OWASP - The Open Web Application Security Project

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

Μηνιαίο Ενημερωτικό Δελτίο – Μάρτιος-Απρίλιος 2007

ΕΛΛΗΝΙΚΗ ΕΠΙΚΑΙΡΟΤΗΤΑ

No news is good news

Μετά από ένα πολυάσχολο για τον τομέα της ασφάλειας (και όχι μόνο) πρώτο δίμηνο του 2007, επανήλθε η ηρεμία. Για την ασφάλεια συνηθίζουμε να λέμε ότι η ηρεμία είναι καλό σημάδι, ένδειξη ότι δεν υπάρχουν επιθέσεις και ότι όλα είναι καλώς προφυλαγμένα. Κάποιοι λιγότερο αισιόδοξοι πιστεύουν ότι την ηρεμία διαδέχονται σημαντικά συμβάντα, που μας κάνουν να… τρέχουμε και να μη φτάνουμε.

Έτσι, ακολουθώντας τα σημάδια των καιρών, αποφασίσαμε να καθυστερήσουμε αυτό το newsletter του OWASP.gr, ελλείψη σημαντικών ειδήσεων. Παράλληλα, είμαστε στην ευχάριστη θέση να σας ανακοινώσουμε στο τεύχος αυτό τη συνεργασία μας με το e-business forum (http://www.ebusinessforum.gr) και συγκεκριμένα με την ομάδα εργασίας ΙΑ4, με αντικείμενο τις Προπαρασκευαστικές δράσεις για την δημιουργία Ελληνικού Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών (GR-CERT). Στα πλαίσια της συνεργασίας αυτής, ο κ. Βασίλης Βλάχος είχε την καλοσύνη να απαντήσει στις ερωτήσεις μας, παραθέτοντας τις απόψεις του για την ασφάλεια και το ανοιχτό λογισμικό.

Ομάδα Εργασίας ΙΑ4 του E-Business Forum

Εδώ και μερικούς μήνες το E-Business Forum (http://www.ebusinessforum.gr/) έχει δημιουργήσει μία ομάδα εργασίας η οποία έχει αναλάβει τις «Προπαρασκευαστικές δράσεις για την δημιουργία Ελληνικού Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών (GR-CERT)». Στη συγκεκριμένη Ομάδα Εργασίας προτείνεται η συμμετοχή στελεχών σε θέματα ασφάλειας τόσο από τον επιχειρηματικό όσο και από τον ακαδημαϊκό χώρο, τα οποία πιθανόν θα αποτελέσουν και τη βάση για την δημιουργία της πρώτης Ομάδας Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών. Επίσης σημαντική θα είναι η συμβολή στελεχών των τμημάτων Πληροφοριακών Συστημάτων από επιχειρήσεις και οργανισμούς προκειμένου να καταθέσουν την εμπειρία τους από προβλήματα τα οποία αντιμετωπίζουν σχετικά με περιστατικά ασφαλείας καθώς και τρόπους για την αμφίδρομη συνδρομή τους με το Κέντρο Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών. Επίσης, προσκαλούνται και στελέχη από επιχειρήσεις και από κρατικές υπηρεσίες που διατηρούν την δυνατότητα παρέμβασης στην λειτουργία του Διαδικτύου εντός της ελληνικής επικράτειας.

Το OWASP.gr καλεί κάθε ενδιαφερόμενο που κρίνει ότι μπορεί να βοηθήσει να επισκεφθεί τα site που περιγράφουν της δραστηριότητες της ομάδας

(http://www.ebusinessforum.gr/teams/teamsall/view/index.php?ctn=102&language=el και http://sense.dmst.aueb.gr/ia4/index.php/Main_Page) ή να επικοινωνήσει κατευθείαν με τον κ. Βασίλη Βλάχο (στοιχεία επικοινωνίας στις παραπάνω ιστοσελίδες). Στο τέλος Μαΐου η ομάδα θα διοργανώσει τη δεύτερη διαβούλευσή της. Στα πλαίσια αυτά μπορείτε να συνδράμετε αν:

