1. Στελέχωση ομάδας Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών

Κάθε ομάδα Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών για να είναι αποτελεσματική πρέπει να απαρτίζεται από ειδικούς σε θέματα ασφάλειας. Οι ειδικοί αυτοί αξιολογούν τις πληροφορίες που έρχονται διαρκώς από διάφορες πηγές και προβαίνουν σε εκτιμήσεις σχετικά με την γενικότερη επικινδυνότητα του Διαδικτύου. Συνήθως η επικινδυνότητα αυτή περιγράφεται με κάποιο χαρακτηριστικό χρωματικό κώδικα (πράσινο, κίτρινο, πορτοκαλί και κόκκινο), ώστε να γίνεται εύκολα αντιληπτή και από λιγότερο έμπειρους χρήστες. Οι απειλές που θα αξιολογούνται από τους εν λόγω ειδικούς περιλαμβάνουν αλλά δεν περιορίζονται στην ανεξέλεγκτη εξάπλωση κάποιας μορφής κακόβουλου λογισμικού και σε πρόσφατα ανακαλυφθέντα κενά ασφάλειας τα οποία είτε ανακοινώνονται επίσημα από την κατασκευάστρια εταιρία του λογισμικού ή κοινοποιούνται από ανεξάρτητους ερευνητές. Επίσης θα αναφέρονται πληροφορίες για διάφορα είδη απατών που ανήκουν στην κατηγόρια των phising, pharming, Νιγηριανή απάτη 4-1-9 και άλλων οι οποίες μπορεί να βρίσκονται σε εξέλιξη. Η δημιουργία της ομάδας ειδικών για την παρακολούθηση της γενικότερης επικινδυνότητας του Internet θα βασισθεί στα πρότυπα του http://isc.incidents.org/. Η συμμετοχή προτείνεται να είναι εθελοντική, ενώ ο απαιτούμενος φόρτος είναι μικρός καθώς απαιτούνται δύο ειδικοί ανά μέρα για να καλύπτουν τις παραπάνω δραστηριότητες. Οι ειδικοί ασφάλειας δε χρειάζεται να αφήσουν το χώρο εργασίας τους, ούτε να ασχολούνται αποκλειστικά με την παραπάνω δραστηριότητα, απλά θα πρέπει ανά τακτά χρονικά διαστήματα να ενημερώνονται για τις γενικότερες εξελίξεις από πηγές που παρέχουν σχετικές πληροφορίες σε πραγματικό χρόνο. Επίσης θα συγγράφουν σύντομη αναφορά (μιας ή δύο παραγράφων) με τα περιστατικά τα οποία έλαβαν χώρα στη βάρδια τους ή με θέματα που χρίζουν της προσοχής των χρηστών.

Στόχος της ομάδας ΙΑ-4 είναι να συγκεντρώσει βιογραφικά ειδικών σε θέματα ασφαλείας τόσο από τον επιχειρηματικό όσο και από τον ακαδημαϊκό χώρο, που ενδιαφέρονται να στελεχώσουν μια τέτοια ομάδα και να τα προωθήσουν στους αρμόδιους φορείς μαζί με τα λοιπά παραδοτέα που θα τεκμηριώνουν την ανάγκη ίδρυση της.

2. Σημεία επικοινωνίας για την κοινοποίηση κενών ασφαλείας

Μέχρι σήμερα δεν έχει γίνει καμία απολύτως ενέργεια ώστε οι ελληνικές εταιρίες που κατασκευάζουν λογισμικό για Έλληνες χρήστες να μπορούν να κοινοποιούν υπεύθυνα τα κενά ασφαλείας που εμφανίζονται στις εφαρμογές τους. Θεωρούμε ως βέλτιστη λύση την ενημέρωση κατά προτεραιότητα του Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών, το οποίο θα αναλάβει την υπεύθυνη διαχείριση της συγκεκριμένης πληροφορίας ενημερώνοντας τους εκτεθειμένους χρήστες. Η ομάδα ΙΑ-4 θα περιγράψει αναλυτικά ολόκληρη τη διαδικασία που πρέπει να ακολουθηθεί από την ανακάλυψη ενός κενού ασφαλείας μέχρι την τελική του κοινοποίηση στους χρήστες. Συγκεκριμένα θα καταγράφουν συστηματικά τα βήματα που πρέπει να ακολουθήσει ένας ανεξάρτητος ερευνητής ή μια εταιρία λογισμικού

από την ανακάλυψη ενός κενού ασφαλείας μέχρι την τελική του κοινοποίηση. Η προτεινόμενη μεθοδολογία θα εκδοθεί και σε σχετικό φυλλάδιο.

3. Δημιουργία μητρώου με στελέχη επιχειρήσεων που έχουν στην αρμοδιότητα τους θέματα ασφαλείας

Σε πολλές εταιρίες δεν έχει προβλεφθεί η θέση του υπεύθυνου ασφαλείας τόσο για το λογισμικό που ενδέχεται να κατασκευάζει όσο και για το λογισμικό που χρησιμοποιεί γενικότερα η κάθε εταιρία. Συνεπώς ακόμα και αν εντοπιστούν κενά ασφαλείας είναι δύσκολο να ενημερωθούν τα κατάλληλα άτομα στις επιχειρήσεις και τους οργανισμούς και να λάβουν τα απαιτούμενα μέτρα. Το ίδιο ισχύει και σε έκτακτες περιπτώσεις όπως π.χ σε μια επιδημία κακόβουλου λογισμικού όπου απαιτείται άμεση και συντονισμένη δράση τόσο του ιδιωτικού όσο και του δημόσιου τομέα. Παραδοτέο της ομάδας ΙΑ-4 θα είναι σχετικό φυλλάδιο το οποίο θα παραθέτει αναλυτικά τα πλεονεκτήματα της ύπαρξης υπεύθυνου ασφαλείας σε κάθε επιχείρηση και οργανισμό. Επίσης θα αναφέρονται οι αρμοδιότητες που πρέπει να έχει ένας υπεύθυνος ασφαλείας. Παράλληλα θα δημιουργηθεί μια λίστα-μητρώο με στελέχη επιχειρήσεων και οργανισμών που έχουν κάποιες από τις παραπάνω αρμοδιότητες για να μπορούν να ενημερώνονται άμεσα από το Κέντρο Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών.