ΜΙΑ ΠΡΟΣΕΓΓΙΣΗ ΓΙΑ ΤΟΝ ΤΡΟΠΟ ΔΗΜΙΟΥΡΓΙΑΣ ΜΙΑΣ ΟΜΑΔΑΣ CSIRT

Παραδοτέο WP2006/5.1(CERT-D1/D2)

Ευρετήριο

1 Διαχειριστική Σύνοψη

Το ανά χείρας έγγραφο περιγράφει τη διαδικασία δημιουργίας Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές (CSIRT) από κάθε συναφή άποψη, όπως η επιχειρηματική διαχείριση, η διαδικαστική διαχείριση και η τεχνική προσέγγιση. Το παρόν έγγραφο περιέχει δύο από τα παραδοτέα που περιγράφονται στο Πρόγραμμα Εργασιών του ENISA για το 2006 (κεφάλαιο 5.1), ήτοι:

- το παρόν έγγραφο: *Έγγραφη αναφορά επί της προσέγγισης βήμα προς βήμα για τον τρόπο δημιουργίας ομάδας CERT ή παρόμοιων εγκαταστάσεων, συμπεριλαμβανομένων παραδειγμάτων* **(CERT-D1),**
- κεφάλαιο 12 και εξωτερικά αρχεία: *Απόσπασμα οδικού χάρτη σε λεπτομερή μορφή που επιτρέπει την εύκολη εφαρμογή του οδικού χάρτη στην πράξη* **(CERT-D2).**

2 Ανακοίνωση Νομικού Περιεχομένου

Θα πρέπει να σημειωθεί ότι η παρούσα έκδοση εκφράζει τις απόψεις και ερμηνείες των συντακτών και εκδοτών, εκτός εάν δηλώνεται διαφορετικά. Η παρούσα έκδοση δεν θα πρέπει να εκλαμβάνεται ως δράση του ENISA ή των φορέων του ENISA, εκτός εάν υιοθετείται σύμφωνα με τον κοινοτικό κανονισμό περί ENISA αριθ. 460/2004. Η παρούσα έκδοση δεν αντιπροσωπεύει απαραιτήτως τις τελευταίες εξελίξεις και ενδέχεται κατά καιρούς να ενημερώνεται.

Οι πηγές τρίτων αναφέρονται με τον προσήκοντα τρόπο. Ο ENISA δεν φέρει ευθύνη για το περιεχόμενο εξωτερικών πηγών, συμπεριλαμβανομένων των εξωτερικών ιστοτόπων που αναφέρονται στην παρούσα έκδοση.

Η παρούσα έκδοση διατίθεται αποκλειστικά για εκπαιδευτικούς και ενημερωτικούς σκοπούς. Ούτε ο ENISA ούτε άλλο πρόσωπο που ενεργεί εκ μέρους του φέρουν ευθύνη για την ενδεχόμενη χρήση των πληροφοριών που περιλαμβάνονται στην παρούσα έκδοση.

3 Ευχαριστίες

Ο ENISA επιθυμεί να ευχαριστήσει όλους τους φορείς και άτομα που συνέβαλαν στο παρόν έγγραφο. Θα ήθελε να απευθύνει ιδιαίτερες ευχαριστίες στους παρακάτω συντελεστές:

- τον Henk Bronk, ο οποίος με την ιδιότητα του συμβούλου συνέταξε την πρώτη έκδοση του παρόντος εγγράφου,
- το Κέντρο Συντονισμού CERT και ιδιαίτερα την ομάδα ανάπτυξης CSIRT που συνεισέφεραν το πιο χρήσιμο υλικό και το δείγμα υλικού του μαθήματος που περιλαμβάνεται στο παράρτημα,
- τον GovCERT.NL για την παροχή του *CERT-in-a-box,*
- την ομάδα TRANSITS που συνεισέφερε το δείγμα υλικού του μαθήματος που περιλαμβάνεται στο παράρτημα,
- τους συναδέλφους από την υπηρεσία Πολιτικών Ασφαλείας του Τεχνικού Τμήματος που συνεισέφεραν το κεφάλαιο 6.6,
- τους αμέτρητους ανθρώπους που προέβησαν σε επισκόπηση του παρόντος εγγράφου.

4 Εισαγωγή

Τα επικοινωνιακά δίκτυα και τα πληροφοριακά συστήματα έχουν καταστεί ουσιαστικός παράγοντας στην οικονομική και κοινωνική ανάπτυξη. Η πληροφορική και η δικτύωση αποτελούν πλέον ευρέως διαδεδομένα αγαθά όπως η ηλεκτροδότηση ή η ύδρευση.

Η ασφάλεια των επικοινωνιακών δικτύων και των πληροφοριακών συστημάτων και ιδιαίτερα η διαθεσιμότητά τους απασχολούν επομένως ολοένα και περισσότερο την κοινωνία. Αυτό απορρέει από τον κίνδυνο προβλημάτων σε βασικά πληροφοριακά συστήματα, εξαιτίας της πολυπλοκότητας των συστημάτων, ατυχημάτων, σφαλμάτων και επιθέσεων στις υλικές υποδομές που παρέχουν κρίσιμες υπηρεσίες για την ευημερία των πολιτών της Ε.Ε.

Στις 10 Μαρτίου 2004 δημιουργήθηκε ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[1]. Σκοπός του ήταν να διασφαλισθεί ένα υψηλό και αποτελεσματικό επίπεδο ασφάλειας δικτύων και πληροφοριών εντός της Κοινότητας και να δημιουργηθεί μια φιλοσοφία για την ασφάλεια δικτύων και πληροφοριών προς όφελος των πολιτών, των καταναλωτών, των εταιρειών και των οργανισμών του δημοσίου τομέα εντός της Ευρωπαϊκής Ένωσης, συμβάλλοντας κατ' αυτόν τον τρόπο στην ομαλή λειτουργία της εσωτερικής αγοράς.

Εδώ και αρκετά χρόνια διάφορες κοινότητες ασφάλειας στην Ευρώπη, όπως οι CERT/CSIRT, οι Ομάδες Διαχείρισης Περιστατικών Κατάχρησης (Abuse Teams) και τα Σημεία Συναγερμού και Προειδοποίησης (WARP), συνεργάζονται για ένα ασφαλέστερο Διαδίκτυο. Ο ENISA προτίθεται να υποστηρίξει τις εν λόγω κοινότητες στις επιδιώξεις τους, παρέχοντας πληροφορίες σχετικά με τα μέτρα διασφάλισης του κατάλληλου επιπέδου ποιότητας υπηρεσιών. Επιπλέον, ο ENISA σκοπεύει να ενισχύσει την ικανότητά του να παρέχει συμβουλές στα κράτη μέλη της ΕΕ και τα όργανα της ΕΕ για ζητήματα σχετικά με την κάλυψη συγκεκριμένων ομάδων χρηστών IT από τις κατάλληλες υπηρεσίες ασφαλείας. Επομένως, με βάση τα πορίσματα της ad hoc Ομάδας Εργασίας για το Συντονισμό και Υποστήριξη των CERT που δημιουργήθηκε το 2005, αυτή η νέα Ομάδα Εργασίας θα ασχοληθεί με ζητήματα τα οποία σχετίζονται με την παροχή επαρκών υπηρεσιών ασφαλείας ("Υπηρεσίες CERT") σε συγκεκριμένες (κατηγορίες ή ομάδες) χρηστών.

Ο ENISA υποστηρίζει τη δημιουργία νέων ομάδων CSIRT μέσω της δημοσίευσης της παρούσας αναφοράς ENISA με τίτλο "*Μια προσέγγιση βήμα προς βήμα για τον τρόπο δημιουργίας μιας ομάδας CSIRT με συμπληρωματικό κατάλογο ελέγχου",* που θα σας βοηθήσει να δημιουργήσετε τη δική σας ομάδα CSIRT.

[1] Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10ης Μαρτίου 2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών. "Κοινοτική υπηρεσία" είναι ένα όργανο που έχει συσταθεί από την ΕΕ για να εκτελέσει ένα πολύ ειδικό τεχνικό, επιστημονικό ή διοικητικό έργο, στα πλαίσια του "πρώτου πυλώνα" της ΕΕ.

4.1 Κοινό-στόχος

Οι κύριες ομάδες αποδεκτών της παρούσας αναφοράς είναι κυβερνητικοί και άλλοι οργανισμοί που αποφασίζουν να δημιουργήσουν μια ομάδα CSIRT, προκειμένου να προστατεύσουν την υποδομή IT που διαθέτουν οι ίδιοι ή οι εμπλεκόμενοι φορείς τους.

4.2 Τρόπος χρήσης του παρόντος εγγράφου

Το παρόν έγγραφο παρέχει πληροφορίες για τον ορισμό μιας ομάδας CSIRT, τις υπηρεσίες που μπορεί να παράσχει και τα βήματα που είναι απαραίτητα ως αφετηρία. Κατ' αυτόν τον τρόπο παρέχεται στον αναγνώστη μια καλή και πραγματική επισκόπηση της προσέγγισης, της δομής και του περιεχομένου σχετικά με τον τρόπο δημιουργίας μιας ομάδας CSIRT.

Κεφάλαιο 4 *"Εισαγωγή"*
Εισαγωγή της παρούσας αναφοράς.

Κεφάλαιο 5 *"Συνολική στρατηγική σχεδιασμού και δημιουργίας μιας ομάδας CSIRT"*
Η πρώτη ενότητα περιγράφει σε τι συνίσταται μια ομάδα CSIRT. Επίσης, παρέχει πληροφορίες για τα διάφορα περιβάλλοντα στα οποία μπορούν να λειτουργήσουν οι ομάδες CSIRT και τι είδους υπηρεσίες μπορούν να παράσχουν.

Κεφάλαιο 6 *"Αναπτύσσοντας το Επιχειρηματικό Σχέδιο"*
Το εν λόγω κεφάλαιο περιγράφει την προσέγγιση της επιχειρηματικής διαχείρισης στη διαδικασία της δημιουργίας.

Κεφάλαιο 7 *"Προωθώντας το Επιχειρηματικό Σχέδιο"*
Το εν λόγω κεφάλαιο ασχολείται με ζητήματα επιχειρηματικής πρακτικής και χρηματοδότησης.

Κεφάλαιο 8 *"Παραδείγματα λειτουργικών και τεχνικών διαδικασιών"*
Το εν λόγω κεφάλαιο περιγράφει τη διαδικασία απόκτησης πληροφοριών και μετατροπής τους σε ένα ενημερωτικό δελτίο ασφαλείας. Επίσης, το κεφάλαιο παρέχει περιγραφή μιας ροής εργασιών διαχείρισης περιστατικών.

Κεφάλαιο 9 *"Εκπαίδευση CSIRT"*
Το εν λόγω κεφάλαιο παρέχει μια σύνοψη της διαθέσιμης εκπαίδευσης CSIRT. Ως επεξήγηση, παρέχεται δείγμα υλικού μαθημάτων στο παράρτημα.

Κεφάλαιο 10 *"Άσκηση: δημιουργία συμβουλευτικού"*
Το εν λόγω κεφάλαιο περιέχει μια άσκηση για τον τρόπο επιτέλεσης μιας από τις βασικές (ή κύριες) υπηρεσίες CSIRT: την παραγωγή ενός ενημερωτικού δελτίου ασφαλείας (ή συμβουλευτικού).

Κεφάλαιο 12 *"Περιγραφή Σχεδίου Έργου"*
Το εν λόγω κεφάλαιο παραπέμπει στο συμπληρωματικό σχέδιο έργου (κατάλογος ελέγχου) που παρέχεται με αυτόν τον οδηγό. Το εν λόγω σχέδιο έχει ως στόχο να αποτελέσει ένα εύχρηστο εργαλείο για την υλοποίηση του παρόντος οδηγού.

4.3 Συμβάσεις που χρησιμοποιούνται στο παρόν έγγραφο

Ως καθοδήγηση για τον αναγνώστη, κάθε κεφάλαιο ξεκινά με μια σύνοψη των βημάτων που έχουν πραγματοποιηθεί έως εκείνη τη στιγμή στη διαδικασία δημιουργίας μιας ομάδας CSIRT. Αυτού του είδους η σύνοψη περικλείεται σε πλαίσια όπως το παρακάτω:

Πραγματοποιήσαμε το πρώτο βήμα

Κάθε κεφάλαιο θα ολοκληρώνεται με ένα πρακτικό παράδειγμα των βημάτων που αναλύθηκαν. Στο παρόν έγγραφο η “Εικονική ομάδα CSIRT” θα είναι μια μικρή ανεξάρτητη ομάδα CSIRT για μια εταιρεία ή έναν οργανισμό μεσαίου μεγέθους. Μια σύνοψη παρέχεται στο παράρτημα.

Εικονική ομάδα CSIRT

5 Συνολική στρατηγική σχεδιασμού και δημιουργίας μιας ομάδας CSIRT

Για μια επιτυχημένη έναρξη της διαδικασίας δημιουργίας μιας ομάδας CSIRT είναι σημαντικό να έχει κανείς στη διάθεσή του σαφή εικόνα των πιθανών υπηρεσιών που μπορεί να παρέχει η ομάδα στους πελάτες της που είναι γνωστοί ως "κοινότητα αποδεκτών" στον κόσμο της CSIRT. Επομένως, είναι απαραίτητο να κατανοήσει κανείς ποιες είναι οι ανάγκες της κοινότητας αποδεκτών, προκειμένου να παρέχονται οι κατάλληλες υπηρεσίες την κατάλληλη χρονική στιγμή και στην κατάλληλη ποιότητα.

5.1 Τι είναι μια ομάδα CSIRT;

CSIRT σημαίνει Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές. Ο όρος CSIRT χρησιμοποιείται πρωτίστως στην Ευρώπη για τον όρο CERT, που είναι κατοχυρωμένος στις ΗΠΑ από το Κέντρο Συντονισμού CERT (CERT/CC).
Υπάρχουν διάφορες συντομογραφίες που χρησιμοποιούνται για το ίδιο είδος ομάδων:

- CERT ή CERT/CC (Ομάδας Αντιμετώπισης Έκτακτων Περιστατικών σε Υπολογιστές / Κέντρο Συντονισμού),
- CSIRT (Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές),
- IRT (Ομάδα Αντιμετώπισης Περιστατικών),
- CIRT (Ομάδα Αντιμετώπισης Περιστατικών σε Υπολογιστές),
- SERT (Ομάδα Αντιμετώπισης Έκτακτων Περιστατικών Ασφαλείας).

Το πρώτο μεγάλο ξέσπασμα ιού στην παγκόσμια υποδομή IT πραγματοποιήθηκε στα τέλη της δεκαετίας του 1980. Ο ιός ονομάστηκε Morris[2] και μεταδόθηκε γρήγορα, προσβάλλοντας σοβαρά έναν μεγάλο αριθμό πληροφοριακών συστημάτων ανά τον κόσμο.

Το εν λόγω περιστατικό λειτούργησε ως αφύπνιση: ξαφνικά οι άνθρωποι συνειδητοποίησαν την έντονη ανάγκη συνεργασίας και συντονισμού μεταξύ των διαχειριστών συστημάτων και IT των διευθυντικών στελεχών, προκειμένου να αντιμετωπισθούν περιπτώσεις όπως αυτή. Εξαιτίας του γεγονότος ότι ο χρόνος ήταν κρίσιμος παράγοντας, έπρεπε να υιοθετηθεί μια πιο οργανωμένη και δομημένη προσέγγιση για την αντιμετώπιση περιστατικών ασφαλείας πληροφοριακών συστημάτων. Επομένως, μερικές ημέρες μετά το "Περιστατικό Morris" η Υπηρεσία Έρευνας Προηγμένων Αμυντικών Προγραμμάτων (DARPA) δημιούργησε την πρώτη CSIRT: το Κέντρο Συντονισμού CERT (CERT/CC[3]) στο Πανεπιστήμιο Carnegie Mellon University του Pittsburgh (Pennsylvania).

Σύντομα το εν λόγω μοντέλο υιοθετήθηκε στην Ευρώπη και το 1992 ο ολλανδικός ακαδημαϊκός παροχέας υπηρεσιών SURFnet δημιούργησε την πρώτη CSIRT στην Ευρώπη με την επωνυμία SURFnet-CERT[4]. Αρκετές ομάδες ακολούθησαν και επί του

[2] Περισσότερες πληροφορίες για τον ιό Morris μπορείτε να βρείτε στη διεύθυνση http://en.wikipedia.org/wiki/Morris_worm

[3] CERT-CC, http://www.cert.org

[4] SURFnet-CERT: http://cert.surfnet.nl/

παρόντος ο *Κατάλογος του ENISA για τις δραστηριότητες των CERT στην Ευρώπη*[5] περιλαμβάνει περισσότερες από 100 γνωστές ομάδες με έδρα την Ευρώπη.

Με την πάροδο των ετών, οι ομάδες CERT επέκτειναν τις δυνατότητές τους και από μια απλή ομάδα αντίδρασης μετατράπηκαν σε ολοκληρωμένους φορείς παροχής υπηρεσιών ασφαλείας, παρέχοντας και προληπτικές υπηρεσίες όπως συναγερμούς, συμβουλευτικά ασφαλείας, εκπαίδευση και υπηρεσίες διαχείρισης ασφαλείας. Σύντομα ο όρος "CERT" κρίθηκε ανεπαρκής. Έτσι υιοθετήθηκε ο νέος όρος "CSIRT" στα τέλη της δεκαετίας του 1990. Επί του παρόντος, χρησιμοποιούνται και οι δύο όροι (CERT και CSIRT) ως συνώνυμοι, αλλά ο όρος CSIRT είναι πιο ακριβής.

5.1.1 Ο όρος Κοινότητα Αποδεκτών

Εφεξής ο καθιερωμένος (στις κοινότητες CSIRT) όρος "κοινότητα αποδεκτών" θα χρησιμοποιείται όταν γίνεται αναφορά στην πελατειακή βάση μιας CSIRT. Ένας μεμονωμένος πελάτης θα αναφέρεται ως "αποδέκτης" και μια ομάδα ως "κοινότητα αποδεκτών".

5.1.2 Ορισμός μιας ομάδας CSIRT

Μια ομάδα CSIRT είναι μια ομάδα ειδικών στην ασφάλεια πληροφοριακών συστημάτων, η κύρια δραστηριότητα των οποίων είναι να αντιμετωπίζουν περιστατικά ασφαλείας σε υπολογιστές. Παρέχει τις απαραίτητες υπηρεσίες για την αντιμετώπισή τους και την υποστήριξη της κοινότητας αποδεκτών τους, ώστε να ξεπερνούν τις παραβιάσεις ασφαλείας.

Προκειμένου να μετριάσουν τους κινδύνους και να ελαχιστοποιήσουν τον αριθμό των απαιτούμενων αποκρίσεων, οι περισσότερες ομάδες CSIRT παρέχουν επίσης προληπτικές και εκπαιδευτικές υπηρεσίες στην κοινότητα αποδεκτών τους. Εκδίδουν συμβουλευτικά για αδυναμίες του λογισμικού και του υλικού που χρησιμοποιείται και ενημερώνουν τους χρήστες για τα κενά ασφαλείας και τους ιούς που εκμεταλλεύονται τις εν λόγω αδυναμίες. Κατ' αυτόν τον τρόπο οι αποδέκτες μπορούν γρήγορα να διορθώσουν προσωρινά και να ενημερώσουν τα συστήματά τους. Βλέπε το κεφάλαιο *5.2 Πιθανές υπηρεσίες* για έναν πλήρη κατάλογο των ενδεχόμενων υπηρεσιών.

5.1.3 Τα οφέλη που παρέχει η ομάδα CSIRT

Η ύπαρξη μιας ειδικευμένης ομάδας ασφάλειας πληροφοριακών συστημάτων βοηθά έναν οργανισμό να μετριάσει και να αποτρέψει κύρια περιστατικά και τον βοηθά να προστατεύσει τους πολύτιμους πόρους του.

Άλλα πιθανά οφέλη είναι τα εξής:

- ύπαρξη ενός κεντρικού συντονισμού για ζητήματα ασφάλειας πληροφοριακών συστημάτων εντός του οργανισμού (Σημείο Επαφής, PoC),
- κεντρική και εξειδικευμένη αντιμετώπιση και απόκριση σε περιστατικά πληροφοριακών συστημάτων,
- ύπαρξη διαθέσιμου ειδικού για την υποστήριξη και την υποβοήθηση των χρηστών, ώστε να ανακάμψουν γρήγορα μετά από περιστατικά ασφαλείας,

[5] Κατάλογος ENISA http://www.enisa.europa.eu/cert_inventory/

- αντιμετώπιση νομικών ζητημάτων και διατήρηση αποδεικτικών στοιχείων σε περίπτωση μήνυσης,
- παρακολούθηση εξελίξεων στον τομέα της ασφάλειας,
- τόνωση της συνεργασίας εντός της κοινότητας αποδεκτών σε θέματα ασφάλειας πληροφοριακών συστημάτων (ενίσχυση ευαισθητοποίησης).

Εικονική ομάδα CSIRT (βήμα 0)
Κατανοώντας τι είναι μια ομάδα CSIRT: Η δοκιμαστική ομάδα CSIRT θα πρέπει να εξυπηρετεί έναν οργανισμό μεσαίου μεγέθους που αποτελείται από προσωπικό 200 μελών. Ο οργανισμός διαθέτει το δικό του τμήμα πληροφοριακών συστημάτων και δύο άλλα υποκαταστήματα στην ίδια χώρα. Τα πληροφοριακά συστήματα παίζουν βασικό ρόλο για την εταιρεία, επειδή χρησιμοποιούνται για την εσωτερική επικοινωνία, το δίκτυο δεδομένων και τη διεξαγωγή ηλεκτρονικών επιχειρηματικών συναλλαγών 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα. Ο οργανισμός διαθέτει το δικό του δίκτυο και μια ταχύτατη σύνδεση στο Διαδίκτυο μέσω δύο διαφορετικών Παροχών Υπηρεσιών Διαδικτύου (ISP).

5.1.4 Περιγραφή των διαφορετικών περιβαλλόντων της ομάδας CSIRT

Πραγματοποιήσαμε το πρώτο βήμα

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί αυτή να προσφέρει.

>> Το επόμενο βήμα είναι να απαντηθεί το ερώτημα: “Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;”

Κατά τη δημιουργία μιας ομάδας CSIRT (όπως σε οποιονδήποτε άλλο τομέα) είναι πολύ σημαντικό να αναπτυχθεί πολύ γρήγορα μια σαφής εικόνα της κοινότητας αποδεκτών και του είδους του περιβάλλοντος στο οποίο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT. Επί του παρόντος διακρίνουμε τους παρακάτω "κλάδους" που αναφέρονται με αλφαβητική σειρά:

- Ομάδα CSIRT Ακαδημαϊκού Κλάδου
- Ομάδα CSIRT Εμπορικού Κλάδου
- Ομάδα CSIRT Κλάδου CIP/CIIP
- Ομάδα CSIRT Κυβερνητικού Κλάδου
- Εσωτερική Ομάδα CSIRT
- Ομάδα CSIRT Στρατιωτικού Κλάδου
- Εθνική Ομάδα CSIRT
- Ομάδα CSIRT Κλάδου Μικρομεσαίων Επιχειρήσεων (ΜΜΕ)
- Ομάδα CSIRT Προμηθευτών

Ομάδα CSIRT Ακαδημαϊκού Κλάδου
Εστίαση
Μια ομάδα CSIRT του ακαδημαϊκού κλάδου παρέχει υπηρεσίες CSIRT σε ακαδημαϊκά και εκπαιδευτικά ιδρύματα, όπως πανεπιστήμια ή ερευνητικοί φορείς, και στα διαδικτυακά περιβάλλοντά τους εντός της πανεπιστημιούπολης.

Κοινότητα αποδεκτών
Οι τυπικοί αποδέκτες της ομάδας CSIRT αυτού του τύπου είναι το προσωπικό και οι φοιτητές των πανεπιστημίων.

Ομάδα CSIRT Εμπορικού Κλάδου
Εστίαση
Μια εμπορική ομάδα CSIRT παρέχει εμπορικές υπηρεσίες CSIRT στους αποδέκτες. Σε περίπτωση ενός Παροχέα Διαδικτυακών Υπηρεσιών, η ομάδα CSIRT παρέχει κυρίως υπηρεσίες αντιμετώπισης καταχρήσεων σε πελάτες-τελικούς χρήστες (Dial-in, ADSL) και υπηρεσίες CSIRT στους επαγγελματίες πελάτες τους.

Κοινότητα αποδεκτών
Οι εμπορικές ομάδες CSIRT συνήθως παρέχουν τις υπηρεσίες τους σε αποδέκτες που καταβάλλουν αντίτιμο γι' αυτές.

Ομάδα CSIRT Κλάδου CIP/CIIP
Εστίαση
Η ομάδα CSIRT σε αυτόν τον κλάδο εστιάζει πρωτίστως στην Προστασία Κρίσιμων Πληροφοριών (CIP) ή/και στην Προστασία Κρίσιμων Πληροφοριών και Υποδομής (CIIP). Στις περισσότερες περιπτώσεις, αυτή η εξειδικευμένη ομάδα CSIRT συνεργάζεται στενά με ένα Κυβερνητικό Τμήμα CIIP. Καλύπτει όλους τους κρίσιμους τομείς των πληροφοριακών συστημάτων της χώρας και προστατεύει τους πολίτες της εν λόγω χώρας.

Κοινότητα αποδεκτών
Κυβέρνηση, κρίσιμοι τομείς πληροφοριακών συστημάτων, πολίτες.

Ομάδα CSIRT Κυβερνητικού Κλάδου
Εστίαση
Μια κυβερνητική ομάδα CSIRT παρέχει υπηρεσίες σε κυβερνητικούς φορείς και σε ορισμένες χώρες στους πολίτες.

Κοινότητα αποδεκτών
Κυβερνήσεις και κυβερνητικές υπηρεσίες, σε ορισμένες δε χώρες οι υπηρεσίες συναγερμού παρέχονται και στους πολίτες (για παράδειγμα Βέλγιο, Ουγγαρία, Ολλανδία, Ηνωμένο Βασίλειο, Γερμανία).

Εσωτερική Ομάδα CSIRT
Εστίαση
Μια εσωτερική ομάδα CSIRT παρέχει υπηρεσίες αποκλειστικά στον οργανισμό στον οποίο εντάσσεται. Κατ' αυτόν τον τρόπο περιγράφεται περισσότερο η λειτουργία παρά ένας κλάδος. Για παράδειγμα, πολλοί οργανισμοί τηλεπικοινωνιών και πολλές τράπεζες

διαθέτουν τις δικές τους εσωτερικές ομάδες CSIRT. Συνήθως δεν διατηρούν ιστοτόπο για το ευρύ κοινό.

Κοινότητα αποδεκτών
Εσωτερικό προσωπικό και τμήμα πληροφοριακών συστημάτων του οργανισμού.

Ομάδα CSIRT Στρατιωτικού Κλάδου
Εστίαση
Μια ομάδα CSIRT σε αυτόν τον κλάδο παρέχει υπηρεσίες σε στρατιωτικούς οργανισμούς, έχοντας την ευθύνη για την υποδομή των πληροφοριακών συστημάτων που απαιτούνται για αμυντικούς σκοπούς.

Κοινότητα αποδεκτών
Προσωπικό στρατιωτικών οργανισμών ή στενά συνδεδεμένων φορέων, για παράδειγμα το Υπουργείο Εθνικής Άμυνας.

Εθνική Ομάδα CSIRT
Εστίαση
Μια ομάδα CSIRT με εθνική εστίαση θεωρείται σημείο επαφής για την ασφάλεια μιας χώρας. Σε ορισμένες περιπτώσεις, η κυβερνητική ομάδα CISRT λειτουργεί και ως εθνικό Σημείο Επαφής (όπως η UNIRAS στο Ηνωμένο Βασίλειο).

Κοινότητα αποδεκτών
Η ομάδα CSIRT αυτού του είδους συνήθως δεν έχει άμεσους αποδέκτες, καθώς η εθνική ομάδα CSIRT απλώς διαδραματίζει ρόλο διαμεσολαβητή για ολόκληρη τη χώρα.

Ομάδα CSIRT Κλάδου Μικρομεσαίων Επιχειρήσεων (ΜΜΕ)
Εστίαση
Μια ομάδα CSIRT που οργανώνεται από μόνη της και παρέχει τις υπηρεσίες της στον δικό της κλάδο δραστηριοτήτων ή σε παρόμοια ομάδα χρηστών.

Κοινότητα αποδεκτών
Οι αποδέκτες τέτοιων ομάδων CSIRT μπορεί να είναι οι ΜΜΕ και το προσωπικό τους ή ομάδες ειδικών συμφερόντων όπως η "Ένωση Δήμων και Κοινοτήτων" μιας χώρας.

Ομάδα CSIRT Προμηθευτών
Εστίαση
Μια ομάδα CSIRT προμηθευτή εστιάζει στην υποστήριξη των προϊόντων ενός συγκεκριμένου προμηθευτή. Συνήθως, στόχος της είναι να αναπτύσσει και να παρέχει λύσεις, προκειμένου να αποκατασταθούν οι αδυναμίες και να μετριάζονται οι ενδεχόμενες αρνητικές επιπτώσεις των ελαττωμάτων.

Κοινότητα αποδεκτών
Κάτοχοι του προϊόντος.

Όπως περιγράφηκε στην παράγραφο σχετικά με την εθνική ομάδα CSIRTS, είναι πιθανό μια ομάδα να εξυπηρετεί περισσότερους από έναν κλάδους. Αυτό, για παράδειγμα, έχει αντίκτυπο στην ανάλυση της κοινότητας αποδεκτών και των αναγκών της.

Εικονική ομάδα CSIRT (βήμα 1)
Φάση έναρξης Κατά τη φάση έναρξης, η νέα ομάδα CSIRT σχεδιάζεται ως εσωτερική ομάδα CSIRT, παρέχοντας τις υπηρεσίες της στην εταιρεία στην οποία εντάσσεται, στο τοπικό τμήμα πληροφοριακών συστημάτων και στο προσωπικό. Επίσης, υποστηρίζει και συντονίζει την αντιμετώπιση περιστατικών σχετικών με την ασφάλεια πληροφοριακών συστημάτων μεταξύ των διαφόρων υποκαταστημάτων.

5.2 Πιθανές υπηρεσίες που μπορεί να παράσχει μια ομάδα CSIRT

Πραγματοποιήσαμε τα δύο πρώτα βήματα

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί να προσφέρει.
2. Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;

>> Το επόμενο βήμα είναι να απαντηθεί το ερώτημα *Τι είδους υπηρεσίες θα παρασχεθούν στους αποδέκτες;*

Υπάρχουν πολλές υπηρεσίες που μπορεί να παρέχει μια ομάδα CSIRT, αλλά έως τώρα καμία υπάρχουσα ομάδα CSIRT δεν τις παρέχει όλες. Επομένως, η επιλογή της κατάλληλης ομάδας υπηρεσιών αποτελεί καίρια απόφαση. Παρακάτω θα βρείτε μια σύντομη επισκόπηση όλων των γνωστών υπηρεσιών CSIRT, όπως ορίζονται στο "Εγχειρίδιο Ομάδων CSIRT" που εκδίδεται από το CERT/CC[6].

[6] Εγχειρίδιο Ομάδων CSIRT του CERT/CC CSIRT http://www.cert.org/archive/pdf/csirt-handbook.pdf

Υπηρεσίες Αντίδρασης	**Υπηρεσίες Πρόληψης**	**Αντιμετώπιση ευρημάτων**
• **Συναγερμοί και προειδοποιήσεις** • **Αντιμετώπιση περιστατικών** • **Ανάλυση περιστατικών** • **Υποστήριξη απόκρισης σε περιστατικά** • **Συντονισμός απόκρισης σε περιστατικά** • Επιτόπια απόκριση σε περιστατικά • Αντιμετώπιση αδυναμιών • Ανάλυση αδυναμιών • Απόκριση σε αδυναμίες • Συντονισμός απόκρισης σε αδυναμίες	• **Ανακοινώσεις** • Παρακολούθηση τεχνολογίας • Έλεγχοι ή αξιολογήσεις ασφαλείας • Διαμόρφωση και διατήρηση ασφαλείας • Ανάπτυξη εργαλείων ασφαλείας • Υπηρεσίες εντοπισμού εισβολής • Διάχυση πληροφοριών για την ασφάλεια	• *Ανάλυση ευρημάτων* • *Απόκριση σε ευρήματα* • *Συντονισμός απόκρισης σε ευρήματα* ***Διαχείριση ποιότητας ασφαλείας*** • *Ανάλυση κινδύνου* • *Επιχειρηματική συνέχεια και ανάκαμψη από καταστροφή* • *Συμβουλευτικές υπηρεσίες ασφαλείας* • *Ενίσχυση ευαισθητοποίησης* • *Εκπαίδευση/κατάρτιση* • *Αξιολόγηση ή πιστοποίηση προϊόντος*

Σχήμα 1 Κατάλογος υπηρεσιών CSIRT από το CERT/CC[7]

Οι βασικές υπηρεσίες (επισημαίνονται με έντονους χαρακτήρες): υπάρχει διάκριση μεταξύ υπηρεσιών αντίδρασης και υπηρεσιών πρόληψης. Οι υπηρεσίες πρόληψης στοχεύουν στην αποτροπή περιστατικών μέσω της ενίσχυσης της ευαισθητοποίησης και της κατάρτισης, ενώ οι υπηρεσίες αντίδρασης στοχεύουν στην αντιμετώπιση περιστατικών και το μετριασμό της προκύπτουσας ζημίας.

Η αντιμετώπιση ευρημάτων περιλαμβάνει την ανάλυση οποιουδήποτε αρχείου ή αντικειμένου βρίσκεται σε ένα σύστημα και το οποίο ενδέχεται να εμπλέκεται σε κακόβουλες ενέργειες, όπως υπολείμματα ιών, ''σκουληκιών'', σεναρίων, δούρειων ίππων κ.λπ. Επίσης, περιλαμβάνει την αντιμετώπιση και διανομή των προκυπτουσών πληροφοριών στους προμηθευτές και άλλους ενδιαφερόμενους φορείς, προκειμένου να αποφευχθεί η περαιτέρω εξάπλωση κακόβουλου κώδικα και να μετριασθούν οι κίνδυνοι.

Οι υπηρεσίες διαχείρισης ασφαλείας και ποιότητας είναι υπηρεσίες με μακροπρόθεσμους στόχους και περιλαμβάνουν την παροχή συμβουλευτικών υπηρεσιών και εκπαιδευτικών μέτρων.

Βλέπε παράρτημα για μια λεπτομερή επεξήγηση των υπηρεσιών CSIRT.

Η επιλογή των κατάλληλων υπηρεσιών για τους αποδέκτες σας είναι ένα σημαντικό βήμα και θα γίνει περαιτέρω αναφορά σε αυτό στο κεφάλαιο *6.1 Καθορισμός οικονομικού μοντέλου*.

[7] Κατάλογος υπηρεσιών CSIRT από το CERT/CC: http://www.cert.org/csirts/services.html

Οι περισσότερες ομάδες CSIRT ξεκινούν με τη διανομή "Συναγερμών και Προειδοποιήσεων", την πραγματοποίηση "Ανακοινώσεων" και την παροχή αντιμετώπισης περιστατικών για τους αποδέκτες τους. Οι εν λόγω βασικές υπηρεσίες συνήθως παρέχουν ένα καλό προφίλ και ιδιαίτερη αξία στην κοινότητα αποδεκτών και θεωρούνται κυρίως υπηρεσίες πραγματικής "προστιθέμενης αξίας".

Μια καλή πρακτική είναι να ξεκινήσει κανείς με μια μικρή ομάδα "πιλοτικών" αποδεκτών, να παρέχει τις βασικές υπηρεσίες για ένα πιλοτικό χρονικό διάστημα και κατόπιν να ζητήσει υλικό ανατροφοδότησης.
Οι ενδιαφερόμενοι πιλοτικοί χρήστες συνήθως παρέχουν εποικοδομητικό υλικό ανατροφοδότησης και βοηθούν στην ανάπτυξη προσαρμοσμένων υπηρεσιών.

Εικονική ομάδα CSIRT (βήμα 2)
Επιλέγοντας τις κατάλληλες υπηρεσίες
Κατά τη φάση έναρξης αποφασίζεται ότι η νέα ομάδα CSIRT θα εστιάσει κυρίως στην παροχή ορισμένων από τις βασικές υπηρεσίες στους υπαλλήλους.

Αποφασίζεται ότι μετά από την πιλοτική φάση μπορεί να εξετασθεί η επέκταση του χαρτοφυλακίου υπηρεσιών και ενδέχεται να προστεθούν ορισμένες "Υπηρεσίες Διαχείρισης Ασφαλείας". Η εν λόγω απόφαση θα ληφθεί με βάση το υλικό ανατροφοδότησης από τους πιλοτικούς αποδέκτες και σε στενή συνεργασία με το Τμήμα Διασφάλισης Ποιότητας.

5.3 Ανάλυση κοινότητας αποδεκτών και δήλωση αποστολής

Πραγματοποιήσαμε τα τρία πρώτα βήματα:

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί να προσφέρει.
2. Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;
3. Τι είδους υπηρεσίες μπορεί να προσφέρει μια ομάδα CSIRT στην κοινότητα αποδεκτών της;

>> Το επόμενο βήμα είναι να απαντηθεί το ερώτημα, *Τι είδους προσέγγιση θα πρέπει να επιλεγεί για τη δημιουργία της ομάδας CSIRT;*

Το επόμενο βήμα είναι μια λεπτομερέστερη εξέταση της κοινότητας αποδεκτών, με κύριο στόχο την επιλογή των κατάλληλων διαύλων επικοινωνίας:

- καθορισμός της επικοινωνιακής προσέγγισης προς τους αποδέκτες,
- καθορισμός της δήλωσης αποστολής,
- πραγματοποίηση ενός ρεαλιστικού σχεδίου υλοποίησης/έργου,
- καθορισμός των υπηρεσιών CSIRT,
- καθορισμός της οργανωτικής δομής,
- καθορισμός της πολιτικής περί Ασφάλειας Πληροφοριών,
- πρόσληψη του κατάλληλου προσωπικού,

- αξιοποίηση του γραφείου CSIRT,
- αναζήτηση συνεργασίας μεταξύ άλλων ομάδων CSIRT και πιθανών εθνικών πρωτοβουλιών.

Τα εν λόγω βήματα θα περιγραφούν λεπτομερέστερα στις παρακάτω παραγράφους και μπορούν να χρησιμοποιηθούν ως εισαγωγή στο επιχειρηματικό σχέδιο και το σχέδιο έργου.

5.3.1 Επικοινωνιακή προσέγγιση προς την κοινότητα αποδεκτών

Όπως προαναφέρθηκε, είναι πολύ σημαντικό να γνωρίζετε τις ανάγκες της κοινότητας αποδεκτών καθώς και τη δική σας στρατηγική επικοινωνίας, συμπεριλαμβανομένων των επικοινωνιακών διαύλων που είναι οι πλέον κατάλληλοι ώστε να παράσχετε πληροφορίες στους αποδέκτες.

Η θεωρία της διαχείρισης προτείνει αρκετές πιθανές προσεγγίσεις στο εν λόγω πρόβλημα ανάλυσης μιας ομάδας αποδεκτών. Στο παρόν έγγραφο περιγράφουμε δύο από αυτές: την ανάλυση SWOT και την ανάλυση PEST.

Ανάλυση SWOT
Μια Ανάλυση SWOT είναι ένα στρατηγικό εργαλείο σχεδιασμού που χρησιμοποιείται για την αξιολόγηση των Δυνατών σημείων, των Αδύνατων σημείων, των Ευκαιριών και των Απειλών που παρουσιάζονται σε ένα έργο ή μια επιχείρηση ή οποιαδήποτε άλλη κατάσταση που απαιτεί τη λήψη απόφασης. Η τεχνική αποδίδεται στον Albert Humphrey, ο οποίος ηγήθηκε ενός ερευνητικού προγράμματος στο Πανεπιστήμιο του Stanford κατά τις δεκαετίες του 1960 και του 1970, χρησιμοποιώντας δεδομένα από τις εταιρείες της λίστας Fortune 500[8].

Δυνατά σημεία	**Αδύνατα σημεία**
Ευκαιρίες	**Απειλές**

Σχήμα 2 Ανάλυση SWOT

[8] Ανάλυση SWOT στο Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Ανάλυση PEST

Η ανάλυση PEST είναι άλλο ένα σημαντικό και ευρέως χρησιμοποιούμενο εργαλείο για την ανάλυση της κοινότητας αποδεκτών με στόχο την κατανόηση των Πολιτικών, Οικονομικών, Κοινωνικο-πολιτισμικών και Τεχνολογικών συνθηκών του περιβάλλοντος στο οποίο λειτουργεί μια ομάδα CSIRT. Θα βοηθήσει στο να καθορισθεί εάν ο σχεδιασμός εξακολουθεί να εναρμονίζεται με το περιβάλλον και πιθανώς βοηθά στην αποφυγή ενεργειών που πραγματοποιούνται εξαιτίας εσφαλμένων υποθέσεων.

Πολιτικά	**Οικονομικά στοιχεία**
• Οικολογικά/ περιβαλλοντικά ζητήματα • Υφιστάμενη νομοθεσία συγκεκριμένης αγοράς • Μελλοντική νομοθεσία • Ευρωπαϊκή/διεθνής νομοθεσία • Εποπτικοί φορείς και διαδικασίες • Κυβερνητικές πολιτικές • Θητεία και αλλαγή κυβέρνησης • Εμπορικές πολιτικές • Χρηματοδότηση, επιχορηγήσεις και πρωτοβουλίες • Ομάδες συμφερόντων/ομάδες άσκησης πίεσης συγκεκριμένης αγοράς • Διεθνείς ομάδες πίεσης	• Οικονομική κατάσταση συγκεκριμένης χώρας • Οικονομικές τάσεις συγκεκριμένης χώρας • Διεθνείς οικονομίες και τάσεις • Γενικά θέματα φορολογίας • Φορολογία συγκεκριμένων προϊόντων ή υπηρεσιών • Ζητήματα εποχικότητας/καιρικών συνθηκών • Κύκλοι αγοράς και εμπορίου • Παράγοντες συγκεκριμένου τομέα • Κατευθύνσεις της αγοράς και τάσεις διανομής • Οδηγοί πελατών/τελικών χρηστών • Επιτόκια και συναλλαγματικές ισοτιμίες
Κοινωνικά στοιχεία	**Τεχνολογικά στοιχεία**
• Τάσεις τρόπου ζωής • Δημογραφικά στοιχεία • Συμπεριφορές και απόψεις καταναλωτών • Απόψεις μέσων ενημέρωσης • Μεταβολές νομοθεσίας που επηρεάζουν κοινωνικούς παράγοντες • Εικόνα επωνυμίας, εταιρείας, τεχνολογίας • Μοντέλα αγοραστικών συνηθειών των καταναλωτών • Μοντέλα μόδας και ρόλων • Κύρια γεγονότα και επιρροές • Αγοραστική πρόσβαση και τάσεις • Εθνικοί/θρησκευτικοί παράγοντες • Διαφήμιση και προβολή	• Ανάπτυξη ανταγωνιστικής τεχνολογίας • Χρηματοδότηση έρευνας • Συναφείς/εξαρτημένες τεχνολογίες • Τεχνολογία/λύσεις αντικατάστασης • Ωριμότητα τεχνολογίας • Κατασκευαστική ωριμότητα και ικανότητα • Πληροφορίες και επικοινωνίες • Καταναλωτές που αγοράζουν μηχανήματα ή τεχνολογία • Νομοθεσία περί τεχνολογίας • Προοπτική καινοτομίας • Τεχνολογική πρόσβαση, άδειες, ευρεσιτεχνίες • Ζητήματα πνευματικής ιδιοκτησίας

Σχήμα 3 Μοντέλο ανάλυσης Pest

Μια λεπτομερής περιγραφή της ανάλυσης PEST διατίθεται στο Wikipedia[9].

Και τα δύο εργαλεία παρέχουν μια ολοκληρωμένη και δομημένη επισκόπηση των αναγκών των αποδεκτών. Τα αποτελέσματα θα συμπληρώσουν την επιχειρηματική πρόταση και κατ' αυτόν τον τρόπο θα συμβάλουν στη λήψη χρηματοδότησης για τη δημιουργία της ομάδας CSIRT.

Δίαυλοι επικοινωνίας

[9] Ανάλυση PEST στο Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Ένα σημαντικό θέμα που θα πρέπει να συμπεριληφθεί στην ανάλυση είναι οι πιθανές επικοινωνιακές μέθοδοι και μέθοδοι διανομής πληροφοριών ("Πώς επικοινωνώ με την κοινότητα αποδεκτών;").

Εάν είναι δυνατό θα πρέπει να εξετασθεί το ενδεχόμενο τακτικών προσωπικών επισκέψεων των αποδεκτών. Έχει αποδειχθεί ότι οι προσωπικές συναντήσεις διευκολύνουν τη συνεργασία. Εάν και οι δύο πλευρές έχουν την πρόθεση να συνεργασθούν, οι εν λόγω συναντήσεις θα οδηγήσουν σε μια πιο ανοικτή σχέση.

Συνήθως, οι ομάδες CSIRT χρησιμοποιούν ένα σύνολο επικοινωνιακών διαύλων. Τα παρακάτω αποδείχθηκαν χρήσιμα στην πράξη και αξίζει τον κόπο να ληφθούν υπόψη:

- δημόσιος ιστότοπος,
- κλειστή περιοχή μελών στον ιστότοπο,
- ηλεκτρονικά έντυπα αναφοράς περιστατικών,
- λίστες αλληλογραφίας,
- εξατομικευμένος λογαριασμός ηλεκτρονικού ταχυδρομείου,
- τηλέφωνο / φαξ,
- μηνύματα SMS,
- ''αναχρονιστικές'' έντυπες επιστολές,
- μηνιαίες ή ετήσιες αναφορές.

Εκτός από τη χρήση του ηλεκτρονικού ταχυδρομείου, των ηλεκτρονικών εντύπων, του τηλεφώνου ή του φαξ για διευκόλυνση της αντιμετώπισης περιστατικών (για τη λήψη αναφορών περιστατικών από την κοινότητα αποδεκτών, το συντονισμό με άλλες ομάδες ή την παροχή υλικού ανατροφοδότησης και υποστήριξης στο θύμα), οι περισσότερες ομάδες CSIRT δημοσιεύουν τα δικά τους συμβουλευτικά ασφαλείας σε έναν ιστότοπο που διατίθεται στο ευρύ κοινό και μέσω καταλόγων αλληλογραφίας.

Εάν είναι δυνατό, οι πληροφορίες θα πρέπει να διανέμονται με ασφαλή τρόπο. Για παράδειγμα, τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να φέρουν ψηφιακή υπογραφή με το πρόγραμμα PGP (Pretty Good Privacy), ενώ τα ευαίσθητα δεδομένα για τα περιστατικά θα πρέπει πάντοτε να αποστέλλονται κρυπτογραφημένα.

Για περισσότερες πληροφορίες βλέπε το κεφάλαιο *8.5 Διαθέσιμα εργαλεία CSIRT*. Βλέπε επίσης το κεφάλαιο *2.3* του *RFC2350*[10].

Εικονική ομάδα CSIRT (βήμα 3α)

Πραγματοποίηση ανάλυσης της κοινότητας αποδεκτών και των κατάλληλων επικοινωνιακών διαύλων

Μια σύσκεψη ανταλλαγής ιδεών με μερικά βασικά στελέχη της διοίκησης και εκπροσώπους της κοινότητας αποδεκτών είχε ως αποτέλεσμα τη δημιουργία επαρκούς υλικού για μια ανάλυση SWOT. Η εν λόγω διαδικασία οδήγησε στο συμπέρασμα ότι υφίσταται ανάγκη για τις εξής βασικές υπηρεσίες:

[10] http://www.ietf.org/rfc/rfc2350.txt

- συναγερμοί και προειδοποιήσεις,
- αντιμετώπιση περιστατικών (ανάλυση, υποστήριξη απόκρισης και συντονισμός απόκρισης),
- ανακοινώσεις.

Θα πρέπει να εξασφαλισθεί ότι οι πληροφορίες διανέμονται με σωστά οργανωμένο τρόπο, ώστε να απευθύνονται σε όσο το δυνατόν μεγαλύτερο τμήμα της κοινότητας αποδεκτών. Επομένως, λαμβάνεται η απόφαση να δημοσιευθούν συναγερμοί, προειδοποιήσεις και ανακοινώσεις με τη μορφή συμβουλευτικών ασφαλείας σε έναν εξειδικευμένο ιστότοπο και να διανεμηθούν μέσω ενός καταλόγου αλληλογραφίας. Η ομάδα CSIRT διαθέτει ηλεκτρονικό ταχυδρομείο, τηλέφωνο και φαξ για τη λήψη των αναφορών περιστατικών. Ένα ενιαίο ηλεκτρονικό έντυπο σχεδιάζεται για το επόμενο βήμα.

Ανατρέξτε στην επόμενη σελίδα για ένα δείγμα ανάλυσης SWOT.

Δυνατά σημεία • Η εταιρεία διαθέτει κάποια γνώση • Της αρέσει το σχέδιο και είναι πρόθυμη να συνεργασθεί • Υποστήριξη και χρηματοδότηση από το διοικητικό συμβούλιο	**Αδύνατα σημεία** • Δεν υπάρχει αρκετή επικοινωνία μεταξύ των διαφόρων τμημάτων και υποκαταστημάτων • Δεν υπάρχει συντονισμός με το τμήμα περιστατικών των πληροφοριακών συστημάτων • Πολυάριθμα "μικρά τμήματα"
Ευκαιρίες • Τεράστια ροή μη δομημένων πληροφοριών για τις αδυναμίες του συστήματος • Έντονη ανάγκη συντονισμού • Μείωση απωλειών εξαιτίας περιστατικών • Αρκετά ανοικτά σημεία στο θέμα των πληροφοριακών συστημάτων • Εκπαίδευση προσωπικού στην ασφάλεια πληροφοριακών συστημάτων	**Απειλές** • Δεν υπάρχουν αρκετά χρήματα διαθέσιμα • Δεν υπάρχει αρκετό διαθέσιμο προσωπικό • Υψηλές προσδοκίες • Φιλοσοφία

Σχήμα 4 Δείγμα ανάλυσης SWOT

5.3.2 Δήλωση αποστολής

Μετά την ανάλυση των αναγκών και των επιθυμιών της κοινότητας χρηστών από τις υπηρεσίες CSIRT, το επόμενο βήμα θα πρέπει να είναι η σύνταξη μιας δήλωσης αποστολής.

Η δήλωση αποστολής περιγράφει τη βασική λειτουργία του οργανισμού στην κοινωνία, από την πλευρά των προϊόντων και των υπηρεσιών που προσφέρει στους αποδέκτες του. Επιτρέπει τη σαφή ενημέρωση για την ύπαρξη και τη λειτουργία της νέας ομάδας CSIRT.

Αποτελεί ορθή πρακτική να συντάξετε μια συνοπτική δήλωση αποστολής αλλά όχι υπερβολικά συνοπτική, καθώς συνήθως παραμένει αμετάβλητη για δύο χρόνια περίπου.

Ιδού ορισμένα παραδείγματα δηλώσεων αποστολής από υφιστάμενες ομάδες CSIRT:

“Η <όνομα ομάδας CSIRT> παρέχει πληροφορίες και υποστήριξη στους <αποδέκτες της (ορίστε τους αποδέκτες σας)> εφαρμόζοντας προληπτικά μέτρα για τη μείωση των κινδύνων που προέρχονται από περιστατικά ασφαλείας σε υπολογιστές και ταυτόχρονα αντιμετωπίζοντας τα εν λόγω περιστατικά όταν προκύπτουν.”