- Είστε σε θέση να βοηθήσετε να εξασφαλίσουμε μια Επιστολή Υποστήριξης (Letter of Support) από τον οργανισμό που εργάζεστε ή τον συλλογικό φορέα που τον εκπροσωπεί. Ανεξάρτητες αρχές, συλλογικοί φορείς και δημόσιοι οργανισμοί αποτελούν πρώτη προτεραιότητα μας.
- Διαθέτετε υλικό (Business Plan κλπ) από την υποβολή προτάσεων σχετικών με το αντικείμενο της ομάδας IA4, το οποίο πιθανόν θα μπορούσε να επαναχρησιμοποιηθεί σε αυτή τη προσπάθεια (και δεν έχετε αντίρρηση να το μοιραστείτε μαζί μας).
- Μπορείτε να συμβάλετε με κάποιον άλλο συγκεκριμένο και σαφώς καθορισμένο τρόπο, ο οποίος δεν εμπίπτει στις παραπάνω γενικές κατηγορίες.

Συνέντευξη με τον κ. Βασίλη Βλάχο

Ο κ. Βασίλης Βλάχος είναι υποψήφιος διδάκτορας του Τμήματος Διοικητικής Επιστήμης και Τεχνολογίας του Οικονομικού Πανεπιστημίου Αθηνών, υπό την επίβλεψη του Αν. Καθ. κ. Σπινέλλη. Το αντικείμενο της έρευνάς του περιστρέφεται γύρω από την ασφάλεια πληροφοριών. Ο κ. Βλάχος, ως μέλος της ερευνητικής ομάδας του κ. Σπινέλλη, έχει εκτεταμένη εμπειρία σε έργα που σχετίζονται με την ασφάλεια πληροφοριών και το λογισμικό ανοιχτού κώδικα. Στη συνέχεια, παραθέτουμε τις απαντήσεις του στις ερωτήσεις που του θέσαμε:

OWASP.gr: - Ασφάλεια και Λογισμικό Ανοιχτού Κώδικα (ΛΑΚ): οξύμωρο; Κάποιοι υποστηρίζουν ότι εύκολα μπορεί κανείς να εισάγει κακόβουλα κομμάτια κώδικα σε ΛΑΚ χωρίς να γίνει αντιληπτός. Συμμερίζεστε την άποψη αυτή;
Βασίλης Βλάχος: - Όχι ιδιαίτερα. Πιστεύω ότι είναι εξαιρετικά δύσκολο κάποιος να καταφέρει να προσθέσει κομμάτια κακόβουλου κώδικα σε μεγάλα projects ΛΑΚ περνώντας απαρατήρητος. Τα περισσότερα έργα ΛΑΚ διαθέτουν εσωτερικές δομές ελέγχου, ώστε κάθε κομμάτι κώδικα
που καταλήγει στο κεντρικό repository, να έχει ελεγχθεί αρκετές φορές από έμπιστα μέλη του projects. Σε γενικές γραμμές θεωρώ ότι είναι πολύ μεγαλύτερος ο κίνδυνος να εισαχθεί κακόβουλος κώδικας σε Κλειστό - Εμπορικό Λογισμικό από κάποιο δυσαρεστημένο προγραμματιστή, παρά σε οποιαδήποτε γνωστή εφαρμογή ΕΛ/ΛΑΚ.

OWASP.gr: - Τίθεται κατά τη γνώμη σας θέμα σύγκρισης της ασφάλειας εφαρμογών ΕΛ/ΛΑΚ σε σχέση με τις υπόλοιπες εμπορικές εφαρμογές;
B.B.: - Δεν νομίζω ότι μπορεί να γίνει άμεση σύγκριση. Σε μια εμπορική εφαρμογή εμπιστεύεσαι αποκλειστικά το όνομα, το ιστορικό σε θέματα ασφαλείας και το κύρος της εταιρίας που την κατασκευάζει. Αντίθετα, στο ΕΛ/ΛΑΚ εάν κάποιος είναι "παρανοϊκός" με την ασφάλεια ή αν η συγκεκριμένη εφαρμογή προορίζεται να χρησιμοποιηθεί σε τεχνολογικά κρίσιμες υποδομές, υπάρχει η δυνατότητα ελέγχου της γραμμής προς γραμμή.

