των διαβατηρίων που χρησιμοποιούν RFID τεχνολογία, να σπάνε ή ακόμα και να κλωνοποιούν μέσα σε 5 λεπτά τέτοια διαβατήρια. Έτσι, μετά το τέλος της ομιλίας, στα πηγαδάκια που δημιουργήθηκαν συζητήθηκε έντονα το θέμα της ασφάλειας και οι πιθανές επιπτώσεις μαζικών επιθέσεων ενώ μάλλον όλοι κατέληγαν ότι η τεχνολογία RFID περισσότερο αφαιρεί παρά προσθέτει στην ασφάλεια των διαβατηρίων και των μετακινήσεων γενικότερα.

Έκθεση του Συνηγόρου του Πολίτη για τις δυσκολίες έκδοσης νέων διαβατηρίων

Στις 12 Δεκεμβρίου ο Συνήγορος του Πολίτη έδωσε στη δημοσιότητα ειδική έκθεση με θέμα «Δυσλειτουργίες στην έκδοση διαβατηρίων από τις αστυνομικές αρχές, με βάση τον ν. 3103/2003», στην οποία εκθέτει όχι μόνο τα διαδικαστικά προβλήματα τα οποία λίγο πολύ όλοι είχαμε αντιμετωπίσει ή ακούσει, αλλά και πολύ σοβαρά νομικά προβλήματα. Εντύπωση προκαλεί η εξαρχής επισήμανση ότι η μεταφορά της αρμοδιότητας της έκδοσης διαβατηρίων από τις νομαρχίες στην αστυνομία έγινε κυρίως για λόγους ασφαλείας, μιας και η αστυνομία είναι περισσότερο κατάλληλη στον έλεγχο ταυτότητας. Παράλληλα όμως, σε όλο το κείμενο της έκθεσης αναφέρεται συχνά η ανάγκη σεβασμού των δικαιωμάτων και των προσωπικών ελευθεριών των πολιτών.
Αφού παρουσιαστούν αναλυτικά τα πρακτικά προβλήματα που κατά καιρούς απασχόλησαν και τις ειδήσεις, όπως οι προδιαγραφές των φωτογραφιών, η εξυπηρέτηση με αριθμούς προτεραιότητας κλπ., δίνεται έμφαση σε προβλήματα οικονομικού (παράβολο παλαιών διαβατηρίων, χρέωση κακέκτυπων διαβατηρίων) και νομικού χαρακτήρα. Ειδικότερα, αναφέρεται ότι σε πολλές περιπτώσεις η αστυνομία έδειξε υπερβάλλοντα ζήλο στον έλεγχο των στοιχείων των αιτούντων, ελέγχοντας πέρα από την ταυτότητά τους και το αν υπάρχουν απαγορεύσεις εξόδου από τη χώρα, και το αν εκκρεμεί κάποια δίωξη εναντίον τους. Ο Συνήγορος του Πολίτη δίνει ιδιαίτερη έμφαση σε αυτό το θέμα και μάλιστα δεσμεύεται ότι θα επανέλθει με νέα ειδική έκθεση. Τέλος, παραθέτει προτάσεις προς τις αρμόδιες αρχές για την αντιμετώπιση των προβλημάτων που εκτέθηκαν.
Πέρα από το ενδιαφέρον του κειμένου, που εν ολίγοις παρουσιάζει ιστορίες καθημερινής τρέλας από την ελληνική γραφειοκρατία, είναι ιδιαίτερα ευχάριστο να διαπιστώνει κανείς για ακόμα μία φορά ότι οι ανεξάρτητες αρχές της χώρας είναι πάντα σε εγρήγορση, επιτελώντας το έργο τους με σοβαρότητα και συνέπεια, κυριολεκτικά στην υπηρεσία του πολίτη.