"Για την προσφορά υποστήριξης στους <Αποδέκτες> σχετικά με την πρόληψη και την αντιμετώπιση Περιστατικών που σχετίζονται με την Ασφάλεια των Πληροφοριακών Συστημάτων."[11]
Η δήλωση αποστολής είναι ένα πολύ σημαντικό και απαραίτητο βήμα από το οποίο πρέπει να ξεκινήσετε. Ανατρέξτε στο κεφάλαιο *2.1* του *RFC2350*[12] για μια πιο λεπτομερή περιγραφή των πληροφοριών τις οποίες θα πρέπει να δημοσιεύει μια ομάδα CSIRT.

Εικονική ομάδα CSIRT (βήμα 3β)
Η διοίκηση της εικονικής ομάδας CSIRT συνέταξε την παρακάτω δήλωση αποστολής: *"Η Εικονική Ομάδα CSIRT παρέχει πληροφορίες και υποστήριξη στο προσωπικό της εταιρείας στην οποία εντάσσεται, προκειμένου να μειωθούν οι κίνδυνοι που παρέχονται από περιστατικά ασφαλείας σε υπολογιστές, καθώς και να αντιμετωπίζονται τα εν λόγω περιστατικά όταν προκύπτουν.”* Μέσω αυτού, η εικονική ομάδα CSIRT διευκρινίζει ότι αποτελεί εσωτερική ομάδα CSIRT και ότι η κύρια δραστηριότητά της είναι να αντιμετωπίζει τα ζητήματα ασφαλείας πληροφοριακών συστημάτων.

[11] Δήλωση αποστολής του Govcert.nl: http://www.govcert.nl

[12] http://www.ietf.org/rfc/rfc2350.txt

6 Ανάπτυξη του Επιχειρηματικού Σχεδίου

Πραγματοποιήσαμε τα εξής βήματα:

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί να προσφέρει.
2. Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;
3. Τι είδους υπηρεσίες μπορεί να προσφέρει μια ομάδα CSIRT στην κοινότητα αποδεκτών της;
4. Ανάλυση του περιβάλλοντος και των αποδεκτών.
5. Καθορισμός της δήλωσης αποστολής.

>> Το επόμενο βήμα είναι ο καθορισμός του επιχειρηματικού σχεδίου.

Το αποτέλεσμα της ανάλυσης σας παρέχει μια καλή επισκόπηση των αναγκών και των (υποτιθέμενων) αδυναμιών της κοινότητας αποδεκτών και επομένως λαμβάνεται ως εισαγόμενο για το επόμενο βήμα.

6.1 Καθορισμός του οικονομικού μοντέλου

Μετά την ανάλυση, επιλέχθηκαν δύο βασικές υπηρεσίες ως αφετηρία. Το επόμενο βήμα είναι η εξέταση του οικονομικού μοντέλου: ποιες παράμετροι παροχής υπηρεσιών είναι ταυτόχρονα κατάλληλες και χρηματοδοτούμενες.

Σε έναν τέλειο κόσμο η χρηματοδότηση θα προσαρμοζόταν στις ανάγκες της κοινότητας αποδεκτών, αλλά στην πραγματικότητα το χαρτοφυλάκιο υπηρεσιών που μπορεί να παρασχεθεί θα πρέπει να προσαρμοσθεί σε έναν δεδομένο προϋπολογισμό. Επομένως, είναι πιο ρεαλιστικό να ξεκινήσετε με το σχεδιασμό των χρηματικών ζητημάτων.

6.1.1 Μοντέλο κόστους

Οι δύο κύριοι παράγοντες που επηρεάζουν το κόστος είναι ο καθορισμός των ωρών παροχής των υπηρεσιών, αλλά και των ατόμων (και της ποιότητας) του προσωπικού που θα απασχοληθεί. Είναι αναγκαία η παροχή αντιμετώπισης περιστατικών και τεχνικής υποστήριξης 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα, ή μήπως οι εν λόγω υπηρεσίες θα παρέχονται μόνο σε ώρες γραφείου;

Ανάλογα με την επιθυμητή διαθεσιμότητα και τον εξοπλισμό γραφείου (είναι για παράδειγμα δυνατή η εργασία από το σπίτι;), μπορεί να είναι καλύτερη η παροχή υπηρεσιών σε βάρδιες κατόπιν κλήσης ή σε προγραμματισμένες βάρδιες.

Ένα πιθανό σενάριο είναι η παροχή των υπηρεσιών πρόληψης και των υπηρεσιών αντίδρασης κατά τις ώρες γραφείου. Εκτός ωρών γραφείου θα παρέχονται μόνο περιορισμένες υπηρεσίες, για παράδειγμα μόνο σε περίπτωση μεγάλων καταστροφών και περιστατικών, από μέλος του προσωπικού κατόπιν κλήσης.

Άλλη μια επιλογή είναι η αναζήτηση διεθνούς συνεργασίας μεταξύ άλλων ομάδων CSIRT. Υπάρχουν ήδη παραδείγματα υφιστάμενης συνεργασίας “Ακολουθώντας τη

Sun". Για παράδειγμα, η συνεργασία μεταξύ ευρωπαϊκών και αμερικανικών ομάδων αποδείχθηκε ωφέλιμη και προσέφερε έναν καλό τρόπο ανταλλαγής ικανοτήτων. Για παράδειγμα, η ομάδα CSIRT της Sun Microsystems, που διαθέτει πολλά υποκαταστήματα σε διαφορετικές ζώνες ώρας ανά τον κόσμο (αλλά όλα είναι μέλη της ίδιας ομάδας CSIRT), παρέχει υπηρεσίες 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα με συνεχώς εναλλασσόμενες βάρδιες μεταξύ των ομάδων σε ολόκληρη την υφήλιο. Αυτό περιορίζει το κόστος, επειδή οι ομάδες πάντοτε εργάζονται μόνο κατά τις συνήθεις ώρες γραφείου και παρέχουν επίσης υπηρεσίες κατά τη διάρκεια της νύχτας σε ένα τμήμα του κόσμου.

Αποτελεί καλή πρακτική η ιδιαίτερη ανάλυση της ανάγκης για παροχή υπηρεσιών 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα στην κοινότητα αποδεκτών. Οι Συναγερμοί και οι Προειδοποιήσεις που παρέχονται κατά τις νυχτερινές ώρες δεν έχουν ιδιαίτερο νόημα όταν ο αποδέκτης θα τις διαβάσει το επόμενο πρωί. Είναι λεπτός ο διαχωρισμός μεταξύ "της ανάγκης για μια υπηρεσία" και "της επιθυμίας για μια υπηρεσία", αλλά ιδιαίτερα οι εργάσιμες ώρες διαφοροποιούν σημαντικά τον αριθμό του προσωπικού και των απαιτούμενων εγκαταστάσεων και, ως εκ τούτου, έχουν σημαντικό αντίκτυπο στο μοντέλο κόστους.

6.1.2 Μοντέλο εσόδων

Όταν γνωρίζετε το κόστος, σε επόμενο στάδιο καλό είναι να εξετάσετε τα πιθανά μοντέλα εσόδων: πώς μπορούν να χρηματοδοτηθούν οι προβλεπόμενες υπηρεσίες; Ιδού ορισμένα πιθανά σενάρια προς αξιολόγηση:

Χρήση υφιστάμενων πόρων
Είναι πάντοτε ωφέλιμο να εκτιμάτε τους ήδη υφιστάμενους πόρους σε άλλα τμήματα της εταιρείας. Απασχολείται ήδη κατάλληλο προσωπικό (για παράδειγμα στο υφιστάμενο τμήμα πληροφοριακών συστημάτων) με το απαιτούμενο υπόβαθρο και την απαιτούμενη εξειδίκευση; Πιθανότατα μπορεί να γίνει διευθέτηση με τη διοίκηση για τη μετάθεση αυτού του προσωπικού στην ομάδα CSIRT για τη φάση έναρξης ή για την παροχή υποστήριξης επί τούτου στην ομάδα CSIRT.

Συνδρομή μέλους
Άλλη μια πιθανότητα είναι να πωλήσετε τις υπηρεσίες σας στην κοινότητα αποδεκτών, μέσω ετήσιας ή τρίμηνης συνδρομής μέλους. Οι επιπρόσθετες υπηρεσίες θα μπορούν να χρεώνονται ανάλογα με τη χρήση, για παράδειγμα οι συμβουλευτικές υπηρεσίες ή οι έλεγχοι ασφαλείας.

Άλλο ένα πιθανό σενάριο: οι υπηρεσίες που παρέχονται (εσωτερικά) στην κοινότητα αποδεκτών είναι δωρεάν, αλλά οι υπηρεσίες που παρέχονται σε εξωτερικούς πελάτες ενδέχεται να χρεώνονται. Άλλη μια ιδέα είναι η δημοσίευση συμβουλευτικών και ενημερωτικών δελτίων στο δημόσιο ιστότοπο και η δημιουργία μιας ενότητας αποκλειστικά για τα μέλη με εξειδικευμένες, λεπτομερέστερες ή προσαρμοσμένες πληροφορίες.

Έχει αποδειχθεί στην πράξη ότι "Η εγγραφή ανά υπηρεσία CSIRT" έχει μόνο περιορισμένη χρήση στην παροχή επαρκούς χρηματοδότησης, ιδιαίτερα κατά τη φάση έναρξης. Υπάρχουν, για παράδειγμα, πάγιες βασικές δαπάνες για την ομάδα και τον εξοπλισμό που πρέπει να καταβληθούν εκ των προτέρων. Η χρηματοδότηση των εν

λόγω δαπανών μέσω της πώλησης των υπηρεσιών CSIRT είναι δύσκολη και απαιτείται εξαιρετικά λεπτομερής ανάλυση ώστε να βρεθεί η “χρυσή τομή”.

Επιχορήγηση
Άλλη μια πιθανότητα που αξίζει τον κόπο να εξετάσετε είναι να υποβάλετε αίτηση για επιχορήγηση του έργου που παρέχεται από την κυβέρνηση ή έναν κυβερνητικό φορέα, καθώς σήμερα οι περισσότερες χώρες διαθέτουν κονδύλια για έργα ασφάλειας πληροφοριακών συστημάτων. Η επικοινωνία με το Υπουργείο Εσωτερικών μπορεί να είναι μια καλή αρχή.

Ένα μίγμα διαφορετικών μοντέλων εσόδων είναι ασφαλώς δυνατό.

6.2 Καθορισμός της οργανωτικής δομής

Η κατάλληλη οργανωτική δομή μιας ομάδας CSIRT εξαρτάται σε μεγάλο βαθμό από την υφιστάμενη δομή του οργανισμού στον οποίο εντάσσεται και της κοινότητας αποδεκτών. Επίσης, εξαρτάται από την προσβασιμότητα των ειδημόνων που θα προσληφθούν μόνιμα ή σε προκαθορισμένη βάση.

Μια τυπική ομάδα CSIRT αναθέτει τους παρακάτω ρόλους εντός της ομάδας:

Γενικά
- Γενικός διευθυντής

Προσωπικό
- Διευθυντής γραφείου
- Λογιστής
- Σύμβουλος επικοινωνίας
- Νομικός σύμβουλος

Λειτουργική Τεχνική ομάδα
- Επικεφαλής τεχνικής ομάδας
- Τεχνικοί της τεχνικής ομάδας CSIRT που παρέχουν τις υπηρεσίες CSIRT
- Ερευνητές

Εξωτερικοί σύμβουλοι
- Προσλαμβάνονται όταν είναι απαραίτητο

Είναι εξαιρετικά χρήσιμο να έχετε στην ομάδα έναν εξειδικευμένο νομικό, ιδιαίτερα κατά τη φάση έναρξης της ομάδας CSIRT. Θα αυξηθεί το κόστος, αλλά στο τέλος θα εξοικονομήσετε χρόνο και θα γλυτώσετε από νομικά προβλήματα.

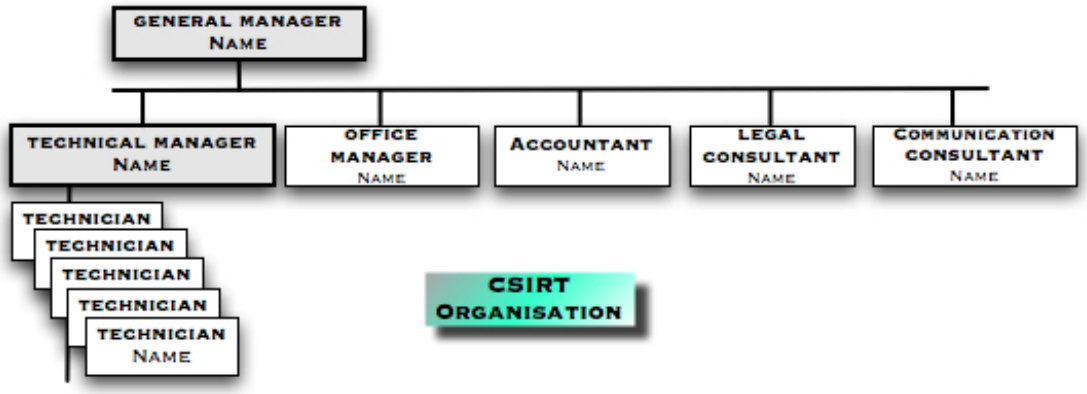
Ανάλογα με τα διαφορετικά επίπεδα εξειδίκευσης εντός της κοινότητας αποδεκτών, καθώς επίσης όταν η ομάδα CSIRT διαθέτει ισχυρό προφίλ στα μέσα ενημέρωσης, έχει αποδειχθεί ιδιαίτερα χρήσιμο να διαθέτει η ομάδα και έναν ειδικό επικοινωνιών. Οι εν λόγω ειδικοί μπορούν να εστιάσουν στην κατανόηση των δύσκολων τεχνικών ζητημάτων, μεταφέροντας με πιο κατανοητό τρόπο τα μηνύματα για τους αποδέκτες ή τους εκπροσώπους των μέσων ενημέρωσης. Επίσης, ο ειδικός επικοινωνιών παρέχει υλικό ανατροφοδότησης από την κοινότητα αποδεκτών προς τους εξειδικευμένους

τεχνικούς και επομένως μπορεί να ενεργεί ως "μεταφραστής" και "διαμεσολαβητής" μεταξύ των δύο αυτών ομάδων.

Ακολουθούν ορισμένα παραδείγματα οργανωτικών μοντέλων που χρησιμοποιούνται σε υφιστάμενες ομάδες CSIRT.

6.2.1 Το ανεξάρτητο επιχειρηματικό μοντέλο

Η ομάδα CSIRT βρίσκεται εκτός του οργανισμού και λειτουργεί ως ανεξάρτητος φορέας με τη δική του διοίκηση και τους δικούς του υπαλλήλους.

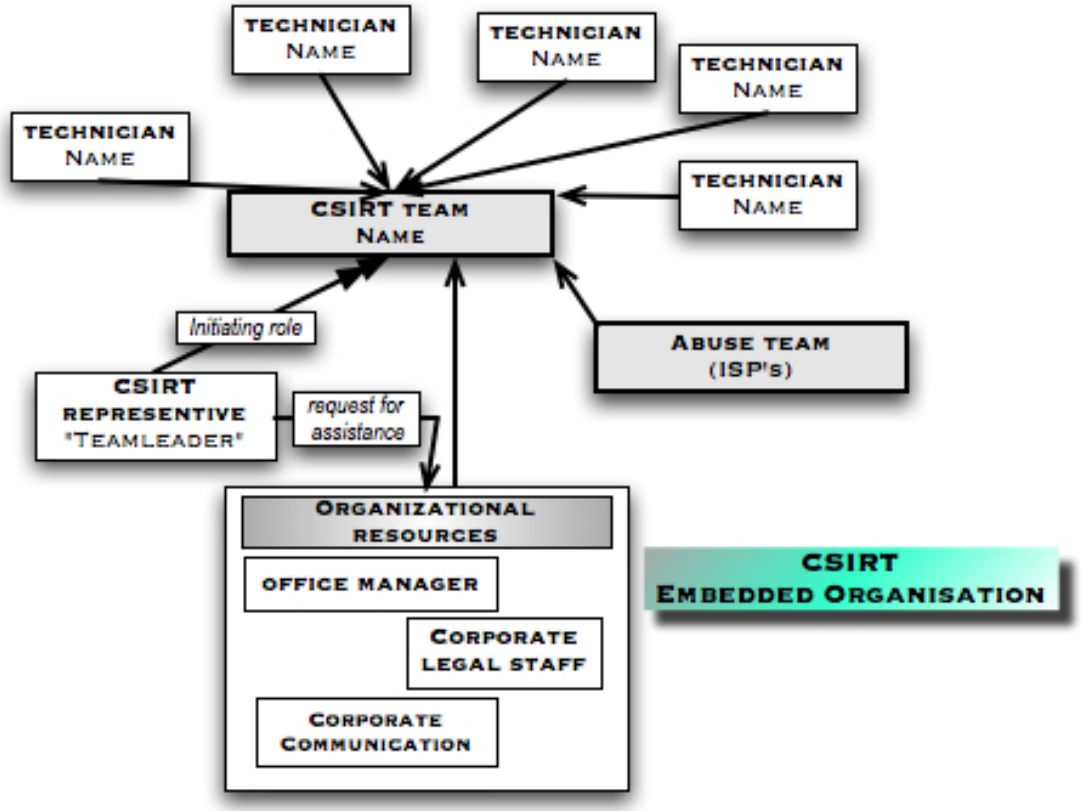


Σχήμα 5 Ανεξάρτητο επιχειρηματικό μοντέλο

6.2.2 Το ενσωματωμένο μοντέλο

Το εν λόγω μοντέλο μπορεί να χρησιμοποιηθεί εάν μια ομάδα CSIRT πρόκειται να δημιουργηθεί εντός ενός υφιστάμενου οργανισμού χρησιμοποιώντας για παράδειγμα το υφιστάμενο τμήμα πληροφοριακών συστημάτων. Της CSIRT ηγείται ένας επικεφαλής ομάδας και είναι υπεύθυνος για τις δραστηριότητες της ομάδας CSIRT. Ο επικεφαλής της ομάδας συγκεντρώνει τους απαραίτητους τεχνικούς κατά την επίλυση περιστατικών ή την ενασχόληση με τις δραστηριότητες της ομάδας CSIRT. Μπορεί να ζητήσει υποστήριξη εντός του υφιστάμενου οργανισμού για εξειδικευμένη βοήθεια.

Επίσης, το εν λόγω μοντέλο μπορεί να προσαρμόζεται για συγκεκριμένες συνθήκες όταν προκύπτουν. Σε αυτήν την περίπτωση, η ομάδα διαθέτει έναν συγκεκριμένο αριθμό Ισοδύναμων Πλήρους Απασχόλησης (FTE). Για παράδειγμα, η υπηρεσία εντοπισμού καταχρήσεων ενός Παροχέα Υπηρεσιών Διαδικτύου είναι οπωσδήποτε εργασία πλήρους απασχόλησης για ένα ή (στις περισσότερες περιπτώσεις) περισσότερα FTE.

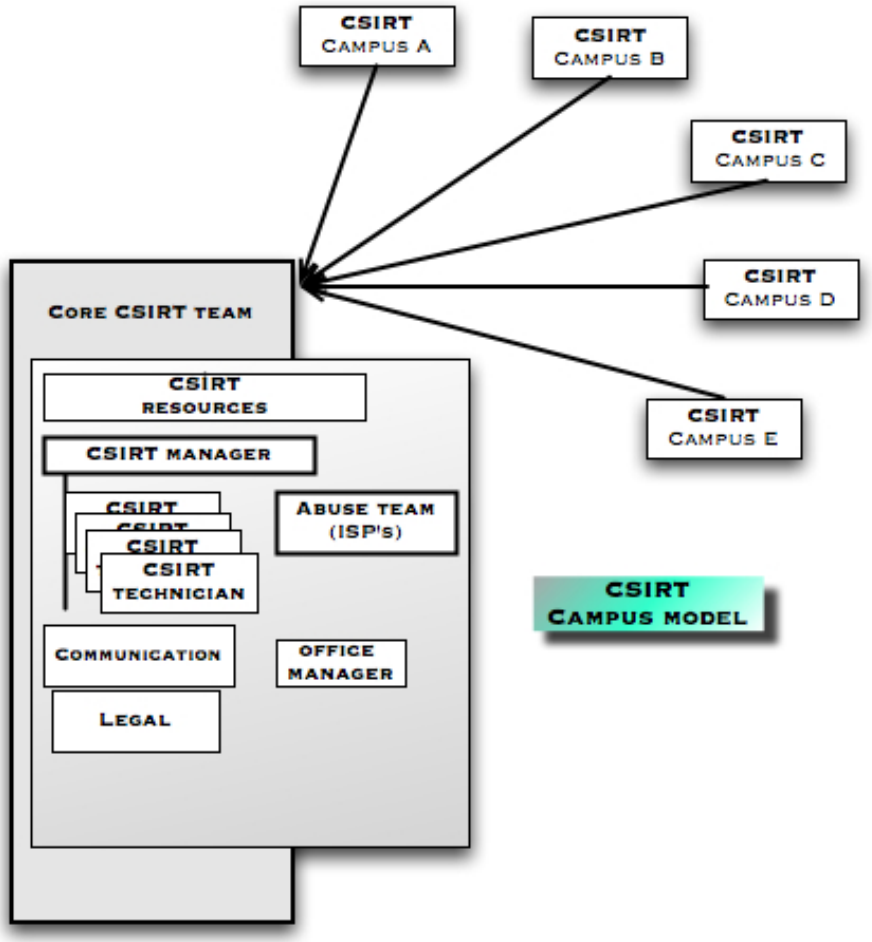


Σχήμα 6 Οργανωτικό ενσωματωμένο μοντέλο

6.2.3 Το μοντέλο της πανεπιστημιούπολης

Το μοντέλο της πανεπιστημιούπολης, όπως υποδηλώνει και το όνομά του, υιοθετείται κυρίως από ακαδημαϊκές και ερευνητικές ομάδες CSIRT. Οι περισσότεροι ακαδημαϊκοί και ερευνητικοί οργανισμοί αποτελούνται από διάφορες πανεπιστημιακές εγκαταστάσεις και πανεπιστημιουπόλεις σε διαφορετικές τοποθεσίες, οι οποίες καλύπτουν μια ευρύτερη περιοχή ή ακόμη και ολόκληρη τη χώρα (όπως στην περίπτωση των Εθνικών Ερευνητικών Δικτύων (NREN). Συνήθως, οι εν λόγω οργανισμοί είναι ανεξάρτητοι μεταξύ τους και συχνά διαθέτουν τη δική τους ομάδα CSIRT. Οι εν λόγω ομάδες CSIRT συνήθως οργανώνονται υπό τη σκέπη της ''μητρικής'' ή βασικής ομάδας CSIRT. Η βασική ομάδα CSIRT συντονίζει και είναι το ενιαίο σημείο επικοινωνίας με τον έξω κόσμο. Στις περισσότερες περιπτώσεις η βασική ομάδα CSIRT θα παρέχει και τις βασικές υπηρεσίες CSIRT, ενώ θα διανέμει και πληροφορίες για περιστατικά στην αρμόδια CSIRT της πανεπιστημιούπολης.

Ορισμένες ομάδες CSIRT εναλλάσσουν τις βασικές υπηρεσίες CSIRT με τις άλλες ομάδες CSIRT της πανεπιστημιούπολης, με αποτέλεσμα τη μείωση των πάγιων εξόδων για τη βασική ομάδα CSIRT.



Σχήμα 7 Μοντέλο πανεπιστημιούπολης

6.2.4 Το εθελοντικό μοντέλο

Το εν λόγω οργανωτικό μοντέλο περιγράφει μια ομάδα ανθρώπων (ειδικών) που συγκεντρώνονται για την παροχή συμβουλών και υποστήριξης ο ένας προς τον άλλο (και σε τρίτους) σε εθελοντική βάση. Είναι μια χαλαρή κοινότητα και εξαρτάται σε μεγάλο βαθμό από την κινητοποίηση των συμμετεχόντων.

Για παράδειγμα, το εν λόγω μοντέλο έχει υιοθετηθεί από την κοινότητα WARP[13].

6.3 Πρόσκληση του κατάλληλου προσωπικού

Έχοντας αποφασίσει για τις υπηρεσίες και το επίπεδο υποστήριξης που θα παρασχεθεί και έχοντας επιλέξει ένα οργανωτικό μοντέλο, το επόμενο βήμα είναι η εξεύρεση του κατάλληλου αριθμού εξειδικευμένων ατόμων για τη δουλειά.

Είναι σχεδόν αδύνατο να παρέχουμε συγκεκριμένα αριθμητικά στοιχεία για το τεχνικό προσωπικό που απαιτείται από αυτήν την προσέγγιση, αλλά οι παρακάτω βασικές τιμές έχει αποδειχθεί ότι αποτελούν μια καλή προσέγγιση:

- Προκειμένου να παρασχεθούν οι δύο βασικές υπηρεσίες της διανομής συμβουλευτικών δελτίων και της αντιμετώπισης περιστατικών: τουλάχιστον **4** FTE.

- Για μια πλήρη υπηρεσία CSIRT κατά τις ώρες γραφείου και τη συντήρηση των συστημάτων: τουλάχιστον **6 έως 8** FTE.

- Για μια πλήρως στελεχωμένη βάρδια 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα (2 βάρδιες εκτός ωρών γραφείου), η ελάχιστη απαίτηση είναι περίπου **12** FTE.

Οι εν λόγω αριθμοί περιλαμβάνουν και εφεδρείες σε περίπτωση ασθενειών, διακοπών, κ.λπ. Επίσης, είναι απαραίτητο να ελεγχθούν οι τοπικές συλλογικές συμβάσεις εργασίας. Εάν ορισμένα άτομα εργάζονται εκτός ωρών γραφείου, ενδέχεται να προκύψουν επιπρόσθετες δαπάνες με τη μορφή επιπρόσθετων επιδομάτων που πρέπει να καταβληθούν.

Ακολουθεί μια σύντομη επισκόπηση των βασικών προσόντων των εξειδικευμένων τεχνικών για μια ομάδα CSIRT.