OWASP.gr: - Υπάρχει, ή θα μπορούσε να υπάρξει κάποιος μηχανισμός ελέγχου ή πιστοποίησης της ασφάλειας των εφαρμογών ΕΛ/ΛΑΚ;
B.B.: - Δε γνωρίζω κάποιον μηχανισμού ελέγχου που να παρέχει πιστοποιητικά ασφάλειας για εφαρμογές ΕΛ/ΛΑΚ. Από την άλλη πλευρά, υπάρχουν εξαιρετικά εργαλεία που χρησιμοποιούνται για την ανάλυση ή/και την μεταγλώττιση του

πηγαίου κώδικα, τα οποία μπορούν να εντοπίσουν και να απαλείψουν κενά ασφάλειας. Συνεπώς, υπάρχει όλη η απαιτούμενη υποδομή για να αναπτυχθεί πολύ ασφαλές ΕΛ/ΛΑΚ.

OWASP.gr: - Συνοπτικά, ποιος είναι ο στόχος του Software Quality Observatory for Open Source Software (http://www.sqo-oss.eu/);
B.B: - Το ερευνητικό έργο SQO-OSS χρηματοδοτείται από την Ευρωπαϊκή Ένωση και στοχεύει να αποτελέσει ένα παρατηρητήριο για την ποιότητα των εφαρμογών ΕΛ/ΛΑΚ. Πιστεύουμε, ότι με αυτό το τρόπο θα διευκολύνουμε τις επιχειρήσεις και τους πολίτες να επιλέξουν λογισμικό που να ικανοποιεί τις απαιτήσεις τους, δίνοντας τους την δυνατότητα να αποκτήσουν μια ολοκληρωμένη εικόνα, τόσο ως τον τρόπο με τον οποίο κατασκευάζεται (αριθμός προγραμματιστών, παραγωγικότητα, χρόνος αντιμετώπισης προβλημάτων), όσο και ως προς τη δομή του (ασφάλεια, αξιοπιστία, λειτουργικότητα, ακρίβεια, απόδοση, συντηρησιμότητα).

OWASP.gr: - Στα πλαίσια αυτά, έχουν υιοθετηθεί κάποια κριτήρια σχετικά με την ασφάλεια και την ανάπτυξη ασφαλούς λογισμικού;
B.B: - Η ασφάλεια αποτελεί βασικό παράγοντα για την υιοθέτηση ή την απόρριψη κάθε εφαρμογής λογισμικού, συνεπώς δε θα μπορούσαμε σε καμία περίπτωση να παραβλέψουμε ένα τόσο σημαντικό ζήτημα, από την διαδικασία αξιολόγησης του SQO-OSS. Επειδή όμως οι συνέπειες από την έλλειψη πρόνοιας σε ζητήματα ασφάλειας δεν γίνονται άμεσα αντιληπτές στον τελικό χρήστη, καθώς δεν επηρεάζουν την λειτουργικότητα ενός προγράμματος, απαιτείται ειδική μεθοδολογία για την αξιολόγηση της ασφάλειας των εφαρμογών ΕΛ/ΛΑΚ. Είναι κάτι το οποίο μας απασχολεί έντονα, δουλεύουμε αρκετά πάνω σε αυτό και θα έχουμε σύντομα περισσότερα πράγματα να ανακοινώσουμε.