Διευκρινήσεις για τις συναλλαγές με PIN στα ATM
Διευκρινήσεις αναγκάστηκε να δώσει η Ένωση Ελληνικών Τραπεζών σχετικά με τη χρήση των PIN στα ATM, μετά από σχετικό chain mail που διαδόθηκε. Συγκεκριμένα, διαδόθηκε ευρύτατα ένα chain mail το οποίο πρότεινε σε χρήστες ATM να πληκτρολογήσουν το PIN τους ανάποδα αν κάποιος τους εξαναγκάσει με τη βία να πραγματοποιήσουν ανάληψη. Στην περίπτωση αυτή, σύμφωνα με το mail, το σύστημα θα μπλόκαρε και θα ειδοποιούσε τις αρχές. Φαίνεται ότι η θεωρία αυτή γρήγορα έλαβε διαστάσεις επιδημίας (δεν αποκλείεται να μπλόκαραν αρκετές κάρτες κάποιων που ίσως θέλησαν να το δοκιμάσουν και στην πράξη), και έτσι η ΕΕΤ αναγκάστηκε να εκδώσει ανακοίνωση στην οποία ανέφερε ότι η ανάστροφη πληκτρολόγηση του PIN αναγνωρίζεται ως λανθασμένη και τίποτα περισσότερο. Με την ευκαιρία μάλιστα, και εν όψει εορτών, υπενθύμισε στους συναλλασσόμενους να χρησιμοποιούν την κάρτα τους και το PIN με την απαραίτητη προσοχή. Το ευχάριστο στην υπόθεση είναι ότι η ΕΕΤ επέδειξε γρήγορα αντανακλαστικά. Ακόμα πιο ευχάριστο θα ήταν να επεδείκνυε εξίσου γρήγορα αντανακλαστικά σε περιπτώσεις phishing ή συμβάντων ασφάλειας γενικότερα.

Νέος ορισμός της λέξης "hacker"
Ιδιαίτερος θόρυβος δημιουργήθηκε στις αρχές του Δεκεμβρίου σχετικά με τη διαφάνεια των προσλήψεων επαγγελματιών οπλιτών. Συγκεκριμένα, τα αποτελέσματα που δημοσιεύτηκαν στη σελίδα του Υπουργείου Άμυνας άλλαξαν τρεις φορές. Η αντιπολίτευση κατηγόρησε την κυβέρνηση για αδιαφανείς διαδικασίες. Κύκλοι όμως του ΥΠΕΘΑ απέδωσαν τις αλλαγές στην ιστοσελίδα σε «ηλεκτρονικούς φαρσέρ». Ως συνήθως οι σχετικές συζητήσεις επικεντρώθηκαν στην πολιτική διάσταση του θέματος, παραβλέποντας το γεγονός ότι πολύ εύκολα κάποιος

άλλαξε τρεις φορές τη σελίδα του ΥΠΕΘΑ, τουλάχιστον όπως ισχυρίζεται η κυβέρνηση.

Απάτη με dialers
Στις αρχές του νέου χρόνου η αστυνομία συνέλαβε επιχειρηματία ο οποίος παγίδευε ιστοσελίδες με dialers. Ο 57χρονος, που μόνο το 2005 είχε αποκομίσει πάνω από 8 εκατομμύρια ευρώ από την παράνομη αυτή δραστηριότητα, είχε παγιδεύσει ακόμα και σελίδες του Δημοσίου. Μάλιστα, μόλις έμαθε ότι θα συλληφθεί υπέστη εγκεφαλικό και νοσηλεύεται σε νοσοκομείο φρουρούμενος. Απ' ότι φαίνεται πάντως οι σελίδες Υπουργείων και του Δημοσίου γενικότερα αποτελούν ένα συνηθισμένο και ίσως και εύκολο στόχο.

Νέα απάτη με κινητά
Απάτη με κινητά τηλέφωνα αποκαλύφθηκε πρόσφατα. Ωστόσο, οι πληροφορίες που διατίθενται από τα μέσα είναι αρκετά συγκεχυμένες. Συγκεκριμένα αναφέρθηκε ότι οι δράστες έστελναν μηνύματα ή πραγματοποιούσαν αναπάντητες κλήσεις σε κινητά θυμάτων, «αναγκάζοντάς» τα να τους τηλεφωνήσουν. Στη συνέχεια, ενώ τα θύματα πίστευαν ότι καλούσαν ένα απλό κινητό τηλέφωνο, η κλήση «εκτρεπόταν» σε αριθμούς υψηλής χρέωσης. Δυστυχώς δεν υπάρχουν περισσότερες τεχνικές πληροφορίες, οπότε οι υποθέσεις για τον ακριβή τρόπο υλοποίησης της απάτης είναι πολλές.