Στοιχεία περιγραφής θέσης γενικού τεχνικού προσωπικού:

Προσωπικά προσόντα

- ευέλικτοι, δημιουργικοί και με καλό ομαδικό πνεύμα,
- ανεπτυγμένες δεξιότητες ανάλυσης,
- δυνατότητα επεξήγησης δύσκολων τεχνικών θεμάτων με εύκολη διατύπωση,
- καλή αίσθηση της εμπιστευτικότητας και της εργασίας σε διαδικαστικά θέματα,
- καλές δεξιότητες,
- αντοχή στην πίεση,

[13] Η πρωτοβουλία WARP http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

- ανεπτυγμένες δεξιότητες στην επικοινωνία και το γραπτό λόγο,
- ανοικτόμυαλοι και με θέληση για μάθηση.

Τεχνικά προσόντα
- ευρεία γνώση τεχνολογίας και πρωτοκόλλων Διαδικτύου,
- γνώση των συστημάτων Linux και Unix (ανάλογα με τον εξοπλισμό της κοινότητας αποδεκτών),
- γνώση των συστημάτων Windows (ανάλογα με τον εξοπλισμό της κοινότητας αποδεκτών),
- γνώση του εξοπλισμού υποδομής δικτύου (δρομολογητής, διακόπτες, DNS, Proxy, Mail κ.λπ.),
- γνώση των εφαρμογών Διαδικτύου (SMTP, HTTP, FTP, telnet, SSH κ.λπ.),
- γνώση των απειλών ασφαλείας (Διανεμημένες Επιθέσεις Άρνησης Παροχής Υπηρεσιών-DDoS, Αλίευση στοιχείων-Phising, Βανδαλισμοί Δικτυακών Τόπων-Defacing, Παρακολούθηση Δεδομένων-Sniffing κ.λπ.),
- γνώση εκτίμησης κινδύνου και πρακτικών εφαρμογών.

Επιπρόσθετα προσόντα
- πρόθυμοι να εργασθούν σε βάρδιες 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα ή κατόπιν κλήσης (ανάλογα με το μοντέλο της υπηρεσίας),
- μέγιστη απόσταση διαμετακόμισης (σε περίπτωση έκτακτης διαθεσιμότητας στο γραφείο, μέγιστος χρόνος διαμετακόμισης),
- επίπεδο εκπαίδευσης,
- εργασιακή εμπειρία στον τομέα της ασφάλειας πληροφοριακών συστημάτων.

Εικονική ομάδα CSIRT (βήμα 4)

Καθορισμός του Επιχειρηματικού Σχεδίου

Οικονομικό μοντέλο

Εξαιτίας του γεγονότος ότι η εταιρεία πραγματοποιεί ηλεκτρονικές συναλλαγές 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα και διαθέτει επίσης τμήμα πληροφοριακών συστημάτων που λειτουργεί τις ίδιες ώρες και ημέρες, αποφασίστηκε να παρέχεται πλήρης εξυπηρέτηση κατά τις ώρες γραφείου και εξυπηρέτηση κατόπιν κλήσης εκτός ωρών γραφείου. Οι υπηρεσίες θα παρέχονται δωρεάν στην κοινότητα αποδεκτών, αλλά η πιθανότητα παροχής υπηρεσιών σε εξωτερικούς πελάτες θα εξετάζεται κατά την πιλοτική φάση και τη φάση αξιολόγησης.

Μοντέλο εσόδων

Κατά τη φάση έναρξης και την πιλοτική φάση, η ομάδα CSIRT θα χρηματοδοτείται μέσω της εταιρείας στην οποία εντάσσεται. Κατά την πιλοτική φάση και τη φάση αξιολόγησης, θα συζητηθεί η τυχόν επιπρόσθετη χρηματοδότηση, συμπεριλαμβανομένης της πιθανότητας πώλησης υπηρεσιών σε εξωτερικούς πελάτες.

Οργανωτικό μοντέλο

Ο οργανισμός είναι μια μικρή εταιρεία και επομένως επιλέγεται το ενσωματωμένο μοντέλο.
Κατά τις ώρες γραφείου, προσωπικό τριών ατόμων θα παρέχει τις βασικές υπηρεσίες (διανομή συμβουλευτικών ασφαλείας και αντιμετώπιση περιστατικών ή συντονισμός).

Το τμήμα πληροφοριακών συστημάτων της εταιρείας απασχολεί ήδη άτομα με τα κατάλληλα προσόντα. Έχει συναφθεί συμφωνία με το εν λόγω τμήμα, ώστε η νέα ομάδα CSIRT να μπορεί να ζητήσει υποστήριξη κατά περίπτωση όταν απαιτείται. Επίσης μπορεί να χρησιμοποιηθεί η 2η σειρά των τεχνικών που βρίσκονται σε επαγρύπνηση.
Θα υπάρχει μια βασική ομάδα CSIRT με τέσσερα μέλη πλήρους απασχόλησης και πέντε επιπρόσθετα μέλη της ομάδας CSIRT. Ένα από αυτά θα είναι επίσης διαθέσιμο σε κυκλική βάρδια.

Προσωπικό
Ο επικεφαλής της ομάδας CSIRT διαθέτει προηγούμενη εμπειρία σε θέματα ασφάλειας και υποστήριξης 1ου και 2ου επιπέδου και έχει εργασθεί στο πεδίο της διαχείρισης κρίσης αντοχής. Τα άλλα τρία μέλη της ομάδας είναι ειδικοί σε θέματα ασφάλειας. Τα μέλη της ομάδας CSIRT με καθεστώς μερικής απασχόλησης από το τμήμα πληροφοριακών συστημάτων είναι ειδικοί ο καθένας στο δικό του τμήμα της υποδομής της εταιρείας.

6.4 Χρήση και εξοπλισμός του γραφείου

Ο εξοπλισμός και η χρήση του χώρου του γραφείου και η υλική ασφάλεια είναι πολύ ευρεία θέματα και επομένως δεν μπορεί να δοθεί εξαντλητική περιγραφή στο παρόν έγγραφο. Το παρόν κεφάλαιο έχει ως στόχο να παράσχει μια σύντομη επισκόπηση του εν λόγω θέματος.

Περισσότερες πληροφορίες σχετικά με την υλική ασφάλεια διατίθενται στις παρακάτω διευθύνσεις:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

"Θωρακίζοντας το κτίριο"
Επειδή οι ομάδες CSIRT συνήθως διαχειρίζονται πολύ ευαίσθητες πληροφορίες, αποτελεί καλή πρακτική να επιτρέψετε στην ομάδα να αναλάβει την υλική ασφάλεια του γραφείου. Αυτό θα εξαρτηθεί σε μεγάλο βαθμό από τις υφιστάμενες εγκαταστάσεις και την υποδομή, καθώς και την υφιστάμενη πολιτική ασφάλειας πληροφοριών της εταιρείας στην οποία εντάσσεται.

Για παράδειγμα, οι κυβερνήσεις εργάζονται με οργανωμένα πλαίσια διαβαθμίσεων και είναι πολύ αυστηρές στον τρόπο διαχείρισης των εμπιστευτικών πληροφοριών. Επικοινωνήστε με τη δική σας εταιρεία ή τον δικό σας οργανισμό σχετικά με τους τοπικούς κανόνες και πολιτικές.

Συνήθως, μια νέα ομάδα CSIRT θα πρέπει να εξαρτάται από τη συνεργασία του οργανισμού στον οποίο εντάσσεται, προκειμένου να ενημερωθεί για τους τοπικούς κανόνες, τις πολιτικές και άλλα νομικά ζητήματα.

Η εκτεταμένη περιγραφή του συνόλου του εξοπλισμού και των μέτρων ασφαλείας που θα απαιτηθούν δεν εμπίπτει στους σκοπούς του παρόντος εγγράφου. Εντούτοις, παρακάτω θα βρείτε έναν σύντομο κατάλογο των βασικών εγκαταστάσεων για την ομάδα CSIRT που θα δημιουργήσετε:

Γενικοί κανόνες για το κτίριο
- χρήση ελέγχων πρόσβασης,
- καταστήστε τουλάχιστον το γραφείο CSIRT προσβάσιμο αποκλειστικά για το προσωπικό της ομάδας CSIRT,
- παρακολουθείτε τα γραφεία και τις εισόδους με κάμερες,
- αρχειοθετείτε τις εμπιστευτικές πληροφορίες σε θυρίδες ή σε χρηματοκιβώτιο,
- χρησιμοποιείτε ασφαλή πληροφοριακά συστήματα.

Γενικοί κανόνες για τον πληροφοριακό εξοπλισμό
- μπορεί να υποστηρίξει το προσωπικό,
- θωρακίζετε όλα τα συστήματα,
- επιδιορθώνετε και ενημερώνετε όλα τα συστήματά σας προτού τα συνδέσετε στο Διαδίκτυο,
- χρησιμοποιείτε λογισμικό ασφαλείας (τείχη προστασίας, πολλαπλά αντιβιοτικά προγράμματα, προγράμματα εντοπισμού λογισμικού υποκλοπής).

Διατηρείτε διαύλους επικοινωνίας
- δημόσιος ιστότοπος,
- κλειστή περιοχή μελών στον ιστότοπο,
- ηλεκτρονικά έντυπα αναφοράς περιστατικών,
- ηλεκτρονικό ταχυδρομείο (υποστήριξη PGP/GPG/S/MIME),
- λογισμικό λίστας αλληλογραφίας,
- έχετε διαθέσιμη μια αποκλειστική γραμμή τηλεφώνου για την κοινότητα αποδεκτών:
  - τηλέφωνο
  - φαξ
  - SMS.

Σύστημα(τα) εντοπισμού μητρώου
- βάση δεδομένων επαφών με στοιχεία για τα μέλη της ομάδας, άλλες ομάδες κ.λπ.,
- εργαλεία,
- σύστημα διαχείρισης κλήσεων για περιστατικά.

Χρησιμοποιείτε το "εταιρικό στιλ" από την αρχή για:
- συνήθη διάταξη των μηνυμάτων ηλεκτρονικού ταχυδρομείου και των συμβουλευτικών δελτίων,
- ''αναχρονιστικές'' έντυπες επιστολές,
- μηνιαίες ή ετήσιες αναφορές,
- δελτίο αναφοράς περιστατικών.

Άλλα ζητήματα
- προβλέπετε την επικοινωνία εκτός ζώνης σε περίπτωση επιθέσεων,
- δυνατότητα σύνδεσης στο Διαδίκτυο.

Για περισσότερες πληροφορίες σχετικά με συγκεκριμένα εργαλεία CSIRT ανατρέξτε στο κεφάλαιο *8.5 Διαθέσιμα εργαλεία CSIRT.*

6.5 Αναπτύσσοντας μια πολιτική ασφάλειας πληροφοριών

Ανάλογα με το είδος της ομάδας CSIRT, θα έχετε μια προσαρμοσμένη πολιτική ασφάλειας πληροφοριών. Εκτός από την περιγραφή της επιθυμητής κατάστασης των λειτουργικών και διοικητικών διεργασιών και διαδικασιών, η εν λόγω πολιτική θα πρέπει να ευθυγραμμίζεται με τη νομοθεσία και τα πρότυπα, ιδιαίτερα ως προς την ευθύνη της ομάδας CSIRT. Η ομάδα CSIRT συνήθως δεσμεύεται από εθνικούς νόμους και κανονισμούς, οι οποίοι συχνά εφαρμόζονται στα πλαίσια της ευρωπαϊκής νομοθεσίας (συνήθως κοινοτικές οδηγίες) και άλλων διεθνών συμφωνιών. Τα πρότυπα δεν είναι απαραιτήτως δεσμευτικά με άμεσο τρόπο, αλλά μπορεί να επιβάλλονται ή να συνιστώνται από νόμους και κανονισμούς.

Ακολουθεί ένας σύντομος κατάλογος πιθανών νόμων και πολιτικών:

Εθνική νομοθεσία
- διάφοροι νόμοι περί τεχνολογίας των πληροφοριών, τηλεπικοινωνιών και μέσων ενημέρωσης,
- νόμοι περί προστασίας δεδομένων και ιδιωτικότητας,
- νόμοι και κανονισμοί περί διατήρησης δεδομένων,
- νομοθεσία για οικονομικά ζητήματα, λογιστικά ζητήματα και ζητήματα εταιρικής διαχείρισης,
- κώδικες δεοντολογίας για εταιρική διακυβέρνηση και διαχείριση πληροφοριακών συστημάτων.

Ευρωπαϊκή νομοθεσία
- οδηγία περί ηλεκτρονικών υπογραφών (1993/93/ΕΕ),
- οδηγίες περί προστασίας δεδομένων (1995/46/ΕΕ) και ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες (2002/58/ΕΕ),
- οδηγίες περί ηλεκτρονικών επικοινωνιακών δικτύων και υπηρεσιών (2002/19/ΕΕ - 2002/22/ΕΕ),
- οδηγίες περί εταιρικού νόμου (π.χ. 8η οδηγία περί εταιρικού νόμου).

Διεθνής νομοθεσία
- Συμφωνία Βασιλείας ΙΙ (ιδιαίτερα αναφορικά με τη διαχείριση του λειτουργικού κινδύνου),
- Σύμβαση του Συμβουλίου της Ευρώπης για το Ηλεκτρονικό Έγκλημα,
- Σύμβαση Ανθρωπίνων Δικαιωμάτων του Συμβουλίου της Ευρώπης (άρθρο 8 περί ιδιωτικότητας),
- Διεθνή Λογιστικά Πρότυπα (IAS, προβλέπουν ως ένα βαθμό ελέγχους πληροφοριακών συστημάτων).

Πρότυπα
- Βρετανικό Πρότυπο BS 7799 (Ασφάλεια Πληροφοριών),
- Διεθνή Πρότυπα ISO2700x (Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών),
- Γερμανικό IT-Grundschutzbuch, Γαλλικό EBIOS και άλλες εθνικές εκδοχές.

Για να διαπιστώσετε εάν η ομάδα CSIRT που δημιουργήσατε ενεργεί σύμφωνα με την εθνική και τη διεθνή νομοθεσία, συμβουλευτείτε τον νομικό σας σύμβουλο.

Τα πιο βασικά ερωτήματα που πρέπει να απαντηθούν στις πολιτικές διαχείρισης πληροφοριών που θα υιοθετήσετε είναι τα εξής:

- Πώς "επισημαίνεται" ή "ταξινομείται" η εισερχόμενη πληροφορία;
- Πώς αντιμετωπίζεται η πληροφορία και ιδιαίτερα ως προς την αποκλειστικότητα;
- Ποιες προσεγγίσεις υιοθετούνται για την δημοσιοποίηση πληροφοριών, ιδιαίτερα εάν μεταβιβάζονται πληροφορίες σχετικά με περιστατικά σε άλλες ομάδες ή ιστοτόπους;
- Υπάρχουν νομικά ζητήματα που πρέπει να ληφθούν υπόψη σε σχέση με τη διαχείριση πληροφοριών;
- Εφαρμόζετε πολιτική για τη χρήση κρυπτογραφίας, προκειμένου να προστατεύεται η αποκλειστικότητα και ακεραιότητα κατά τη μεταβίβαση αρχείων ή/και δεδομένων και ιδιαίτερα μέσω ηλεκτρονικού ταχυδρομείου;
- Περιλαμβάνει η εν λόγω πολιτική πιθανές περιπτώσεις νομικών περιορισμών, όπως εγγύηση κλειδιού ή δυνατότητα εφαρμογής αποκρυπτογράφησης σε περίπτωση μηνύσεων;

Εικονική ομάδα CSIRT (βήμα 5)

Εξοπλισμός και τοποθεσία γραφείου

Εξαιτίας του γεγονότος ότι η εταιρεία διαθέτει ήδη επαρκή υλική ασφάλεια στο χώρο, η νέα ομάδα CSIRT είναι απολύτως καλυμμένη από αυτή την άποψη. Παρέχεται μια αποκαλούμενη “αίθουσα μάχης”, ώστε να διευκολύνεται ο συντονισμός σε περίπτωση έκτακτου περιστατικού. Αγοράζεται ένα χρηματοκιβώτιο για το υλικό κρυπτογράφησης και τα ευαίσθητα έγγραφα. Εγκαταστάθηκε ξεχωριστή τηλεφωνική γραμμή συμπεριλαμβανομένου ενός κεντρικού πίνακα για τη διευκόλυνση της γραμμής επικοινωνίας κατά τις ώρες γραφείου και τη βάρδια "κατόπιν κλήσης" σε κινητό τηλέφωνο εκτός ωρών γραφείου με τον ίδιο τηλεφωνικό αριθμό.

Μπορεί επίσης να χρησιμοποιηθεί ο υφιστάμενος εξοπλισμός και ο εταιρικός ιστότοπος για την ανακοίνωση πληροφοριών σχετικά με την ομάδα CSIRT. Έχει εγκατασταθεί και διατηρείται μια λίστα αλληλογραφίας με μια ενότητα περιορισμένης πρόσβασης για την επικοινωνία μεταξύ των μελών της ομάδας και άλλες ομάδες. Όλα τα στοιχεία επικοινωνίας των μελών του προσωπικού έχουν αποθηκευθεί σε μια βάση δεδομένων, ενώ μια εκτύπωσή τους φυλάσσεται στο χρηματοκιβώτιο.

Κανονισμός

Εξαιτίας του γεγονότος ότι η ομάδα CSIRT είναι ενσωματωμένη σε μια εταιρεία με υφιστάμενες πολιτικές ασφάλειας πληροφοριών, οι αντίστοιχες πολιτικές για την ομάδα CSIRT έχουν διαμορφωθεί με τη βοήθεια του νομικού συμβούλου της εταιρείας.

6.6 Αναζήτηση συνεργασίας μεταξύ άλλων ομάδων CSIRT και πιθανών εθνικών πρωτοβουλιών

Η ύπαρξη άλλων πρωτοβουλιών CSIRT και η έντονη ανάγκη για συνεργασία μεταξύ τους έχει ήδη αναφερθεί αρκετές φορές στο παρόν έγγραφο. Αποτελεί καλή πρακτική να επικοινωνήσετε με άλλες ομάδες CSIRT το συντομότερο δυνατό, ώστε να αποκτήσετε την απαραίτητη επαφή με τις κοινότητες CISRT. Συνήθως, οι άλλες ομάδες CSIRT είναι πολύ πρόθυμες να βοηθήσουν νεοδημιουργηθείσες ομάδες στο ξεκίνημά τους.

Ο *Κατάλογος δραστηριοτήτων CERT του ENISA στην Ευρώπη*[14] είναι ένα πολύ καλό σημείο αφετηρίας για την αναζήτηση άλλων ομάδων CSIRT στη χώρα ή εθνικών δραστηριοτήτων συντονισμού CSIRT.

Εάν χρειάζεσθε υποστήριξη για την εύρεση της κατάλληλης πηγής πληροφοριών CSIRT, επικοινωνήστε με τους ειδικούς CSIRT του ENISA στη διεύθυνση:

CERT-Relations@enisa.europa.eu

Ακολουθεί επισκόπηση των δραστηριοτήτων της κοινότητας CSIRT. Ανατρέξτε στον *Κατάλογο* για μια πληρέστερη περιγραφή και περαιτέρω πληροφορίες.

Ευρωπαϊκή πρωτοβουλία CSIRT

TF-CSIRT[15]
Η Ειδική Ομάδα TF-CSIRT προωθεί τη συνεργασία μεταξύ Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές (CSIRT) στην Ευρώπη. Κύριοι στόχοι της εν λόγω Ειδικής Ομάδας είναι η παροχή ενός φόρουμ για την ανταλλαγή εμπειριών και γνώσης, η παροχή πιλοτικών υπηρεσιών για την ευρωπαϊκή κοινότητα CSIRT και η παροχή βοήθειας για τη δημιουργία νέων ομάδων CSIRT.

Οι κύριοι στόχοι της Ειδικής Ομάδας είναι οι εξής:
- παροχή ενός φόρουμ για την ανταλλαγή εμπειριών και γνώσης,
- παροχή πιλοτικών υπηρεσιών για την ευρωπαϊκή κοινότητα CSIRT,
- προώθηση κοινών προτύπων και διαδικασιών για την αντιμετώπιση περιστατικών ασφαλείας,
- παροχή βοήθειας στη δημιουργία νέων ομάδων CSIRT και την εκπαίδευση του προσωπικού των ομάδων CSIRT,
- οι δραστηριότητες της TF-CSIRT εστιάζουν στην Ευρώπη και τις χώρες, σύμφωνα με το Καταστατικό που εγκρίθηκε από την Τεχνική Επιτροπή TERENA στις 15 Σεπτεμβρίου 2004.

Παγκόσμια πρωτοβουλία CSIRT

FIRST[16]
Ο FIRST είναι ο παλαιότερος οργανισμός και αναγνωρισμένος παγκόσμιος ηγέτης στην αντιμετώπιση περιστατικών. Η συμμετοχή στον FIRST με την ιδιότητα του μέλους επιτρέπει στις ομάδες αντιμετώπισης περιστατικών να ανταποκρίνονται αποτελεσματικότερα σε περιστατικά απόκρισης - τόσο με υπηρεσίες αντίδρασης όσο και με υπηρεσίες πρόληψης.

Ο FIRST συγκεντρώνει μια πληθώρα ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές από κυβερνητικούς, εμπορικούς και εκπαιδευτικούς οργανισμούς. Ο FIRST στοχεύει στην ενίσχυση της συνεργασίας και του συντονισμού για την πρόληψη

[14] Κατάλογος ENISA: http://www.enisa.europa.eu/cert_inventory/

[15] TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

[16] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

περιστατικών, την τόνωση της ταχείας αντίδρασης σε περιστατικά και την προώθηση της ανταλλαγής πληροφοριών μεταξύ των μελών και της κοινότητας γενικότερα.

Εκτός από το κλειστό δίκτυο που δημιουργεί ο FIRST στην παγκόσμια κοινότητα αντιμετώπισης περιστατικών, παρέχει και υπηρεσίες προστιθέμενης αξίας.

Εικονική ομάδα CSIRT (βήμα 6)
Αναζήτηση συνεργασίας Χρησιμοποιώντας τον Κατάλογο του ENISA βρέθηκαν γρήγορα ορισμένες ομάδες CSIRT στην ίδια χώρα και πραγματοποιήθηκε επικοινωνία μαζί τους. Προγραμματίσθηκε μια επιτόπια επίσκεψη σε μια από αυτές από τον νεοπροσληφθέντα επικεφαλής της ομάδας. Έμαθε για τις εθνικές δραστηριότητες CSIRT και παρακολούθησε μια συνάντηση. Η συνάντηση ήταν κάτι παραπάνω από χρήσιμη για τη συλλογή παραδειγμάτων μεθόδων εργασίας και την εξασφάλιση υποστήριξης από άλλες ομάδες.

7 Προωθώντας το Επιχειρηματικό Σχέδιο

Πραγματοποιήσαμε τα εξής βήματα μέχρι στιγμής:

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί να προσφέρει.
2. Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;
3. Τι είδους υπηρεσίες μπορεί να προσφέρει μια ομάδα CSIRT στην κοινότητα αποδεκτών της;
4. Ανάλυση του περιβάλλοντος και των αποδεκτών.
5. Καθορισμός της δήλωσης αποστολής.
6. Ανάπτυξη του Επιχειρηματικού Σχεδίου
    α. Καθορισμός του οικονομικού μοντέλου
    β. Καθορισμός της οργανωτικής δομής
    γ. Έναρξη πρόσληψης προσωπικού
    δ. Χρήση και εξοπλισμός γραφείου
    ε. Αναπτύσσοντας μια πολιτική ασφάλειας πληροφοριών
    στ. Αναζήτηση εταίρων συνεργασίας.

>> Το επόμενο βήμα είναι να ενσωματωθούν τα παραπάνω σε ένα σχέδιο έργου και να ξεκινήσετε!

Μια καλή αρχή για τον καθορισμό του έργου σας είναι να σκεφθείτε μια επιχειρηματική πρακτική. Η εν λόγω επιχειρηματική πρακτική θα χρησιμοποιηθεί ως βάση για το σχέδιο έργου και θα χρησιμοποιηθεί επίσης για τη διοικητική υποστήριξη και την εξασφάλιση κονδυλίων ή άλλων πόρων.

Αποδείχθηκε χρήσιμη η συνεχής αναφορά στη διοίκηση, προκειμένου να διατηρείται υψηλή ευαισθητοποίηση για προβλήματα ασφάλειας πληροφοριακών συστημάτων και κατ' αυτόν τον τρόπο για τη συνεχή υποστήριξη της ίδιας της ομάδας CSIRT.

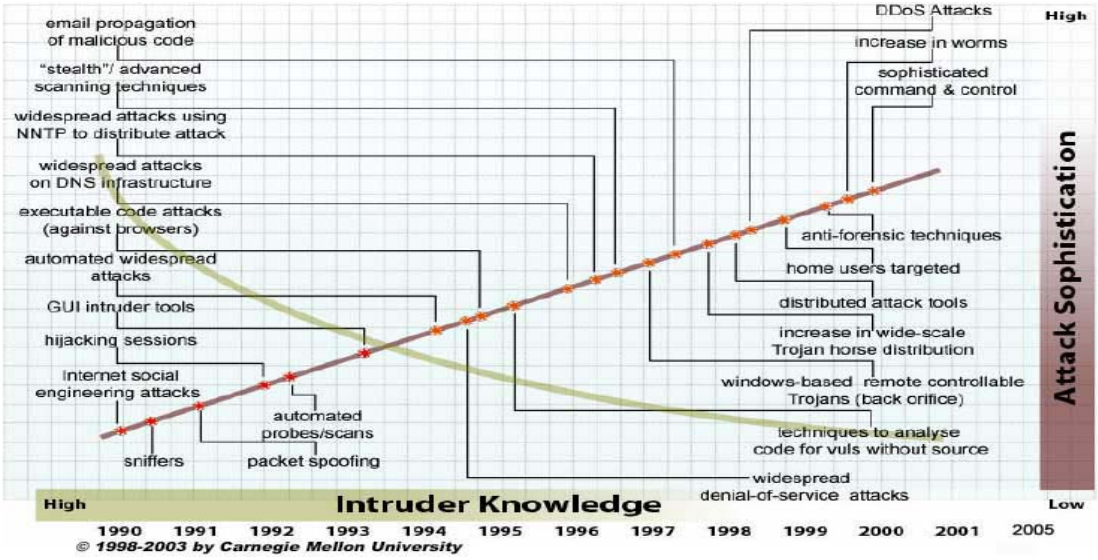
Η δημιουργία μιας επιχειρηματικής πρακτικής ξεκινά με την ανάλυση των προβλημάτων και των ευκαιριών χρησιμοποιώντας ένα μοντέλο ανάλυσης, όπως περιγράφεται στο κεφάλαιο *5.3 Ανάλυση της κοινότητας αποδεκτών*, και την επιδίωξη στενής επαφής με την πιθανή κοινότητα αποδεκτών.

