ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ
ΕΔΕΤ Α.Ε.
ΕΘΝΙΚΟ ΔΙΚΤΥΟ ΕΡΕΥΝΑΣ & ΤΕΧΝΟΛΟΓΙΑΣ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠ. ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ
ΥΠ. ΕΣΩΤ., ΔΗΜ. ΔΙΟΙΚ. & ΑΠΟΚΕΝΤΡΩΣΗΣ

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
«ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ»

ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

ΕΡΓΟ ΣΥΓΧΡΗΜΑΤΟΔΟΤΟΥΜΕΝΟ ΚΑΤΑ 75% ΑΠΟ ΤΟ

ΕΥΡΩΠΑΪΚΟ ΤΑΜΕΙΟ ΠΕΡΙΦΕΡΕΙΑΚΗΣ ΑΝΑΠΤΥΞΗΣ

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ»

ΑΞΟΝΑΣ: 3 Ανάπτυξη & Απασχόληση στην Ψηφιακή Οικονομία

ΜΕΤΡΟ: 3.1 Δημιουργία ευνοϊκού περιβάλλοντος για την οικονομική ανάπτυξη

Ομάδα Ια4 Προπαρασκευαστικές δράσεις για την δημιουργία Ελληνικού Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών (GR-CERT)

ΠΑΡΑΔΟΤΕΟ Μελέτη καταγραφής των πορισμάτων της Ομάδας Εργασίας Ια4 του forum

Ομάδα εργασίας:
Διομήδης Σπινέλλης, Αναπλ. Καθηγητής Οικον. Πανεπιστήμιο Αθήνας
Στέφανος Γκρίτζαλης, Αναπλ. Καθηγητής, Πανεπιστήμιο Αιγαίου
Βασίλειος Βλάχος, Οικονομικό Πανεπιστήμιο Αθήνας
Πέτρος Μπέλσης, Πανεπιστήμιο Αιγαίου
Ιωάννα – Αγάθη Μαντζουράτου, Οικονομικό Πανεπιστήμιο Αθηνών

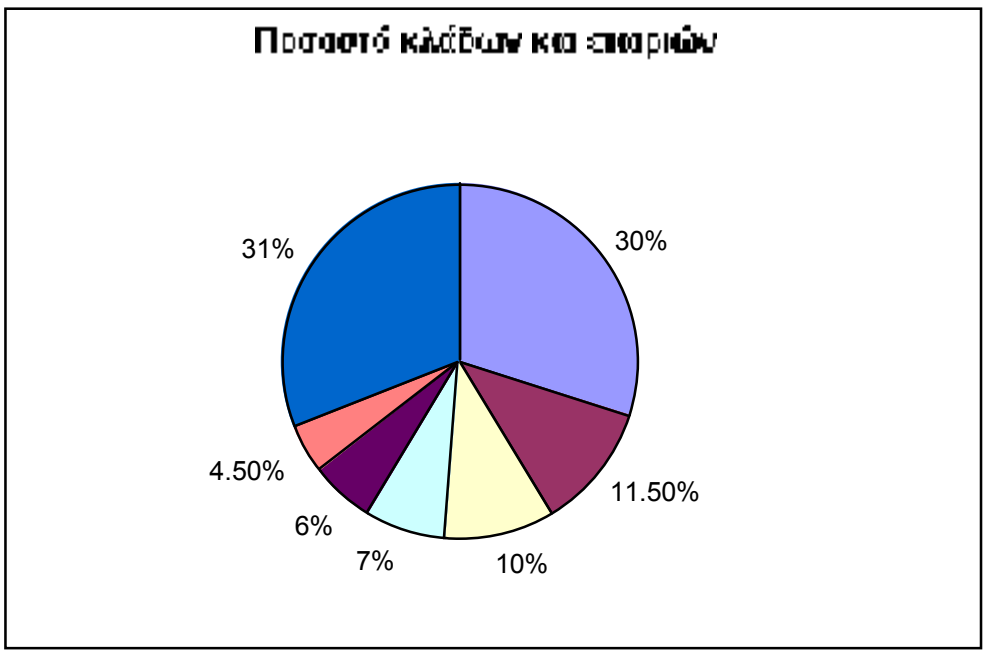
ΑΘΗΝΑ 2007

ΠΕΡΙΕΧΟΜΕΝΑ

Η ομάδα εργασίας ΙΑ4 λειτούργησε από τον Σεπτέμβριο του 2006 έως και τον Αύγουστο του 2007 στα πλαίσια του ebusinessforum. Το ebusinessforum είναι ένας μόνιμος μηχανισμός διαβούλευσης της Πολιτείας με δημόσιους φορείς, τον ακαδημαϊκό χώρο και τις επιχειρήσεις. Συνεπώς, οι προτάσεις και τα συμπεράσματα τα οποία προέκυψαν απευθύνονται πρωτίστως στην Πολιτεία, ώστε να τα αξιολογήσει σε πρώτο στάδιο και να αποφανθεί για την περαιτέρω υλοποίηση τους.

Στην ομάδα ΙΑ4 δήλωσαν συμμετοχή περίπου εκατό άτομα με διαφορετική εργασιακή εμπειρία, προερχόμενοι από τον ευρύτερο δημόσιο τομέα, τον ακαδημαϊκό χώρο, εταιρίες τηλεπικοινωνιών και νομικά γραφεία, όπως φαίνεται από το σχετικό γράφημα.

Κλάδοι και εταιρίες	**Ποσοστό**
Πανεπιστημιακός χώρος	30%
Εταιρίες τηλεπικοινωνιών	11.50%
Τραπεζικός κλάδος	10%
Εταιρίες Πληροφορικής	7%
Κυβερνητικοί Οργανισμοί	6%
Νομικός τομέας	4.50%
Άλλες εταιρίες και ιδρύματα	31%



Συντονισμός και οργάνωση της ομάδας ΙΑ4

Η παρούσα μελέτη αποτελεί το αντικείμενο της δουλειάς των συντονιστών, των βοηθών συντονιστών και των μελών της ομάδας ΙΑ4. Καθ' όλη την διάρκεια της λειτουργίας της ομάδας επιχειρήθηκε από τους συντονιστές η μέγιστη δυνατή εμπλοκή όλων των μελών σε αυτή τη προσπάθεια. Για την επίτευξη των παραπάνω εγκαταστάθηκαν οι εξής υποδομές

IA4Wiki

Το IA4Wiki εγκαταστάθηκε, ώστε να συμβάλλει στο βέλτιστο συντονισμό των μελών της ομάδας ΙΑ4. Ειδικότερα επέτρεψε την έγκυρη ενημέρωση των μελών για διάφορες εξελίξεις σε θέματα ασφάλειας και επίσης χρησίμευσε ως αποθετήριο υλικού, σχετικού με το αντικείμενο της ομάδας ΙΑ4, όπως μελέτες για την σύσταση και λειτουργία ανάλογων ομάδων του εξωτερικού. Στο δικτυακό τόπο του IA4Wiki ξεκίνησε η συλλογική συγγραφή τμημάτων του παραδοτέου από τα μέλη της ομάδας με σχετική εμπειρία. Επίσης το IA4Wiki συνέβαλε στην δημιουργία επαφών και διαύλων επικοινωνίας με άλλες ομάδες με σχετικό αντικείμενο.

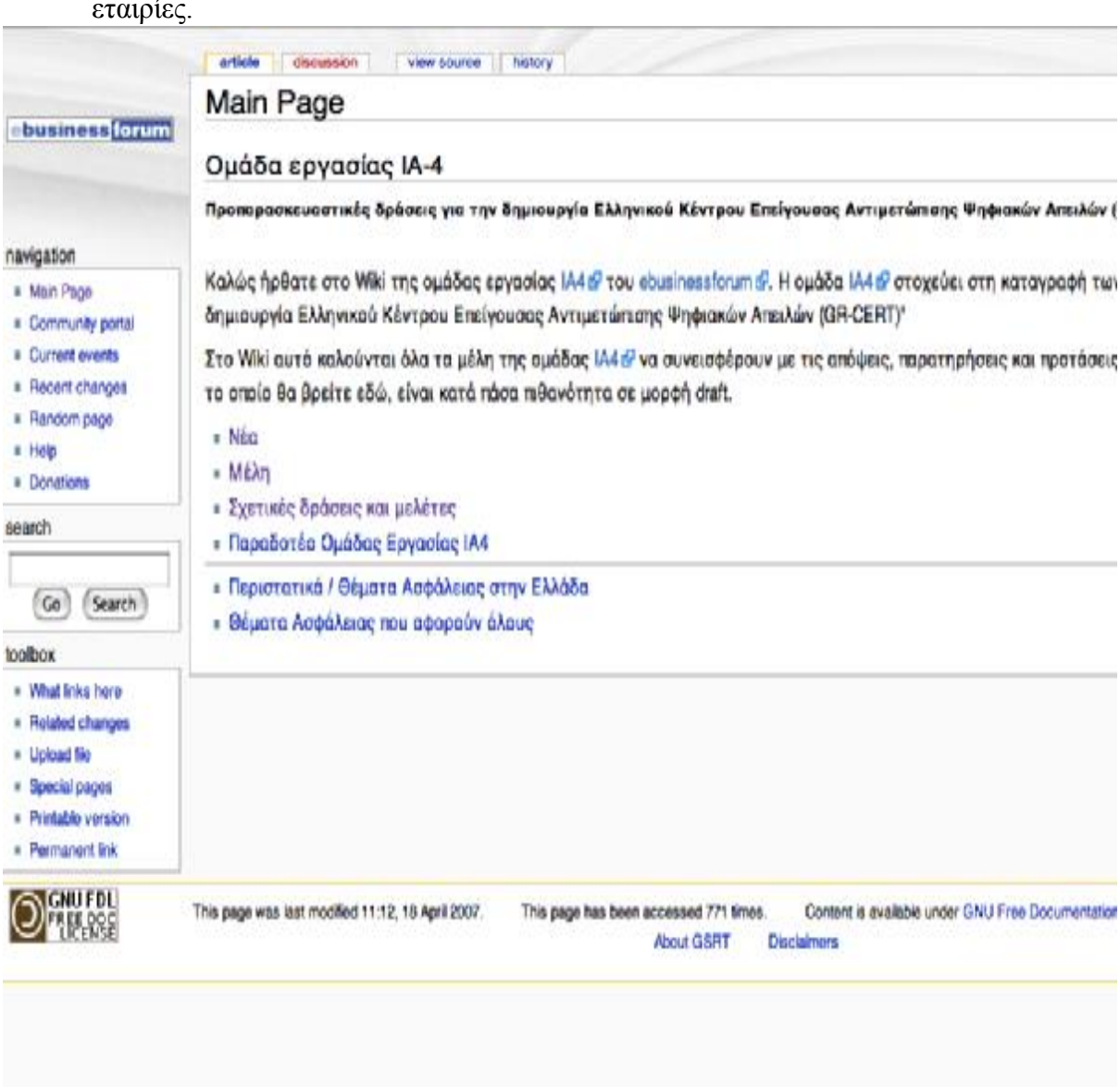
Το IA4Wiki υπήρξε ιδιαίτερα χρήσιμο, καθώς βοήθησε στην περαιτέρω αξιοποίηση των ιδιαίτερων ικανοτήτων και γνώσεων των μελών της ομάδας ΙΑ4. Συγκεκριμένα, συστήθηκαν δύο υπό-ομάδες ανάλογα με το θεωρητικό υπόβαθρο και την εμπειρία των συμμετεχόντων. Ειδικότερα, σχηματίστηκαν οι εξής υπό-ομάδες:

- Ομάδα Ειδικών Αναλυτών σε Θέματα Ασφάλειας (Ομάδα Α). Η ομάδα απαρτίζεται από μέλη που διαθέτουν ειδικές γνώσεις σε θέματα ασφαλείας, έτσι ώστε το εγχείρημα του GR-CERT να οργανωθεί, να παρακολουθηθεί και να υποστηριχθεί από ειδικούς επιστήμονες σε θέματα ασφάλειας.
- **Ομάδα Συντονισμού, Οργάνωσης, Τεκμηρίωσης και Υποστήριξης (Ομάδα Β)**. Στην ομάδα Β συμμετέχουν τα μέλη της ομάδας ΙΑ4 που:
    - Διαθέτουν εμπειρία στην υποβολή προτάσεων για την ίδρυση ενός CERT, SIRT, Cases, κλπ. Έχουν την δυνατότητα να επικοινωνήσουν με οργανισμούς και εταιρίες (όπως Τράπεζες, ISPs, Μικρο-Μεσαίες Επιχειρήσεις, Δημόσιους Οργανισμούς κλπ), ώστε να παρουσιάσουν τη προσπάθεια που βρίσκεται σε εξέλιξη και να εξασφαλιστεί η υποστήριξή τους.

- Έχουν ειδικές γνώσεις σε εξειδικευμένα ζητήματα (όπως πχ νομικά θέματα).

Στόχος της Ομάδας Συντονισμού, Οργάνωσης, Τεκμηρίωσης και Υποστήριξης είναι να συμβάλει στην σύνταξη μιας πλήρους και ολοκληρωμένης πρότασης. Σημαντικά σημεία τα οποία επιχειρήθηκε να αντιμετωπισθούν είναι:

- Η κατά το δυνατόν μείωση του κόστους μέσω της ανάπτυξης των κατάλληλων συνεργιών.
- Η αντιμετώπιση των νομικών και άλλων ζητημάτων που ενδεχομένως να προκύψουν.
- Η εξασφάλιση της ευρύτερης δυνατής υποστήριξης από φορείς και εταιρίες.



Λίστες ηλεκτρονικού ταχυδρομείου

Προκειμένου να διαφυλαχθούν τα στοιχεία επικοινωνίας των μελών της ομάδας ΙΑ4, αλλά το κυριότερο να υπάρχει μια ευελιξία στον τρόπο με τον οποίο πραγματοποιείται η ανταλλαγή μηνυμάτων μεταξύ των συμμετεχόντων σε αυτή τη προσπάθεια, δημιουργήθηκαν δύο λίστες επικοινωνίας. Οι λίστες ηλεκτρονικού ταχυδρομείου παραμένουν σε λειτουργία και μετά την λήξη των εργασιών της ομάδας ΙΑ4 και στοχεύουν στην διατήρηση της κοινότητας ειδικών σε θέματα ασφάλειας που σχηματίσθηκε με αντικείμενο την δημιουργία του κέντρου άμεσης αντιμετώπισης περιστατικών ασφάλειας, καθότι αναμένεται να αποβούν πολλαπλά ωφέλιμες και στο μέλλον. Συγκεκριμένα δημιουργήθηκαν οι παρακάτω δύο λίστες:

- Ia4admin. Στη λίστα αυτή περιλαμβάνονται τα μέλη της ομάδας συντονισμού και όσοι γενικότερα είχαν κάποιο οργανωτικό ρόλο στη προσπάθεια αυτή.
- Ia4announce. Η λίστα περιλαμβάνει όλα τα μέλη τα οποία συμμετείχαν στις εργασίες της ομάδας ΙΑ4, καθώς και άλλους χρήστες και οργανισμούς που θέλησαν να παρακολουθήσουν από κοντά τις εξελίξεις.

Η απόφαση για την συντήρηση των παραπάνω λιστών αποτελεί το πρώτο βήμα για να μπορούν να επικοινωνούν και στο μέλλον, οι ειδικοί που δραστηριοποιούνται σε θέματα ασφάλειας στην Ελλάδα.

Διαβουλεύσεις

Στα πλαίσια της λειτουργίας της ομάδας ΙΑ4 πραγματοποιήθηκαν δύο διαβουλεύσεις, οι οποίες επέτρεψαν την χρήσιμη ανταλλαγή απόψεων μεταξύ των ειδικών σε θέματα ασφαλείας και καθόρισαν τα επόμενα στάδια και τον προγραμματισμό των εργασιών. Στις διαβουλεύσεις αυτές ελήφθησαν κάποια σύντομα πρακτικά, τα οποία έχουν αναρτηθεί στον δικτυακό τόπο της ομάδας ΙΑ4. Στη δεύτερη διαβούλευση χρησιμοποιήθηκαν και οι δυνατότητες της τηλεδιάσκεψης προκειμένου να συμμετάσχουν και μέλη της ομάδας, τα οποία εργάζονται εκτός Αθηνών.

Ευχαριστίες

Οι συντάκτες του παρόντος κειμένου αισθάνονται την ανάγκη να ευχαριστήσουν όλα τα μέλη της ομάδας εργασίας ΙΑ4, για το χρόνο τους και την συμβολή τους σε αυτή τη προσπάθεια. Χωρίς την δική τους συμμετοχή και ενδιαφέρον είναι σίγουρο ότι δεν θα μπορούσε να έχει επιτεθεί σε ικανοποιητικό βαθμό κανένα από τα τελικά αποτελέσματα τα οποία προέκυψαν. Επίσης, καθοριστική υπήρξε η βοήθεια του ειδικού προσωπικού του ΕΔΕΤ για την μέριμνα που έδειξε σε όλα διοικητικά και οργανωτικά ζητήματα, τους οποίους ευχαριστούμε θερμά.

Εισαγωγή

Η πρώτη ομάδα αντιμετώπισης ψηφιακών απειλών δημιουργήθηκε το 1989, από το 2000 δε παρατηρείται γεωμετρική αύξηση στον αριθμό των ομάδων, προκειμένου να αντιμετωπιστεί η δραματική αύξηση των επιθέσεων ασφάλειας. Η δημιουργία αντίστοιχων ομάδων θεωρείται ως ένας από τους αποτελεσματικότερους τρόπους αντιμετώπισης επιθέσεων ασφάλειας διότι παρέχουν μία ολοκληρωμένη υποδομή για τη γρήγορη, τη συντονισμένη και τη συνεργάσιμη απόκριση σε περιστατικά ασφάλειας. Σκοπός των ομάδων είναι η παροχή υπηρεσιών αντίδρασης, πρόληψης και αποτελεσματικής διαχείρισης σε θέματα ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων. Η παροχή αυτών των υπηρεσιών γίνεται σε έναν ή περισσότερους οργανισμούς σύμφωνα με την αποστολή και το είδος της ομάδας. Οι υπηρεσίες αντίδρασης αποσκοπούν στην άμεση ανάλυση, υποστήριξη και απόκριση σε περιστατικά και αδυναμίες ασφάλειας καθώς και την αξιολόγηση και ανάλυση των χρησιμοποιούμενων εργαλείων επιθέσεων. Οι υπηρεσίες πρόληψης αποσκοπούν στην υλοποίηση διαδικασιών για την άμεση μείωση των περιστατικών ασφάλειας, ενώ οι υπηρεσίες διαχείρισης της ασφάλειας για την έμμεση μείωση τους. Το κλειδί της επιτυχίας των ομάδων είναι η μεταξύ τους επικοινωνία για το συντονισμό και τη συνεργασία σε θέματα ασφάλειας. Η επικοινωνία πραγματοποιείται είτε μεταξύ διάσπαρτων ομάδων που αναλαμβάνουν την προστασία του ίδιου οργανισμού, είτε μεταξύ ομάδων από διαφορετικούς οργανισμούς. Αυτή η επικοινωνία αποτελεί το βασικό πλεονέκτημα των CSIRTs σε σχέση με τις άλλες ομάδες ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων. Αναλυτικότερα, τα περιστατικά ασφάλειας πραγματοποιούνται μεταξύ πολλαπλών δικτύων και συστημάτων τα οποία είναι διάσπαρτα σε διαφορετικούς οργανισμούς και χώρες. Έτσι απαιτείται μία βασισμένη στη συνεργασία απόκριση καθώς και κατάλληλος συντονισμός των ομάδων. Επιπλέον, λόγω της συνήθως χαμηλής σχετικά χρηματοδότησης δεν είναι συχνά εφικτό η κάθε ομάδα από μόνη της να παρέχει επαρκείς υπηρεσίες για τη θωράκιση των οργανισμών που αποσκοπεί. Συνεπώς η συνεργασία προβάλλει ως εναλλακτική και μόνη αποτελεσματική λύση. Οι βασικές προδιαγραφές που πρέπει να έχει μία γρήγορη, αποτελεσματική και αποδοτική επικοινωνία είναι τέσσερις [14]:

- Η πρώτη προδιαγραφή αφορά την προκαθορισμένη γνώση των στοιχείων και του τρόπου επικοινωνίας με την κατάλληλη ομάδα. Κατάλληλη ομάδα θεωρείται η ομάδα που έχει τις ικανότητες και την εξειδίκευση για να βοηθήσει μια άλλη ομάδα στην παροχή μιας τρέχουσας υπηρεσίας.
- Η επόμενη προδιαγραφή αφορά τη διασφάλιση των απαιτήσεων ασφάλειας των πληροφοριών κατά τη φάση της ανταλλαγής τους για εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα και μη αποποίηση ευθύνης.
- Η τρίτη προδιαγραφή απαιτεί την ύπαρξη εμπιστοσύνης μεταξύ των επικοινωνούντων ομάδων, ώστε να διασφαλίζεται η επιθυμητή χρήση των πληροφοριών που διαμοιράζονται. Δηλαδή να διασφαλίζεται η εμπιστευτικότητα και η ιδιωτικότητα των πληροφοριών οι οποίες περιέχουν ευαίσθητα δεδομένα για τον οργανισμό στον οποίο ανήκουν.
- Τέλος, η τέταρτη προδιαγραφή αφορά τη χρήση ενός κοινού πρότυπου μορφοποίησης των πληροφοριών ώστε να είναι εύκολη και γρήγορη η κατανόηση τους.

Τα πλαίσια εργασίας που έχουν υλοποιηθεί από την κοινότητα των CSIRTs και όχι μόνο, διαχωρίζονται σε δύο κατηγορίες. Η πρώτη κατηγορία επικεντρώνεται στην υλοποίηση ενός "έμπιστου δικτύου" μεταξύ των ομάδων ικανοποιώντας τις δυο πρώτες προδιαγραφές. Η δεύτερη κατηγορία ικανοποιεί την τέταρτη προδιαγραφή με την υλοποίηση ενός κοινού πρότυπου μορφοποίησης για την περιγραφή και την ανταλλαγή πληροφοριών που αφορούν τις υπηρεσίες των ομάδων. Αν και οι δυο κατηγορίες προσπαθούν να ικανοποιήσουν εν' μέρει την τρίτη προδιαγραφή οι λύσεις που προτείνουν δε θεωρούνται αποτελεσματικές. Τα υπάρχοντα πλαίσια επικοινωνίας προσπαθούν να διασφαλίζουν την ιδιωτικότητα και την εμπιστευτικότητα των πληροφοριών των ομάδων και κατ' επέκταση των οργανισμών που προστατεύουν, όταν οι πληροφορίες χρησιμοποιούνται από τις άλλες ομάδες μέσω της κοινής υπογραφής συμφωνιών μη αποκάλυψης πληροφοριών. Όμως αυτή η τεχνική δεν μπορεί να διασφαλίσει απόλυτα τις παραπάνω απαιτήσεις ασφάλειας με αποτέλεσμα οι ομάδες να αποθαρρύνονται στο να συμμετάσχουν σε μεταξύ τους επικοινωνία. Έρευνες αναφέρουν ότι το 50% των οργανισμών δεν αναφέρουν περιστατικά ασφάλειας σε τρίτους οργανισμούς για λόγους μείωσης της φήμης τους και για λόγους αρνητικής εκμετάλλευσης των περιστατικών από τους ανταγωνιστές τους, σε βάρος αυτών των οργανισμών. Καθίσταται λοιπόν προφανές ότι η επιτυχία της

διασφάλισης της ιδιωτικότητας των ομάδων είναι ένας αρκετά σημαντικός και καθοριστικός παράγοντας για τη διαφύλαξη του κύρους του συνόλου των ομάδων έναντι των οργανισμών που συμμετέχουν στην υποστήριξή τους. Στο δίκτυο των συμμετεχόντων ομάδων απαιτείται να γίνεται χρήση ειδικών προτύπων ανταλλαγής πληροφοριών. Συγκεκριμένα πρέπει υποστηρίζονται τα παρακάτω πρότυπα μορφοποίησης και αναπαράστασης των πληροφοριών που ανταλλάσσονται μεταξύ των ομάδων:

• Incident Object Description and Exchange Format (IODEF) για τις πληροφορίες της υπηρεσίας χειρισμού περιστατικών ασφάλειας.

• The European Information Security Promotion Programme Common Advisory Format (CAF) για τις πληροφορίες της υπηρεσίας διανομής συμβουλών σε αδυναμίες ασφάλειας: Τα παραπάνω πρότυπα θα εξελιχθούν ώστε να διασφαλίσουν και αυτά με τη σειρά τους την ανωνυμία και την ιδιωτικότητα των CSIRTs. Συνάμα η χρήση των προτύπων έχει και συγκεντρωτικό χαρακτήρα, δηλαδή συσχετίζονται μεταξύ τους με χρήση δεικτών- αναφορών. Έτσι παρέχονται δυνατότητες συσχετισμών και στατιστικών αναλύσεων των πληροφοριών που ανταλλάσσουν οι CSIRTs.

Ομάδες Αντιμετώπισης περιστατικών Ασφάλειας

Οι Ομάδες Απόκρισης σε Πληροφοριακά Περιστατικά Ασφάλειας «CSIRTs» είναι ομάδες με εξειδίκευση σε θέματα ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων. Γενικότερα είναι ομάδες προορισμένες να υποστηρίζουν τη λειτουργία ενός οργανισμού με το να προστατεύουν και να βελτιώνουν την ασφάλειά του. Άρα οι CSIRTs είναι ομάδες εξειδικευμένες σε θέματα ασφάλειας. Προκειμένου για τη μελέτη του τρόπου λειτουργίας των CSIRT θα πρέπει πρώτα να τεθεί το εννοιολογικό πλαίσιο που αφορά στη διαχείριση των πληροφοριακών συστημάτων, των οποίων η προστασία απαιτεί την κύρια προτεραιότητα.

Πληροφοριακό σύστημα, δεδομένα και πληροφορία

Πριν ξεκινήσουμε με την αναλυτικότερη παρουσίαση των ομάδων αντιμετώπισης περιστατικών ασφάλειας που αφορούν σε πληροφοριακά συστήματα (ΠΣ), χρήσιμο θα ήταν να δώσουμε κάποιους ορισμούς που αφορούν στο τι είναι ένα Π.Σ και στο τι

εννοούμε λέγοντας Ασφάλεια ΠΣ. Τα Πληροφοριακά Συστήματα αποτελούν συστήματα ανθρώπινης δραστηριότητας σύμφωνα με τον Checkland [15], διακρίνονται δε, από δύο βασικά χαρακτηριστικά:

(α) την αναζήτηση ενός σκοπού και

(β) το δυναμικό τους χαρακτήρα.

Αυτό βέβαια δε σημαίνει ότι όλοι αντιλαμβάνονται το σκοπό του συστήματος με τον ίδιο τρόπο. Όσον αφορά στη δυναμικότητα του χαρακτήρα τους, αυτή οφείλεται στην παρουσία του ανθρώπινου παράγοντα που διακρίνεται από μη προβλέψιμη συμπεριφορά, ανάλογα με την ιδιοσυγκρασία του κάθε ατόμου και ανάλογα με τις συνθήκες, στις οποίες ο κάθε άνθρωπος αντιδρά διαφορετικά.

Οι περισσότεροι ορισμοί που δίνονται στη βιβλιογραφία επικεντρώνουν το βάρος τους στην τεχνική διάσταση της επεξεργασίας των πληροφοριών. Συχνά μάλιστα γίνεται και εναλλαγή της έννοιας της πληροφορίας (information), με αυτή των δεδομένων (data). Ένας ορισμός των δεδομένων είναι:

Οι περισσότεροι ορισμοί στη βιβλιογραφία δίνουν έμφαση στην τεχνική πλευρά των πληροφοριακών συστημάτων, παρουσιάζοντάς τα ως συστήματα επεξεργασίας πληροφοριών, αγνοώντας τη σημασία του ανθρώπινου παράγοντα. Ένας πλήρης ορισμός του πληροφοριακού συστήματος είναι [16]:

‘‘ Πληροφοριακό σύστημα είναι ένα σύνολο από πέντε αλληλεπιδρώντα στοιχεία: άνθρωποι, δεδομένα (data), υλικός εξοπλισμός (hardware, λογισμικό (software), διαδικασίες (procedures, methods)’’.

Ασφάλεια πληροφοριακών συστημάτων

Η ασφάλεια πληροφοριών αναφέρεται στην προστασία της πληροφορίας, στην ολότητά της και των σχετικών με την ασφάλεια ιδιοτήτων. Ως τέτοιες ιδιότητες (attributes), ορίζονται:

- η ακεραιότητα (integrity),
- η εμπιστευτικότητα (confidentiality) και
- η διαθεσιμότητα (availability).

Οι τρεις αυτές ιδιότητες ορίζονται ως εξής:

Ακεραιότητα (Integrity): Η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

Εμπιστευτικότητα (Confidentiality): Η αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένα άτομα.

Διαθεσιμότητα (Availability): Η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες.

Η δυσκολία προσδιορισμού της έννοιας της ασφάλειας πληροφοριών, έγκειται στο γεγονός ότι το νόημα της πληροφορίας τροποποιείται ανάλογα με το πλαίσιο (context) στο οποίο εμφανίζονται τα δεδομένα, τροποποιώντας την σημασία τους ανάλογα.

Παράλληλα, η ασφάλεια πληροφοριών από μόνη της, δεν επαρκεί για τη διασφάλιση της ασφάλειας ολόκληρου του συστήματος. Η ασφάλεια πληροφοριακών συστημάτων είναι πολύ ευρύτερη έννοια, που περιλαμβάνει το σύνολο των αρχών, κανονισμών, μεθοδολογιών, τεχνικών και εργαλείων, που δημιουργούμε με στόχο την προστασία του Π.Σ., ή κάποιων από τις συνιστώσες του, από ενδεχόμενες απειλές. Επομένως, αν και μελετάται κατά κανόνα η ασφάλεια πληροφοριών, προκειμένου για την ασφάλεια του πληροφοριακού συστήματος, πρέπει να ληφθεί μέριμνα τόσο για τα δομικά στοιχεία που το απαρτίζουν, αλλά και το σύστημα ως ολότητα.

Εννοιολογικό και θεωρητικό μοντέλο διαχείρισης γνώσης που αφορά σε προβλήματα ασφάλειας

Επιλογή μεθοδολογίας

Με τη βοήθεια της βιβλιογραφικής αλλά και εμπειρικής αλλά και βιβλιογραφικής έρευνας έχουν καταγραφεί μία σειρά από ζητήματα που αφορούν στη διαχείριση της πληροφορίας και τη γνώσης που σχετίζεται μα την αντιμετώπιση περιστατικών ασφάλειας, γεγονός που είναι και το ζητούμενο από τις ομάδες υποστήριξης και αντιμετώπισης περιστατικών ασφάλειας [17] Η εμπειρική έρευνα δίνει τη δυνατότητα καταγραφής της τρέχουσας κατάστασης στο χώρο της ασφάλειας των Π.Σ., αποτυπώνοντας την οπτική που έχουν οι ειδικοί της ασφάλειας. Από την επεξεργασία των αποτελεσμάτων της έρευνας, σε συνδυασμό με τη βοήθεια της βιβλιογραφίας, έχουν προταθεί θεωρητικά μοντέλα με στόχο την κατηγοριοποίηση της γνώσης που αφορά στην ασφάλεια και την αποτύπωση της δομής της, όπως αυτή προέκυψε μέσα από την εμπειρική έρευνα. Παράλληλα έχει επιχειρηθεί προσαρμογή των μοντέλων, στις κατηγορίες ασφάλειας, όπως αυτές αποτυπώνονται στο πρότυπο ISO 17799. Στην επόμενη παράγραφο προκειμένου να ληφθούν υπόψη οι απαιτήσεις σε επίπεδο

οργανισμού, θα μελετηθεί εν συντομία το οργανωσιακό μοντέλο δημιουργίας και διάχυσης της γνώσης.

Οι άξονες δράσης ενός οργανισμού προκειμένου για την αποτελεσματικότερη αντιμετώπιση των περιστατικών ασφάλειας θα πρέπει να εστιάζονται στους εξής διαφορετικούς τομείς [18]:

α) *Δημιουργία βάσεων γνώσης (knowledge repositories)*.

Δημιουργία βάσεων που θα επιτρέπουν τη φύλαξη και την αναζήτηση τόσο τεχνικής όσο και προσανατολισμένης στη διοικητική επιστήμη, γνώσης.

β) *Δημιουργία βάσεων γνώσης που σχετίζονται με τις βέλτιστες πρακτικές και πείρα από μαθήματα του παρελθόντος (best practices and lesson learned systems)*.

Βάσεις γνώσεις που σχετίζονται με την ανάκληση γνώσης.

γ) *Δημιουργία ανθρώπινων δικτύων (expert networks)*.

Δίκτυα ανθρώπινα με εξειδίκευση σε κάποιο επαγγελματικό τομέα και που ηλεκτρονικά επικοινωνούν μεταξύ τους σε ερωτήματα που προκύπτουν και αφορούν στην πείρα που έχουν γύρω από το θέμα.

δ) *Συμμετοχή σε κοινότητες πρακτικής (communities of practice)*.

Δίκτυα ανθρώπινα που οργανώνονται με πρωτοβουλία των μελών τους και μοιράζονται κοινά ενδιαφέροντα, ζώντας σε γεωγραφικά απομακρυσμένες περιοχές.

Καταγραφή της τρέχουσας πραγματικότητας στο χώρο της ασφάλειας

Η ανάγκη για ολοκληρωμένη αντιμετώπιση του προβλήματος της ασφάλειας, αναδεικνύεται μέσα από την παρατηρούμενη απουσία μιας ολοκληρωμένης προσέγγισης όσον αφορά στην υποστήριξη του έργου των ατόμων των επιφορτισμένων με το δύσκολο έργο της ασφάλειας του οργανισμού. Τόσο σε θεωρητικό επίπεδο, όσο και πρακτικό, προβάλλεται η ανάγκη για υποστήριξη του ειδικού στα θέματα ασφάλειας, με χρήση αυτοματοποιημένων εργαλείων ή με την παροχή καλύτερης τεκμηρίωσης.

Σύντομη αναφορά σε θεωρητικές έννοιες

Στην παρούσα ενότητα θα αναφερθούμε εν συντομία σε ορισμένες βασικές θεωρητικές έννοιες που αφορούν στη διαχείριση της γνώσης που σχετίζεται με θέματα ασφάλειας.

Η γνώση όπως έχει ήδη αναφερθεί, μπορεί να διακριθεί, σύμφωνα με την κατηγοριοποίηση του φιλόσοφου Michael Polanyi, σε ρητή (explicit) και άρρητη (tacit) [19]. Ο Polanyi υποστηρίζει ότι η προσωπική, άρρητη γνώση παίζει πολύ σημαντικό ρόλο στην ανθρώπινη πορεία προς την κατάκτηση της γνώσης. Η ρητή και η άρρητη γνώση αλληλοσυμπληρώνουν η μία την άλλη και κατά τις δημιουργικές απόπειρες των ατόμων αλληλεπιδρούν και επηρεάζουν η μία την άλλη. Για παράδειγμα, η καινοτομία που είναι θεμελιώδης έννοια στη διαδικασία δημιουργίας γνώσης στον οργανισμό, δεν μπορεί να ερμηνευτεί με όρους επεξεργασίας της πληροφορίας ή επίλυσης προβλημάτων. Η καινοτομία μπορεί να ερμηνευτεί σαν μια διαδικασία όπου ο οργανισμός δημιουργεί και καθορίζει προβλήματα και κατόπιν δημιουργεί νέα γνώση για την επίλυσή τους, μέσα από τη δημιουργική συνεργασία των μελών του.

Κοινωνική αλληλεπίδραση και σχηματισμός γνώσης

Παρόλο που οι έννοιες εμφανίζονται από μεμονωμένα άτομα, στο σχηματισμό της γνώσης παίζει πολύ σημαντικό ρόλο ο σχηματισμός κοινοτήτων ατόμων, που στόχο έχουν τον τελικό σχηματισμό και την αποκρυστάλλωσή της (Nonaka, 1994). Η ανθρώπινη γνώση δημιουργείται και επαυξάνεται μέσα από μια διαδικασία κοινωνικής αλληλεπίδρασης που αποκαλείται μετατροπή γνώσης (knowledge conversion). Αυτή η μετατροπή συμβαίνει μεταξύ των ατόμων στο εσωτερικό του οργανισμού.

Οι τέσσερις μορφές μετασχηματισμού γνώσης

Σύμφωνα με τον Nonaka (1994), (Nonaka et al.,1995), μπορούμε να διακρίνουμε τέσσερις τρόπους μετασχηματισμού της γνώσης (Σχ. 1):

(1) από άρρητη σε άρρητη (tacit to tacit), μέσω της διαδικασίας κοινωνικοποίησης,

(2) από ρητή σε ρητή (explicit to explicit), μέσω μιας διαδικασίας που αποκαλείται συνδυασμός,

(3) από άρρητη σε ρητή (tacit to explicit) μέσα από μια διαδικασία που καλείται εξωτερίκευση και

(4) από ρητή σε άρρητη (explicit to tacit), μέσα από μια διαδικασία που καλείται εσωτερίκευση.

Από \ Σε	Άρρητη γνώση	Ρητή γνώση
Άρρητη γνώση	Κοινωνικοποίηση (Socialization)	Εξωτερίκευση (Externalization)
Ρητή γνώση	Εσωτερίκευση (Internalization)	Συνδυασμός (Combination)

Σχ. 1 Τρόποι δημιουργίας γνώσης (Nonaka 1994)

Αναλυτικότερα:

(1) Κοινωνικοποίηση (Socialization): Η ανταλλαγή εμπειριών όπου η προσωπική γνώση δημιουργείται με τη βοήθεια διανοητικών μοντέλων. Παραδείγματα αποτελούν η εκπαίδευση μέσα από την πρακτική εξάσκηση (on the job training), η μέσω δοκιμής-λάθους εκμάθηση, η εξάσκηση, η ανταλλαγή ιδεών ή η συνομιλία με τρίτους.

(2) Εξωτερίκευση (Externalization): Προσωπική ή άρρητη γνώση μπορεί να μετατραπεί σε ρητή με χρήση μεταφορών, αναλογιών, υποθέσεων, μοντέλων. Σύμφωνα με τους Nonaka και Takeuchi, η διαδικασία εξωτερίκευσης είναι θεμελιώδης στη μετατροπή της γνώσης επειδή μέσω αυτής γεννιούνται νέα και σαφή σχέδια.

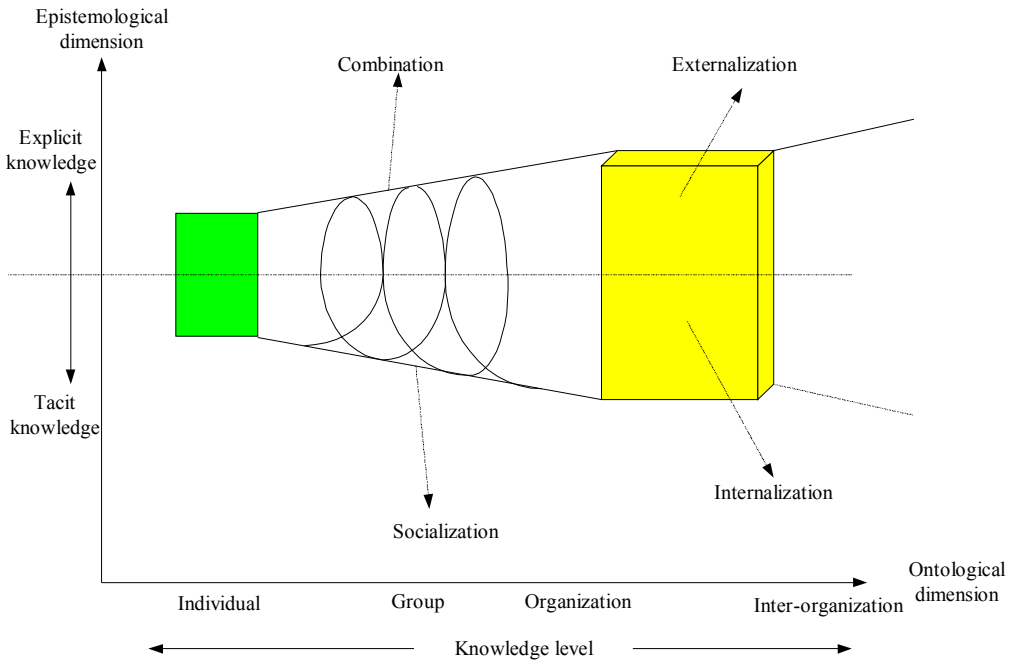
(3) Συνδυασμός (Combination): Οι άνθρωποι ανταλλάσσουν γνώση, με τη βοήθεια εγγράφων, συσκέψεων, τηλεφωνικών συζητήσεων, και με τη βοήθεια των δικτύων δεδομένων. Νέα γνώση μπορεί να προκύψει μέσα από διαδικασίες ταξινόμησης, προσθήκης, συνδυασμό και κατηγοριοποίηση της υπάρχουσας ρητής γνώσης. Ο συνδυασμός, είναι η δημιουργία γνώσης με τις συνήθεις διαδικασίες εκπαίδευσης. Τυπικό παράδειγμα της κατηγορίας αυτής είναι τα πληροφοριακά συστήματα.

(4) Εσωτερίκευση (Internalization): Είναι η διαδικασία με την οποία η ρητή γνώση μετατρέπεται σε άρρητη. Είναι η περίπτωση που κάποιος μαθαίνει περισσότερα για κάτι με το οποίο ασχολείται. Ένας τρόπος να συμβεί αυτό είναι η αναζήτηση γραπτών πηγών. Παραδείγματα εσωτερίκευσης είναι οι διαλέξεις που δίνουν ειδικοί σε κάποιο χώρο, ή η γνώση που αποκτά ένας συγγραφέας όταν αποφασίσει να γράψει μια βιογραφία και αναζητήσει τις πηγές για αυτό με το οποίο θα ασχοληθεί. Βασική προϋπόθεση αποτελεί η ανάληψη δράσης.

Η έλικα της γνώσης

Ενώ κάθε ένας από τους τέσσερις τύπους της γνώσης μπορεί να δημιουργεί γνώση ανεξάρτητα, σύμφωνα με το μοντέλο της οργανωσιακής γνώσης [21] υπάρχει μια δυναμική αλληλεπίδραση μεταξύ των διαφόρων μορφών μετασχηματισμού της γνώσης. Συγκεκριμένα, η δημιουργία γνώσης βρίσκεται στο επίκεντρο μεταξύ ρητής και άρρητης γνώσης και κυρίως μεταξύ εσωτερίκευσης και εξωτερίκευσης.

Η δημιουργία γνώσης στο εσωτερικό του οργανισμού, σαν διαφορετική λειτουργία από την ατομική δημιουργία γνώσης, επιτυγχάνεται όταν και οι τέσσερις τύποι δημιουργίας γνώσης ελέγχονται μέσα σε ένα συνεχή κύκλο. Υπάρχουν διάφορες αιτίες που πυροδοτούν τις μεταβάσεις μεταξύ των διαφορετικών τύπων. Πρώτα, η κοινωνικοποίηση ξεκινά με τη δημιουργία μιας ομάδας αλληλεπίδρασης. Αυτή η ομάδα μοιράζεται τις εμπειρίες και τις προοπτικές. Στη συνέχεια, η φάση της εξωτερίκευσης ξεκινά μέσα από δημιουργικό διάλογο. Σε αυτή τη φάση, σημαντικός είναι ο ρόλος της χρήσης μεταφορών, που δίνουν τη δυνατότητα συγκεκριμενοποίησης ασαφών εννοιών, με στόχο να γίνουν κοινό κτήμα και των υπολοίπων μελών της ομάδας, αποκαλύπτοντας έτσι γνώση που δεν θα μπορούσε μα άλλο τρόπο να αξιοποιηθεί. Έννοιες που σχηματίζονται από ομάδες, μπορούν να συνδυαστούν με υπάρχοντα δεδομένα και καταγεγραμμένη σε αρχεία του οργανισμού γνώση, με στόχο τη δημιουργία μιας πιο συμπαγούς μορφής γνώσης. Με τον πειραματισμό και με επαναληπτικές διαδικασίες δοκιμής – λάθους, πυροδοτείται η διαδικασία της εσωτερικοποίησης (μάθησης στην πράξη). Ενώ η άρρητη γνώση βρίσκεται στην καρδιά της διαδικασίας δημιουργίας γνώσης, τα πρακτικά πλεονεκτήματα αυτής της μορφής γνώσης επικεντρώνονται στην εξωτερίκευσή της και στον πολλαπλασιασμό της μέσα από τη δυναμική μετάβασή της από τους τέσσερις τύπους μετασχηματισμού γνώσης. Έτσι, η άρρητη γνώση μετασχηματίζεται μέσα από μια σπειροειδή κίνηση που τείνει να κλιμακώνεται και να επιταχύνεται, καθώς όλο και περισσότερα μέλη του οργανισμού συμμετέχουν σ’ αυτή τη διαδικασία (Σχ. 2). Η εκκίνηση της διαδικασίας αυτής γίνεται στο επίπεδο ενός ατόμου, προχωρώντας στο επίπεδο του οργανισμού και πολλές φορές επεκτείνεται ξεπερνώντας τα γεωγραφικά όρια του ενός οργανισμού.



Σχ. 2 Η έλικα της γνώσης (Nonaka 1994) [20]

Γνώση και πληροφορία

Η γνώση είναι μια έννοια που επιδέχεται πολλών ερμηνειών. Οι έννοιες γνώση και πληροφορία πολλές φορές συγχέονται μεταξύ τους, χωρίς ωστόσο να ταυτίζονται. Σύμφωνα με τον Nonaka, η πληροφορία είναι μια ροή μηνυμάτων, ενώ η γνώση δημιουργείται από τη ροή των πληροφοριών, όπως αυτές προσαρμόζονται στις προσωπικές πεποιθήσεις του κατόχου της. Η αντίληψη αυτή δίνει έμφαση στη σύνδεση της γνώσης με την ανθρώπινη δραστηριότητα.

Η ανάλυση μεταξύ γνώσης και πληροφορίας μπορεί να επεκταθεί περισσότερο. Η πληροφορία είναι το αναγκαίο μέσο για τη θεμελίωση και την τυποποίηση της γνώσης και μπορεί να ειδωθεί από την συντακτική ή τη σημασιολογική άποψη. Η συντακτική άποψη βασίζεται στην ανάλυση του Shannon στην οποία η αξία της πληροφορίας σχετίζεται με τον όγκο της, χωρίς να αποδίδεται σημασία στο περιεχόμενό της. Αντίθετα, η σημασιολογική άποψη είναι πολύ πιο σημαντική, καθώς εστιάζει στο νόημα που αποδίδεται στην πληροφορία.

Προκειμένου για την αποδοτική διαχείριση της γνώσης σε ένα οργανισμό, απαιτείται να υπάρχει δυνατότητα γρήγορης αναζήτησης της υπάρχουσας γνώσης και της πληροφορίας. Πρακτική απαίτηση λοιπόν, απαιτεί να είναι εφικτή από

όλους η πρόσβαση στην πληροφορία με τον ελάχιστο αριθμό βημάτων. Για το σκοπό αυτό,

α) τα μέλη του οργανισμού θα πρέπει να γνωρίζουν ποιος είναι ο κάτοχος της πληροφορίας και

β) θα πρέπει να απαιτείται να έρθουν σε επαφή με όσο το δυνατόν λιγότερους συναδέλφους τους, ώστε να μην τροφοδοτούνται με πληροφορία περισσότερη από όση μπορούν να χειριστούν ικανοποιητικά.

Η διαδικασία της δημιουργίας γνώσης σε επίπεδο οργανισμού.

Θα επιχειρήσουμε στη συνέχεια να συσχετίσουμε την διαδικασία δημιουργίας γνώσης μέσα στο πλαίσιο του οργανισμού, ακολουθώντας την προσέγγιση που περιγράφεται στο [20].

- *Εμπλουτισμός της ατομικής γνώσης*

Η πρωταρχική ώθηση στη διαδικασία δημιουργίας γνώσης στον οργανισμό είναι το άτομο. Η ποιότητα της άρρητης γνώσης που κατέχει το άτομο ωστόσο, επηρεάζεται από δύο κυρίως παράγοντες: Ο ένας είναι η ποικιλία στις εμπειρίες του. Εάν η εμπειρία αυτή περιορίζεται σε δουλειές ρουτίνας, η ποιότητα της γνώσης ελαττώνεται με το χρόνο. Ωστόσο, η αύξηση της ποιότητας της εμπειρίας από μόνη της, δεν αποτελεί προϋπόθεση για την αύξηση της ποιότητας της άρρητης γνώσης. Ο δεύτερος παράγοντας είναι η υψηλής ποιότητας πείρα, που περιλαμβάνει ορισμένες φορές τον πλήρη επαναπροσδιορισμό της φύσης της εργασίας.

Προσαρμόζοντας τις γενικές αυτές διαπιστώσεις στον τομέα του ενδιαφέροντός μας που είναι η ασφάλεια πληροφοριακών συστημάτων, καθίσταται προφανής η ανάγκη η δουλειά του ειδικού της ασφάλειας να επαναπροσδιορίζεται σε τακτά χρονικά διαστήματα, ώστε να μην μετατρέπεται σε διαδικασία ρουτίνας, αλλά σε δημιουργική δραστηριότητα παραγωγής γνώσης.

- *Δημιουργία αυτοδιοικούμενων ομάδων*

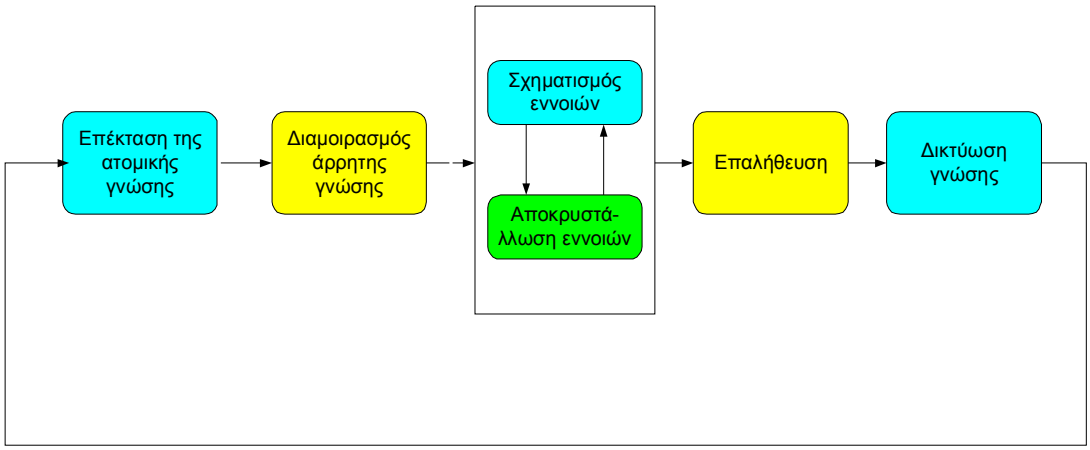
Η ατομική γνώση για να μπορέσει να ενσωματωθεί στο ευρύτερο κοινωνικό πλαίσιο και να πολλαπλασιαστεί, είναι αναγκαίο να βρεθεί σε ένα κατάλληλο πεδίο ανάδειξης των ατομικών πεποιθήσεων και επίλυσης μέσα από διάλογο μεταξύ των αντιθέτων απόψεων. Βασική προϋπόθεση η ύπαρξη αυτονομίας, στο εσωτερικό μικρών ευέλικτων ομάδων, που δημιουργούνται με στόχο την εξάπλωση της γνώσης μεταξύ των μελών της. Μέσα σε μια τέτοια ομάδα, η δημιουργία γνώσης επέρχεται σαν αποτέλεσμα δύο διαδικασιών:

α) τη δημιουργία αμοιβαίας εμπιστοσύνης μεταξύ των μελών της και τη μεταβίβαση της εμπειρίας των παλαιότερων στους υπόλοιπους και

β) ένα σύνολο απόψεων γίνεται κοινά αποδεκτό μέσα από τον ομαδικό διάλογο.

- *Δικτύωση της γνώσης*

Ο σχηματισμός νέων εννοιών, όπως περιγράφηκε ήδη, αναπαριστά μια καινούργια πραγματικότητα στο δίκτυο γνώσης του οργανισμού. Μετά τα στάδια του σχηματισμού οργανωσιακής γνώσης και επαλήθευσης της εγκυρότητας των νέων εννοιών, ακολουθεί το στάδιο της αφομοίωσης και ολοκλήρωσης στη βάση γνώσης του οργανισμού. Έτσι, δημιουργείται ένα δίκτυο στο εσωτερικό του οποίου κυκλοφορεί η υπάρχουσα γνώση και μέσα από μια διαδικασία της υπάρχουσας γνωσιακής βάσης, αφομοιώνονται οι νέες έννοιες με τις παλιές.



Σχ. 3 Διαδικασία δημιουργίας οργανωσιακής γνώσης (Nonaka, 1994)

Ζωτικότητα της γνώσης που σχετίζεται με την ασφάλεια για τον οργανισμό

Η χρησιμότητα των λειτουργιών διαχείρισης γνώσης είναι εμφανής και στα τρία επίπεδα ενός οργανισμού. Στο στρατηγικό επίπεδο, δηλαδή το επίπεδο που σχετίζεται με τα μακροπρόθεσμα σχέδια [15] η σχεδίαση των επιχειρηματικών δραστηριοτήτων επιβάλλεται να γίνει εξετάζοντας την υπάρχουσα γνώση και τη γνώση που σχετίζεται με μελλοντικές διαδικασίες. Στο τακτικό επίπεδο, ο οργανισμός προσπαθεί να προσδιορίσει και να τυποποιήσει την υπάρχουσα γνώση, να αποκτήσει νέα γνώση για μελλοντική χρήση και να την αρχειοθετήσει σε οργανωσιακές μνήμες και να δημιουργήσει συστήματα που θα επιτρέπουν την αποδοτική χρήση της γνώσης μέσα στον οργανισμό. Στο τεχνικό επίπεδο, η

γνώση χρησιμοποιείται στην καθημερινή πρακτική, που την αξιοποιεί για την εκτέλεση των καθημερινών του ασχολιών, και που πρέπει να μπορεί να έχει πρόσβαση στη χρήσιμη γνώση, στον κατάλληλο τόπο και χρόνο.

Συμπερασματικά μπορούμε να πούμε ότι η αξιοποίηση της γνώσης που σχετίζεται με την ασφάλεια αποσκοπεί στην αύξηση της ευελιξίας του οργανισμού και της ικανότητας αντιμετώπισης των προβλημάτων και των προκλήσεων που σχετίζονται με αυτό. Προκειμένου για να επιτευχθεί αυτό απαιτείται τόσο να υπάρχει υποστήριξη από λογισμικό και υποδομές, όσο και από την ύπαρξη ενός δικτύου ειδικών τόσο από τον ίδιο τον οργανισμό όσο και από άλλους οργανισμούς, μέσα από τη συνεργασία των οποίων θα μπορεί να αξιοποιηθεί καλύτερα η γνώση που αφορά στην ασφάλεια και κατά συνέπεια συμβάλει στην ομαλή λειτουργία του ΠΣ.

ΜΕΡΟΣ Β – Ομάδες αντιμετώπισης ψηφιακών απειλών

Ιστορικά στοιχεία

Μετά την πρώτη εμφάνιση μαζικής επίθεσης όπως για παράδειγμα το ιομορφικό λογισμικό που δημιούργησε ο Morris το 1988 αποφασίστηκε η δημιουργία ομάδων που θα χειρίζονταν περιστατικά ασφάλειας. Η εξάπλωση, η αποτελεσματικότητα και η ζημιά που επέφερε η συγκεκριμένη επίθεση ήταν πρωτοφανής για εκείνη την εποχή. Λίγες μέρες μετά την εμφάνισή της επίθεσης, συνεδρίασε το «National Computer Security Center (NCSC)» της NSA από κοινού με το «Defense Advanced Research Projects Agency (DARPA)», προκειμένου να εντοπίσουν τις αιτίες για την αποτελεσματικότητα της συγκεκριμένης επίθεσης. Ο σκοπός της συνεργασίας ήταν η δημιουργία ενός πλαισίου εργασίας ώστε να αποτραπεί και να αντιμετωπιστεί αποτελεσματικά τυχόν παρόμοια μελλοντική επίθεση. Το αποτέλεσμα της διαβούλευσης ήταν ότι υπήρξαν πολύ σημαντικά προβλήματα στο μηχανισμό αντιμετώπισης του προβλήματος και το συντονισμό πολύ σοβαρότερα από ότι το τεχνικό επίπεδο του ίδιου του προβλήματος. Δηλαδή οι οργανισμοί που προσβλήθηκαν από την επίθεση δε συνεργάστηκαν και δε συντονίστηκαν ώστε [14]:

- Να ανιχνευτεί η επίθεση γρηγορότερα.
- Να αναλυθεί η επίθεση γρηγορότερα, άρα να δημιουργηθούν και να υλοποιηθούν γρηγορότερα τα αντίμετρα προστασίας σε αυτήν την επίθεση.
- Να διανεμηθούν τα αντίμετρα προστασίας γρηγορότερα ώστε να προστατευτούν οργανισμοί που δεν είχαν ακόμα προσβληθεί από την επίθεση, καθώς και να μην ξαναπροσβληθούν από την επίθεση.

Με βάση τις παραπάνω παρατηρήσεις το «DARPA» ανάθεσε στο «Software Engineering Institute» του πανεπιστημίου Carnegie Mellon τη δημιουργία ενός συντονιστικού κέντρου για την απόκριση σε περιστατικά ασφάλειας. Το κέντρο αυτό ονομάστηκε «Computer Emergency Response Team Coordination Center (CERT/CC)» [5] το οποίο θα επίλυε το πρόβλημα της αποτελεσματικότητας παρόμοιων επιθέσεων, παρέχοντας μία μεθοδολογία συντονισμού και συνεργασίας μεταξύ ειδικών σε θέματα ασφάλειας. Αυτή η μεθοδολογία θα αποσκοπούσε στον

αποδοτικό χειρισμό, ανάλυση και απόκριση σε περιστατικά ασφάλειας. Επιπλέον, το κέντρο είχε την ευθύνη της καλλιέργειας επίγνωσης σε θέματα ασφάλειας στην κοινότητα των χρηστών του διαδικτύου. Το Δεκέμβριο του 1989 ξεκίνησε η λειτουργία του «CERT/CC» από το πανεπιστήμιο Carnegie Mellon [6]. Πολύ σύντομα άρχισαν να εκτιμώνται τα πρώτα αποτελέσματα της λειτουργίας του «CERT/CC», τα οποία ήταν εντυπωσιακά. Το κέντρο κατάφερε να συντονιστεί και να συνεργαστεί με ειδικούς ασφάλειας για την αντιμετώπιση του ιομορφικού λογισμικού WANK περιορίζοντας σημαντικά το εύρος και τις επιπτώσεις του. Λόγω αυτής της αποτελεσματικότητας, αποφασίστε να γίνει το επόμενο βήμα για την αποτελεσματική προστασία των πληροφοριακών συστημάτων. Αυτό το βήμα ήταν η δημιουργία ενός δικτύου από CSIRTs για τη διευκόλυνση της συνεργασίας και του συντονισμού μεταξύ αυτών των ομάδων. Έτσι, το Νοέμβριο του 1990 δημιουργήθηκε το «Forum of Incident Response and Security Teams (FIRST)» [7], όπου οι συμμετέχουσες ομάδες μπορούσαν να διαμοιραστούν πληροφορίες, γνώσεις και να αλληλοβοηθούν, με απώτερο σκοπό τη γρήγορη, τη συνεργαζόμενη και τη συντονισμένη απόκριση σε περιστατικά ασφάλειας. Απαραίτητη προϋπόθεση να διατηρείται η εμπιστευτικότητα των δεδομένων που αξιοποιούνται από το CERT και να δημιουργείται ένα έμπιστο δίκτυο μεταξύ των διαφορετικών ομάδων. Με την πάροδο των χρόνων δημιουργούνταν CSIRTs για την προστασία κάθε φορά και διαφορετικού οργανισμού: Dutch research network «Cert-NL» το 1992, German Research Network «DFN-CERT» το 1993, Asia Pacific Security Incident Response Coordination CERT «APSIRC» το 1997. Το 1999 δημιουργήθηκε από τον οργανισμό Trans-European Research and Education Network Association «TERENA» [8] η ομάδα εργασίας TF-CSIRT [9]. Η ομάδα είχε κοινό σκοπό με τον οργανισμό FIRST αλλά επικεντρωνόταν στις CSIRTs της Ευρώπης. Συγκεκριμένα οι στόχοι της ομάδας είναι οι εξής:

- Παροχή forum για την ανταλλαγή εμπειριών και γνώσεων.
- Υλοποίηση πιλοτικών υπηρεσιών για τις Ευρωπαϊκές CSIRTs.
- Προώθηση κοινών προτύπων και διαδικασιών για την απόκριση σε περιστατικά ασφάλειας.

- Παροχή βοήθειας για την εγκαθίδρυση καινούργιων CSIRTs και την εκπαίδευση του προσωπικού τους.

Την ίδια χρονική περίοδο ο οργανισμός TERENA δημιουργεί μια διαδικασία διασφάλισης εμπιστοσύνης μεταξύ των συνεργαζόμενων CSIRTs. Αυτή η διαδικασία ονομάστηκε «TERENA Trusted Introducer» [10] και παρέχει ένα "έμπιστο δίκτυο" μεταξύ των CSIRTs της Ευρώπης, όπως και το αντίστοιχο δίκτυο του οργανισμού FIRST. Ακόμα, ο οργανισμός «TERENA» δημιούργησε το «European CSIRT Network (eCSIRT.net)»[11], το οποίο λειτούργησε από το 2002 μέχρι το 2003 και αποσκοπούσε στην υλοποίηση τεχνικών λειτουργιών για:

- Την ανταλλαγή και τη διαμοίραση πληροφοριών μεταξύ των CSIRTs βάσει των προτύπων IODEF και IDMEF.
- Την υλοποίηση ευκρινών και σαφών προτυποποιήσεων για την ανταλλαγή πληροφοριών, τη συλλογή στατιστικών στοιχείων και για την παραγωγή προειδοποιήσεων και συναγερμών που σχετίζονται με περιστατικά ασφάλειας.

Σήμερα ο οργανισμός «FIRST» έχει πάνω από 170 μέλη ενώ ο «TERENA TI» πάνω από 100. Το «eCSIRT.net» εκπλήρωσε τους στόχους του δημιουργώντας μια κοινή σημασιολογία για την ανταλλαγή και τη διαμοίραση πληροφοριών βάση του IODEF και του IDMEF. Αναλυτικά, το δίκτυο δημιούργησε μια συνάρτηση για τη συγκέντρωση και την παραγωγή στατιστικών γραφημάτων που αφορούσαν δεδομένα καταγραφής συστημάτων ανίχνευσης εισβολών. Επιπρόσθετα δημιούργησε ένα πλαίσιο εργασίας για την αναφορά και τη διανομή προειδοποιήσεων και συναγερμών που αφορούσαν περιστατικά ασφάλειας. Η παροχή των παραπάνω διευκολύνσεων για τη συνεργασία και το συντονισμό των CSIRTs και ταυτόχρονα η αύξηση των περιστατικών ασφάλειας είχε ως αποτέλεσμα τη γεωμετρική αύξηση του αριθμού των ομάδων. Ανατρέχοντας στην ιστορία των CSIRTs παρατηρείται ότι έχει δοθεί μεγάλη έμφαση τη συνεργασία και στο συντονισμό αυτών των ομάδων. Ένα κατανοητό, γρήγορο και ασφαλές πλαίσιο εργασίας που θα διευκολύνει τη συγκεκριμένη επικοινωνία θα αυξήσει την ικανότητα των ομάδων για γρήγορη και αποτελεσματική απόκριση σε περιστατικά ασφάλειας. Μέχρι το 2003 αρκετοί οργανισμοί διαφόρων τύπων έχουν δημιουργήσει CSIRTs. Το 43% από αυτούς είναι οργανισμοί της βόρειας Αμερικής, το 44% της Ευρώπης και το υπόλοιπο 13% της Ασίας, της Αυστραλίας και της Νότιας Αμερικής. Το 50% αυτών των οργανισμών ξοδεύουν από 100.000$ έως 1.000.000$ για τη λειτουργία των CSIRTs τους.

Σύγχρονες Απειλές

Τα τελευταία χρόνια πληροφοριακά και επικοινωνιακά συστήματα απειλούνται κυρίως από *ιούς (viruses), μη επιθυμητά ηλεκτρονικά μηνύματα (spam)* και *κακόβουλο λογισμικό (κυρίως phishing)*. Οι ιοί (viruses) είναι προγράμματα, που μπορούν να έχουν καταστρεπτική επίδραση στους υπολογιστές και εξαπλώνονται μέσω ανταλλαγής στοιχείων. Σύμφωνα με μία έρευνα του FBI: Computer Crime and Security Survey, το 65% από τις επιθέσεις σε συστήματα υπολογιστών που αποκαλύφθηκαν το 2006, αποτελείτο από επιθέσεις ιών και προκάλεσαν ζημιές 15.700.000 $ Η αποστολή μη επιθυμητών ηλεκτρονικών μηνυμάτων (spam) αυξήθηκε το 2006 κατά 86,2%. Σύμφωνα με μία έκθεση της εταιρίας MessageLabs ο αριθμός των spam που φιλτραρίστηκαν το 2006 έφτασε τα 180 εκατ. καθημερινά (πρβλ. http://www.messagelabs.com/Threat_Watch/Threat_Statistics) Σύμφωνα με στοιχεία της εταιρίας GMX μόνον το download των spam κόστισε το 2003 12 δισ. €. Phishing ονομάζονται τα ηλεκτρονικά μηνύματα που έχουν σκοπό την κλοπή εμπιστευτικών πληροφοριών και ιδιαίτερα στοιχείων τραπεζικών λογαριασμών. Σύμφωνα με μία έρευνα της εταιρίας ασφάλειας συστημάτων Symantec, καθημερινά αποστέλλονται 7,19 εκατομμύρια μηνύματα Phishing, κατά μέσο όρο, ενώ μία μελέτη του Ινστιτούτου αγοράς Gartner, αναφέρει ότι μόνο το έτος 2005 η αποστολή Phishing προκάλεσε στις ΗΠΑ οικονομική ζημιά ύψους 2,4 δισεκατομμυρίων δολαρίων (σχετικά με τους κινδύνους και τους τρόπου πραγματοποίησης αυτής της απειλής βλ. http://www.antiphishing.org/)

Ομάδες Αντιμετώπισης Περιστατικών Ασφαλείας: Διεθνής Εμπειρία

Η ομάδα CERT® του πανεπιστημίου Carnegie Mellon στο Pittsburgh της Pennsylvania. Αποτελεί τμήμα του Software Engineering Institute (SEI), ένα ομοσπονδιακά χρηματοδοτούμενο κέντρο έρευνας και ανάπτυξης. Ιδρύθηκε μετά την επίθεση του Morris που προκάλεσε αναστολή της λειτουργίας των συστημάτων παγκοσμίως το Νοέμβριο του 1988. Το Defense Advanced Research Projects Agency (DARPA) επιφόρτισε το SEI με την ανάπτυξη ενός κέντρου που θα συντονίζει την επικοινωνία μεταξύ ειδικών ασφάλειας στη διάρκεια επειγόντων περιστατικών και παράλληλα θα έχει στόχο την πρόληψη μελλοντικών περιστατικών. Το κέντρο αυτό ονομάστηκε CERT Coordination Center (CERT/CC). Ενώ ο βασικός ρόλος του

κέντρου στη διάρκεια των ετών παρέμεινε η απάντηση σε βασικά περιστατικά ο ρόλος του κέντρου επεκτάθηκε στη διάρκεια των ετών. Παράλληλα με την ανάπτυξη του διαδικτύου και τη χρήση του για βασικές δραστηριότητες, έχει επέλθει και μία σημαντική πρόοδος στις χρησιμοποιούμενες τεχνικές για επιθέσεις μέσω δικτύου, στις προκαλούμενες ζημιές και παράλληλα στη δυσκολία ανίχνευσης μίας επιτυχούς επίθεσης κάτι που συνιστά σε αυξημένη δυσκολία εντοπισμού των εισβολέων. Προκειμένου για την αποτελεσματικότερη διαχείριση των παραπάνω, η ομάδα CERT/CC είναι πλέον μέλος ενός μεγαλύτερου προγράμματος που σαν κύριους στόχους έχει τη διαφύλαξη ότι κατάλληλες τεχνολογίες και τεχνικές διαχείρισης συστημάτων χρησιμοποιούνται για τη την αντιμετώπιση των επιθέσεων σε διαδικτυωμένα συστήματα και για τον περιορισμό των ζημιών από επιτυχείς επιθέσεις καθώς και τη διαφύλαξη της ομαλούς λειτουργίας των συστημάτων.

Τομείς δραστηριότητας

Από τους κύριους στόχους είναι η ανάλυση των απαιτήσεων ασφάλειας σε περιβάλλοντα διαδικτύου και η διάχυση των σχετικών πληροφοριών σε διαχειριστές συστημάτων, διαχειριστές δικτύου και σε όλους τους χρήστες του διαδικτύου. Βασική προϋπόθεση είναι η ύπαρξη εμπιστοσύνης που τυγχάνει το CERT από οργανισμούς που εμπιστεύονται σημαντικά δεδομένα για την ανάλυσή τους στο CERT, το οποίο έχει αποδεδειγμένα διατηρήσει την ανωνυμία των παραπάνω οργανισμών. Παράλληλα το CERT έχει διατηρήσει την ουδετερότητα του, παραμένοντας ουδέτερο σε οποιεσδήποτε διαμάχες μπορεί να ξεσπάσουν για λόγους εμπορικού ανταγωνισμού μεταξύ εταιριών λογισμικού. Η ομάδα CERT/CC παρακολουθεί δημόσιες πηγές πληροφόρησης σχετικές με την ευπάθεια προιόντων και συστημάτων και λαμβάνει τακτικά πληροφορίες σχετικές με την ευπάθεια αυτών των δεδομένων. Μετά τη λήψη μίας αναφοράς η ομάδα αναλύει τη δυνητική ευπάθεια και προχωρά με τους δημιουργούς της κάθε τεχνολογίας σχετικά με την διαπιστωθείσα ευπάθεια του προϊόντος τους και επιχειρεί να τους βοηθήσει στην αντιμετώπιση του συγκεκριμένου προβλήματος. Παράλληλα μία ομάδα ειδικών αναλυτών ασχολείται με την ανάλυση κακόβουλου κώδικα και τεχνικών επιθέσεων. Η ανάλυση που προκύπτει μέσω των παραπάνω δραστηριοτήτων καταγράφεται σε σχετικές δημοσιεύσεις που κοινοποιούνται μέσα από το δικτυακό τόπο του CERT. Υψηλότερη προτεραιότητα αντιστοιχείται σε επιθέσεις που έχουν στόχο τις υποδομές (Internet, internet service

providers, domain name servers, and routers). Το προσωπικό της ομάδας έχει στόχο να ευαισθητοποιήσει τους κατασκευαστές προϊόντων λογισμικού και υλικού να βελτιώσουν τη βασική ασφάλεια των προϊόντων τους και να συμπεριλάβουν θέματα ασφάλειας στη βασική εκπαίδευση που παρέχουν στους πελάτες τους. Σαν τμήμα αυτής της δουλειάς οι αναλυτές του CERT αναλύουν τις βασικές αιτίες τις εμφάνισης ευπαθειών και προτείνουν τακτικές συγγραφής ασφαλούς κώδικα για την αντιμετώπισή τους. Εφαρμόζοντας τις παραπάνω τακτικές οι προγραμματιστές μπορούν να βελτιώσουν τόσο την ποιότητα όσο και τη γενικότερη ασφάλεια του λογισμικού τους. Η κλιμάκωση των διαδικτυωμένων υποδομών και η ποικιλομορφία των κοινοτήτων χρηστών καθιστούν αναγκαία την ύπαρξη υποστήριξης από διαφορετικά σημεία της υφηλίου σε αντίστοιχες κοινότητες. Επομένως βασικό άξονα της πολιτικής του CERT/CC είναι η υποστήριξη και διάδοση της ανάπτυξης ομάδων αντιμετώπισης επειγόντων περιστατικών computer security incident response teams (CSIRTs) και η καθοδήγηση και εκπαίδευση τόσο σε νέες όσο και σε υπάρχουσες ομάδες.

- Διαχείριση Επιβίωσης Επιχειρήσεων

Ο στόχος της διαχείρισης βιωσιμότητας επιχειρήσεων είναι να βοηθηθούν οι οργανισμοί να προστατέψουν και να υπερασπιστούν τις υποδομές τους από επιθέσεις. Στην κατεύθυνση αυτή έχουν αναπτυχθεί τεχνικές αξιολόγησης επικινδυνότητας που βοηθούν τους οργανισμούς να προσδιορίσουν και να αξιολογήσουν τις πληροφοριακές τους υποδομές και να προσδιορίσουν τον κίνδυνο που αυτές διατρέχουν. Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν τα αποτελέσματα αυτής της αξιολόγησης και να δημιουργήσουν τη δική τους στρατηγική για τη θωράκιση των συστημάτων τους. Η επιχειρησιακή ανάλυση κρίσιμων απειλών, πόρων και ευπαθειών, (The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM - OCTAVE®) είναι μία τεχνική που επιτρέπει στους οργανισμούς να εφαρμόζουν μία αυτο-αξιολόγηση των συστημάτων και ων αλλαγών που επέρχονται σε αυτά στην πάροδο του χρόνου. Η μέθοδος αυτή που προσαρμόζεται στις ανάγκες του κάθε οργανισμού, λαμβάνει υπόψη της τους πόρους, τις απειλές και τις ευπάθειες (οργανωσιακής αλλά και τεχνολογικής φύσεως) ώστε ο οργανισμός να αποκτήσει μία σαφή εικόνα της ασφάλειας των συστημάτων του. Τέλος, με τη βοήθεια μίας παραλλαγής της μεθόδου OCTAVE, της OCTAVE-S μπορεί η ίδια τεχνική να

εφαρμοστεί σε οργανισμούς μικρότερου μεγέθους. Στα πλαίσια της εφαρμογής τεχνικών που αφορούν σε συστήματα διακυβέρνησης γίνεται προσπάθεια να ενθαρρυνθούν οι οργανισμοί να κατακτήσουν ένα κατάλληλο επίπεδο ασφάλειας. Στα πλαίσια αυτά έχουν αναπτυχθεί τεχνικές διαχείρισης ασφάλειας επιχειρήσεων (enterprise security management - ESM)καθώς και σχετικά πρωτόκολλα όπως για παράδειγμα το Mission Assurance Analysis Protocol (MAAP). Η τεχνική ESM λαμβάνει υπόψη της το σύνολο των εσωτερικών διαδικασιών και βέλτιστων πρακτικών μίας επιχείρησης και τις ολοκληρώνει σε μία γενικότερη διαδικασία που μπορεί να προσδιοριστεί αλλά και να μετρηθεί ως προς την αποτελεσματικότητα της. Η MAAP αντίστοιχα, είναι μία τεχνική που διασφαλίζει την ολοκλήρωση συγκεκριμένων διαδικασιών προσδιορίζοντας και αναλύοντας την επικινδυνότητα που σχετίζεται με κρίσιμες διαδικασίες. Εκπαίδευση και εξάσκηση Μία από τις βασικές προκλήσεις που προκύπτουν σαν αποτέλεσμα της διαδικτύωσης είναι να εκπαιδευτούν όσοι τα χρησιμοποιούν ώστε να μπορέσουν βελτιώσουν την ασφάλεια αλλά και την ικανότητα ανάκαμψης των συστημάτων. Στα πλαίσια αυτά η ομάδα CERT/CC προσφέρει μαθήματα στο τεχνικό και διαχειριστικό προσωπικό των συστημάτων προκειμένου για τη διαχείριση της ασφάλειας των συγκεκριμένων συστημάτων. Συμμετοχή σε κοινότητες Το CERT συνεργάζεται με άλλους οργανισμούς με στόχο τη βελτίωση της ασφάλειας του διαδικτύου και της βιωσιμότητας των δικτυακών συστημάτων. Συμμετοχή σε οργανισμούς Το CERT/CC συμμετέχει σε μία σειρά από οργανισμούς, όπως: Forum of Incident Response and Security Teams (FIRST) – Το CERT/CC αποτελεί ιδρυτικό μέλος της κοινότητας FIRST, η οποία είναι ένας συνασπισμός από μεμονωμένες ομάδες του είδους ανά τον κόσμο. Κάθε ομάδα μέσω της ενίσχυσης των δεσμών αμοιβαίας εμπιστοσύνης συνεισφέρει στην επίλυση των προβλημάτων που απασχολούν τα μέλη του συνόλου των αντίστοιχων ομάδων. Τα μέλη της ομάδας FIRST συνεργάζονται προκειμένου για γεγονότα που ξεπερνούν τα σύνορα μίας ομάδας ή χώρας και εκδίδουν οδηγίες για την αντιμετώπιση των σχετικών περιστατικών ασφάλειας. Internet Engineering Task Force (IETF) – Το IETF είναι μία διεθνή οργάνωση που ασχολείται με την ανάπτυξη προτύπων που αφορούν στη λειτουργία του internet. National Security Telecommunications Advisory Committee's Network Security Information Exchange (NSTAC NSIE) – Η ομάδα NSTAC NSIE εργάζεται με στόχο την ελάττωση των ευπαθειών σε κρίσιμες υποδομές. Προσπάθειες σε εθνικό επίπεδο Το CERT καλείται προκειμένου να γνωματεύσει σε κυβερνητικές επιτροπές ή να παρέχει υπηρεσίες

συμβουλευτικού επιπέδου. Το CERT/CC συνεργάζεται επίσης με άλλες ομάδες σε εθνικό επίπεδο που στόχο έχουν τη θωράκιση της εθνικής ασφάλειας και την προστασία συστημάτων από επιθέσεις του κυβερνοχώρου καθώς και τη δημιουργία τεχνικών που καθιστούν τα συστήματα ικανά να ανταποκρίνονται σε δικτυακές απειλές.

Τρέχουσα κατάσταση στον χώρο των CSIRT.

Στη συγκεκριμένη ενότητα θα περιγραφεί η τρέχουσα κατάσταση όσον αφορά τη δομή, τη λειτουργία και την αποστολή των CSIRT. Αρχικά θα περιγραφεί το εννοιολογικό πλαίσιο των CSIRTs, θέματα που έχουν να κάνουν με την ιστορική εξέλιξη των ομάδων αυτών και στη συνέχεια θέματα οργάνωσης και λειτουργίας. Στη συνέχεια θα αναλυθεί το πλαίσιο εργασίας που διέπει τις CSIRTs αναλύοντας τις σχέσεις τους με τους οργανισμούς που προστατεύουν καθώς και τις πολιτικές, τις διαδικασίες και την ποιότητα που έχει αυτό το πλαίσιο εργασίας. Κατόπιν θα αναφέρουμε τα μοντέλα λειτουργίας των ομάδων CSIRT. Στη συνέχεια θα αναλυθούν οι διαδικασίες που ακολουθούνται από τις ομάδες CSIRT προκειμένου να παρέχουν αποτελεσματικές μεθόδους προστασίας του συγκεκριμένου οργανισμού δίνοντας έμφαση στις μεθόδους αντιμετώπισης περιστατικών ασφάλειας Σύμφωνα με το Internet Security Glossary 1 και το Expectations for Computer Security Incident Response [2][14] , ομάδες Απόκρισης σε Πληροφοριακά Περιστατικά Ασφάλειας « Computer Security Incident Response Teams (CSIRTs) » είναι ομάδες που συντονίζουν και υποστηρίζουν την απόκριση σε περιστατικά ασφάλειας τα οποία επιδρούν στα πληροφοριακά συστήματα ενός καθορισμένου προστατευόμενου οργανισμού. Για να θεωρηθεί μία ομάδα ως CSIRT πρέπει να εκτελεί τις παρακάτω λειτουργίες:

- Παροχή ενός ασφαλούς καναλιού για παραλαβή αναφορών που αφορούν ύποπτα περιστατικά ασφάλειας
- Παροχή βοήθειας στα μέλη του προστατευόμενου οργανισμού για το χειρισμό των περιστατικών ασφάλειας.

- Διασπορά πληροφοριών που σχετίζονται με περιστατικά ασφάλειας προς τον προστατευόμενο οργανισμό και προς άλλες ομάδες που εμπλέκονται στα περιστατικά.

Τι ωστόσο μπορεί να περιγραφεί με τον όρο περιστατικό ασφάλειας; Είναι ένα συμβάν που εμφανίζεται σε ένα σύστημα και σχετίζεται με την ασφάλειά του, όπου αυτό το γεγονός εμπλέκεται σε μία παραβίαση των απαιτήσεων ασφάλειας του συστήματος. Ένας περισσότερο τεχνικός ορισμός σύμφωνα με τα παραπάνω RFC, είναι ο εξής:

- Είναι ένα ύποπτο ή εχθρικό γεγονός που παραβιάζει κάποια όψη της ασφάλειας ενός υπολογιστικού συστήματος ή ενός υπολογιστικού δικτύου.
- Προκαλείται σκόπιμα ή τυχαία από χρήστες ή συστήματα
- Μπορεί να επιθυμεί την παραβίαση της ασφάλειας αλλά να μην καταφέρει να επιτύχει κάτι τέτοιο, δηλαδή μπορεί να μην είναι επιζήμιο στα συστήματα ή στο δίκτυο.

Η παραβίαση της ασφάλειας αφορά την παραβίαση των απαιτήσεων ασφάλειας που έχει η πληροφοριακή και επικοινωνιακή υποδομή ενός οργανισμού. Αυτές οι απαιτήσεις είναι οι εξής [3]:

- Εμπιστευτικότητα: Αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους.
- Ακεραιότητα: Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.
- Αυθεντικότητα: Αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας ή χρήσης ενός υπολογιστικού πόρου.
- Διαθεσιμότητα: Αποφυγή καθυστερήσεων στην εξουσιοδοτημένη προσπέλαση πληροφοριών και υπολογιστικών πόρων.

Οργάνωση, στόχοι και σκοποί των ομάδων CSIRT.

Η ωριμότητα που επέρχεται από την λειτουργία ομάδων τύπου CSIRT έχει συντελέσει στην εντυπωσιακή βελτίωση της ποιότητας των υπηρεσιών που οι ομάδες αυτές παρέχουν. Αναλυτικά μια CSIRT είναι υπεύθυνη:

- Για την παραλαβή και τον έλεγχο αναφορών σε περιστατικά ασφάλειας.
- Για την ανάλυση των περιστατικών ασφάλειας ώστε να καθοριστούν:
    - Οι ενέργειες που διέπραξαν.
    - Η απειλή που αποτελούν για την ασφάλεια των συστημάτων.
    - Η επίπτωση που έχουν στην ασφάλεια των συστημάτων που είχαν ως στόχο.
    - Η ζημιά που προκάλεσαν στα συστήματα που είχαν ως στόχο.
    - Η στρατηγική ανάκαμψης των συστημάτων που προσβλήθηκαν.
- Για την εφαρμογή των στρατηγικών απόκρισης, μέσω αντίμετρων προστασίας ώστε:
    - Να ανακάμψουν τα συστήματα από τα περιστατικά ασφάλειας.
    - Να προστατευτούν τα συστήματα από τυχόν παρόμοια μελλοντικά περιστατικά.
    - Να γίνει συντονισμός στη διανομή πληροφοριών η οποία αποσκοπεί στην αύξηση της επίγνωσης ασφάλειας όσον αφορά τα περιστατικά ασφάλειας.

Μια CSIRT έχει ως βασικό στόχο το χειρισμό περιστατικών ασφάλειας ώστε να προστατεύσει τα πληροφοριακά συστήματα ενός οργανισμού. Άρα η ευθύνη μιας CSIRT αφορά την αποτελεσματική και γρήγορη απόκριση σε περιστατικά ασφάλειας με την παροχή μίας υπηρεσίας χειρισμού αυτών των περιστατικών. Όμως ο χειρισμός περιστατικών από μόνος του δεν μπορεί να επιφέρει αποτελεσματική προστασία σε ένα οργανισμό, έναντι της συνεχόμενης ραγδαίας αύξησης της αποτελεσματικότητας των περιστατικών ασφάλειας. Αναλυτικά τα περιστατικά ασφάλειας βελτιώνουν συνεχώς τη φιλοσοφία των δικτυακών επιθέσεων που πραγματοποιούν [12] με αποτέλεσμα να υπάρχει:

• Αύξηση αυτοματισμού και ταχύτητας εργαλείων επίθεσης.

• Αύξηση ευφυΐας και πολυπλοκότητας εργαλείων επίθεσης.

• Γρηγορότερη ανακάλυψη των αδυναμιών ασφάλειας.

• Αύξηση της διαπεραστικότητας των αναχωμάτων ασφάλειας.

• Αύξηση συντονισμένων επιθέσεων που χρησιμοποιούν πολλαπλά συστήματα.

Σχεδόν όλες οι CSIRTs έχουν ως πρωταρχικό στόχο την παροχή υπηρεσίας χειρισμού περιστατικών ασφάλειας. Ταυτόχρονα όμως παρέχουν επιπλέον υπηρεσίες για την καλύτερη προστασία του προστατευόμενου οργανισμού. Αυτές οι υπηρεσίες αποσκοπούν στην άμεση και προληπτική αντιμετώπιση περιστατικών και αδυναμιών ασφάλειας. Έτσι η αποστολή μιας CSIRT είναι η εκπλήρωση των υπηρεσιών που παρέχει σε έναν οργανισμό, για την προστασία του από περιστατικά ασφάλειας [13]. Όλες οι υπηρεσίες έχουν τέσσερις στόχους τη γρήγορη και αποτελεσματική ανίχνευση, απόκριση, αποτροπή και ανάκαμψη σε περιστατικά ασφάλειας. Δια ταύτα, η επίτευξη της αποστολής μιας CSIRT γίνεται με την αποτελεσματική και ποιοτική ικανοποίηση των παραπάνω στόχων. Οι στόχοι μιας CSIRT αποβλέπουν στη βελτίωση της ασφάλειας του προστατευόμενου οργανισμού, μέσω της άμεσης και της προληπτικής αντιμετώπισης των περιστατικών ασφάλειας που τον στοχεύουν. Η επίτευξη των στόχων και κατ' επέκταση της αποστολής μιας CSIRT έχει ως αποτέλεσμα την προστασία και τη διατήρηση της ασφάλειας του οργανισμού. Δηλαδή άμεση αλλά και έμμεση προστασία του οργανισμού παρέχοντας διαδικασίες διαχείρισης ασφάλειας. Όσον αφορά την άμεση προστασία επιτυγχάνεται:

- Γρήγορη παραγωγή και διανομή των μέτρων προστασίας και ανάκαμψης, ώστε να γίνεται γρήγορη ανάκτηση των συστημάτων που έχουν μολυνθεί από το περιστατικό και ταυτόχρονα αποτροπή ενδεχόμενων μελλοντικών συμβάντων του συγκεκριμένου περιστατικού.
- Ελαχιστοποίηση και έλεγχος των επιπτώσεων των περιστατικών ασφάλειας.
- Περιορισμός των συστημάτων που μπορεί να προσβληθούν από περιστατικά ασφάλειας.
- Συλλογή αποδεικτικών στοιχείων για την κατάθεση τους στις δικαστικές αρχές.
- Εναρμόνιση με τους νόμους για την προστασία πληροφοριακών αγαθών και προσωπικών ευαίσθητων δεδομένων [14].

Αντίστοιχα όσον αφορά τη διαχείριση της ασφάλειας επιτυγχάνεται:

- Πλήρης κατανόηση των ενεργειών που υλοποιούν τα περιστατικά ασφάλειας, δηλαδή κατανόηση των απειλών, των κινδύνων και των αδυναμιών ασφάλειας που έχει ο οργανισμός.

- Παροχή ρεαλιστικών και αυθεντικών δεδομένων για απειλές, κινδύνους και αδυναμίες ασφάλειας εκτοξεύοντας την αποτελεσματικότητα και την ποιότητα της ανάλυσης επικινδυνότητας, με αποτέλεσμα να εκτοξεύεται και η μείωση της.
- Εκπαίδευση και απόκτηση επίγνωσης στα μέλη του οργανισμού, βάσει βέλτιστων πρακτικών σε θέματα ασφάλειας του οργανισμού.
- Παροχή μιας καλύτερης γενική εικόνα της ασφάλειας του οργανισμού μέσω της πείρας και της ειδίκευσής που αποκτιέται από την καθημερινή αντιμετώπιση των περιστατικών ασφάλειας.

Ακόμα, η αποστολή μίας CSIRT πρέπει να υιοθετεί και να εξυπηρετεί την αποστολή του προστατευόμενου οργανισμού. Έτσι είναι απαραίτητη η συνεργασία και η επικοινωνία με τα άλλα τμήματα του οργανισμού προκείμενου να του παρέχει αποτελεσματική προστασία. Συγκεκριμένα μια CSIRT μέσα σε ένα οργανισμό αποτελεί:

- Έναν αμυντικό μηχανισμό για την αντιμετώπιση απειλών, αδυναμιών και επιθέσεων ασφάλειας που στοχεύουν τα συστήματα του οργανισμού.
- Ένα κεντρικό σημείο επαφής για την αναφορά περιστατικών ασφάλειας.
- Μια ομάδα συντονισμού και υποστήριξης για την εκτέλεση αποκρίσεων σε περιστατικά ασφάλειας που επηρεάζουν την ασφάλεια του οργανισμού.
- Έναν έγκυρο σύνδεσμο για την επικοινωνία και τη συνεργασία με άλλα εσωτερικά τμήματα του οργανισμού, αλλά και με εξωτερικές CSIRTs, με ειδικούς ασφάλειας και με δικαστικές αρχές.
- Ένα κέντρο διανομής μέτρων προστασίας και μέτρων ανάκαμψης σε περιστατικά ασφάλειας.
- Ένα δείκτη ότι ο οργανισμός ενδιαφέρεται και ασχολείται με την ασφάλειά του.

Μία CSIRT πέρα από την εκπλήρωση της αποστολής της, έχει και κάποιες υποχρεώσεις προς τον προστατευόμενο οργανισμό [2]. Καταρχήν η CSIRT πρέπει να δημοσιεύει τις πολιτικές και τις διαδικασίες της προς τα μέλη του οργανισμού. Το περιεχόμενο αυτών των δημοσιεύσεων πρέπει να είναι ξεκάθαρο και κατανοητό ώστε οι χρήστες να αναφέρουν γρήγορα και αποτελεσματικά τα περιστατικά ασφάλειας στην CSIRT. Επίσης θα ξεκαθαρίζει τους τρόπους και τα σημεία μέσω των οποίων τα μέλη του οργανισμού επικοινωνούν με την CSIRT. Έτσι οι χρήστες θα έχουν υπόψη τους τις απαιτήσεις που πρέπει να έχουν από την CSIRT, όσον αφορά τις υπηρεσίες που τους παρέχει. Μια επιπλέον υποχρέωση των CSIRTs είναι η ύπαρξη σχέσεων με άλλες CSIRTs και γενικότερα με ειδικούς ασφάλειας, ώστε να αυξάνεται η αποτελεσματικότητα των υπηρεσιών τους. Επιπρόσθετα οι CSIRTs είναι υποχρεωμένες να παρέχουν ασφαλές επικοινωνίες μεταξύ των μελών του οργανισμού και μεταξύ των εξωτερικών οντοτήτων που επικοινωνούν. Τα τρέχοντα ερευνητικά θέματα στο πεδίο των CSIRTs εστιάζουν κυρίως στη μεταξύ τους επικοινωνία [14]. Συγκεκριμένα, τα σημεία με τα οποία ασχολείται η ερευνητική κοινότητα των CSIRTs είναι τα εξής:

- Καλλιέργεια εμπιστοσύνης μεταξύ των CSIRTs με σκοπό τη μεταξύ τους συνεργασία και συντονισμό.
- Μηχανισμοί αναγνώρισης και επαλήθευσης CSIRTs.
- Διαμοιρασμός και ανταλλαγή δεδομένων μεταξύ των CSIRTs τα οποία απαρτίζουν περιστατικά ασφάλειας μεταξύ των CSIRTs.

- Τυποποίηση διαδικασιών και μορφοποίηση πληροφοριών που αφορούν περιστατικά, αδυναμίες και συμβουλές ασφάλειας.

- Συντονισμός λειτουργιών για τη διαμοίραση ειδικευμένων γνώσεων και της ανάλυσης των περιστατικών ασφάλειας.

- Απαιτήσεις για την εγκαθίδρυση των CSIRTs.
- Αποκάλυψη αδυναμιών ασφάλειας με τέτοιο τρόπο ώστε να μην μπορούν να εκμεταλλευτούν από επιτιθέμενους.

- Πιστοποίηση και εκπαίδευση των μελών των CSIRTs.
- Υλοποίηση εργαλείων χειρισμού περιστατικών ασφάλειας.

Αντίστοιχα τα τρέχοντα προβλήματα που έχει η εγκαθίδρυση και η λειτουργία των CSIRTs αφορούν ελλείψεις:

- Στη χρηματοδότηση τους
- Στην υποστήριξη τους από τη διοίκηση.
- Στο εξειδικευμένο και εκπαιδευμένο προσωπικό τους.
- Στους γρήγορους, κατανοητούς και ασφαλείς μηχανισμούς επικοινωνίας.
- Σε εργαλεία λογισμικού για το χειρισμό των περιστατικών ασφάλειας.

Συμπερασματικά μπορούμε να πούμε ότι μία CSIRT είναι μία ομάδα από διαδικασίες και μεθοδολογίες για την παροχή ανακοινώσεων και ειδοποιήσεων ασφάλειας, για το χειρισμό περιστατικών ασφάλειας και για τη συνεργασία, το συντονισμό των λειτουργιών της με άλλες CSIRTs. Το μέγεθος και η απαιτούμενη χρηματοδότηση μιας CSIRT εξαρτούνται από την αποστολή της, από το είδος της, από τον τομέα και τη δομή του προστατευόμενου οργανισμού καθώς και από τη στρατηγική αυτού του οργανισμού όσον αφορά τη διαχείριση της ασφάλειάς του.

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.

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.

Οργανισμοί – αντικείμενο προστασίας των ομάδων CSIRT

Μια CSIRT έχει ως αποστολή την προστασία και τη βελτίωση της ασφάλειας ενός οργανισμού. Στην αγγλική ορολογία έχει επικρατήσει ο όρος "constituency" για τον οργανισμό που προστατεύει μία CSIRT. Σε αυτήν την περίπτωση οργανισμός θεωρείται μια ομάδα από πληροφοριακά συστήματα, από επικοινωνιακά συστήματα και από τους χρήστες αυτών των συστημάτων. Έτσι ο προστατευόμενος οργανισμός δεν περιορίζεται σε γεωγραφικά, ή χωροταξικά σύνορα, μπορεί δε να θεωρηθεί και με την ευρεία έννοια του όρου και μία συνένωση διαφορετικών οργανωσιακών μονάδων. Μπορεί να αποτελείται από πολλούς οργανισμούς που έχουν κοινά χαρακτηριστικά όπως είναι οι επιχειρήσεις μίας χώρας, οι χρήστες ενός δικτύου δεδομένων, μια πολυεθνική εταιρία κτλ. Παραδείγματος χάρη η «DFN-CERT» έχει ως προστατευόμενο οργανισμό τα συστήματα και τους χρήστες του γερμανικού ερευνητικού δικτύου υπολογιστών, ενώ η «US-CERT» έχει τα συστήματα και τους χρήστες των Ηνωμένων Πολιτειών. Η αποστολή και κατ' επέκταση το πλαίσιο λειτουργίας μιας CSIRT είναι άμεσα συνδεδεμένη με την αποστολή, το είδος και τη δομή του προστατευόμενου οργανισμού. Το πλαίσιο λειτουργίας που διέπει τη λειτουργία μίας CSIRT πρέπει να υιοθετήσει και να καθοδηγηθεί από τα χαρακτηριστικά του οργανισμού, ώστε να μπορέσει με επιτυχία να προστατεύσει και να βελτιώσει την ασφάλειά του, επειδή η ασφάλεια ενός οργανισμού επικεντρώνεται στις ιδιαίτερες ανάγκες που έχει η πληροφοριακή και επικοινωνιακή υποδομή του. Υπάρχουν διαφορετικά είδη CSIRTs ανάλογα με το είδος του οργανισμού που προστατεύουν ώστε να εστιάσουν στις συγκεκριμένες ανάγκες και απαιτήσεις του, όπως προαναφέρθηκε. Με βάση το είδος του οργανισμού η CSIRT έχει την ανάλογη εξουσιοδότηση στα συστήματα και στις λειτουργίες του. Στην κοινωνία των CSIRTs υπάρχουν μέχρι στιγμή εφτά είδη CSIRTs. Αυτά τα είδη είναι το διεθνές συντονιστικό κέντρο, οι εθνικές CSIRTs, ο πάροχος υπηρεσιών δικτύων, ο κατασκευαστής προϊόντων πληροφορικής, εταιρικές CSIRTs, το κέντρο ανάλυσης και ο πάροχος υπηρεσιών απόκρισης. Το διεθνές συντονιστικό κέντρο έχει ως προστατευόμενο οργανισμό γενικά όλα τα πληροφοριακά και επικοινωνιακά συστήματα που υπάρχουν. Η αποστολή της CSIRT αυτού του είδους είναι η απόκτηση γνώσης από μια παγκόσμια πλευρά για της απειλές, τις αδυναμίες και τους κινδύνους ασφάλειας μέσω του συντονισμού και της συνεργασίας με τους χρήστες

των συστημάτων ή με τα μέλη των CSIRTs ανά την υφήλιο. Μία γνωστή ομάδα αυτού του είδους είναι η «CERT/CC» όπου το αντικείμενο της είναι:

- Ο συντονισμός για ανίχνευση, απόκριση και ανάκτηση περιστατικών ασφάλειας μεταξύ πολλών CSIRTs.
- Η παροχή τεχνικής υποστήριξης για την απόκριση σε περιστατικά ασφάλειας μέσω του συντονισμού με άλλες CSIRTs.
- Η τεκμηρίωση τεχνικών οδηγιών για απειλές και αδυναμίες ασφάλειας.
- Η δημιουργία και η δημοσίευση πληροφοριών για ανίχνευση και παρεμπόδιση περιστατικών ασφάλειας καθώς και για την ανάκτηση των συστημάτων που έχουν προσβληθεί από αυτά τα περιστατικά.

Ο προστατευόμενος οργανισμός μιας εθνικής CSIRT είναι τα πληροφοριακά και επικοινωνιακά συστήματα μια χώρας. Η αποστολή αυτής της CSIRT είναι η παροχή ενός εθνικού σημείου επαφής για απειλές, αδυναμίες ασφάλειας και η μείωση των περιστατικών ασφάλειας που διαπράττονται ή έχουν ως στόχο τα συστήματα μιας χώρας. Η «US-CERT» είναι μια ομάδα αυτού του είδους η οποία προστατεύει την πληροφοριακή υποδομή των Ηνωμένων Πολιτειών. Το αντικείμενο μιας εθνικής CSIRT είναι:

- Η παροχή τεχνικής υποστήριξης για την απόκριση σε περιστατικά ασφάλειας στην εθνική γλώσσα και στη χρονική ζώνη της συγκεκριμένης χώρας.
- Η τεκμηρίωση τεχνικών οδηγιών για απειλές ασφάλειας.
- Η δημιουργία και η δημοσίευση πληροφοριών για ανίχνευση και παρεμπόδιση περιστατικών ασφάλειας που πραγματοποιούνται στη χώρα, καθώς και για την ανάκτηση των συστημάτων της χώρας που έχουν προσβληθεί από αυτά τα περιστατικά.
- Η λειτουργία ως συνδέσμου σε νομικές υπηρεσίες.

Ο πάροχος υπηρεσιών ασφαλείας έχει ως προστατευόμενο οργανισμό τα πληροφοριακά και επικοινωνιακά συστήματα του δικτύου του. Η αποστολή του παρόχου είναι η παροχή ενός ασφαλούς περιβάλλοντος για τη συνδεσιμότητα των χρηστών του δικτύου του. Μια γνωστή ομάδα είναι η DFN-CERT για το ερευνητικό δίκτυο της Γερμανίας. Το αντικείμενο αυτού του είδους ομάδας είναι:

- Η παροχή τεχνικής υποστήριξης για απόκριση σε περιστατικά ασφάλειας που λαμβάνουν χώρα στα συστήματα των πελατών τους.
- Η ικανοποίηση των απαιτήσεων ασφάλειας της δικτυακής υποδομής.
- Η λειτουργία ως σύνδεσμος με εθνικές και με άλλες CSIRTs.

Οι ομάδες των κατασκευαστών προϊόντων πληροφορικής έχουν ως στόχο να προστατέψουν χρήστες που χρησιμοποιούν τα προϊόντα τους και η αποστολή τους είναι η βελτίωση της ασφάλειας αυτών των προϊόντων που παράγουν. Μια τέτοια γνωστή ομάδα είναι η «Cisco Systems Product (SIRT)». Οι CSIRTs αυτού του είδους έχουν ως αντικείμενο:

- Την παροχή τεχνικής υποστήριξης για απόκριση σε αδυναμίες ασφάλειας των προϊόντων τους μέσω της δημοσίευσης προειδοποιήσεων για αδυναμίες που έχουν, καθώς και της δημοσίευσης επιδιορθώσεων ασφάλειας «patches» σε αυτές τις αδυναμίες.
- Τη συνεργασία με άλλες CSIRTs για την ανίχνευση των πηγών των αδυναμιών ασφάλειας στα προϊόντα τους.

Η προστατευόμενη ομάδα μιας εταιρικής (ή αλλιώς εσωτερικής) CSIRT είναι η εταιρία στην οποία ανήκει. Η αποστολή της CSIRT αυτού του είδους είναι η προστασία και η βελτίωση της ασφάλειας των πληροφοριακών και επικοινωνιακών συστημάτων που ανήκουν στην εταιρία. Σε αυτήν την περίπτωση η εταιρία μπορεί να είναι μια επιχειρηματική εταιρία όπως είναι η «Boeing CERT», ένας κυβερνητικός οργανισμός όπως η «DOD-CERT» για το υπουργείο άμυνας των Ηνωμένων Πολιτειών, ή ένας στρατιωτικός οργανισμός όπως η «Air Force CERT» για την πολεμική αεροπορία των Ηνωμένων Πολιτειών. Το αντικείμενο μιας εταιρικής CSIRT είναι:

- Η παροχή ενός επιχειρησιακού κέντρου απόκρισης σε περιστατικά ασφάλειας για τα συστήματα και τα μέλη της εταιρίας.
- Η παροχή τεχνικών λειτουργιών για την απόκριση σε περιστατικά ασφάλειας με απώτερο σκοπό την ανάκαμψη των συστημάτων της εταιρίας, από επιθέσεις ασφάλειας.
- Η δημιουργία και η δημοσίευση πληροφοριών για την ανίχνευση και την παρεμπόδιση περιστατικών ασφάλειας που πραγματοποιούνται στην εταιρία

καθώς και για την ανάκτηση των συστημάτων της εταιρίας που έχουν προσβληθεί από αυτά τα περιστατικά.

Το κέντρο ανάλυσης έχει ως προστατευόμενο οργανισμό τους χρήστες και τους οργανισμούς με τους οποίου συνεργάζεται. Συνήθως τα κέντρα παρέχουν τις υπηρεσίες τους σε όλη την κοινότητα του διαδικτύου και δεν επικεντρώνονται σε κάποιους οργανισμούς, με το να δημοσιεύουν τα αποτελέσματα των υπηρεσιών τους στο ευρύ κοινό. Η αποστολή του κέντρου είναι η σύνθεση δεδομένων που αφορούν περιστατικά ασφάλειας με σκοπό την κατανόησή και την αποτροπή τους. Ένα τέτοιο κέντρο είναι το «The Information Assurance Technology Analysis Center» [1] και το αντικείμενο των CSIRTs αυτού του είδους είναι:

- Η δημιουργία στατιστικών, συνηθειών και μοτίβων που αποσκοπούν στην πρόβλεψη μελλοντικών περιστατικών.
- Η παροχή βοήθειας στην ανάλυση δεδομένων που απαρτίζουν περιστατικά ασφάλειας.
- Η παραγωγή γρήγορων και πρώιμων ειδοποιήσεων ασφάλειας.

Ο προστατευόμενος οργανισμός του παρόχου υπηρεσιών απόκρισης είναι τα πληροφοριακά και επικοινωνιακά συστήματα του οργανισμού πελάτη του. Δηλαδή οι ομάδες που ανήκουν σε αυτή την κατηγορία παρέχουν υπηρεσίες απόκρισης επί πληρωμή σε οποιοδήποτε οργανισμό. Έτσι η αποστολή του πάροχου είναι η απόκριση σε περιστατικά ασφάλειας που συμβαίνουν στα συστήματα των πελατών τους. Οι πάροχοι των υπηρεσιών απόκρισης είναι γνωστοί και ως πάροχοι διαχείρισης υπηρεσιών ασφάλειας. Ένας γνωστός πάροχος είναι ο «IBM Managed Security Services». Το αντικείμενο αυτού του είδους των CSIRTs είναι:

- Η παροχή ενός επιχειρησιακού κέντρου απόκρισης σε περιστατικά ασφάλειας για τα συστήματα και τα μέλη του πελάτη τους.
- Η παροχή τεχνικών λειτουργιών για την απόκριση σε περιστατικά ασφάλειας με απώτερο σκοπό την ανάκαμψη των συστημάτων του πελάτη τους, από επιθέσεις ασφάλειας.
- Η δημιουργία και η δημοσίευση πληροφοριών για την ανίχνευση και την παρεμπόδιση περιστατικών ασφάλειας που πραγματοποιούνται στα

συστήματα του πελάτη τους, καθώς και για την ανάκτηση αυτών των συστημάτων που έχουν προσβληθεί από περιστατικά ασφάλειας.

Όπως γίνεται αντιληπτό από τα παραπάνω, μια CSIRT προστατεύει και βελτιώνει την ασφάλεια του προστατευόμενου οργανισμού με διάφορους τρόπους μέσω δραστικών και άμεσων αποκρίσεων σε περιστατικά ασφάλειας, μέσω τεχνικής υποστήριξης, μέσω προειδοποιήσεων και συναγερμών ασφάλειας, καθώς και μέσω συμβουλών και τεχνικών αναλύσεων σε θέματα ασφάλειας. Ανάλογα τον τρόπο προστασίας που παρέχει μια CSIRT και το είδος του προστατευόμενου οργανισμού υπάρχουν διαφορετικά επίπεδα εξουσιοδότησης της CSIRT σε αυτόν τον οργανισμό. Δηλαδή μια CSIRT έχει διάφορες βαθμίδες εξουσιοδότησης στα πληροφοριακά και επικοινωνιακά συστήματα του προστατευόμενου οργανισμού της. Αυτή η εξουσιοδότηση αφορά την ευθύνη και τον έλεγχο που έχει η CSIRT για τις δικές τις λειτουργίες καθώς και για τις λειτουργίες του προστατευόμενου σε θέματα που αφορούν την προστασία και τη βελτίωση της ασφάλειάς του. Τα επίπεδα εξουσιοδότησης μιας CSIRT είναι τρία: Η πλήρης, η διαμοιρασμένη και η καθόλου εξουσιοδότηση. Τα επίπεδα καθορίζουν τη συμμετοχή της CSIRT στη διαδικασία λήψης αποφάσεων του οργανισμού, για τις λειτουργίες που πρέπει να εκτελεστούν ώστε να προστατευτεί και να βελτιωθεί η ασφάλειά του. Στην πλήρη εξουσιοδότηση η CSIRT καθοδηγεί τον προστατευόμενο οργανισμό για την εκτέλεση λειτουργιών, υπαγορεύοντας του προτάσεις δράσης. Στη διαμοιρασμένη εξουσιοδότηση η CSIRT συνεργάζεται με τον προστατευόμενο οργανισμό ώστε να επηρεάσει τη διαδικασία λήψης αποφάσεων. Όταν η CSIRT δεν έχει καθόλου εξουσιοδότηση τότε αναλαμβάνει να πληροφορήσει τον προστατευόμενο οργανισμό ώστε να τον συμβουλεύσει κατά τη διαδικασία λήψεων αποφάσεων δράσης. Έτσι, ανάλογα με το επίπεδο εξουσιοδότησης η CSIRT είναι υπεύθυνη για την υπαγόρευση, για τον επηρεασμό ή για τη συμβουλή των λειτουργιών που πρέπει να εκτελέσει ο προστατευόμενος οργανισμό. Το επίπεδο εξουσιοδότησης εξαρτάται από τις ευθύνες και τις υποχρεώσεις που έχει θέσει η διοίκηση ενός οργανισμού σε μια CSIRT. Όμως κάθε CSIRT έχει συγκεκριμένες εξουσιοδοτήσεις ανάλογα με το είδος της.

Οι πολιτικές των CSIRTs αποτελούνται από αρχές, οδηγίες και κατευθύνσεις που πρέπει να υιοθετούν. Το περιεχόμενο των πολιτικών περιγράφει τις διαδικασίες, τους ρόλους, τις ευθύνες και τις αλληλεπιδράσεις με τα άλλα τμήματα που πρέπει να έχει η

CSIRT. Επίσης η CSIRT πρέπει να συμμορφώνεται και να ακολουθεί τις λειτουργικές, νομικές και οργανωσιακές αρχές του οργανισμού που προστατεύει 2. Δια ταύτα, το πλαίσιο εργασίας των CSIRTs πρέπει να λειτουργεί βάσει των πολιτικών τους. Το περιεχόμενο των πολιτικών αφορά τον τρόπο με τον οποίο μια CSIRT υλοποιεί τις υπηρεσίες της και τον τρόπο με τον οποίο τις παρέχει στον προστατευόμενο οργανισμό. Άρα οι πολιτικές των CSIRTs αποτελούνται από επιμέρους μικρότερες πολιτικές όπου η καθεμία από αυτές επικεντρώνεται σε ένα συγκεκριμένο τομέα που υλοποιεί και κατ' επέκταση παρέχουν οι CSIRTs. Τα βασικά χαρακτηριστικά αυτών των πολιτικών, όπως και κάθε είδους πολιτικής, είναι οι ιδιότητες και το περιεχόμενό τους. Οι ιδιότητες που πρέπει να έχει μία πολιτική είναι η υποστήριξη της από τη διοίκηση, η κατανόηση της από όλα τα μέλη της CSIRT ανεξαρτήτως των τεχνικών και οργανωτικών γνώσεών τους και η πληρότητα, ώστε να καλύπτει όλα τις αναγκαίες περιοχές μιας CSIRT. Ακόμα η πολιτική πρέπει να είναι περιληπτική, ώστε να μην περιέχει πλεονάζουσες πληροφορίες καθώς και να είναι χρήσιμη, υλοποιήσιμη και επιβλητική ώστε να εφαρμόζεται από την CSIRT και τον οργανισμό. Αντίστοιχα, το περιεχόμενο μιας πολιτικής πρέπει να περιέχει τις απαραίτητες πληροφορίες για τη λειτουργία του πλαισίου εργασίας της CSIRT. Αναλυτικά, η πολιτική πρέπει να αναφέρει τη σύνδεσή της με την αποστολή της CSIRT, περιγράφοντας τους τρόπου με τους οποίους απορρέει από αυτήν την αποστολή. Συνάμα πρέπει να καθορίζει τους ρόλους, τις ευθύνες και τις υποχρεώσεις που έχει η CSIRT. Επίσης η πολιτική πρέπει να καθορίζει τις βασικές αρχές των διαδικασιών που εκτελεί η CSIRT καθώς και τις σχέσεις που έχει η πολιτική με τις παρεχόμενες υπηρεσίες και με άλλες πολιτικές της CSIRT. Τέλος, απαιτείται η αναφορά του εννοιολογικού πλαισίου της CSIRT καθώς και η αναφορά των τρόπων διατήρησης και ανανέωσης της πολιτικής. Οι ελάχιστες πληροφορίες που πρέπει να περιέχονται στις πολιτικές των CSIRTs σύμφωνα με τις προσδοκίες για τις CSIRTs 2 διαχωρίζονται σε τρεις κατηγορίες. Η πρώτη κατηγορία αναφέρει τα είδη των περιστατικών ασφάλειας που χειρίζεται η CSIRT και το επίπεδο της υποστήριξης που παρέχει για την απόκριση σε αυτά. Έτσι τα μέλη της CSIRT και του οργανισμού γνωρίζουν τις δυνατότητες της CSIRT και το επίπεδο της προστασίας που παρέχει στον οργανισμό. Στην επόμενη κατηγορία οι πολιτικές πρέπει να περιγράφουν τις οντότητες με τις οποίες συνεργάζεται η CSIRT, επισημαίνοντας τις πληροφορίες που τους αποκαλύπτει, τις πληροφορίες που διαμοιράζονται μεταξύ τους και τον απώτερο σκοπό αυτής της συνεργασίας. Μέσω αυτών των πολιτικών τα μέλη της CSIRT έχουν

τις απαραίτητες οδηγίες και κατευθύνσεις για μια αποτελεσματική συνεργασία με άλλες CSIRTs ή άλλες ομάδες ειδικών ασφάλειας. Επίσης οι χρήστες του προστατευόμενου οργανισμού γνωρίζουν αν η ομάδα αποκαλύπτει ευαίσθητες προσωπικές πληροφορίες τους, σε ποίους τις αποκαλύπτει και για πιο λόγο. Η τρίτη κατηγορία αφορά τους μηχανισμούς επικοινωνίας και αυθεντικοποίησης που χρησιμοποιεί η CSIRT, ώστε τα μέλη της να έχουν τη δυνατότητα υλοποίησης γρήγορων και ασφαλών επικοινωνιών. Άρα τα μέλη του οργανισμού ενημερώνονται για τους τρόπους με τους οποίους προστατεύονται τα ευαίσθητα δεδομένα τους που επεξεργάζεται η CSIRT. Όπως αναφέρθηκε προηγουμένως, οι πολιτικές των CSIRTs αποτελούνται από επιμέρους πολιτικές όπου η καθεμία επικεντρώνεται σε μία συγκεκριμένη περιοχή. Σύμφωνα με το εγχειρίδιο χρήσης των CSIRTs 3, μία CSIRT πρέπει να έχει τουλάχιστον τις παρακάτω επιμέρους πολιτικές οι οποίες συνθέτουν την πολιτική της.

- Πολιτική κώδικα διεξαγωγής η οποία είναι ένα σύνολο από κανόνες που καθορίζουν τη συμπεριφορά της CSIRT και παρέχει τις βασικές κατευθύνσεις για αντιδράσεις σε συγκεκριμένες καταστάσεις.
- Πολιτική κατηγοριοποίησης πληροφοριών με βάση το βαθμό ευαισθησίας τους.
- Πολιτική αποκάλυψης πληροφοριών η οποία εξαρτάται από το σκοπό, τον παραλήπτη και την κατηγορία της πληροφορίας που αποκαλύπτεται. Αυτή η πολιτική περιέχει:
- Τις περιπτώσεις κατά τις οποίες δίνει ευαίσθητες πληροφορίες του
- προστατευόμενου οργανισμού και σε ποιες οντότητες τις δίνει.
- Περιορισμούς ιδιωτικότητας που πρέπει να έχει η αποκάλυψη των πληροφοριών.
- Τον τρόπο με τον οποίο γίνεται η αποκάλυψη.
- Πολιτική μέσων ενημέρωσης που περιγράφει τις περιπτώσει και τις διαδικασίες όπου η CSIRT ανακοινώνει δημόσια πληροφορίες οι οποίες αφορούν τον προστατευόμενο οργανισμό.
- Πολιτική ασφάλειας της υποδομής της CSIRT. Αυτή η πολιτική είναι σημαντικότατη επειδή η CSIRT έχει πληροφορίες για νέες αδυναμίες, για αδυναμίες συγκεκριμένων συστημάτων καθώς και πληροφορίες για μέλη του

προστατευόμενου οργανισμού. Δηλαδή η CSIRT είναι δημοφιλής στόχος των επιτιθέμενων

- Πολιτική ανθρώπινων λαθών η οποία αναφέρει τις διαδικασίες που ακολουθεί η CSIRT όταν κάποιο μέλος της εκτέλεσε λανθασμένα την παροχή μιας υπηρεσίας της.

Όταν τελειώσει η συγγραφή μιας πολιτικής η CSIRT είναι υπεύθυνη για την αξιολόγησή της, ώστε να διαπιστωθεί αν ακολουθεί και εκπληρώνει την αποστολή της καθώς και αν δεν αντιτίθεται με άλλες πολιτικές που έχει η CSIRT ή ο προστατευόμενος οργανισμός. Στη συνέχεια η CSIRT αναλαμβάνει την υλοποίηση της στο πλαίσιο εργασίας της και τη δημοσίευσή της στα μέλη του προστατευόμενου οργανισμού. Με την καθημερινή χρήση της πολιτικής η CSIRT πρέπει να έχει δυνατότητες βελτίωσής της ώστε να εξαλειφθούν τυχόν προβλήματα που δημιουργεί και να βελτιωθεί η ποιότητα των παρεχόμενων υπηρεσιών.

Οργανωτικά μοντέλα ομάδων CSIRT

Μια CSIRT διαθέτει δομή, στόχους, υπηρεσίες, ανθρώπινο δυναμικό και αλληλεπιδρά με εξωτερικές οντότητες. Βέβαια θεωρείται μέλος ενός ευρύτερου οργανισμού τον οποίου προστατεύει και βελτιώνει την ασφάλειά του. Έτσι το οργανωτικό μοντέλο της CSIRT πρέπει να υιοθετεί σε ένα βαθμό και να συνυπάρχει με τις βασικές αρχές και τη γενικότερη οργάνωση του προστατευόμενου οργανισμού. Το οργανωτικό μοντέλο της CSIRT σχετίζεται με τις ευθύνες και τους ρόλους των μελών της καθώς και με την κυκλοφορία των εισερχόμενων και εξερχόμενων πληροφοριών. Ακόμα σχετίζεται με τη φυσική τοποθεσία της CSIRT και τη θέση και ρόλο της μέσα στα πλαίσια του οργανισμού που ανήκει και προστατεύει. Φυσικά το οργανωτικό μοντέλο έχει να κάνει και με τις αλληλεπιδράσεις που έχει η CSIRT με τα υπόλοιπα τμήματα του οργανισμού τον οποίο προστατεύει. Ανάλογα με τη δομή που χαρακτηρίζει μία CSIRT χαρακτηρίζεται και το είδος της. Κυριότερο χαρακτηριστικό που διακρίνει μία CSIRT από άλλες ομάδες ασφάλειας είναι η επικοινωνία της με άλλες παρόμοιες ομάδες. Θα μπορούσαμε να διακρίνουμε τις CSIRT’s στα εξής είδη [2]: εσωτερική κατανεμημένη, εσωτερική συγκεντρωτική, συνδυασμό εσωτερικής κατανεμημένης και συγκεντρωτικής, όπως και τη συντονιστική CSIRT. Σε αυτές τις περιπτώσεις ο όρος εσωτερική αντιπροσωπεύει την εσωτερική και οργανωσιακή φυσική τοποθεσία της CSIRT στον προστατευόμενο

οργανισμό. Δηλαδή μια CSIRT που είναι εθνικό συντονιστικό κέντρο μπορεί να έχει μόνο το οργανωτικό μοντέλο της συντονιστικής CSIRT. Η επιλογή του οργανωτικού μοντέλου που θα ακολουθήσει μία CSIRT εξαρτάται από πολλούς παράγοντες. Αυτοί οι παράγοντες πηγάζουν από τις ιδιαιτερότητες του προστατευόμενου οργανισμού και την αναμενόμενη λειτουργία της CSIRT. Συγκεκριμένα η επιλογή εξαρτάται από:

- Την αποστολή, τους στόχους, τους πόρους και τη χρηματοδότηση της CSIRT.
- Τους ρόλους και τις ευθύνες που έχουν τα μέλη της CSIRT σύμφωνα με τις οδηγίες της διοίκησης του προστατευόμενου οργανισμού.
- Τις αλληλεπιδράσεις και τη συνεργασία με τα τμήματα του προστατευόμενου οργανισμού.
- Τη φυσική τοποθεσία της CSIRT στον προστατευόμενο οργανισμό.
- Τον αριθμό, το εύρος και το επίπεδο των υπηρεσιών που παρέχει η CSIRT.
- Το επίπεδο εξουσιοδότησης που έχει η CSIRT στις λειτουργίες του προστατευόμενου οργανισμού.
- Το μέγεθος, το είδος και τη γεωγραφική κατανομή του προστατευόμενου οργανισμού.
- Τις ανάγκες ασφάλειας που έχει η πληροφοριακή και επικοινωνιακή υποδομή του προστατευόμενου οργανισμού.

Εσωτερική κατανεμημένη ομάδα

Η εσωτερική κατανεμημένη CSIRT αποτελείται από υπάρχοντα μέλη του προστατευόμενου οργανισμού τα οποία είναι διάσπαρτα σε όλα τα τμήματά του. Τα μέλη της CSIRT αναφέρουν και συντονίζονται από έναν διαχειριστή. Αυτός ο διαχειριστής βρίσκεται σε κεντρικό σημείο του προστατευόμενου οργανισμού και αποτελεί σύνδεσμο με τα άλλα τμήματα του, όπως είναι η διοίκηση και το νομικό τμήμα, αλλά και με εξωτερικές ομάδες όπως είναι οι CSIRTs. Συνηθισμένα είδη προστατευόμενων οργανισμών που χρησιμοποιούν αυτό το οργανωτικό μοντέλο είναι κατανεμημένοι οργανισμοί, όπως είναι οι πολυεθνικές εταιρίες, τα εκπαιδευτικά ιδρύματα και οι κυβερνητικοί οργανισμοί. Στην προκειμένη περίπτωση η CSIRT έχει πλήρη εξουσιοδότηση, δηλαδή έχει δικαίωμα να υπαγορεύσει τις ενέργειες που πρέπει να γίνουν στα συστήματα του οργανισμού για την προστασία και τη βελτίωση της ασφάλειάς τους. Αυτή η εξουσιοδότηση προέρχεται από τη διοίκηση του οργανισμού προς το διαχειριστή της ομάδας, ο οποίος με τη σειρά του τη μεταβιβάζει

στα διάσπαρτα μέλη της CSIRT. Οι αρμοδιότητες των μελών της CSIRT είναι κυρίως διαχειριστικές των συστημάτων στα τμήματα στα οποία ανήκουν. Άρα τα συγκεκριμένα μέλη συνεχίζουν να εξυπηρετούν τον πρωταρχικό ρόλο τους στον οργανισμό. Όμως ως μέλη της CSIRT αναλαμβάνουν να προωθήσουν στα τμήματά τους βέλτιστες πρακτικές ασφάλειας και στρατηγικές αντιμετώπισης περιστατικών ασφάλειας σύμφωνα με τις καθοδηγήσεις του διαχειριστή τους. Όσον αφορά την αντιμετώπιση των περιστατικών ασφάλειας αναλαμβάνουν να εκτελέσουν τις παρακάτω διαδικασίες στο τμήμα στο οποίο ανήκουν:

- Ανάκαμψη των συστημάτων που έχουν προσβληθεί από περιστατικά ασφάλειας.
- Εφαρμογή αντίμετρων για την προστασία και τη βελτίωση της ασφάλειας των συστημάτων.
- Καλλιέργεια επίγνωσης σε θέματα ασφάλειας.

Επιπλέον τα κατανεμημένα μέλη της CSIRT συμμετέχουν στην ανάλυση και στην απόκριση των περιστατικών ασφάλειας για όλο τον προστατευόμενο οργανισμό, όπου ο διαχειριστής από τη μεριά του έχει ευθύνη για να:

- Συνθέτει τις αναφορές για περιστατικά ασφάλειας που παραλαμβάνει από τα διάφορα τμήματα του προστατευόμενου οργανισμού.
- Αναγνωρίζει συνήθειες, μοτίβα, ζημιές και εύροι των περιστατικών ασφάλειας που πραγματοποιούνται σε όλο τον προστατευόμενο οργανισμό.

- Συντονίζει την εργασία των διάσπαρτων μελών της CSIRT παρέχοντας οδηγίες και κατευθύνσεις

- Γνωρίζει την εξειδίκευση κάθε μέλος της CSIRT ώστε να κάνει σωστή διανομή της ανάλυσης των περιστατικών ασφάλειας. Η σημαντικότερη διαδικασία σε αυτό το οργανωτικό μοντέλο είναι η επικοινωνία μεταξύ των κατανεμημένων μελών της CSIRT. Η επικοινωνία αποσκοπεί στη συνεργασία και στο συντονισμό, στην υλοποίηση των αποκρίσεων σε περιστατικά ασφάλειας και στη μεταξύ τους διανομή και διαμοιρασμό σχετικών πληροφοριών. Οι βασικότερες υπηρεσίες που πρέπει να παρέχει μια CSIRT αυτού του είδους είναι η αποστολή προειδοποιήσεων, ανακοινώσεων και

συναγερμών ασφάλειας, η ανάλυση περιστατικών ασφάλειας και η παροχή τεχνικής υποστήριξης για απόκριση σε περιστατικά ασφάλειας. Ακόμα πρέπει να παρέχει μέσω του διαχειριστή συντονισμό της απόκρισης σε περιστατικά και αδυναμίες ασφάλειας. Αυτό το είδος της CSIRT συμβάλει και στην αύξηση της ποιότητας στη διαχείριση της ασφάλειας. Συγκεκριμένα ο διαχειριστής παρέχει τις ανάλογες υπηρεσίες στο αντίστοιχο τμήμα του προστατευόμενου οργανισμού όπως είναι το ελεγκτικό τμήμα, ενώ τα διάσπαρτα μέλη της CSIRT προωθούν την επίγνωση σε θέματα ασφάλειας στα τμήματά τους. Τα πλεονεκτήματα μιας εσωτερικής κατανεμημένης CSIRT πηγάζουν από την κεντρική ευθύνη του διαχειριστή και τη διασπορά των μελών της στον προστατευόμενο οργανισμό.

Αναλυτικά:

- Υπάρχει κεντρική υπευθυνότητα για την παροχή των υπηρεσιών.
- Υπάρχει κεντρικό σύστημα συγκέντρωσης και παρακολούθησης των περιστατικών ασφάλειας που πραγματοποιούνται σε όλο τον οργανισμό.

- Υπάρχει συντονισμός για την αναφορά, την ανάλυση και την απόκριση σε περιστατικά ασφάλειας σε όλο τον οργανισμό.
- Υπάρχει η δυνατότητα αναγνώρισης συνηθειών, μοτίβων και στατιστικών παρέχοντας μια γενικής εικόνα για το επίπεδο της ασφάλειας του οργανισμού.
- Το κατανεμημένο προσωπικό έχει τη δυνατότητα να γνωρίζει τις ιδιαίτερες ανάγκες και τα χαρακτηριστικά των συστημάτων του τμήματός του και επιπλέον να μπορεί να εφαρμόσει άμεσα τα αντίμετρα προστασίας.

Τα μειονεκτήματα πηγάζουν και αυτά με τη σειρά τους το χαρακτηριστικό της διασποράς των μελών της CSIRT, καθώς και από το γεγονός ότι η συμμετοχή στην CSIRT δεν αποτελεί την πρωταρχική δουλεία τους. Αναλυτικά:

- Είναι δύσκολη η αποδοχή της εξουσίας της CSIRT σε κάθε τμήμα του οργανισμού.
- Είναι δύσκολες οι επικοινωνίες μεταξύ των διάσπαρτων μελών της CSIRT.
- Είναι δύσκολη η συντήρηση σωστής λίστας με την εξειδίκευση που έχει κάθε διάσπαρτο μέλος της CSIRT.

- Είναι δύσκολη η επαλήθευση της σωστής υλοποίησης των αντίμετρων προστασίας, τα οποία προτείνει η απόκριση στα περιστατικά ασφάλειας.
- Τα μέλη της CSIRT έχουν ως πρώτη προτεραιότητα τη διαχείριση των συστημάτων του τμήματος τους και όχι την προστασία και τη βελτίωση της ασφάλειάς τους.
- Τα μέλη της CSIRT δεν έχουν τις απαιτούμενες εξειδικευμένες γνώσεις για την ανάλυση και την απόκριση σε περιστατικά ασφάλειας

Εσωτερική συγκεντρωτική CSIRT

Η εσωτερική συγκεντρωτική CSIRT βρίσκεται στο κεντρικό σημείο του προστατευόμενου οργανισμού και έχει πλήρη ευθύνη για αναφορά, ανάλυση και απόκριση σε περιστατικά ασφάλειας. Δηλαδή η CSIRT και κατ' επέκταση τα μέλη της βρίσκονται σε μία μοναδική φυσική τοποθεσία. Συνηθισμένοι οργανισμοί που έχουν αυτό το είδος της CSIRT είναι μικροί οργανισμοί όπου ο εξοπλισμός και τα μέλη του οριοθετούνται σε ένα κεντρικό χώρο, ή μεγάλοι οργανισμοί όπου η CSIRT βρίσκεται στο κεντρικό σημείο τους μαζί με το τμήμα της διοίκηση τους. Οι αρμοδιότητες αυτής της CSIRT είναι η συλλογή και η σύνθεση πληροφοριών που αφορούν περιστατικά ασφάλειας από όλα τα τμήματα του προστατευόμενου οργανισμού. Η αναφορά αυτών των περιστατικών γίνεται από όλα τα μέλη του οργανισμού και όχι μόνο από εξειδικευμένα μέλη του σε θέματα ασφάλειας. Συνάμα η CSIRT έχει ευθύνη για τη συγκέντρωση των πληροφοριών και των αναφορών, η οποία γίνεται κατευθείαν σε ένα κεντρικό σημείο, χωρίς να επεμβαίνουν ενδιάμεσα διάσπαρτα μέλη της CSIRT. Η CSIRT είναι υπεύθυνη ακόμα και για τη διακήρυξη της επίγνωσης και της εκπαίδευσης σε θέματα ασφάλειας μέσω τεχνικών και συμβουλευτικών τεκμηριώσεων που διανέμει σε όλο τον προστατευόμενο οργανισμό. Η CSIRT του συγκεκριμένου είδους συνεργάζεται με τα υπεύθυνα μέλη των τμημάτων, τα οποία είναι εξωτερικά προς την ομάδα, για την εκτέλεση των παραπάνω ενεργειών στα συστήματά τους. Οι βασικές υπηρεσίες που πρέπει να παρέχει το συγκεκριμένο είδος CSIRT είναι η διανομή προειδοποιήσεων, ανακοινώσεων και συναγερμών ασφάλειας, όπως και η ανάλυση περιστατικών ασφάλειας. Ακόμα παρέχει συμβουλευτική υποστήριξη για απόκριση σε περιστατικά, αδυναμίες ασφάλειας και συντονισμό αυτής της απόκρισης. Η κρισιμότερη υπηρεσία που παρέχει η εσωτερική συγκεντρωτική CSIRT είναι η διανομή πληροφοριών για

θέματα ασφάλειας που απασχολούν τον προστατευόμενο οργανισμό. Αυτή η διανομή γίνεται είτε με την αποστολή των πληροφοριών στα υπεύθυνα άτομα των συστημάτων κάθε τμήματος, είτε με την ανάρτηση των πληροφοριών σε ειδικό ιστοχώρο της CSIRT προκειμένου να είναι διαθέσιμες σε όλα τα μέλη του οργανισμού. Οι υπηρεσίες της CSIRT αυτού του είδους παρέχονται από τα εξειδικευμένα μέλη της τα οποία έχουν ως μοναδική αρμοδιότητα την παροχή αυτών των υπηρεσιών, σε αντίθεση με τα μέλη της εσωτερικής κατανεμημένης CSIRT. Επιπρόσθετα, μέσω της συγκεντρωτικής φύσης αυτής της CSIRT, υπάρχει η δυνατότητα παραγωγής στατιστικών και συνηθειών για τα περιστατικά ασφάλειας που διεξάγονται στον προστατευόμενο οργανισμό. Τα αποτελέσματα αυτής της δυνατότητας προωθούνται στα τμήματα ελεγκτικής ασφάλειας και ανάλυσης επικινδυνότητας του οργανισμού, με αποτέλεσμα να βελτιώνεται η διαχείριση της ασφάλειας του. Τα πλεονεκτήματα μιας εσωτερικής συγκεντρωτικής CSIRT είναι τα εξής:

- Η CSIRT ασχολείται μόνο με τις υπηρεσίες της.
- Η CSIRT έχει εξειδικευμένο και κατάλληλα εκπαιδευμένο προσωπικό.
- Γίνεται απευθείας καταγραφή πληροφοριών σε ένα κεντρικό σύστημα συγκέντρωσης και παρακολούθησης περιστατικών ασφάλειας. Έτσι υπάρχει η δυνατότητα γρήγορης ανίχνευσης περιστατικών ασφάλειας και η δυνατότητα δημιουργίας συνηθειών, μοτίβων, και στατιστικών παρέχοντας μια γενική εικόνα για το επίπεδο της ασφάλειας του οργανισμού.
- Εφόσον τα μέλη της ομάδας βρίσκονται στον ίδιο φυσικό χώρο επιτυγχάνεται άμεση και αποτελεσματικότερη μεταξύ τους επικοινωνία.

Αντίστοιχα τα μειονεκτήματα αυτού του είδους της CSIRT είναι τα εξής:

- Αν δεν υπάρχει σωστή διοίκηση η CSIRT θα είναι απομονωμένη από τον υπόλοιπο προστατευόμενο οργανισμό.
- Είναι δύσκολος ο συντονισμός και η συνεργασία με τα απομακρυσμένα μέλη του οργανισμού.

- Απαιτεί επιπλέον εξοπλισμό και προσωπικό, άρα έχει επιπλέον κόστος.
- Υπάρχουν καθυστερήσεις μέχρι να φτάσουν οι πληροφορίες στην CSIRT από τα μέλη του οργανισμού.

- Τα μέλη της CSIRT δεν έχουν γνώση και εμπειρία για την επιχειρησιακή λειτουργία της πληροφοριακής υποδομής του οργανισμού.

Μικτό μοντέλο κατανεμημένης και συγκεντρωτικής ομάδας. Στη συγκεκριμένη περίπτωση υπάρχει μία κεντρική CSIRT σε μια κεντρική φυσική τοποθεσία του προστατευόμενου οργανισμού η οποία συντονίζεται και συνεργάζεται με υποομάδες CSIRTs, οι οποίες είναι κατανεμημένες σε όλα τα τμήματα αυτού του οργανισμού. Για να είναι αποτελεσματική μια CSIRT αυτού του είδους, πρέπει να υπάρχουν ασφαλή κανάλια επικοινωνίας μεταξύ της κεντρικής ομάδας και των υποομάδων της. Επίσης πρέπει να υπάρχει μία κεντρική βάση για περιστατικά ασφάλειας στην οποία θα έχουν πρόσβαση όλες οι κατανεμημένες υποομάδες. Οργανισμοί που έχουν αυτό το είδος της CSIRT είναι μεγάλοι κατανεμημένοι οργανισμοί οι οποίοι μπορούν να αντεπεξέλθουν στο υψηλό κόστος που έχει αυτό το οργανωτικό μοντέλο. Η κεντρική ομάδα του συνδυασμού αναλαμβάνει το συντονισμό και την παροχή πλαισίου συνεργασίας μεταξύ όλων των κατανεμημένων υποομάδων. Η βασική της αρμοδιότητα είναι η παροχή ενός υψηλού επιπέδου ανάλυση περιστατικών ασφάλειας μέσω της προηγούμενης επικοινωνίας. Συγκεκριμένα συλλέγει σε κεντρικό σημείο τις αναφορές και τις πληροφορίες από όλο τον προστατευόμενο οργανισμό. Αντίστοιχα μεταβιβάζει ενέργειες ανάλυσης στην ανά περίπτωση κατάλληλη κατανεμημένη ομάδα, με βάση την εξειδίκευση που έχει και την τοποθεσία της. Σε επόμενο στάδιο προτείνει και διανέμει στις κατανεμημένες υποομάδες στρατηγικές απόκρισης και ανάκαμψης από τα περιστατικά ασφάλειας. Οι κατανεμημένες υποομάδες είναι υπεύθυνες για την υλοποίηση των οδηγιών και των κατευθύνσεων που τους παρέχει η κεντρική, στα τμήματά τους. Επίσης συλλέγουν τις αναφορές σε περιστατικά ασφάλειας από τα τμήματά τους και στη συνέχεια τα μεταβιβάζουν στην κεντρική ομάδα. Ο βαθμός εξουσιοδότησης του συγκεκριμένου οργανωτικού μοντέλου είναι πλήρης, προκειμένου για την ανάλυση των περιστατικών ασφάλειας. Για την απόκριση, την ανάκαμψη και την απομάκρυνση των περιστατικών ασφάλειας στα συστήματα του προστατευόμενου οργανισμού ο βαθμός εξουσιοδότησης είναι μοιρασμένος. Δηλαδή η κεντρική ομάδα συμμετέχει στη λήψη αποφάσεων με διοίκηση του οργανισμού για την εκτέλεση των παραπάνω διαδικασιών και σε επόμενο στάδιο η εξουσιοδότηση της εκτέλεσης μεταβιβάζεται στις διάσπαρτες υποομάδες. Οι βασικές υπηρεσίες που πρέπει να παρέχει το συγκεκριμένο είδος CSIRT είναι η διανομή προειδοποιήσεων, ανακοινώσεων και συναγερμών

ασφάλειας, όπως και η ανάλυση περιστατικών ασφάλειας. Ταυτόχρονα, η CSIRT παρέχει τόσο τεχνική όσο και συμβουλευτική υποστήρίξη για απόκριση σε περιστατικά ασφάλειας. Η κεντρική ομάδα επιπρόσθετα παρέχει συντονισμό της απόκρισης σε περιστατικά και αδυναμίες ασφάλειας καθώς και διανομή πληροφοριών για θέματα ασφάλειας που απασχολούν τον προστατευόμενο οργανισμό. Τα πλεονεκτήματα και τα μειονεκτήματα μιας συνδυαστικής κατανεμημένης και συγκεντρωτικής αποτελούν το συνδυασμό των αντίστοιχων ειδών των CSIRT. Όμως ένα επιπρόσθετο μειονέκτημα που έχει αυτό το είδος είναι το αυξημένο κόστος σε εξοπλισμό και εξειδικευμένο προσωπικό, ενώ τα επιπρόσθετα πλεονεκτήματα του σε σχέση με τα άλλα είδη είναι τα εξής:

- Αποτελείται από ένα κεντρικό και ειδικευμένο προσωπικό για την ανάλυση και την απόκριση σε περιστατικά, καθώς και από ένα κατανεμημένο προσωπικό με εμπειρία στα συστήματα των τμημάτων τους και στην επιχειρησιακή τους λειτουργία.
- Η κεντρική ομάδα έχει ολοκληρωμένη και πλήρη εικόνα για την ασφάλεια του προστατευόμενου οργανισμού. Άρα έχει τις απαιτούμενες γνώσεις και εμπειρίες για να υλοποιήσει προληπτική ασφάλεια, όπως είναι η καλλιέργεια επίγνωσης και η εκπαίδευση σε θέματα ασφάλειας.

Συμπεράσματα

Η ομάδα εργασίας ΙΑ4 κατέγραψε τους λόγους για τους οποίους είναι απαραίτητη η δημιουργία των κατάλληλων δομών για την προστασία των κρίσιμων τεχνολογικών υποδομών της Χώρας. Παρόμοιες ομάδες βρίσκονται σε λειτουργία σε όλα τα ανεπτυγμένα κράτη για αρκετά χρόνια, καθώς έχει γίνει ευρύτερα αντιληπτή η σημασία που έχει η διαρκής και αδιάλειπτη λειτουργία των πληροφοριακών συστημάτων του δημόσιου και ιδιωτικού τομέα. Με βάση τις παραπάνω διαπιστώσεις και σε συνδυασμό με το γεγονός ότι στην Ελλάδα παρατηρείται το τελευταίο διάστημα αξιόλογη διείσδυση των Τεχνολογιών Πληροφορικής και Επικοινωνιών, τόσο σε επίπεδο χρηστών, όσο και η ανάλογη υιοθέτηση τους από τη Δημόσια Διοίκηση, προκύπτει η αναγκαιότητα για την ανάπτυξη κατάλληλων μηχανισμών ασφάλειας.

Η ομάδα εργασίας ΙΑ4 αφού μελέτησε σε βάθος ανάλογες προσπάθειες που έχουν υλοποιηθεί στο εξωτερικό και εξέτασε τα επιμέρους χαρακτηριστικά τους, ανάλογα με το κοινό στο οποίο απευθύνονται, την χρηματοδότηση την οποία λαμβάνουν και άλλα επιμέρους στοιχεία, είναι σε θέση να παράσχει όλες τις απαιτούμενες πληροφορίες στην Πολιτεία, όταν αποφασίσει να δημιουργήσει κάποιον ανάλογο φορέα.

Στην ομάδα εργασίας ΙΑ4 εγγράφηκαν και συνέβαλαν με τις γνώσεις και την εμπειρία τους περίπου 100 επαγγελματίες και ειδικοί από διάφορους σχετικούς χώρους, όπως:

- Δημόσιοι φορείς και οργανισμοί
- Τράπεζες
- Εταιρίες παροχής υπηρεσιών Διαδικτύου
- Εταιρίες ασφάλειας πληροφοριακών συστημάτων
- Επιμελητήρια και επαγγελματικές ενώσεις
- Νομικά γραφεία

Στα πλαίσια των διαβουλεύσεων και των λοιπών συζητήσεων που διεξήχθησαν, εκτιμήθηκαν οι βασικές απαιτήσεις για την δημιουργία ενός ανάλογου κέντρου ή ομάδας στην Ελλάδα. Το σύνολο των συμμετεχόντων συμφώνησε ότι η δημιουργία μιας ομάδας στα πρότυπα και το μέγεθος των γνωστότερων CERTs του εξωτερικού εμπεριέχει πάρα πολλές απαιτήσεις, τόσο στην στελέχωσή της από το κατάλληλο προσωπικό, όσο και στην εκταμίευση πολλών πόρων για την χρηματοδότηση και λειτουργία της. Συνεπώς, είναι δύσκολη η δημιουργία ενός ανάλογου κέντρου, χωρίς την ύπαρξη των κατάλληλων υποδομών και της πρότερης εμπειρίας. Υπό αυτή την έννοια θα ήταν σαφώς ρεαλιστικότερη η σύσταση μιας ομάδας CSIRT, όπου θα μπορούσε να υλοποιηθεί με λιγότερες απαιτήσεις. Σε θέματα ανθρώπινου δυναμικού προκύπτει ότι υπάρχουν διαθέσιμοι επιστήμονες σε θέματα ασφάλειας, οι οποίοι θα μπορούσαν να δραστηριοποιηθούν ενεργά στη σύσταση και λειτουργία μιας ομάδας CSIRT. Επιπλέον ένα μεγάλο ποσοστό μελών της ομάδας ΙΑ4 κατέχει θέσεις με διοικητικές αρμοδιότητες σε οργανισμούς και επιχειρήσεις με στρατηγική σημασία, όσον αφορά το κοινό στο οποίο απευθύνεται η προτεινόμενη ομάδα CSIRT. Επίσης άλλα μέλη της ομάδας διαθέτουν ειδικές γνώσεις σε περιοχές εκτός των

Πληροφοριακών Συστημάτων που όμως είναι βασικής σημασίας για τη λειτουργία μιας ανάλογης ομάδας. Τέτοια θέματα αφορούν κυρίως νομικά ζητήματα, τα οποία όμως προκύπτουν διαρκώς, λόγω της πολύπλοκης νομικής φύσης που διέπει το Διαδίκτυο. Συμπερασματικά, από τις συνολικές δράσεις της ομάδας εργασίας IA4 είναι εμφανές ότι υπάρχει ήδη στην Ελλάδα μια κοινότητα χρηστών και ειδικών, ή οποία είναι ιδιαίτερα δραστήρια σε θέματα ασφάλειας που θα μπορούσε να συνδράμει καθοριστικά στην λειτουργία ενός CSIRT.

Συνεπώς, εφόσον το πρόβλημα εύρεσης του κατάλληλου ανθρωπίνου δυναμικού που θα στελεχώσει μια ομάδα CSIRT μπορεί άμεσα να αντιμετωπιστεί, όπως φαίνεται από το ενδιαφέρον που εκδηλώθηκε στην συμμετοχή της ομάδας, τα οποία ζητήματα μπορεί να ανακύψουν αφορούν κυρίως θέματα χρηματοδότησης και επόπτευσης της ομάδας ή του φορέα που θα ιδρυθεί. Τα παραπάνω θέματα αν και σημαντικά, αποτελούν πολιτικές αποφάσεις που σχετίζονται με την αξία που αποδίδει το κάθε κράτος στην προστασία των τεχνολογικών υποδομών του.

Βιβλιογραφία

[1]: RFC 2828 - Internet Security Glossary

[2]: RFC 2350: Expectations for Computer Security Incident Response

[3]: Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ. Ασφάλεια δικτύων υπολογιστών, Αθήνα 2003 εκδόσεις Παπασωτηρίου

[4]: Software Engineering Institute. Available at http://www.sei.cmu.edu

[5]: Computer Emergency Response Team Coordination Center "CERT/CC". Available at http://www.cert.org

[6]: Carnegie Mellon University. Available at http://www.cmu.edu

[7]: FIRST. Available at www.first.org

[8]: Trans-European Research and Education Network Association. Available at http:///www.terena.nl

[9]: Trans-European Research and Education Network Association TF-CSIRT. Available at http:///www.terena.nl/tech/task-forces/tf-csirt/default.htm

[10]: TERENA Trusted Introducer. Available at www.titerena.nl

[11]: European CSIRT Network. Available at www.ecsirt.net

[12]: State of the Practice of CSIRTs. Available at http://www.cert.org/archive/pdf/03tr001.pdf

[13]: Handbook for Computer Security Incident Response. Available at http://www.cert.org/archive/pdf/csirt-handbook.pdf

[14] «Δημιουργία πλαισίου εργασίας στην επικοινωνία των CSIRTs», Βιδάκη Γρηγόρη, Μεταπτυχιακή Διατριβή, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου, 2006

[15] Checkland P., (1981). ''Systems thinking, systems practice''. John Wiley and Sons, Chichester, UK.

[16] Κιουντούζης Ε. (1997). ''Μεθοδολογίες Ανάλυσης και σχεδιασμού Πληροφοριακών Συστημάτων'', εκδ. Ε. Μπένου, Αθήνα.

[17] Μπέλσης Π. «Διαχείριση Γνώσης Ασφάλειας Πληροφοριακών Συστημάτων», Μεταπτυχιακή διατριβή, Τμ. Πληροφορικής, Οικονομικό Παν. Αθήνας, 2002

[18] King W., Marks P., McCoy S., (2002). "The most important issues in Knowledge Management", Communications of the ACM, Sept. 2002, vol.45, No. 9

[19] Polanyi (1966). “The Tacit Dimension”, Routledge & Kegan Paul, London
[20] Nonaka I. (1994). “A Dynamic Theory of Organizational Knowledge Creation”, Organization Science, vol. 5, No. 1, pp. 14-37.