OWASP.gr

OWASP Newsletter
Πρόσφατα το OWASP εξέδωσε το πρώτο του newsletter το οποίο διανεμήθηκε στη λίστα, ενώ διαδικτυακά μπορεί κανείς να το βρει στη διεύθυνση:
https://www.owasp.org/index.php/OWASP_Newsletter_1
Το newsletter, που αναμένεται να εκδίδεται κάθε 1-2 εβδομάδες, περιλαμβάνει νέα της παγκόσμιας OWASP κοινότητας, πληροφορίες και νέα που αφορούν στα project που εκτελούνται αυτή τη στιγμή, αλλά και νεώτερα σχετικά με την ασφάλεια εφαρμογών.

Συνδρομή στο OWASP
Το OWASP αποτελεί ένα μη κερδοσκοπικό οργανισμό που λειτουργεί με την εθελοντική προσφορά των μελών του. Για την ενίσχυση των προσπαθειών του έχει θεσπίσει πρόγραμμα ετήσιων συνδρομών για ιδιώτες και εταιρίες. Πλεονεκτήματα της συνδρομής περιλαμβάνουν εμπορικές άδειες χρήσης του υλικού που προσφέρεται, εκπτώσεις σε συνέδρια, και άλλα. Για περισσότερες πληροφορίες μπορείτε να επισκεφθείτε τη σελίδα: http://www.owasp.org/index.php/Membership

ΔΙΕΘΝΗ ΚΑΙ ΑΛΛΑ

Ευρωπαϊκή Ένωση εναντίον Spam
Τον περασμένο μήνα η επίτροπος της Ευρωπαϊκής Ένωσης για την Κοινωνία της Πληροφορίας κα Vivian Reding δήλωσε: «Ήρθε η ώρα να μετατραπεί η πολιτική ανησυχία για το spam σε απτές πράξεις για την καταπολέμησή του. […] Ακολουθώντας τη γραμμή της Ευρωπαϊκής νομοθεσίας, οι ολλανδικές αρχές κατάφεραν να μειώσουν το τοπικό spam κατά 85%. Θα ήθελα να δω και άλλες χώρες

να πετυχαίνουν παρόμοια αποτελέσματα χρησιμοποιώντας πιο αποτελεσματικά μέσα.»
Παράλληλα η Ευρωπαϊκή Ένωση εξέδωσε τον περασμένο Νοέμβριο ανακοίνωση σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού. Στην ανακοίνωση αυτή, αφού εκτεθεί το σχετικό πρόβλημα, προτείνονται μέτρα και δράσεις για την καταπολέμησή του τόσο σε τοπικό όσο και σε ευρωπαϊκό επίπεδο. Μάλιστα, στην προσπάθεια αυτή το ρόλο συμβούλου αναλαμβάνει ο ENISA. Μένει να δούμε πόσο σύντομα τα κράτη-μέλη θα αναλάβουν δράση για τον περιορισμό του spam. Η κα Reding πάντως δεσμεύθηκε να επανέλθει σε ένα χρόνο για να επιβάλει επιπρόσθετα νομοθετικά μέτρα, αν αυτό κριθεί απαραίτητο.

Κλοπή προσωπικών λιστών διευθύνσεων από το Gmail
Πρόσφατα βρέθηκε ότι μπορεί εύκολα να υποκλαπεί η λίστα διευθύνσεων ενός χρήστη στο Gmail, αρκεί αυτός ο χρήστης να είναι online τη στιγμή της επίθεσης. Η επίθεση χρησιμοποιεί μια μορφή Cross Site Scripting και εκμεταλλεύεται το γεγονός ότι το Gmail αποθηκεύει τις λίστες αυτές σε αρχεία javascript. Παρόμοιο πρόβλημα υπήρχε και παλαιότερα με τη συγκεκριμένη υπηρεσία και ίσως αυτό σε συνδυασμό με άλλα προβλήματα αποτελεί το λόγο που παραμένει ακόμα σε beta μορφή.

Antivirus για Vista
Ύστερα από τη σωστή παρατήρηση αναγνωστών οφείλουμε να διευκρινίσουμε ότι στο προηγούμενο τεύχος εκ παραδρομής αναφέρθηκε πως δεν είχε κυκλοφορήσει αντικό συμβατό με τα Windows Vista. Για την ακρίβεια των πραγμάτων, αναφέρουμε ότι στις 14 Νοεμβρίου ανακοινώθηκε η συμβατότητα του NOD32 με τα Windows Vista, ενώ στις 23 Νοεμβρίου η Sophos ανακοίνωσε το Sophos Antivirus 6.5 που επίσης υποστηρίζει τα Windows Vista. Αν και η αλήθεια είναι πως το συγκεκριμένο άρθρο γράφτηκε πριν από αυτές τις ημερομηνίες, το OWASP.gr θα ήθελα να ευχαριστήσει για τη σωστή επισήμανση.

ΕΠΙΣΤΗΜΟΝΙΚΑ ΚΑΙ ΟΧΙ ΜΟΝΟ

RFID Guardian
Η ομάδα του A.S. Tanenbaum στο πανεπιστήμιο Vrije της Ολλανδίας σχεδίασε και κατασκεύασε μια επαναστατική πλατφόρμα για τη διαχείριση της ασφάλειας και της ιδιωτικότητας στα RFID. Ουσιαστικά πρόκειται για ένα RFID firewall, με το οποίο ο κάτοχος του RFID μπορεί να επιβλέπει και να ελέγχει την πρόσβαση στο tag του. Οι δυνατότητες του RFID Guardian επεκτείνονται στη διαχείριση κλειδιών, την αυθεντικοποίηση, τον έλεγχο πρόσβασης κ.α. Αναμφισβήτητα πρόκειται για ένα πολύ σημαντικό επίτευγμα το οποίο μάλιστα ανακοινώθηκε σε μια εποχή αυξανόμενης χρήσης αλλά και έντονης αμφισβήτησης της συγκεκριμένης τεχνολογίας.

Πηγή: M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006.

Ο ήχος της εκμετάλλευσης
Ο ελληνικής καταγωγής Pascal Cretain με έδρα το Λονδίνο παρουσίασε πρόσφατα ένα ενδιαφέρον καλλιτεχνικό πείραμα. Δημιούργησε ιδιότροπα ηχοτοπία στο χώρο του experimental ambient/noise χρησιμοποιώντας ως «πρώτη ύλη» πηγαίο κώδικα exploits και δημοφιλή εκτελέσιμα αρχεία από το χώρο της ασφάλειας πληροφοριών.

Η ελληνική ομάδα του OWASP τον προσέγγισε για μερικά σχόλια σε σχέση με τη μεθοδολογία του και τους στόχους του πειράματος:
«Το πείραμα μου δεν περιέχει τίποτα δύσκολο από προγραμματιστικής απόψεως. Χρησιμοποίησα το open source audio mixer Audacity (http://audacity.sourceforge.net), το οποίο παρέχει τη δυνατότητα μετατροπής οποιουδήποτε τύπου δεδομένων (ηχητικού ή μη) σε ηχομορφή με βάση μια τεχνική γνωστή ως PCM (Pulse Code Modulation). Το PCM κάνει sampling δεδομένων ανά τακτά χρονικά διαστήματα και παράγει μια ψηφιακή αναπαράσταση αναλογικών σημάτων. Αφού είχα μία ηχητική βάση για να δουλέψω, τροποποίησα τα δεδομένα αλλάζοντας tempos, speeds, pitches etc etc. Το όλο concept προέκυψε εντελώς φυσιολογικά. Επηρεάζομαι και λειτουργώ και στους τους 2 χώρους (experimental noise/ambient & information security) εδώ και αρκετά χρόνια. Θεωρώ ότι οι κοινότητες αυτές έχουν πάρα πολλά κοινά χαρακτηριστικά, και μοιράζονται αντισυμβατικό τρόπο σκέψης. Το ηχητικό μου πείραμα έχει σαν (ένα) στόχο να φέρει πιο κοντά τις δύο κοινότητες.»

Για περισσότερες πληροφορίες: http://www.myspace.com/pascalcretain

ΗΣΥΧΙΑ, ΤΑΞΗ ΚΑΙ… ΑΣΦΑΛΕΙΑ

- Τελικά το διαβατήριο για μια θέση στο δημόσιο είναι οι hackers
- Ούτε να ανησυχείς για τα RFID ούτε τίποτα
- Σίγουρη θέση και μάλιστα μετά μουσικής
- Ξέρουν να βάζουν σωστά και το PIN τους
- Και όλοι θα νομίζουν ότι πρόκειται για… φάρσα!