Όπως περιγράφηκε προηγουμένως, υπάρχουν πολλά που πρέπει να σκεφθεί κανείς όταν ξεκινά μια ομάδα CSIRT. Είναι καλύτερα να προσαρμόσετε το προαναφερόμενο υλικό στις ανάγκες της ομάδας CSIRT καθώς αναδύονται.

Αποτελεί καλή πρακτική, όταν συντάσσετε αναφορά προς τη διοίκηση, να ενημερώνετε όσο το δυνατόν περισσότερο την πρότασή σας, χρησιμοποιώντας πρόσφατα άρθρα από εφημερίδες ή το Διαδίκτυο και να εξηγείτε τους λόγους για τους οποίους η υπηρεσία CSIRT και ο διεθνής συντονισμός περιστατικών είναι ζωτικά για τη διασφάλιση των πόρων της επιχείρησης. Είναι επίσης απαραίτητο να αποσαφηνίσετε ότι μόνο η συνεχής υποστήριξη σε θέματα ασφάλειας πληροφοριακών συστημάτων οδηγεί σε μια σταθερή επιχείρηση, ιδιαίτερα εάν πρόκειται για εταιρεία ή οργανισμό που εξαρτάται από τα πληροφοριακά συστήματα.

(Μια χαρακτηριστική φράση του Bruce Schneier επισημαίνει ακριβώς αυτό: *"Η ασφάλεια δεν είναι προϊόν, αλλά διαδικασία*[17]*!")*.

Ένα διάσημο εργαλείο για την απεικόνιση των προβλημάτων ασφαλείας είναι το παρακάτω γράφημα του CERT/CC:



Σχήμα 8 Γνώση εισβολέα έναντι υψηλής τεχνολογίας επίθεσης (πηγή CERT-CC[18]*)*

Οπτικοποιεί τις τάσεις στην ασφάλεια πληροφοριακών συστημάτων, ιδιαίτερα τη μείωση στις απαραίτητες δεξιότητες για την πραγματοποίηση ολοένα και πιο εξεζητημένων επιθέσεων.

Άλλο ένα σημείο που θα πρέπει να αναφερθεί είναι το ολοένα και μικρότερο χρονικό περιθώριο μεταξύ της διαθεσιμότητας ενημερώσεων λογισμικού για αποκατάσταση αδυναμιών και της έναρξης επιθέσεων εναντίον τους:

Πρόγραμμα προσωρινής διόρθωσης -> Αξιοποίηση		**Ρυθμός εξάπλωσης**	
Nimda:	11 μήνες	Code red:	Ημέρες
Slammer:	6 μήνες	Nimda:	Ώρες
Nachi:	5 μήνες	Slammer:	Λεπτά
Blaster:	3 εβδομάδες		
Witty:	1 ημέρα (!)		

Η συλλογή δεδομένων για περιστατικά, πιθανές βελτιώσεις και διδάγματα της εμπειρίας οδηγεί επίσης σε μια καλή παρουσίαση.

[17] Bruce Schneier: http://www.schneier.com/

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

7.1 Περιγραφή επιχειρηματικών σχεδίων και εναυσμάτων διαχείρισης

Μια παρουσίαση για τη διοίκηση που περιλαμβάνει αποκλειστικά την προώθηση της ομάδας CSIRT δεν αποτελεί επιχειρηματική πρακτική, αλλά εάν πραγματοποιείται με τον κατάλληλο τρόπο θα οδηγήσει σε υποστήριξη της ομάδας CSIRT από την πλευρά της διοίκησης στις περισσότερες περιπτώσεις. Από την άλλη πλευρά, η επιχειρηματική πρακτική δεν θα πρέπει να εκλαμβάνεται απλώς ως μια αναφορά προς τη διοίκηση, αλλά θα πρέπει να χρησιμοποιείται και για την επικοινωνία με την ομάδα και την κοινότητα αποδεκτών. Ο όρος επιχειρηματική πρακτική μπορεί να ακούγεται πολύ εμπορικός και ξένος για την καθημερινή πρακτική μιας ομάδας CSIRT, αλλά παρέχει καλή εστίαση και κατεύθυνση κατά τη δημιουργία μιας ομάδας CSIRT.

Οι απαντήσεις στα παρακάτω ερωτήματα μπορούν να χρησιμοποιηθούν για τον σχεδιασμό μιας καλής επιχειρηματικής πρακτικής. (Τα παραδείγματα που παρέχονται είναι υποθετικά και χρησιμοποιούνται αποκλειστικά ως επεξήγηση. Οι "πραγματικές" απαντήσεις εξαρτώνται σε μεγάλο βαθμό από τις "πραγματικές" συνθήκες).

- Ποιο είναι το πρόβλημα;
- Τι θέλετε να επιτύχετε με τους αποδέκτες σας;
- Τι θα συμβεί εάν δεν κάνετε τίποτε;
- Τι θα συμβεί εάν αναλάβετε δράση;
- Πόσο θα κοστίσει;
- Ποιο θα είναι το όφελος;
- Πότε ξεκινάτε και πότε ολοκληρώνετε;

Ποιο είναι το πρόβλημα;
Στις περισσότερες περιπτώσεις η ιδέα για τη δημιουργία μιας ομάδας CSIRT προκύπτει όταν η ασφάλεια πληροφοριακών συστημάτων έχει καταστεί ζωτικό τμήμα της βασικής επιχειρηματικής δραστηριότητας μιας εταιρείας ή ενός οργανισμού και όταν τα περιστατικά ασφάλειας πληροφοριακών συστημάτων αποτελούν επιχειρηματικό κίνδυνο, καθιστώντας τον μετριασμό των κινδύνων ασφαλείας μια καθημερινή επιχειρηματική δραστηριότητα.

Η πλειονότητα των εταιρειών ή των οργανισμών διαθέτουν τμήμα τακτικής υποστήριξης ή υπηρεσία υποστήριξης, αλλά στις περισσότερες περιπτώσεις η αντιμετώπιση των περιστατικών ασφαλείας είναι ανεπαρκής και δεν είναι δομημένη με τον κατάλληλο τρόπο. Στις περισσότερες περιπτώσεις το εργασιακό πεδίο των περιστατικών ασφαλείας απαιτεί εξειδικευμένες δεξιότητες και προσοχή. Η υιοθέτηση μιας πιο δομημένης προσέγγισης είναι επίσης ωφέλιμη και θα μετριάσει τους επιχειρηματικούς κινδύνους και τη ζημία προς την εταιρεία.

Στις περισσότερες περιπτώσεις, το πρόβλημα είναι ότι υπάρχει έλλειψη συντονισμού και ότι η υφιστάμενη γνώση δεν χρησιμοποιείται για την αντιμετώπιση περιστατικών που θα απέτρεπε την εμφάνισή τους στο μέλλον και θα απέτρεπε πιθανές οικονομικές απώλειες ή/και τυχόν ζημία για τη φήμη του οργανισμού.

Ποιοι είναι οι στόχοι που πρόκειται να επιτευχθούν με την κοινότητα αποδεκτών;
Όπως εξηγήθηκε νωρίτερα, η ομάδα CSIRT που δημιουργήσατε θα εξυπηρετεί τους αποδέκτες της και θα τους βοηθά στην επίλυση περιστατικών ασφάλειας πληροφοριακών συστημάτων και προβλημάτων. Η άνοδος του επιπέδου γνώσης για την ασφάλεια των πληροφοριακών συστημάτων και η διαμόρφωση μιας φιλοσοφίας ευαισθητοποίησης για την ασφάλεια είναι επιπρόσθετοι στόχοι.

Η εν λόγω φιλοσοφία υποστηρίζει τα προστατευτικά και προληπτικά μέτρα που λαμβάνονται εξαρχής, μειώνοντας κατ' αυτόν τον τρόπο τις λειτουργικές δαπάνες.

Η υιοθέτηση αυτής της φιλοσοφίας συνεργασίας και υποστήριξης σε μια εταιρεία ή έναν οργανισμό μπορεί στις περισσότερες περιπτώσεις να τονώσει γενικά την αποτελεσματικότητα.

Τι θα συμβεί εάν δεν κάνετε τίποτε;
Ένας μη δομημένος τρόπος αντιμετώπισης της ασφάλειας πληροφοριακών συστημάτων μπορεί να οδηγήσει σε περαιτέρω ζημία, και αυτό όχι μόνο για τη φήμη του οργανισμού. Οι οικονομικές απώλειες και οι νομικές συνέπειες μπορεί να είναι άλλα αποτελέσματα.

Τι θα συμβεί εάν αναλάβετε δράση;
Η ευαισθητοποίηση σχετικά με την εμφάνιση προβλημάτων ασφαλείας αυξάνεται. Αυτό βοηθά στην πιο αποτελεσματική επίλυσή τους και την αποφυγή μελλοντικών απωλειών.

Πόσο θα κοστίσει;
Ανάλογα με το οργανωτικό μοντέλο, θα κοστίσει τους μισθούς των μελών της ομάδας CSIRT και τις δαπάνες για την οργάνωση, τον εξοπλισμό, τα εργαλεία και τις άδειες λογισμικού.

Ποιο θα είναι το όφελος;
Ανάλογα με την επιχείρηση και τις απώλειες κατά το παρελθόν, το όφελος θα είναι η μεγαλύτερη διαφάνεια στις διαδικασίες και τις πρακτικές ασφαλείας, προστατεύοντας επομένως ουσιαστικούς πόρους της επιχείρησης.

Ποιο είναι το χρονοδιάγραμμα;
Βλέπε κεφάλαιο *12. Περιγραφή του Σχεδίου έργου* για την περιγραφή ενός υποδείγματος σχεδίου έργου.

Παραδείγματα υφιστάμενων επιχειρηματικών πρακτικών και προσεγγίσεων
Ιδού ορισμένα παραδείγματα επιχειρηματικών πρακτικών CSIRT που αξίζει τον κόπο να μελετηθούν:

- http://www.cert.org/csirts/AFI_case-study.html
  Creating a Financial Institution CSIRT: A Case Study

  Σκοπός του παρόντος εγγράφου είναι να παρουσιασθούν τα διδάγματα της εμπειρίας που αποκόμισε ένας οικονομικός οργανισμός (αναφέρεται στο παρόν έγγραφο ως AFI) καθώς ανέπτυξε και εφάρμοσε σχέδιο αντιμετώπισης προβλημάτων ασφαλείας και μια Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές (CSIRT).

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Σύνοψη της επιχειρηματικής πρακτικής της CERT POLSKA (παρουσίαση διαφανειών σε μορφή PDF).

- http://www.auscert.org.au/render.html?it=2252
  Η δημιουργία μιας Ομάδας Αντιμετώπισης Περιστατικών (IRT) κατά τη δεκαετία του 1990 μπορεί να είναι μια πρόκληση. Αρκετοί άνθρωποι που δημιουργούν μια ομάδα IRT δεν έχουν καθόλου σχετική εμπειρία. Το παρόν άρθρο εξετάζει το ρόλο που μπορεί να διαδραματίσει μια ομάδα IRT στην κοινότητα και τα ζητήματα που θα πρέπει να ληφθούν υπόψη τόσο κατά τη δημιουργία όσο και μετά την έναρξη των λειτουργιών. Μπορεί να είναι επωφελές για τις υφιστάμενες ομάδες IRT, καθώς μπορεί να αυξηθεί η ευαισθητοποίηση για ζητήματα τα οποία δεν έχουν ληφθεί υπόψη στο παρελθόν.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Περιπτωσιολογική Μελέτη στην Ασφάλεια Πληροφοριών, Ασφαλίζοντας την Εταιρεία, του Roger Benton

  Αυτή η πρακτική είναι μια περιπτωσιολογική μελέτη μεταπήδησης μιας Ασφαλιστικής Εταιρείας σε ένα εταιρικό σύστημα ασφαλείας. Σκοπός αυτής της πρακτικής είναι να παρουσιαστεί μια οδός που μπορεί να ακολουθήσει κανείς όταν δημιουργεί ή μεταπηδά σε ένα σύστημα ασφαλείας. Αρχικά, ένα πρωτόγονα δικτυακό σύστημα ασφαλείας ήταν ο μοναδικός μηχανισμός ελέγχου της πρόσβασης στα εταιρικά δεδομένα. Η έκθεση στους κινδύνους ήταν σημαντική - δεν υπήρχαν έλεγχοι ακεραιότητας εκτός του δικτυακού περιβάλλοντος. Οποιοσδήποτε με βασικές γνώσεις προγραμματισμού μπορούσε να προσθέσει, να αλλάξει ή/και να διαγράψει δεδομένα παραγωγής.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Η στρατηγική ηλεκτρονικής ασφάλειας του Marriott: συνεργασία επιχείρησης και πληροφοριακών συστημάτων

  Κατά την εμπειρία του Chris Zoladz του Marriott International, Inc., η ασφάλεια ηλεκτρονικών συναλλαγών είναι μια διαδικασία και όχι ένα έργο. Αυτό ήταν το μήνυμα που έδωσε ο Zoladz στο πρόσφατο Συνέδριο και Έκθεση Ηλεκτρονικής Ασφάλειας στη Βοστόνη με τη χορηγία του Ομίλου Intermedia. Ως αντιπρόεδρος προστασίας πληροφοριών του Marriott, ο Zoladz αναφέρεται στο νομικό τμήμα, παρόλο που δεν είναι δικηγόρος. Η αρμοδιότητά του είναι να εντοπίζει πού είναι αποθηκευμένες οι πιο πολύτιμες επιχειρηματικές πληροφορίες του Marriott και πώς μεταφέρονται εντός και εκτός της εταιρείας. Το Marriott έχει ορίσει ξεχωριστές αρμοδιότητες για την τεχνική υποδομή που υποστηρίζει την ασφάλεια, αρμοδιότητες οι οποίες ανατίθενται στον αρχιτέκτονα της ασφάλειας πληροφοριακών συστημάτων.

Εικονική ομάδα CSIRT (βήμα 7)

Προωθώντας το Επιχειρηματικό Σχέδιο

Αποφασίστηκε να συλλεχθούν δεδομένα και αριθμητικά στοιχεία από το ιστορικό της εταιρείας. Αυτό είναι κάτι παραπάνω από χρήσιμο για μια στατιστική επισκόπηση της κατάστασης της ασφάλειας των πληροφοριακών συστημάτων. Η εν λόγω συλλογή δεδομένων θα πρέπει να συνεχιστεί όταν έχει ολοκληρωθεί η δημιουργία και έχει ξεκινήσει η λειτουργία της ομάδας CSIRT, ώστε να ενημερώνονται τα στατιστικά στοιχεία.

Πραγματοποιήθηκε επικοινωνία και συνεντεύξεις με άλλες εθνικές ομάδες CSIRT σχετικά με τις επιχειρηματικές τους πρακτικές. Παρείχαν υποστήριξη συγκεντρώνοντας μερικές διαφάνειες με στοιχεία σχετικά με τις πρόσφατες εξελίξεις στα περιστατικά ασφαλείας των πληροφοριακών συστημάτων και τις δαπάνες των περιστατικών.

Σε αυτό το παράδειγμα πρακτικής της Εικονικής Ομάδας CSIRT δεν υπήρχε πιεστική ανάγκη να πεισθεί η διοίκηση για τη σημασία των πληροφοριακών συστημάτων και επομένως δεν ήταν δύσκολο να ληφθεί η έγκριση για το πρώτο βήμα. Ετοιμάστηκε η επιχειρηματική πρακτική και το σχέδιο έργου, συμπεριλαμβανομένης μιας εκτίμησης των δαπανών έναρξης και του κόστους λειτουργίας.

8 Παραδείγματα λειτουργικών και τεχνικών διαδικασιών (ροές εργασιών)

Πραγματοποιήσαμε τα εξής βήματα μέχρι στιγμής:

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί να προσφέρει.
2. Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;
3. Τι είδους υπηρεσίες μπορεί να προσφέρει μια ομάδα CSIRT στην κοινότητα αποδεκτών της.
4. Ανάλυση του περιβάλλοντος και των αποδεκτών.
5. Καθορισμός της δήλωσης αποστολής.
6. Αναπτύσσοντας το Επιχειρηματικό Σχέδιο
   α. Καθορίζοντας το οικονομικό μοντέλο
   β. Καθορισμός της οργανωτικής δομής
   γ. Έναρξη πρόσληψης προσωπικού
   δ. Χρήση και εξοπλισμός γραφείου
   ε. Αναπτύσσοντας μια πολιτική ασφάλειας πληροφοριών
   στ. Αναζήτηση εταίρων συνεργασίας.
7. Προωθώντας το Επιχειρηματικό Σχέδιο
   α. Έγκριση επιχειρηματικής πρακτικής
   β. Ενσωμάτωση όλων των στοιχείων σε ένα σχέδιο έργου.

>> Το επόμενο βήμα είναι: να καταστεί λειτουργική η ομάδα CSIRT.

Ο προσδιορισμός των ροών εργασίας θα βελτιώσει την ποιότητα και τον απαιτούμενο χρόνο ανά περιστατικό ή περίπτωση αδυναμίας.

Όπως περιγράφηκε στα πλαίσια των παραδειγμάτων, η Εικονική Ομάδα CSIRT θα προσφέρει τις βασικές υπηρεσίες CSIRT:

- συναγερμοί και προειδοποιήσεις,
- αντιμετώπιση περιστατικών,
- ανακοινώσεις.

Το παρόν κεφάλαιο παρέχει παραδείγματα ροής εργασιών που περιγράφουν τις βασικές υπηρεσίες μιας ομάδας CSIRT. Το παρόν κεφάλαιο περιέχει επίσης στοιχεία για τη συλλογή πληροφοριών από διάφορες πηγές, ελέγχοντας τη συνάφεια και την αυθεντικότητά τους και αναδιανέμοντάς τις στην κοινότητα αποδεκτών. Και τέλος, το παρόν κεφάλαιο περιέχει παραδείγματα των πιο βασικών διαδικασιών και συγκεκριμένων εργαλείων CSIRT.

8.1 Εκτίμηση της βάσης εγκατάστασης της κοινότητας αποδεκτών

Το πρώτο βήμα είναι να πραγματοποιηθεί μια επισκόπηση των πληροφοριακών συστημάτων που είναι εγκατεστημένα στην κοινότητα αποδεκτών σας. Κατ' αυτόν τον τρόπο η ομάδα CSIRT μπορεί να αξιολογήσει τη συνάφεια των εισερχόμενων πληροφοριών και να τις φιλτράρει πριν από την αναδιανομή τους, ώστε οι αποδέκτες να μη δεχθούν έναν καταιγισμό πληροφοριών που ουσιαστικά είναι άχρηστες γι' αυτούς.

Αποτελεί καλή πρακτική να ξεκινήσετε απλά, για παράδειγμα χρησιμοποιώντας ένα φύλλο Excel όπως το παρακάτω:

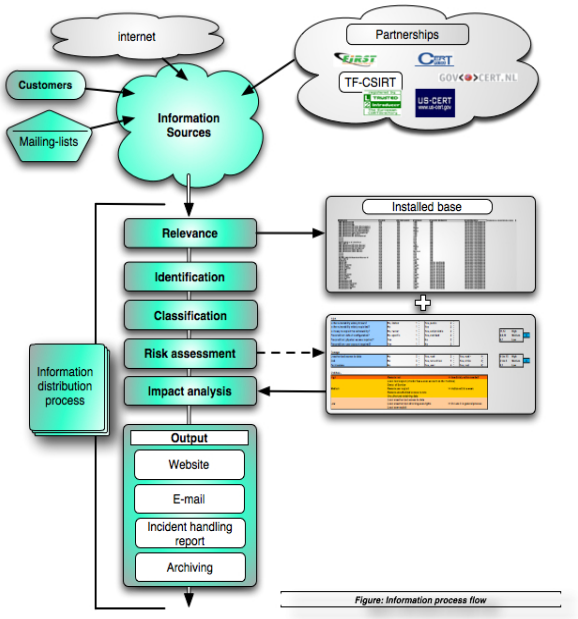
Κατηγορία	Εφαρμογή	Προϊόν λογισμικού	Έκδοση	Λειτουργικό σύστημα	Λειτουργικό σύστημα & έκδοση	Αποδέκτης
Επιφάνεια εργασίας	Office	Excel	x-x-x	Microsoft	XP-prof	A
Επιφάνεια εργασίας	Πρόγραμμα περιήγησης	IE	x-x-	Microsoft	XP-prof	A
Δίκτυο	Δρομολογητής	CISCO	x-x-x	CISCO	x-x-x-	B
Διακομιστής	Διακομιστής	Linux	x-x-x	L-distro	x-x-x	B
Υπηρεσίες	Διακομιστής Ιστού	Apache		Unix	x-x-x	B

Με τη λειτουργία του φίλτρου στο Excel είναι πολύ εύκολο να επιλέξετε το κατάλληλο λογισμικό και να δείτε ποιος αποδέκτης χρησιμοποιεί ποιο λογισμικό.

8.2 Παραγωγή συναγερμών, προειδοποιήσεων και ανακοινώσεων

Η παραγωγή συναγερμών, προειδοποιήσεων και ανακοινώσεων ακολουθεί τις ίδιες ροές εργασιών:

- συλλογή πληροφοριών,
- εκτίμηση της συνάφειας και της πηγής των πληροφοριών,
- αξιολόγηση κινδύνου με βάση τις πληροφορίες που έχουν συλλεχθεί,
- διανομή των πληροφοριών.



Σχήμα 9 : Ροή επεξεργασίας πληροφοριών

Στις παρακάτω παραγράφους θα περιγραφεί αναλυτικότερα η εν λόγω ροή εργασιών.

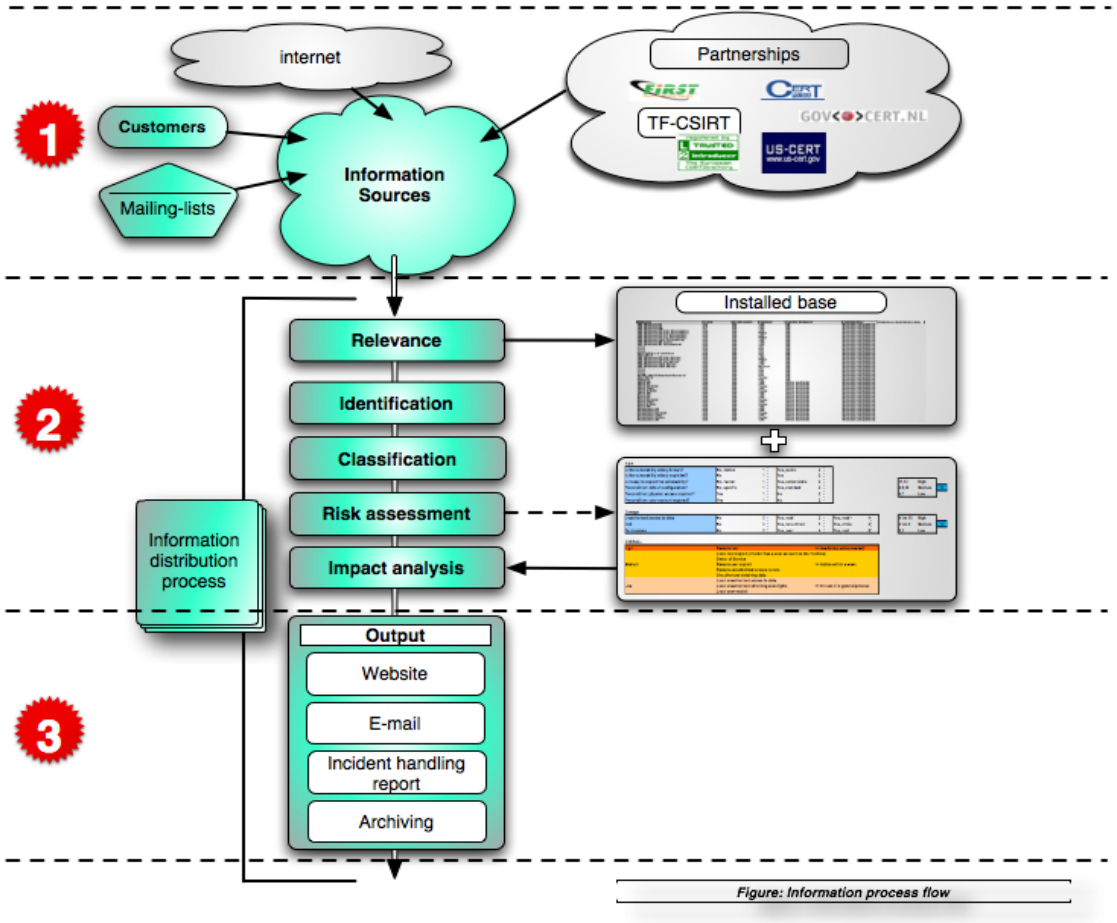


Figure: Information process flow

1 Βήμα 1: Συλλογή πληροφοριών σχετικά με την αδυναμία.

Συνήθως υπάρχουν δύο κύρια είδη πηγών πληροφοριών που παρέχουν πληροφορίες ως εισαγόμενο για τις υπηρεσίες:

- πληροφορίες σχετικά με αδυναμίες των πληροφοριακών (σας) συστημάτων,
- αναφορές περιστατικών.

Ανάλογα με το είδος της επιχείρησης και την πληροφοριακή υποδομή, υπάρχουν πολλές δημόσιες και κλειστές πηγές πληροφοριών σχετικά με αδυναμίες του συστήματος:

- δημόσιες και κλειστές λίστες αλληλογραφίας,
- πληροφορίες αδυναμιών προϊόντος του προμηθευτή,
- ιστότοποι,
- πληροφορίες στο Διαδίκτυο (Google κ.λπ.),
- δημόσιοι και ιδιωτικοί οργανισμοί που παρέχουν πληροφορίες σχετικά με αδυναμίες συστημάτων (FIRST, TF-CSIRT, CERT-CC, US-CERT κ.λπ.).

Όλες αυτές οι πληροφορίες συμβάλλουν στο επίπεδο γνώσης για συγκεκριμένες αδυναμίες πληροφοριακών συστημάτων.

Όπως προαναφέρθηκε, υπάρχουν διαθέσιμες πολλές καλές και εύκολα προσβάσιμες πηγές πληροφοριών ασφαλείας στο Διαδίκτυο. Η ad-hoc ομάδα εργασίας "Υπηρεσίες CERT" του ENISA εκδίδει κατά τη χρονική στιγμή σύνταξης του παρόντος έναν πιο ολοκληρωμένο κατάλογο για το 2006 που αναμένεται να διατεθεί στα τέλη του 2006[19].

Βήμα 2: Αξιολόγηση των πληροφοριών και εκτίμηση του κινδύνου

Το εν λόγω βήμα θα οδηγήσει σε μια ανάλυση του αντίκτυπου μιας συγκεκριμένης αδυναμίας στην πληροφοριακή υποδομή της κοινότητας αποδεκτών.

Αναγνώριση
Οι εισερχόμενες πληροφορίες αδυναμιών θα πρέπει πάντοτε να αναγνωρίζονται από την πηγή τους και θα πρέπει να αποφασίζεται εάν η πηγή είναι αξιόπιστη προτού παρασχεθεί οποιαδήποτε πληροφορία στην κοινότητα αποδεκτών. Σε διαφορετική περίπτωση μπορεί οι άνθρωποι να τεθούν εσφαλμένα σε επαγρύπνηση, με αποτέλεσμα, ενδεχομένως, άσκοπες ενοχλήσεις στις επιχειρηματικές διαδικασίες και τελικά να ζημιωθεί η φήμη της ομάδας CSIRT.

[19] Ad-hoc υπηρεσίες WG CERT: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Η παρακάτω διαδικασία παρουσιάζει ένα παράδειγμα αναγνώρισης της αυθεντικότητας ενός μηνύματος:

Διαδικασία για τον τρόπο αναγνώρισης της αυθεντικότητας ενός μηνύματος και της πηγής του

Γενικός Κατάλογος Ελέγχου
1. Είναι γνωστή η πηγή και καταχωρισμένη ως τέτοια;
2. Έρχονται οι πληροφορίες μέσω κανονικού διαύλου;
3. Περιλαμβάνονται "περίεργες" πληροφορίες που "φαίνονται" εσφαλμένες;
4. Ακολουθήστε το ένστικτό σας· εάν αμφιβάλλετε για μια πληροφορία μην προβείτε σε ενέργειες, αλλά επαληθεύστε την!

Πηγές ηλεκτρονικού ταχυδρομείου
1. Είναι γνωστή η πηγή στον οργανισμό και στον αρχικό κατάλογο;
2. Είναι σωστή η υπογραφή PGP;
3. Εάν αμφιβάλλετε, ελέγξτε την πλήρη κεφαλίδα ενός μηνύματος.
4. Εάν αμφιβάλλετε, χρησιμοποιήστε "nslookup" ή "dig" για να επαληθεύσετε τον τομέα των αποστολέων[20].

Διαδικτυακές πηγές
1. Ελέγξτε τα πιστοποιητικά του προγράμματος περιήγησης όταν συνδέεστε σε έναν ασφαλή ιστότοπο (https://).
2. Ελέγξτε την πηγή από πλευράς περιεχομένου και εγκυρότητας (τεχνικής).
3. Εάν έχετε αμφιβολία, μην κάνετε κλικ σε κανέναν σύνδεσμο ούτε μεταφορτώσετε οποιοδήποτε λογισμικό.
4. Εάν έχετε αμφιβολία, πραγματοποιήστε "lookup" και "dig" στον τομέα και κάνετε "traceroute".

Τηλέφωνο
1. Ακούστε προσεκτικά το όνομα.
2. Αναγνωρίζετε τη φωνή;
3. Εάν αμφιβάλλετε, ζητήστε έναν αριθμό τηλεφώνου και ζητήστε να καλέσετε ξανά το άτομο που σας κάλεσε.

Σχήμα 10 Παράδειγμα διαδικασίας αναγνώρισης πληροφοριών

Συνάφεια
Η επισκόπηση του εγκατεστημένου υλικού και λογισμικού που πραγματοποιήθηκε νωρίτερα μπορεί να χρησιμοποιηθεί για το φιλτράρισμα πληροφοριών των εισερχόμενων αδυναμιών ως προς τη συνάφεια, με στόχο να δοθούν απαντήσεις στα ερωτήματα: "Χρησιμοποιεί η κοινότητα αποδεκτών αυτό το λογισμικό;" ή "Είναι χρήσιμες οι πληροφορίες για τους αποδέκτες;"

Διαβάθμιση
Ορισμένες πληροφορίες που λαμβάνονται μπορεί να είναι διαβαθμισμένες ή να επισημαίνονται ως αποκλειστικές (για παράδειγμα, εισερχόμενες αναφορές

[20] Εργαλεία ελέγχου ταυτοτήτων στην CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

περιστατικών από άλλες ομάδες). Όλες οι πληροφορίες θα πρέπει να περνούν από διαχείριση σύμφωνα με τις απαιτήσεις του αποστολέα και σύμφωνα με την οικεία πολιτική ασφάλειας πληροφοριών. Ένας καλός βασικός κανόνας είναι "*Μη διανέμετε πληροφορίες εάν δεν είναι σαφές ότι διατίθενται προς διανομή. Εάν έχετε αμφιβολίες, ζητήστε άδεια από τον αποστολέα για κάτι τέτοιο.*"

Εκτίμηση κινδύνου & ανάλυση αντικτύπου
Υπάρχουν διάφορες μέθοδοι καθορισμού του κινδύνου και του αντικτύπου μιας (πιθανής) αδυναμίας.

Ως κίνδυνος ορίζεται η πιθανότητα εκμετάλλευσης της αδυναμίας. Υπάρχουν διάφοροι σημαντικοί παράγοντες (μεταξύ άλλων):

- Είναι γνωστή η αδυναμία;
- Είναι ευρέως διαδεδομένη η αδυναμία;
- Είναι εύκολο να εκμεταλλευτεί κάποιος την αδυναμία;
- Πρόκειται για αδυναμία που μπορεί κανείς να εκμεταλλευτεί εξ αποστάσεως;

Όλα αυτά τα ερωτήματα θα σας παρέχουν μια καλή εικόνα της σοβαρότητας της αδυναμίας.
Μια πολύ απλή προσέγγιση για να υπολογίσετε τον κίνδυνο είναι ο παρακάτω τύπος:

Αντίκτυπος = Κίνδυνος Χ Πιθανή ζημία

Η πιθανή ζημία θα μπορούσε να είναι

- μη εξουσιοδοτημένη πρόσβαση σε δεδομένα,
- άρνηση παροχής υπηρεσιών (DOS),
- απόκτηση αδειών.

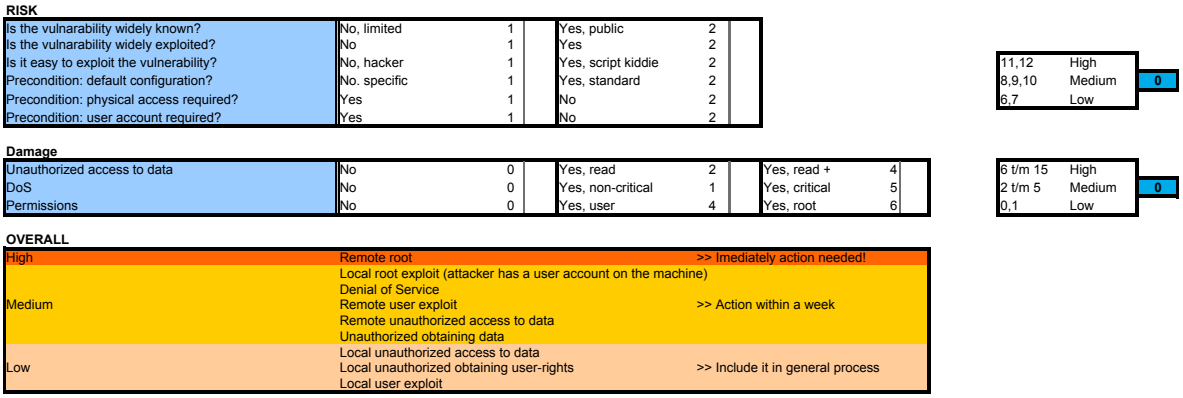
(Για πιο λεπτομερή πλαίσια ταξινόμησης ανατρέξτε στο τέλος του παρόντος κεφαλαίου).

Έχοντας απαντήσει σε αυτά τα ερωτήματα, μπορεί να προστεθεί μια συνολική εκτίμηση στο συμβουλευτικό, ενημερώνοντας για τον πιθανό κίνδυνο και την πιθανή ζημία. Συχνά χρησιμοποιούνται απλοί όροι όπως ΧΑΜΗΛΟΣ, ΜΕΤΡΙΟΣ και ΥΨΗΛΟΣ.

Άλλα πιο περίπλοκα πλαίσια συνολικής εκτίμησης κινδύνου είναι τα εξής:

Πλαίσιο εκτίμησης του GOVCERT.NL[21]
Η ολλανδική κυβερνητική ομάδα CSIRT GOVCERT.NL έχει αναπτύξει μια μήτρα για την εκτίμηση κινδύνου που αναπτύχθηκε κατά τη φάση έναρξης λειτουργίας του Govcert.nl και ανανεώνεται συνεχώς σύμφωνα με τις τελευταίες τάσεις.

[21] Μήτρα αδυναμιών: http://www.govcert.nl/download.html?f=33



RISK

Is the vulnarability widely known?	No, limited	1		Yes, public	2				
Is the vulnarability widely exploited?	No	1		Yes	2				
Is it easy to exploit the vulnerability?	No, hacker	1		Yes, script kiddie	2				
Precondition: default configuration?	No. specific	1		Yes, standard	2				
Precondition: physical access required?	Yes	1		No	2				
Precondition: user account required?	Yes	1		No	2				

11,12	High	0
8,9,10	Medium	
6,7	Low	

Damage

Unauthorized access to data	No	0		Yes, read	2		Yes, read +	4			
DoS	No	0		Yes, non-critical	1		Yes, critical	5			
Permissions	No	0		Yes, user	4		Yes, root	6			

6 t/m 15	High	0
2 t/m 5	Medium	
0,1	Low	

OVERALL

High	Remote root	>> Imediately action needed!
Medium	Local root exploit (attacker has a user account on the machine) Denial of Service Remote user exploit Remote unauthorized access to data Unauthorized obtaining data	>> Action within a week
Low	Local unauthorized access to data Local unauthorized obtaining user-rights Local user exploit	>> Include it in general process

Σχήμα 11 Το πλαίσιο εκτίμησης κινδύνου του GOVCERT.NL

Περιγραφή Κοινής Μορφής Συμβουλευτικού του EISPP[22]

Το Ευρωπαϊκό Πρόγραμμα Προώθησης της Ασφάλειας Πληροφοριών (EISPP) είναι ένα πρόγραμμα που συγχρηματοδοτείται από την Ευρωπαϊκή Κοινότητα μέσω του Πέμπτου Προγράμματος-Πλαισίου. Το πρόγραμμα EISPP στοχεύει στην ανάπτυξη ενός ευρωπαϊκού πλαισίου, όχι μόνο για την ανταλλαγή γνώσεων σε θέματα ασφαλείας, αλλά και για τον καθορισμό του περιεχομένου και των τρόπων διάχυσης πληροφοριών ασφαλείας σε ΜΜΕ. Παρέχοντας στις ευρωπαϊκές ΜΜΕ τις απαραίτητες υπηρεσίες ασφάλειας πληροφοριακών συστημάτων, θα ενθαρρυνθεί η ανάπτυξη της εμπιστοσύνης τους και της χρήσης υπηρεσιών ηλεκτρονικού εμπορίου, οδηγώντας σε αυξημένες και καλύτερες ευκαιρίες για νέες επιχειρήσεις. Το EISPP είναι ένα πρωτοποριακό όραμα της Ευρωπαϊκής Επιτροπής για τη δημιουργία ενός ευρωπαϊκού δικτύου εξειδίκευσης εντός της Ευρωπαϊκής Ένωσης.

Μορφή Συμβουλευτικού του DAF Deutsches[23]

Το DAF είναι μια πρωτοβουλία της γερμανικής ομάδας CERT-Verbund και είναι βασικό στοιχείο της υποδομής για την παραγωγή και την ανταλλαγή συμβουλευτικών ασφαλείας μεταξύ διαφορετικών ομάδων. Το DAF είναι ειδικά προσαρμοσμένο στις ανάγκες των γερμανικών ομάδων CERT. Το πρότυπο αναπτύσσεται και διατηρείται από τις CERT-Bund, DFN-CERT, PRESECURE και Siemens-CERT.

[22] EISSP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

Βήμα 3: Διανομή των πληροφοριών

Μια ομάδα CSIRT μπορεί να επιλέξει από μια σειρά μεθόδων διανομής ανάλογα με τις επιθυμίες των αποδεκτών και την επικοινωνιακή της στρατηγική:

- ιστότοπος,
- ηλεκτρονικό ταχυδρομείο,
- αναφορές,
- αρχειοθέτηση και έρευνα.

Τα συμβουλευτικά ασφαλείας που διανέμονται από μια CSIRT θα πρέπει πάντοτε να ακολουθούν την ίδια δομή. Αυτό θα ενισχύσει την αναγνωσιμότητα και ο αναγνώστης θα βρίσκει γρήγορα όλες τις συναφείς πληροφορίες.

Ένα συμβουλευτικό θα πρέπει να περιλαμβάνει τουλάχιστον τις παρακάτω πληροφορίες:

Τίτλος του συμβουλευτικού
……

Αριθμός αναφοράς
……
Συστήματα που προσβλήθηκαν
- ……
- ……

Σχετικό λειτουργικό σύστημα + έκδοση
……
Κίνδυνος (Υψηλός-Μέτριος-Χαμηλός)
……
Αντίκτυπος/πιθανή ζημία (Υψηλός-Μέτριος-Χαμηλός)
……
Εξωτερικά αναγνωριστικά (CVE, αναγνωριστικά ενημερωτικού αδυναμίας)
……

Επισκόπηση αδυναμίας
……
Αντίκτυπος
……
Λύση
……
Περιγραφή (λεπτομέρειες)
……
Παράρτημα
……

Σχήμα 12 Δείγμα προτύπου συμβουλευτικού

Βλέπε κεφάλαιο *10. Άσκηση,* για να έχετε πλήρες υπόδειγμα συμβουλευτικού ασφαλείας.

8.3 Διαχείριση Περιστατικών

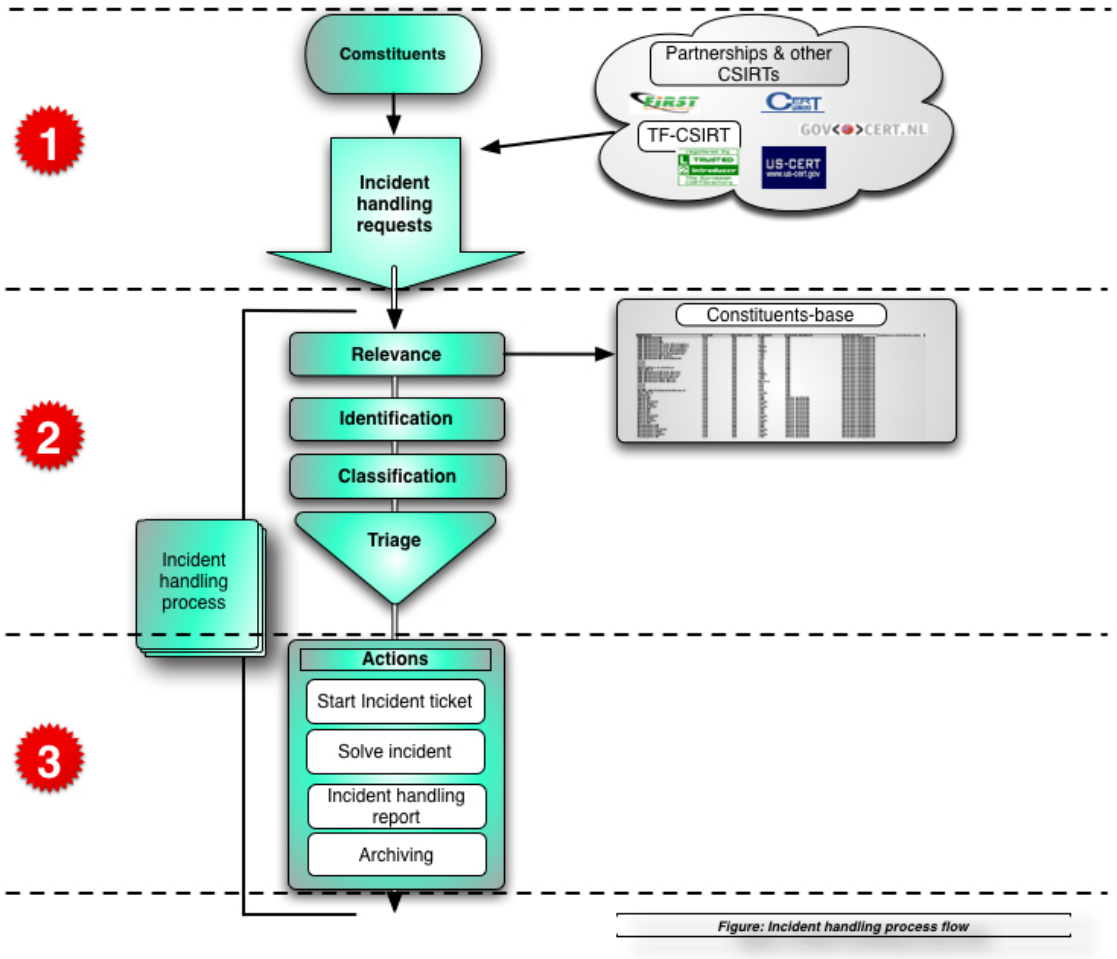
Όπως αναφέρθηκε στην εισαγωγή του παρόντος κεφαλαίου, η διαδικασία διαχείρισης πληροφοριών κατά την αντιμετώπιση περιστατικών μοιάζει πολύ με εκείνη που χρησιμοποιείται κατά τη δημιουργία συναγερμών, προειδοποιήσεων και ανακοινώσεων. Αλλά η διαδικασία συλλογής πληροφοριών συνήθως είναι διαφορετική, καθώς ο συνήθης τρόπος απόκτησης δεδομένων σχετικών με περιστατικά είναι, είτε η λήψη αναφορών περιστατικών από την κοινότητα αποδεκτών ή άλλες ομάδες, είτε η λήψη υλικού ανατροφοδότησης από τους εμπλεκόμενους φορείς κατά τη διαδικασία αντιμετώπισης περιστατικών. Οι πληροφορίες συνήθως έρχονται (κρυπτογραφημένες) μέσω ηλεκτρονικού ταχυδρομείου. Μερικές φορές είναι απαραίτητη η χρήση τηλεφώνου ή φαξ.

Όταν λαμβάνονται πληροφορίες μέσω τηλεφώνου, αποτελεί καλή πρακτική να σημειώνεται ακόμη και η παραμικρή λεπτομέρεια ευθύς αμέσως είτε χρησιμοποιώντας ένα εργαλείο αντιμετώπισης/αναφοράς περιστατικών είτε συντάσσοντας ένα υπόμνημα. Είναι απαραίτητο (προτού ολοκληρωθεί η κλήση) να χρησιμοποιηθεί ένας αριθμός περιστατικού (εάν δεν υπάρχει έως εκείνη τη στιγμή για το εν λόγω περιστατικό) και να δοθεί από τηλεφώνου στο άτομο που αναφέρει το περιστατικό (ή μέσω συνοπτικού μηνύματος ηλεκτρονικού ταχυδρομείου που αποστέλλεται κατόπιν) ως αναφορά για περαιτέρω επικοινωνία.

Στη συνέχεια του παρόντος κεφαλαίου περιγράφεται η βασική διαδικασία αντιμετώπισης περιστατικών. Μια πολύ λεπτομερής ανάλυση ολόκληρης της διαδικασίας διαχείρισης περιστατικών και όλων των συναφών ροών εργασιών και επιμέρους ροών εργασιών διατίθεται στα υποστηρικτικά έγγραφα του CERT/CC *Ορισμός διαδικασιών Διαχείρισης Περιστατικών για ομάδες CSIRT*[24].

[24] Ορισμός Διαδικασιών Διαχείρισης Περιστατικών: http://www.cert.org/archive/pdf/04tr015.pdf

Βασικά, η αντιμετώπιση περιστατικών ακολουθεί την παρακάτω ροή εργασιών:



Σχήμα 13 Ροή επεξεργασίας περιστατικού

Βήμα 1: Λήψη αναφορών περιστατικού

Όπως προαναφέρθηκε, οι αναφορές περιστατικών φθάνουν σε μια ομάδα CSIRT μέσω διαφόρων διαύλων, κυρίως μέσω ηλεκτρονικού ταχυδρομείου, αλλά και μέσω τηλεφώνου ή φαξ.

Όπως προαναφέρθηκε, αποτελεί καλή πρακτική να σημειώνετε όλες τις λεπτομέρειες σε μια προκαθορισμένη μορφή όταν λαμβάνετε μια αναφορά περιστατικού. Κατ' αυτόν τον τρόπο διασφαλίζεται ότι δεν παραλείπεται καμία σημαντική πληροφορία. Ακολουθεί ένα υπόδειγμα εντύπου:

ΔΕΛΤΙΟ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΩΝ
Συμπληρώστε το παρόν έντυπο και στείλτε το με φαξ ή ηλεκτρονικό ταχυδρομείο στο ……. *Τα πεδία που επισημαίνονται με * είναι υποχρεωτικά.* *Όνομα και οργανισμός* 1. Όνομα*: 2. Επωνυμία οργανισμού*: 3. Κλάδος: 4. Χώρα*: 5. Πόλη: 6. Διεύθυνση ηλεκτρονικού ταχυδρομείου*: 7. Αριθμός τηλεφώνου*: 8. Άλλο: *Κεντρικοί υπολογιστές που επλήγησαν* 9. Αριθμός κεντρικών υπολογιστών: 10. Όνομα & διεύθυνση IP κεντρικού υπολογιστή*: 11. Λειτουργία κεντρικού υπολογιστή*: 12. Ζώνη: 13. Υλικό: 14. Λειτουργικό σύστημα: 15. Λογισμικό που προσβλήθηκε: 16. Αρχεία που προσβλήθηκαν: 17. Ασφάλεια: 18. Όνομα & διεύθυνση IP κεντρικού υπολογιστή: 19. Πρωτόκολλο/θύρα: *Περιστατικό* 20. Αριθμός αναφοράς (αναφ. #): 21. Είδος περιστατικού: 22. Έναρξη περιστατικού: 23. Πρόκειται για επαναλαμβανόμενο περιστατικό: ΝΑΙ ΟΧΙ 24. Ώρα και μέθοδος εντοπισμού: 25. Γνωστές αδυναμίες: 26. Ύποπτα αρχεία: 27. Μέτρα αντιμετώπισης: 28. Λεπτομερής περιγραφή*:

Σχήμα 14 Περιεχόμενα αναφοράς περιστατικού

Βήμα 2: Αξιολόγηση περιστατικού

Κατά το εν λόγω βήμα ελέγχεται η αυθεντικότητα και η συνάφεια ενός αναφερόμενου περιστατικού και πραγματοποιείται διαβάθμιση του περιστατικού.

Αναγνώριση

Προκειμένου να αποφευχθεί οποιαδήποτε άσκοπη ενέργεια, αποτελεί καλή πρακτική να ελέγχετε εάν ο αποστολέας είναι αξιόπιστος και εάν ο αποστολέας είναι ένας από τους αποδέκτες σας ή μια από τις άλλες ομάδες CSIRT. Ισχύουν παρόμοιοι κανόνες με εκείνους που περιγράφηκαν στο κεφάλαιο *8.2 Παραγωγή Συναγερμών*.

Συνάφεια

Με αυτό το βήμα ελέγχετε εάν το αίτημα αντιμετώπισης περιστατικού προέρχεται από την κοινότητα αποδεκτών των ομάδων CSIRT ή εάν το αναφερόμενο περιστατικό αφορά πληροφοριακά συστήματα της κοινότητας αποδεκτών σας. Εάν δεν ισχύει τίποτε από τα παραπάνω, η αναφορά συνήθως διαβιβάζεται στην κατάλληλη ομάδα CISRT[25].

Διαβάθμιση

Με αυτό το βήμα προετοιμάζεται η διαλογή μέσω της διαβάθμισης της σοβαρότητας του περιστατικού. Δεν εμπίπτει στους σκοπούς του παρόντος εγγράφου η λεπτομερής περιγραφή της διαβάθμισης περιστατικών. Μια καλή αρχή είναι να χρησιμοποιήσετε το σχέδιο Διαβάθμισης Περιστατικών CSIRT (παράδειγμα για εταιρική ομάδα CSIRT):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Σχήμα 15 Σχέδιο διαβάθμισης περιστατικών (πηγή: FIRST)[26]

[25] Εργαλεία ελέγχου ταυτοτήτων στην CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] Διαβάθμιση Περιστατικών CSIRT http://www.first.org/resources/guides/csirt_case_classification.html

Διαλογή
Η διαλογή είναι ένα σύστημα που χρησιμοποιείται από το ιατρικό προσωπικό ή το προσωπικό πρώτων βοηθειών για την κατανομή περιορισμένων ιατρικών πόρων, όταν ο αριθμός των τραυματιών που απαιτούν φροντίδα υπερβαίνει τους διαθέσιμους πόρους για την παροχή της φροντίδας, προκειμένου να θεραπευθεί ο μεγαλύτερος δυνατός αριθμός ασθενών[27].

Το CERT/CC δίνει την παρακάτω περιγραφή:

Η διαλογή είναι ένα ουσιαστικό στοιχείο κάθε διαδικασίας διαχείρισης περιστατικών, ιδιαίτερα για οποιαδήποτε καθιερωμένη ομάδα CSIRT. Η διαλογή είναι κρίσιμη προκειμένου να καταστεί κατανοητό τι αναφέρεται σε ολόκληρο τον οργανισμό. Χρησιμοποιείται ως το μέσο με το οποίο το σύνολο των πληροφοριών ρέει σε ένα ενιαίο σημείο επαφής, επιτρέποντας μια συνολική παρακολούθηση της συνεχιζόμενης δραστηριότητας και έναν συνολικό συσχετισμό όλων των αναφερόμενων δεδομένων. Η διαλογή επιτρέπει μια αρχική εκτίμηση μιας εισερχόμενης αναφοράς και την θέτει σε σειρά προτεραιότητας για περαιτέρω διαχείριση. Επίσης, παρέχει τη βάση για την έναρξη της αρχικής τεκμηρίωσης και εισαγωγής δεδομένων μιας αναφοράς ή ενός αιτήματος, εφόσον δεν έχει πραγματοποιηθεί ήδη κάτι τέτοιο κατά τη διαδικασία εντοπισμού.

Η λειτουργία της διαλογής παρέχει ένα άμεσο στιγμιότυπο της υφιστάμενης κατάστασης όλων των αναφερόμενων δραστηριοτήτων - ποιες αναφορές βρίσκονται σε εκκρεμότητα ή έχουν κλείσει, ποιες ενέργειες βρίσκονται σε εκκρεμότητα και πόσες αναφορές κάθε είδους έχουν ληφθεί. Η εν λόγω διαδικασία μπορεί να βοηθήσει στον εντοπισμό πιθανών προβλημάτων ασφαλείας και στην προτεραιοποίηση του φόρτου εργασίας. Οι πληροφορίες που συλλέγονται κατά τη διαλογή μπορούν επίσης να χρησιμοποιηθούν για την παραγωγή τάσεων και στατιστικών σχετικά με τις αδυναμίες του συστήματος και τα περιστατικά προς την ανώτερη διοίκηση[28].

Η διαλογή θα πρέπει να πραγματοποιείται από τα πλέον έμπειρα μέλη της ομάδας, διότι απαιτεί βαθιά κατανόηση των πιθανών αντικτύπων των περιστατικών σε συγκεκριμένα τμήματα της κοινότητας αποδεκτών και τη δυνατότητα λήψης αποφάσεων για το μέλος της ομάδας που θα ήταν κατάλληλο ώστε να αντιμετωπίσει το εν λόγω περιστατικό.

Βήμα 3: Ενέργειες

Συνήθως μετά τη διαλογή τα περιστατικά διαβιβάζονται σε μια σειρά αιτημάτων σε προτεραιότητα ενός εργαλείου αντιμετώπισης περιστατικών που χρησιμοποιείται από έναν ή περισσότερους διαχειριστές περιστατικών, οι οποίοι ακολουθούν βασικά τα παρακάτω βήματα.

Έναρξη δελτίου περιστατικού

[27] Διαλογή στο Wikipedia: http://en.wikipedia.org/wiki/Triage

[28] Ορισμός Διαδικασιών Διαχείρισης Περιστατικών: http://www.cert.org/archive/pdf/04tr015.pdf

Ο αριθμός δελτίου του περιστατικού μπορεί να έχει ήδη δημιουργηθεί σε προηγούμενο βήμα (για παράδειγμα όταν αναφέρθηκε το περιστατικό μέσω τηλεφώνου). Εάν όχι, το πρώτο βήμα είναι η δημιουργία του εν λόγω αριθμού που θα χρησιμοποιηθεί σε κάθε περαιτέρω επικοινωνία για το εν λόγω περιστατικό.

Κύκλος ζωής περιστατικού
Η αντιμετώπιση ενός περιστατικού δεν ακολουθεί μια σειρά βημάτων που οδηγούν τελικά σε μια λύση, αλλά ακολουθεί μάλλον έναν κύκλο βημάτων που εφαρμόζονται κατ' επανάληψη έως ότου τελικά επιλυθεί το περιστατικό και λάβουν όλες τις απαραίτητες πληροφορίες όλοι οι ενδιαφερόμενοι. Ο εν λόγω κύκλος, ο οποίος αναφέρεται και ως "Κύκλος Ζωής Περιστατικού", περιλαμβάνει τις παρακάτω διεργασίες:

Ανάλυση:	Αναλύονται όλες οι λεπτομέρειες του αναφερόμενου περιστατικού.
Λήψη στοιχείων επικοινωνίας:	Προκειμένου να καταστεί δυνατή η περαιτέρω αναφορά των πληροφοριών που σχετίζονται με το περιστατικό σε όλους τους ενδιαφερόμενους, όπως άλλες ομάδες CSIRT, θύματα και πιθανώς ιδιοκτήτες των συστημάτων που έχουν χρησιμοποιηθεί για μια επίθεση.
Παροχή τεχνικής υποστήριξης:	Παροχή βοήθειας προς τα θύματα ώστε να επανέλθουν γρήγορα από τα αποτελέσματα του περιστατικού και να συλλεχθούν περισσότερες πληροφορίες σχετικά με την επίθεση.
Συντονισμός:	Ενημέρωση άλλων ενδιαφερομένων, όπως η ομάδα CSIRT που είναι υπεύθυνη για το πληροφοριακό σύστημα που χρησιμοποιήθηκε για μια επίθεση, ή άλλα θύματα.

Η εν λόγω δομή αποκαλείται "κύκλος ζωής", επειδή το ένα βήμα οδηγεί στο άλλο και το τελευταίο, ο συντονισμός, μπορεί κατόπιν να οδηγήσει και πάλι σε νέα ανάλυση, και έτσι ο κύκλος ξεκινά ξανά. Η διαδικασία ολοκληρώνεται όταν όλοι οι ενδιαφερόμενοι έχουν λάβει και αναφέρει όλες τις απαραίτητες πληροφορίες.

Ανατρέξτε στο εγχειρίδιο του CERT/CC CSIRT για μια πιο λεπτομερή περιγραφή του κύκλου ζωής του περιστατικού[29].

Αναφορά αντιμετώπισης περιστατικού
Να είστε έτοιμοι να δεχθείτε ερωτήματα από τη διοίκηση για περιστατικά συντάσσοντας μια αναφορά. Αποτελεί επίσης καλή πρακτική να συντάξετε ένα έγγραφο (αποκλειστικά για εσωτερική χρήση) σχετικά “με τα διδάγματα που αποκομίσατε” για την εκπαίδευση του προσωπικού και την αποφυγή σφαλμάτων σε μελλοντικές διαδικασίες αντιμετώπισης περιστατικών.

Αρχειοθέτηση
Ανατρέξτε στους κανόνες αρχειοθέτησης που περιγράφηκαν νωρίτερα στο κεφάλαιο *6.6 Ανάπτυξη μιας πολιτικής ασφάλειας πληροφοριών*.

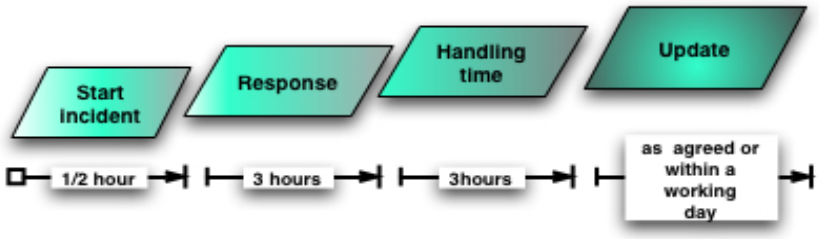
[29] Εγχειρίδιο CSIRT: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Ανατρέξτε στην ενότητα του Παραρτήματος *Α.1 Περαιτέρω παραπομπές* για ολοκληρωμένους οδηγούς διαχείρισης περιστατικών και τον κύκλο ζωής περιστατικών.

8.4 Παράδειγμα χρονοδιαγράμματος απόκρισης

Ο καθορισμός των χρόνων απόκρισης συχνά αγνοείται, αλλά θα πρέπει να αποτελεί μέρος κάθε καλά δομημένης συμφωνίας επιπέδου υπηρεσιών (SLA) μεταξύ μιας ομάδας CSIRT και της κοινότητας αποδεκτών της. Η έγκαιρη παροχή υλικού ανατροφοδότησης στους αποδέκτες κατά την αντιμετώπιση περιστατικών είναι ζωτικής σημασίας, τόσο για την ευθύνη των ίδιων των αποδεκτών όσο και για τη φήμη της ομάδας.
Οι χρόνοι απόκρισης θα πρέπει να αναφέρονται ρητώς στην κοινότητα αποδεκτών προκειμένου να αποφεύγονται οι εσφαλμένες προσδοκίες. Το παρακάτω πολύ βασικό χρονοδιάγραμμα μπορεί να χρησιμοποιηθεί ως αφετηρία για μια πιο λεπτομερή SLA με την κοινότητα αποδεκτών μιας ομάδας CSIRT.

Ιδού ένα παράδειγμα πρακτικού χρονοδιαγράμματος απόκρισης από τη στιγμή της λήψης ενός αιτήματος για υποστήριξη:



Σχήμα 16 Υπόδειγμα χρονοδιαγράμματος απόκρισης

Αποτελεί επίσης καλή πρακτική να δώσετε οδηγίες στην κοινότητα αποδεκτών για τους δικούς της χρόνους απόκρισης, ιδιαίτερα τη χρονική στιγμή κατά την οποία θα πρέπει να επικοινωνούν με την ομάδα CSIRT σε περίπτωση έκτακτου περιστατικού. Στις περισσότερες περιπτώσεις είναι καλύτερο να επικοινωνούν με την ομάδα CSIRT σε αρχικό στάδιο και αποτελεί καλή πρακτική να ενθαρρύνετε την ομάδα αποδεκτών σας να το πράττει όταν έχει αμφιβολίες.

8.5 Διαθέσιμα εργαλεία CSIRT

Το παρόν κεφάλαιο παρέχει ορισμένες υποδείξεις για συνηθισμένα εργαλεία που χρησιμοποιούνται από ομάδες CSIRT. Παρέχει απλώς παραδείγματα. Περισσότερες υποδείξεις είναι διαθέσιμες στα *Εργαλεία Αντιμετώπισης Περιστατικών Clearinghouse*[30] (CHIHT).

Λογισμικό κρυπτογράφησης ηλεκτρονικού ταχυδρομείου και μηνυμάτων

- GNUPG http://www.gnupg.org/
  Το GnuPG είναι η πλήρης και δωρεάν εφαρμογή του προτύπου OpenPGP στο πλαίσιο του προγράμματος όπως ορίζεται στο πρότυπο RFC2440. Το GnuPG σας επιτρέπει να κρυπτογραφείτε και να υπογράφετε τα δεδομένα και την επικοινωνία σας.

- PGP http://www.pgp.com/
  Εμπορική έκδοση

Εργαλείο διαχείρισης περιστατικών

Διαχείριση περιστατικών και παρακολούθησής τους, παρακολούθηση ενεργειών.

- RTIR http://www.bestpractical.com/rtir/
  Το RTIR είναι ένα δωρεάν σύστημα ανοικτού κώδικα για την αντιμετώπιση περιστατικών, το οποίο έχει σχεδιαστεί με βάση τις ανάγκες των ομάδων CERT και άλλων ομάδων αντιμετώπισης περιστατικών.

Εργαλεία CRM

Όταν έχετε πολλούς διαφορετικούς αποδέκτες και πρέπει να καταγράφετε όλες τις συναντήσεις και τις λεπτομέρειες, μια βάση δεδομένων CRM είναι χρήσιμη. Υπάρχουν πολλές διαφορετικές εκδόσεις, ιδού ορισμένα παραδείγματα:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforce (δωρεάν έκδοση ανοικτού κώδικα) http://www.sugarforge.org/

Έλεγχος πληροφοριών

- Πρόγραμμα παρακολούθησης ιστοτόπων http://www.aignes.com/index.htm
  Το εν λόγω πρόγραμμα παρακολουθεί ιστοτόπους για ενημερώσεις και αλλαγές.

- Παρακολούθηση αυτής της σελίδας http://www.watchthatpage.com/
  Η υπηρεσία αποστέλλει πληροφορίες σχετικά με αλλαγές σε ιστοτόπους μέσω ηλεκτρονικού ταχυδρομείου (δωρεάν και εμπορική έκδοση).

Εύρεση στοιχείων επικοινωνίας

Η εύρεση των σωστών στοιχείων επικοινωνίας για την αναφορά περιστατικών δεν είναι απλή διαδικασία. Υπάρχουν μερικές πηγές πληροφοριών που μπορούν να χρησιμοποιηθούν:

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

- RIPE[31]
- IRT-object[32]
- TI[33]

Επιπλέον, η CHIHT αναφέρει ορισμένα εργαλεία εξεύρεσης στοιχείων επικοινωνίας[34].

Εικονική ομάδα CSIRT (βήμα 8)

Καθορισμός ροών διεργασιών και λειτουργικών και τεχνικών διαδικασιών

Η Εικονική Ομάδα CSIRT εστιάζει στην παροχή των βασικών υπηρεσιών CSIRT:

- συναγερμοί και προειδοποιήσεις,
- ανακοινώσεις,
- αντιμετώπιση περιστατικών.

Η Ομάδα ανέπτυξε διαδικασίες που λειτουργούν σωστά και είναι εύκολα κατανοητές από κάθε μέλος της ομάδας. Η Εικονική Ομάδα CSIRT προσέλαβε επίσης έναν νομικό σύμβουλο για την αντιμετώπιση της αστικής ευθύνης και τη διαμόρφωση της πολιτικής ασφάλειας πληροφοριών. Η Ομάδα υιοθέτησε ορισμένα χρήσιμα εργαλεία και βρήκε χρήσιμες πληροφορίες για λειτουργικά ζητήματα συζητώντας με άλλες ομάδες CSIRT.

Δημιουργήθηκε ένα προκαθορισμένο πρότυπο συμβουλευτικών ασφαλείας και αναφορών περιστατικών. Η Ομάδα χρησιμοποιεί το RTIR για την αντιμετώπιση περιστατικών.

[31] RIPE whois: http://www.ripe.net/whois

[32] IRT-object στη βάση δεδομένων RIPE: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Εργαλεία ελέγχου ταυτοτήτων στην CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Εκπαίδευση CSIRT

Πραγματοποιήσαμε τα εξής βήματα μέχρι στιγμής:

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί να προσφέρει.
2. Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;
3. Τι είδους υπηρεσίες μπορεί να προσφέρει μια ομάδα CSIRT στην κοινότητα αποδεκτών της.
4. Ανάλυση του περιβάλλοντος και των αποδεκτών.
5. Καθορισμός της δήλωσης αποστολής.
6. Αναπτύσσοντας το Επιχειρηματικό Σχέδιο
   α. Καθορίζοντας το οικονομικό μοντέλο
   β. Καθορισμός της οργανωτικής δομής
   γ. Έναρξη πρόσληψης προσωπικού
   δ. Χρήση και εξοπλισμός γραφείου
   ε. Αναπτύσσοντας μια πολιτική ασφάλειας πληροφοριών
   στ. Αναζήτηση εταίρων συνεργασίας.
7. Προωθώντας το Επιχειρηματικό Σχέδιο
   α. Έγκριση επιχειρηματικής πρακτικής
   β. Ενσωμάτωση όλων των στοιχείων σε ένα σχέδιο έργου.
8. Καθιστώντας λειτουργική την ομάδα CSIRT
   α. Δημιουργία ροών εργασιών
   β. Εφαρμογή εργαλείων CSIRT.

>> Το επόμενο βήμα είναι: η εκπαίδευση του προσωπικού

Το παρόν κεφάλαιο αναφέρει τις δύο κύριες πηγές για εξειδικευμένη εκπαίδευση CSIRT: τα μαθήματα του προγράμματος TRANSITS και του CERT/CC.

9.1 TRANSITS

Το TRANSITS ήταν ένα ευρωπαϊκό πρόγραμμα για την προώθηση της δημιουργίας Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές (CSIRT) και την ενίσχυση των υφιστάμενων ομάδων CSIRT, αντιμετωπίζοντας το πρόβλημα της έλλειψης εξειδικευμένου προσωπικού CSIRT. Ο εν λόγω στόχος επιτεύχθηκε παρέχοντας εξειδικευμένα εκπαιδευτικά μαθήματα για την εκπαίδευση του προσωπικού των (νέων) ομάδων CSIRT σε οργανωτικά, λειτουργικά και τεχνικά θέματα, ζητήματα της αγοράς, και επίσης νομικά ζητήματα που εμπλέκονται στην παροχή των υπηρεσιών CSIRT.

Συγκεκριμένα το TRANSITS:

- έχει αναπτύξει, ενημερώσει και αναθεωρεί τακτικά το διαρθρωμένο υλικό εκπαιδευτικών μαθημάτων,
- έχει οργανώσει εκπαιδευτικά εργαστήρια όπου παραδόθηκε το υλικό των μαθημάτων,

- έχει καταστήσει δυνατή τη συμμετοχή μελών του προσωπικού (νέων) ομάδων CSIRT στα εν λόγω εκπαιδευτικά εργαστήρια, με ιδιαίτερη έμφαση στη συμμετοχή από τις χώρες προς ένταξη στην ΕΕ,
- έχει δημοσιοποιήσει το υλικό των εκπαιδευτικών μαθημάτων και έχει διασφαλίσει την αξιοποίηση των αποτελεσμάτων.

Ο ENISA υιοθετεί και υποστηρίζει τα μαθήματα του TRANSITS. Εάν χρειάζεσθε πληροφορίες για τον τρόπο υποβολής αίτησης για τα μαθήματα, τις απαιτήσεις και το κόστος, επικοινωνήστε με τους ειδικούς CSIRT του ENISA:

CERT-Relations@enisa.europa.eu

Δείγμα υλικού μαθημάτων διατίθεται στο παράρτημα του παρόντος εγγράφου!

9.2 CERT/CC

Η πολυπλοκότητα των υπολογιστικών και δικτυακών υποδομών και η πρόκληση της διαχείρισης καθιστούν δύσκολη την κατάλληλη διαχείριση της ασφάλειας δικτύων. Οι διαχειριστές δικτύων και συστημάτων δεν έχουν στη διάθεσή τους επαρκή αριθμό ανθρώπων και εφαρμοσμένες πρακτικές ασφαλείας προκειμένου να αμυνθούν έναντι των επιθέσεων και να ελαχιστοποιήσουν τη ζημία. Ως εκ τούτου, παρατηρείται ένας αυξανόμενος αριθμός περιστατικών ασφαλείας σε υπολογιστές.
Όταν προκύπτουν περιστατικά ασφαλείας σε υπολογιστές, οι οργανισμοί θα πρέπει να αντιδρούν γρήγορα και αποτελεσματικά. Όσο πιο γρήγορα αναγνωρίσει, αναλύσει και αντιδράσει ένας οργανισμός σε ένα περιστατικό, τόσο αποτελεσματικότερα μπορεί να περιορίσει τη ζημία και να μειώσει τις δαπάνες αποκατάστασης. Η δημιουργία μιας ''ομάδας αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές'' (CSIRT) είναι ένας εξαιρετικός τρόπος παροχής αυτής της δυνατότητας ταχείας αντίδρασης, ενώ ταυτόχρονα βοηθά στην πρόληψη μελλοντικών περιστατικών.

Το CERT-CC προσφέρει μαθήματα για στελέχη και τεχνικό προσωπικό σε τομείς, όπως η δημιουργία και η διαχείριση ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (CSIRT), η αντιμετώπιση και ανάλυση περιστατικών ασφαλείας και η βελτίωση της ασφάλειας των δικτύων. Εκτός εάν επισημαίνεται κάτι διαφορετικό, όλα τα μαθήματα πραγματοποιούνται στο Pittsburgh της Πενσυλβανίας. Επίσης, μέλη του προσωπικού μας διδάσκουν μαθήματα ασφαλείας στο Πανεπιστήμιο Carnegie Mellon.

Διαθέσιμα μαθήματα του CERT/CC[36] ειδικά για ομάδες CSIRT

Δημιουργώντας μια Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές (CSIRT)
Διαχείριση Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές (CSIRT)
Βασικές Αρχές Αντιμετώπισης Περιστατικών
Αντιμετώπιση Περιστατικών Προχωρημένου Επιπέδου για Τεχνικό Προσωπικό

[35] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

[36] Μαθήματα του CERT/CC: http://www.sei.cmu.edu/products/courses

Δείγμα υλικού μαθημάτων διατίθεται στο παράρτημα του παρόντος εγγράφου!

Εικονική ομάδα CSIRT (βήμα 9)
Εκπαίδευση του προσωπικού Η Εικονική ομάδα CSIRT αποφασίζει να στείλει όλο το τεχνικό προσωπικό της στα επόμενα διαθέσιμα μαθήματα TRANSITS. Επιπροσθέτως, ο επικεφαλής της ομάδας παρακολουθεί το μάθημα *Διαχείριση ομάδας* CSIRT του CERT/CC.

10 Άσκηση: δημιουργία συμβουλευτικού

Πραγματοποιήσαμε τα εξής βήματα μέχρι στιγμής:

1. Κατανοώντας τι είναι μια ομάδα CSIRT και τι οφέλη μπορεί να προσφέρει.
2. Σε ποιον κλάδο θα παρασχεθούν οι υπηρεσίες της ομάδας CSIRT;
3. Τι είδους υπηρεσίες μπορεί να προσφέρει μια ομάδα CSIRT στην κοινότητα αποδεκτών της.
4. Ανάλυση του περιβάλλοντος και των αποδεκτών.
5. Καθορισμός της δήλωσης αποστολής.
6. Αναπτύσσοντας το Επιχειρηματικό Σχέδιο
   α. Καθορίζοντας το οικονομικό μοντέλο
   β. Καθορισμός της οργανωτικής δομής
   γ. Έναρξη πρόσληψης προσωπικού
   δ. Χρήση και εξοπλισμός γραφείου
   ε. Αναπτύσσοντας μια πολιτική ασφάλειας πληροφοριών
   στ. Αναζήτηση εταίρων συνεργασίας.
7. Προωθώντας το Επιχειρηματικό Σχέδιο
   α. Έγκριση επιχειρηματικής πρακτικής
   β. Ενσωμάτωση όλων των στοιχείων σε ένα σχέδιο έργου.
8. Καθιστώντας λειτουργική την ομάδα CSIRT
   α. Δημιουργία ροών εργασιών
   β. Εφαρμογή εργαλείων CSIRT.
9. Εκπαίδευση του προσωπικού.

>> Το επόμενο βήμα είναι η εξάσκηση και η προετοιμασία για την πραγματική εργασία!

Για επεξήγηση, το παρόν κεφάλαιο περιγράφει ένα υπόδειγμα άσκησης για μια καθημερινή δραστηριότητα μιας ομάδας CSIRT: δημιουργία ενός συμβουλευτικού ασφαλείας.

Το έναυσμα ήταν το παρακάτω πρωτότυπο συμβουλευτικό ασφαλείας που εστάλη από τη Microsoft:

Αναγνωριστικό δελτίου	**Δελτίο ασφαλείας της Microsoft MS06-042**
Τίτλος δελτίου	**Ολοκληρωμένη Ενημέρωση Ασφαλείας για τον Internet Explorer (918899)**
Διοικητική σύνοψη	Η παρούσα ενημέρωση επιλύει ορισμένες αδυναμίες του Internet Explorer που θα μπορούσαν να επιτρέπουν την εκτέλεση απομακρυσμένου κώδικα.
Εκτίμηση μέγιστης σοβαρότητας	Κρίσιμη
Αντίκτυπος αδυναμίας	Εκτέλεση απομακρυσμένου κώδικα
Λογισμικό που προσβλήθηκε	**Windows, Internet Explorer.** Για περισσότερες πληροφορίες ανατρέξτε στην ενότητα ''Λογισμικό που Προσβλήθηκε και Τοποθεσίες Λήψης''.

Το εν λόγω δελτίο προμηθευτή σχετίζεται με μια αδυναμία που εντοπίστηκε πρόσφατα στον Internet Explorer. Ο προμηθευτής εκδίδει πολλαπλά διορθωτικά προγράμματα για το εν λόγω λογισμικό για τις διαφορετικές εκδόσεις των Microsoft Windows.

Η Εικονική Ομάδα CSIRT, αφού έλαβε τις εν λόγω πληροφορίες σχετικά με την αδυναμία μέσω μιας λίστας αλληλογραφίας, ξεκινά με τη ροή εργασιών που περιγράφεται στο κεφάλαιο *8.2 Δημιουργία Συναγερμών, Προειδοποιήσεων και Ανακοινώσεων*.