OWASP.gr: - Πώς ακριβώς ελέγχονται μεγάλα projects και πώς γίνεται το benchmarking σε θέματα ασφάλειας;
B.B: - Η πρόσβαση στον πηγαίο κώδικα ενός λογισμικού επιτρέπει την ανάλυση του από εργαλεία που επεξεργάζονται τον κώδικα και εντοπίζουν λάθη και χρήση κακών προγραμματιστικών τεχνικών (static analysis tools), όπως χρήση επισφαλών συναρτήσεων, μη έλεγχος εισερχόμενων από το χρήστη τιμών κτλ. Μια άλλη τεχνική είναι το fuzzing, κατά το οποίο εισάγουμε μεγάλο όγκο δεδομένων, τα οποία το πρόγραμμα δεν αναμένει και με αυτό τον τρόπο τεστάρουμε τη συμπεριφορά του σε ακραίες συνθήκες. Μια ενδεχόμενη κατάρρευση του προγράμματος φανερώνει την ύπαρξη σοβαρών προβλημάτων στην ασφάλεια του, τα οποία μπορούν να εκμεταλλευτούν κακόβουλοι χρήστες.

OWASP.gr: - Δίνεται, κατά τη γνώμη σας, η δέουσα προσοχή στην Ασφάλεια της Πληροφορίας στην Ελλάδα του 2007? Κατά πόσο είναι συνειδητοποιημένοι ως προς την ασφάλεια οι Έλληνες πολίτες, προγραμματιστές αλλά και τα στελέχη των επιχειρήσεων;
B.B: - Δυστυχώς, στην Ελλάδα σε αυτά τα θέματα δίνουμε ελάχιστη σημασία. Αυτό είναι εν μέρει φυσιολογικό, καθώς το μεγαλύτερο κομμάτι του πληθυσμού δεν είναι επαρκώς εξοικειωμένο με τις Τεχνολογίες Πληροφορικής και Επικοινωνιών και φυσικά με τα θέματα που άπτονται αυτών, όπως είναι η ασφάλεια. Από την άλλη πλευρά, είναι ιδιαίτερα ανησυχητικό προγραμματιστές, ακόμα και από μεγάλες ελληνικές εταιρίες, να αγνοούν πλήρως τι είναι το buffer overflow ή το sql injection. Προκειμένου να συμβάλουμε στην ενημέρωση των πιο ευπαθών ομάδων, δηλαδή των μικρομεσαίων επιχειρήσεων που δε διαθέτουν εξειδικευμένο τεχνικό προσωπικό, καθώς και των οικιακών χρηστών, προχωρήσαμε στην σύσταση της ομάδας εργασίας

ΙΑ4, στα πλαίσια του ebusinessforum, που έχει στόχο να καταγράψει τις "Προπαρασκευαστικές δράσεις για την δημιουργία του Ελληνικού Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών (GR-CERT)".

http://www.ebusinessforum.gr/teams/teamsall/view/index.php?ctn=102&language=el

OWASP.gr: - Θα μπορούσε το OWASP να συνδράμει με κάποιο τρόπο στην προσπάθεια αυτή;
B.B: - Η προσπάθεια αυτή είναι ανοικτή σε όλους τους ενδιαφερόμενους. Ωστόσο, το OWASP αποτελεί για μας προνομιακό συνεργάτη λόγω της δραστηριοποίησής του και της τεχνογνωσίας του στο συγκεκριμένο τομέα. Επιπλέον, οι στόχοι και ο προσανατολισμός είναι κοινοί και στις δύο πρωτοβουλίες. Το μεγαλύτερο όφελος από μια ενδεχόμενη συνεργασία με το OWASP, είναι ότι θα μας δώσει την δυνατότητα εκτός από το να ενημερώνουμε έγκαιρα και αποτελεσματικά για διάφορα κενά ασφαλείας σε εφαρμογές που χρησιμοποιούν τα περισσότερα μέλη μας, θα μπορούμε να τους προσφέρουμε αξιόπιστες εναλλακτικές ασφαλείς λύσεις προερχόμενες και από το χώρο του ΕΛ/ΛΑΚ.

OWASP.gr: - Τι προβλέπετε για το μέλλον ως προς αυτόν τον τομέα; Εκτιμάτε π.χ. ότι θα "χρειαστεί" να υπάρξουν σοβαρά περιστατικά ασφάλειας για να υπάρξει και ασφαλέστερο λογισμικό;
B.B.: Συνήθως, έτσι συμβαίνει. Όσον αφορά τη χώρα μας, ευελπιστώ ότι θα μπορούσαμε να αξιοποιήσουμε τη διεθνή εμπειρία και να αποφύγουμε ανάλογα σφάλματα, τα οποία τουλάχιστον στο εξωτερικό κόστισαν ακριβά. Αυτό προϋποθέτει ότι η πολιτεία θα στηρίξει τις οποίες προσπάθειας και πρωτοβουλίες αναλαμβάνονται προς αυτή την κατεύθυνση, όπως το είναι το OWASP και η ομάδα εργασίας ΙΑ4 του Ebusinessforum.

Επίθεση στο site της ΕΠΟ
Δε μας έφτανε η βαριά ήττα από τους Τούρκους στο ποδόσφαιρο, ήρθε το ίδιο βράδυ και η επίθεση στο δικτυακό τόπο της ΕΠΟ από Τούρκους hackers για να «ρίξει» ακόμα περισσότερο την ψυχολογία μας. Συγκεκριμένα, έγινε deface της σελίδας της ΕΠΟ, και τοποθετήθηκε στη θέση της το μήνυμα «Hey Greece, don't speak». Οι υπεύθυνοι του site το έθεσαν γρήγορα εκτός λειτουργίας, ενώ έγιναν και οι απαραίτητες εργασίες θωράκισής του σε συνεργασία με τη Hellas On Line που έχει αναλάβει τη φιλοξενία του.

Επίθεση και στο site της Βουλής
Την ίδια ημέρα, ανήμερα δηλαδή της γιορτής της 25^{ης} Μαρτίου, επίθεση δέχθηκε από Τούρκους hackers και το site του Κοινοβουλίου. Στο site εμφανίστηκαν συνθήματα, απειλές, υβριστικά μηνύματα, κείμενα προπαγάνδας κ.α. Ενδεικτικό του θορύβου που δημιουργήθηκε είναι το γεγονός πως βουλευτές του ΠΑΣΟΚ κατέθεσαν ερώτηση σχετική με το συμβάν στους αρμόδιους υπουργούς. Είναι μάλλον ενθαρρυντικό το ότι οι πολιτικοί μας αρχίζουν και ευαισθητοποιούνται σε θέματα ασφάλειας, έστω και με αυτό τον τρόπο.

…Αλλά και στο site της Νέας Δημοκρατίας
Επίθεση δέχθηκε και το site της Νέας Δημοκρατίας το Πάσχα. Και σε αυτή την περίπτωση δράστες ήταν Τούρκοι hacker. Στο site, που ήταν βασισμένο σε Windows 2000/IIS και έτρεχε κάποια έκδοση του Mambo CMS, εμφανίστηκε η ημισέληνος και ένα… απολογητικό μήνυμα προς τον administrator. Το γεγονός έλαβε μικρή

δημοσιότητα, δεδομένου ότι η επίθεση πραγματοποιήθηκε μεταξύ Μ. Σαββάτου και Κυριακής του Πάσχα.

Πρόβλημα ασφαλείας της On Telecoms δημοσιεύεται στο YouTube
Στις αρχές Απριλίου δημοσιεύθηκε στο YouTube βίντεο που παρουσιάζει την εκμετάλλευση αδυναμίας σε routers της On Telecoms. Ειδικότερα, παρουσίαζε αναλυτικά την επιτυχή είσοδο στον router και τη δυνατότητα αλλαγής σημαντικών ρυθμίσεων βήμα προς βήμα. Αρχικά δημιουργήθηκε η εντύπωση ότι η επίθεση έγινε εναντίον κεντρικών routers της On. Η ποιότητα όμως του video ήταν σχετικά χαμηλή, πράγμα που ενίσχυσε τις φήμες περί hoax. Τελικά, φαίνεται πως η On ορίζει το ίδιο συνθηματικό σε όλους τους routers που πουλάει, με αποτέλεσμα να είναι εύκολο σε οποιονδήποτε μάθει αυτό το συνθηματικό να αποκτήσει πρόσβαση σε αυτούς. Κάτι τέτοιο πρέπει να παρουσιάζει το εν λόγω βίντεο, μία επίθεση δηλαδή σε πελάτη της On χρησιμοποιώντας τη τεχνική των γνωστών/συνηθισμένων συνθηματικών.

Εφημερίδα Καθημερινή: «Επιδημία Ηλεκτρονικού Εγκλήματος»
Η εφημερίδα Καθημερινή της Κυριακής, το Πάσχα αφιέρωσε ένα άρθρο για το ηλεκτρονικό έγκλημα στην Ελλάδα. Το άρθρο εστίαζε την προσοχή του στις απάτες που σχετίζονται με κάθε είδους τραπεζικές συναλλαγές και παρουσίαζε ιδιαίτερο ενδιαφέρον καθώς αποκάλυπτε υποθέσεις και γεγονότα που περνάνε στα «ψιλά» γράμματα τον ειδήσεων ή πολύ περισσότερο που δεν είχαν αποκαλυφθεί ως σήμερα. Έτσι, το άρθρο αποκαλύπτει ότι περίπου 10000 (δέκα χιλιάδες) αριθμοί πιστωτικών καρτών υποκλάπησαν από γνωστή αλυσίδα σούπερ μάρκετ (στην Ελλάδα πάντα) ενώ αναφέρεται διεξοδικά και σε απάτες με ATM και κλωνοποίηση καρτών. Σε κάθε περίπτωση, τα… κέρδη των απατεώνων είναι εντυπωσιακά, ενώ τράπεζες και εμπλεκόμενες εταιρίες και οργανισμοί επιλέγουν να αποσιωπούν τέτοιου είδους γεγονότα, με το φόβο της αρνητικής δημοσιότητας. Ακόμα όμως και αν εκείνοι δεν θέλουν να προστατεύονται επαρκώς, δεν πρέπει οι καταναλωτές να γνωρίζουν για να μπορούν να προστατευθούν οι ίδιοι; Άραγε όλα αυτά είναι αρμοδιότητες κάποιας Αρχής, ή υπάρχει χώρος για κάτι νέο, έστω σε νομοθετικό επίπεδο;

Μέτρα για την ασφάλεια στο Internet από το Υπουργείο Ανάπτυξης
Δέσμη μέτρων για την προστασία των καταναλωτών όσον στο Internet προανήγγειλε ο υφυπουργός Ανάπτυξης κ. Γιάννης Παπαθανασίου, με αφορμή την παρουσίαση έρευνας για τις ηλεκτρονικές αγορές. Συγκεκριμένα, γνωστοποίησε ότι στις προθέσεις του υπουργείου είναι να συστήσει Διεύθυνση Ηλεκτρονικού Εμπορίου, η οποία θα υπάγεται στη Γενική Γραμματεία Καταναλωτή και θα υποστηρίξει το έργο του Εθνικού Συμβουλίου Ηλεκτρονικού Επιχειρείν. Επίσης, ο γενικός γραμματέας Καταναλωτή κ. Γιάννης Οικονόμου παρουσίασε ενημερωτικό φυλλάδιο με τίτλο «Όσα πρέπει να γνωρίζουμε για ασφαλή προήγηση στο διαδίκτυο», το οποίο θα διανέμεται από όλα τα ΚΕΠ. Από την πλευρά του, ο αντιπρόεδρος της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) κ. Ν. Κουλούρης ανέφερε την πρόταση της Επιτροπής για τη σύσταση Ελληνικού Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών, με κύριο αντικείμενο την προστασία των ηλεκτρονικών συστημάτων που χρησιμοποιούν οι τράπεζες, το Χρηματιστήριο οι εφορίες και γενικότερα η Δημόσια Διοίκηση. Τέλος, ο πρόεδρος της Ενωσης Ελλήνων Χρηστών Internet, Νίκος Βασιλάκος γνωστοποίησε ότι προωθείται η σύσταση Ένωσης Καταναλωτών Τηλεπικοινωνιακών Αγορών. (πηγή: in.gr)

OWASP.gr

Spring of Code

Ύστερα από την επιτυχία που γνώρισε το περασμένο Autumn of Code, το OWASP διοργανώνει το Spring of Code με κύριο στόχο την ενίσχυση των project του. Η περίοδος υποβολής προτάσεων έχει πλέον τελειώσει, ενώ περισσότερες πληροφορίες μπορείτε να βρείτε εδώ: https://www.owasp.org/index.php/OWASP_Spring_Of_Code_2007

6th OWASP AppSec Conference – 15-17 Μαΐου 2007 – Μιλάνο

Το OWASP διοργανώνει το 6ο συνέδριο για την ασφάλεια των εφαρμογών, μεταξύ 15 και 17 Μαΐου στο Μιλάνο. Στα πλαίσια του η Microsoft θα παρουσιάσει το πρόγραμμα SDL (Security Development Lifecycle), ενώ θα υπάρξουν ομιλίες σχετικά με την ασφάλεια στα Web Services, AJAX, κλπ. Επίσης, την πρώτη μέρα διοργανώνονται εκπαιδευτικά σεμινάρια σχετικά με την ασφάλεια στα Web Services, την XML και το .NET. Περισσότερες πληροφορίες υπάρχουν εδώ: http://www.owasp.org/index.php/6th_OWASP_AppSec_Conference_-_Italy_2007

ΔΙΕΘΝΗ

Τελικά είναι ασφαλή τα Vista;

Το σήριαλ της ασφάλειας των Windows Vista καλά κρατεί, και θα κρατεί για καιρό ακόμα αφού όπως όλα δείχνουν αργά ή γρήγορα θα κερδίσει μεγάλο μέρος της αγοράς, παρ' όλους τους αρχικούς ενδοιασμούς. Άλλωστε έτσι έγινε και με τα Windows 2000 και τα XP. Αυτή τη φορά, το λόγο πήραν δύο μεγάλες εταίρες ασφάλειας, που ειδικεύονται στη κατασκευή λογισμικού προστασίας ιών για προσωπικούς υπολογιστές. Έτσι, η Kaspersky υποστήριξε πως τα Vista είναι λιγότερο ασφαλή από τα XP, βασιζόμενη στο γεγονός πως το πολυδιαφημισμένο σύστημα UAC (User Account Control) είναι τόσο ενοχλητικό για το χρήστη που συνήθως το απενεργοποιεί. Στον αντίποδα, η Symantec έσπευσε να ανακοινώσει πως τα Windows είναι το ασφαλέστερο λειτουργικό, αφού έχει το μικρότερο αριθμό από patches σε σχέση με άλλα 5 λειτουργικά που παρακολουθεί η εταιρία, μεταξύ των οποίων συμπεριλαμβάνονται το MacOSX, το Red Hat Linux, το HP-UX και άλλα.

ΗΣΥΧΙΑ, ΤΑΞΗ ΚΑΙ… ΑΣΦΑΛΕΙΑ

- Όχι απλά ησυχία… πολλή ησυχία!
- Από τις κάμερες στα αθλητικά, τους χούλιγκαν και τούμπαλιν;
- Θα δούμε. Άλλωστε κάποιοι μίλαγαν για κάμερες στα γήπεδα…

- Ξαφνικά, μέσα στην ησυχία, όλοι θυμήθηκαν τους καταναλωτές
- Και έσπευσαν να τους βοηθήσουν…
- Αρχές, Διευθύνσεις, Ενώσεις Καταναλωτών…
- Ένα είναι σίγουρο πάντως: το ηλεκτρονικό έγκλημα καλά κρατεί και στην Ελλάδα, ενώ εμείς κοιμόμαστε τον ύπνο του… ασφαλή!