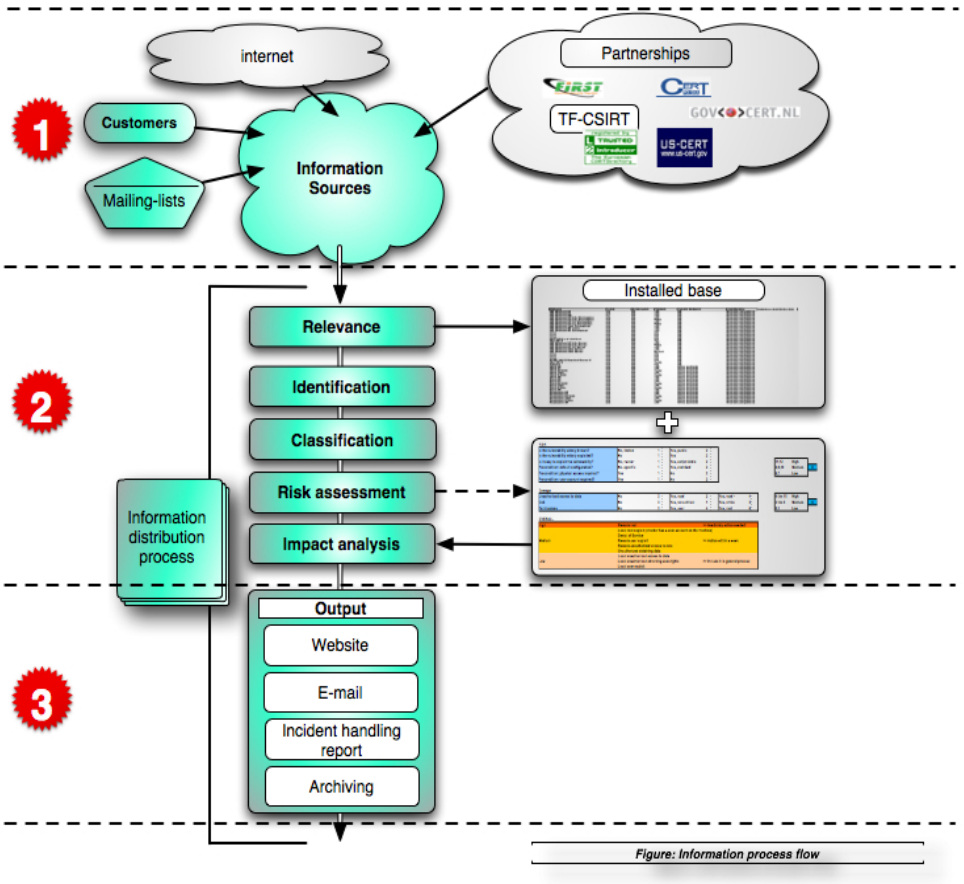


Figure: Information process flow

Βήμα 1: Συλλογή πληροφοριών σχετικά με την αδυναμία

Το πρώτο βήμα είναι η αναζήτηση στον ιστότοπο του προμηθευτή. Εκεί, η Εικονική Ομάδα CSIRT επαληθεύει την αυθεντικότητα των πληροφοριών και συλλέγει περαιτέρω λεπτομέρειες σχετικά με την αδυναμία και τα πληροφοριακά συστήματα που έχουν προσβληθεί.

Βήμα 2: Αξιολόγηση των πληροφοριών και εκτίμηση του κινδύνου

Αναγνώριση
Οι πληροφορίες έχουν ήδη επαληθευθεί μέσω διασταύρωσης των πληροφοριών σχετικά με την αδυναμία που ελήφθησαν μέσω ηλεκτρονικού ταχυδρομείου και του κειμένου που εμφανίζεται στον ιστότοπο του προμηθευτή.

Συνάφεια
Η Εικονική Ομάδα CSIRT ελέγχει τον κατάλογο των συστημάτων που έχουν προσβληθεί, ο οποίος διατίθεται στον ιστότοπο μαζί με τον κατάλογο των συστημάτων που χρησιμοποιούνται από την κοινότητα αποδεκτών. Ανακαλύπτει ότι τουλάχιστον ένας από τους αποδέκτες χρησιμοποιεί τον Internet Explorer και επομένως οι πληροφορίες σχετικά με την αδυναμία είναι πράγματι σχετικές.

Κατηγορία	Εφαρμογή	Λογισμικό προϊόν	Έκδοση	Λειτουργικό σύστημα	Λειτουργικό σύστημα & έκδοση	Αποδέκτης
Επιφάνεια εργασίας	Πρόγραμμα περιήγησης	IE	x-x-	Microsoft	XP-prof	A

Διαβάθμιση
Οι πληροφορίες είναι δημόσιες και επομένως μπορούν να χρησιμοποιηθούν και να αναδιανεμηθούν.

Εκτίμηση κινδύνου & ανάλυση αντικτύπου
Η απάντηση στα ερωτήματα αποδεικνύει ότι ο κίνδυνος και ο αντίκτυπος *είναι υψηλός* (έχει εκτιμηθεί ως *κρίσιμος* από τη Microsoft).

ΚΙΝΔΥΝΟΣ

Είναι γνωστή η αδυναμία;	N
Είναι ευρέως διαδεδομένη η αδυναμία;	N
Είναι εύκολο να εκμεταλλευτεί κάποιος την αδυναμία;	N
Πρόκειται για αδυναμία που μπορεί κανείς να εκμεταλλευτεί εξ αποστάσεως;	N

ΖΗΜΙΑ
Οι πιθανές επιπτώσεις είναι η απομακρυσμένη δυνατότητα πρόσβασης και πιθανώς η εκτέλεση απομακρυσμένου κώδικα. Η εν λόγω αδυναμία περιλαμβάνει πολλαπλά ζητήματα, τα οποία καθιστούν υψηλό *τον κίνδυνο της ζημίας*.

Βήμα 3: Διανομή

Η Εικονική Ομάδα CSIRT είναι μια εσωτερική ομάδα CSIRT. Διαθέτει ηλεκτρονικό ταχυδρομείο, τηλέφωνο και εσωτερικό ιστότοπο ως διαύλους επικοινωνίας. Η ομάδα CSIRT συντάσσει αυτό το συμβουλευτικό με βάση το υπόδειγμα του κεφαλαίου *8.2 Δημιουργία Συναγερμών, Προειδοποιήσεων και Ανακοινώσεων*.

Τίτλος συμβουλευτικού
Πολλαπλές αδυναμίες εντοπίστηκαν στον Internet explorer

Αριθμός αναφοράς
082006-1
Συστήματα που προσβλήθηκαν
Όλα τα συστήματα υπολογιστών που λειτουργούν με εφαρμογές επιφάνειας εργασίας της Microsoft

Σχετικό λειτουργικό σύστημα + έκδοση
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 και Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 και Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 για συστήματα Itanium και Microsoft Windows Server 2003 με SP1 για συστήματα Itanium
- Microsoft Windows Server 2003 x64 Edition

Κίνδυνος (Υψηλός-Μέτριος-Χαμηλός)
ΥΨΗΛΟΣ
Αντίκτυπος/πιθανή ζημία (Υψηλός-Μέτριος-Χαμηλός)
ΥΨΗΛΟΣ
Εξωτερικά αναγνωριστικά (CVE, αναγνωριστικά ενημερωτικού αδυναμίας)
MS-06-42

Επισκόπηση αδυναμίας
Η Microsoft εντόπισε ορισμένες κρίσιμες αδυναμίες στον Internet Explorer που θα μπορούσαν να οδηγήσουν σε εκτέλεση απομακρυσμένου κώδικα.
Αντίκτυπος
Ένας δράστης θα μπορούσε να αναλάβει τον πλήρη έλεγχο του συστήματος, εγκαθιστώντας προγράμματα, προσθέτοντας χρήστες και θέτοντας σε κίνδυνο, αλλάζοντας ή διαγράφοντας δεδομένα. Παράγοντας μετριασμού είναι το γεγονός ότι τα παραπάνω μπορούν να πραγματοποιηθούν μόνο εάν ο χρήστης έχει συνδεθεί στο σύστημα με δικαιώματα διαχειριστή. Οι χρήστες που συνδέονται στο σύστημα με λιγότερα δικαιώματα θα επηρεαστούν λιγότερο.

Λύση
Εκτελέστε διορθωτικό πρόγραμμα του IE άμεσα

Περιγραφή (λεπτομέρειες)
Για περισσότερες πληροφορίες ανατρέξτε στο ms06-042.mspx

Παράρτημα
Για περισσότερες πληροφορίες ανατρέξτε στο ms06-042.mspx

Το εν λόγω εξαγόμενο είναι πλέον έτοιμο προς διανομή. Επειδή αποτελεί κρίσιμο δελτίο, σας συνιστούμε να καλέσετε και όλους τους αποδέκτες όταν είναι δυνατό.

Εικονική ομάδα CSIRT (βήμα 10)
Εξάσκηση
Κατά τις πρώτες εβδομάδες λειτουργίας, η εικονική ομάδα CSIRT χρησιμοποίησε διάφορες εικονικές πρακτικές (που έλαβε ως παράδειγμα από άλλες ομάδες CSIRT) εν είδει εξάσκησης. Επιπλέον, εξέδωσε μερικά συμβουλευτικά ασφαλείας με βάση τις πραγματικές πληροφορίες αδυναμιών που διανεμήθηκαν από προμηθευτές υλικού και λογισμικού, οι οποίες ρυθμίστηκαν και προσαρμόστηκαν στις ανάγκες της κοινότητας αποδεκτών.

11 Επίλογος

Εδώ ολοκληρώνεται ο οδηγός. Το ανά χείρας έγγραφο έχει ως στόχο την παροχή μιας πολύ συνοπτικής επισκόπησης των διαφόρων διαδικασιών που είναι απαραίτητες για τη δημιουργία μιας ομάδας CSIRT. Δεν υποστηρίζει ότι είναι πλήρες ούτε υπεισέρχεται σε συγκεκριμένες λεπτομέρειες. Ανατρέξτε στην ενότητα *Α.1 Περαιτέρω παραπομπές* του παραρτήματος για βιβλιογραφία επί του θέματος που αξίζει τον κόπο να διαβάσετε.

Τα επόμενα σημαντικά βήματα για την Εικονική Ομάδα CSIRT θα ήταν πλέον:

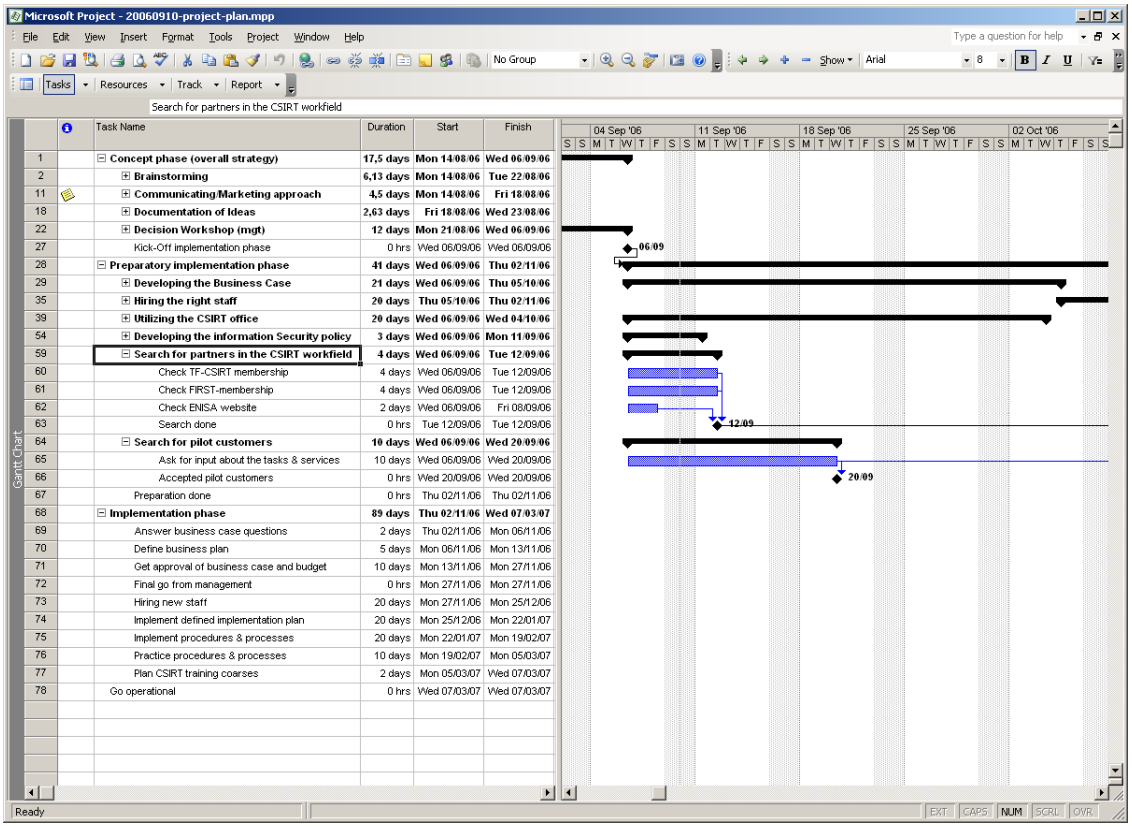
- λήψη υλικού ανατροφοδότησης από την κοινότητα αποδεκτών για την λεπτομερή προσαρμογή των παρεχόμενων υπηρεσιών,
- εξοικείωση με την καθημερινή εργασία,
- εξάσκηση σε συνθήκες έκτακτων περιστατικών,
- διατήρηση της στενής επαφής με τις διάφορες κοινότητες CSIRT, με απώτερο στόχο τη συμβολή στην εθελοντική τους εργασία.

12 Περιγραφή του Σχεδίου Έργου

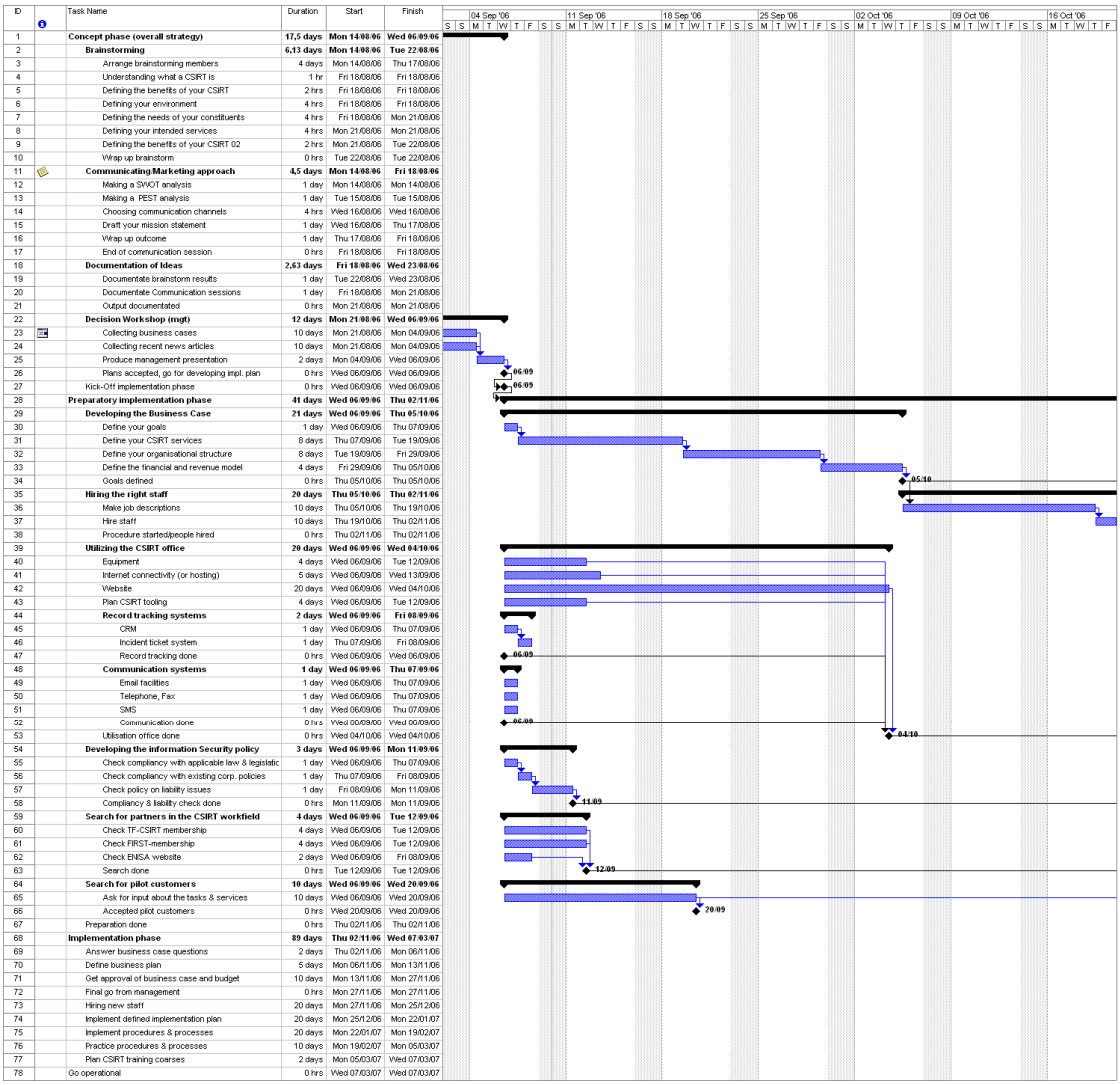
ΣΗΜΕΙΩΣΗ: Το σχέδιο έργου είναι μια πρώτη εκτίμηση του απαραίτητου χρόνου. Ανάλογα με τους διαθέσιμους πόρους, η *πραγματική διάρκεια του έργου μπορεί να είναι διαφορετική.*

Το σχέδιο έργου είναι διαθέσιμο σε διαφορετικές μορφές σε CD και στον ιστότοπο του ENISA. Καλύπτει απολύτως όλες τις διαδικασίες που περιγράφονται στο παρόν έγγραφο.

Η κύρια μορφή θα είναι σε Microsoft Project, ώστε να μπορεί να χρησιμοποιηθεί απευθείας σε αυτό το εργαλείο διαχείρισης έργου.



Σχήμα 17 Σχέδιο έργου



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**41 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilisation office done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the Information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Σχήμα 18 Το σχέδιο έργου με όλες τις εργασίες και ένα μέρος του διαγράμματος Gant

Επίσης, το σχέδιο έργου είναι διαθέσιμο σε μορφή CVS και XML. Περαιτέρω επεξηγήσεις μπορείτε να ζητήσετε από τους ειδικούς CSIRT του ENISA: CERT-Relations@enisa.europa.eu

ΠΑΡΑΡΤΗΜΑ

Α.1 Περαιτέρω παραπομπές

Εγχειρίδιο για ομάδες CSIRT (CERT/CC)
Ένα ολοκληρωμένο έργο αναφοράς για όλα τα θέματα που σχετίζονται με την εργασία μιας ομάδας CSIRT
Πηγή: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Καθορισμός Διαδικασιών Διαχείρισης Περιστατικών για Ομάδες CSIRT: ένα Έργο σε Εξέλιξη
Μια λεπτομερής ανάλυση της διαχείρισης περιστατικών
Πηγή: http://www.cert.org/archive/pdf/04tr015.pdf

Η Υφιστάμενη Πρακτική των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας σε Υπολογιστές (CSIRT)
Μια ολοκληρωμένη ανάλυση της υφιστάμενης κατάστασης σχετικά με το παγκόσμιο τοπίο των ομάδων CSIRT, συμπεριλαμβανομένων ενός ιστορικού, στατιστικών στοιχείων και πολλών άλλων πληροφοριών
Πηγή: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Μια ολοκληρωμένη περιγραφή των διδαγμάτων από τη δημιουργία του GOVCERT.NL και της ''De Waarschuwingsdienst'', της ολλανδικής εθνικής υπηρεσίας προειδοποίησης.
Πηγή: http://www.govcert.nl/render.html?it=69

RFC 2350: Προσδοκίες από την Αντιμετώπιση Περιστατικών Ασφαλείας σε Υπολογιστές
Πηγή: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Οδηγός Αντιμετώπισης Περιστατικών Ασφάλειας σε Υπολογιστές
Πηγή: http://www.securityunit.com/publications/sp800-61.pdf

Κατάλογος του ENISA για τις δραστηριότητες CERT στην Ευρώπη
Ένα έργο αναφοράς που περιλαμβάνει πληροφορίες σχετικά με τις ομάδες SIRT στην Ευρώπη και τις διάφορες δραστηριότητές τους
Πηγή: http://www.enisa.europa.eu/ENISA%20CERT/index.htm

[37] NIST: Εθνικό Ίδρυμα Προτύπων και Τεχνολογιών

A.2 Υπηρεσίες CSIRT

Ιδιαίτερες ευχαριστίες στο CERT/CC, το οποίο παρείχε αυτόν τον κατάλογο.

Υπηρεσίες Αντίδρασης	***Υπηρεσίες Πρόληψης***	***Αντιμετώπιση Ευρημάτων***
• Συναγερμοί και προειδοποιήσεις • Αντιμετώπιση περιστατικών • Ανάλυση περιστατικών • Επιτόπια απόκριση σε περιστατικά • Υποστήριξη απόκρισης σε περιστατικά • Συντονισμός απόκρισης σε περιστατικά • Αντιμετώπιση αδυναμιών • Ανάλυση αδυναμιών • Απόκριση σε αδυναμίες • Συντονισμός απόκρισης σε αδυναμίες	• Ανακοινώσεις • Παρακολούθηση τεχνολογίας • Έλεγχοι ή αξιολογήσεις ασφαλείας • Διαμόρφωση και διατήρηση ασφαλείας • Ανάπτυξη εργαλείων ασφαλείας • Υπηρεσίες εντοπισμού εισβολής • Διάχυση πληροφοριών για την ασφάλεια	• Ανάλυση ευρημάτων • Απόκριση σε ευρήματα • Συντονισμός απόκρισης σε ευρήματα ***Διαχείριση Ποιότητας Ασφαλείας*** • Ανάλυση κινδύνου • Επιχειρηματική συνέχεια και ανάκαμψη από καταστροφή • Συμβουλευτικές υπηρεσίες ασφαλείας • Ενίσχυση ευαισθητοποίησης • Εκπαίδευση/κατάρτιση • Αξιολόγηση ή πιστοποίηση προϊόντος

Σχήμα 19 Κατάλογος υπηρεσιών CSIRT από το CERT/CC

Περιγραφές Υπηρεσιών

Υπηρεσίες Αντίδρασης

Οι υπηρεσίες αντίδρασης είναι σχεδιασμένες με τρόπο ώστε να ανταποκρίνονται σε αιτήματα παροχής υποστήριξης, αναφορές περιστατικών από την κοινότητα αποδεκτών της ομάδας CSIRT και οποιεσδήποτε απειλές ή επιθέσεις ενάντια στα συστήματα CSIRT. Ορισμένες υπηρεσίες μπορεί να εισάγονται μέσω ειδοποίησης τρίτων ή μέσω της παρακολούθησης των ημερολογίων και συναγερμών IDS.

Συναγερμοί και Προειδοποιήσεις

Η εν λόγω υπηρεσία αφορά τη διάχυση πληροφοριών που περιγράφουν την επίθεση ενός εισβολέα, μια αδυναμία ασφαλείας, έναν συναγερμό εισβολής, έναν ιό ή ένα πλαστό μήνυμα και την παροχή οποιασδήποτε βραχυπρόθεσμης ενδεδειγμένης πορείας δράσης για την αντιμετώπιση του σχετικού προβλήματος. Ο συναγερμός, η ειδοποίηση ή το συμβουλευτικό αποστέλλονται ως αντίδραση στο υφιστάμενο πρόβλημα, προκειμένου να ενημερωθούν οι αποδέκτες για τη δραστηριότητα και να παρασχεθεί καθοδήγηση για την προστασία των συστημάτων τους ή την επαναφορά οποιουδήποτε συστήματος έχει προσβληθεί. Οι πληροφορίες μπορεί να συγκεντρωθούν από την ομάδα CSIRT ή

μπορεί να αναδιανεμηθούν από προμηθευτές, άλλες ομάδες CSIRT ή ειδικούς ασφαλείας ή άλλα τμήματα της κοινότητας αποδεκτών.

Αντιμετώπιση Περιστατικών

Η αντιμετώπιση περιστατικών εμπεριέχει τη λήψη, τη διαλογή και την απόκριση σε αιτήματα και αναφορές και τις αναλύσεις περιστατικών και συμβάντων. Συγκεκριμένες δραστηριότητες απόκρισης μπορεί να περιλαμβάνουν τα εξής:

- ανάληψη δράσης για την προστασία των συστημάτων και των δικτύων που προσβλήθηκαν ή απειλήθηκαν από τη δραστηριότητα του εισβολέα,
- παροχή λύσεων και στρατηγικών μετριασμού από σχετικά συμβουλευτικά ή συναγερμούς,
- αναζήτηση δραστηριότητας του εισβολέα σε άλλα τμήματα του δικτύου,
- φιλτράρισμα κυκλοφορίας του δικτύου,
- αναδόμηση συστημάτων,
- προσωρινή επιδιόρθωση ή επισκευή των συστημάτων,
- ανάπτυξη άλλων στρατηγικών απόκρισης ή παράκαμψης.

Εφόσον οι δραστηριότητες αντιμετώπισης περιστατικών εφαρμόζονται με διαφορετικούς τρόπους από τις διαφόρων ειδών ομάδες CSIRT, η εν λόγω υπηρεσία χωρίζεται σε περαιτέρω κατηγορίες με βάση τον τύπο των δραστηριοτήτων που πραγματοποιούνται και τον τύπο της υποστήριξης που παρέχεται ως εξής:

Ανάλυση περιστατικών

Υπάρχουν πολλά επίπεδα ανάλυσης περιστατικών και πολλές επιμέρους υπηρεσίες. Ουσιαστικά, η ανάλυση περιστατικών αποτελεί μια εξέταση όλων των διαθέσιμων πληροφοριών και των υποστηρικτικών αποδεικτικών στοιχείων ή ευρημάτων που σχετίζονται με ένα περιστατικό ή ένα συμβάν. Ο σκοπός της ανάλυσης είναι να διαπιστωθεί το εύρος του περιστατικού, το εύρος της ζημίας που προκλήθηκε από το περιστατικό, η φύση του περιστατικού και οι διαθέσιμες στρατηγικές απόκρισης ή παράκαμψης. Η ομάδα CSIRT μπορεί να χρησιμοποιήσει τα αποτελέσματα της ανάλυσης αδυναμιών και ευρημάτων (περιγράφεται παρακάτω), προκειμένου να κατανοήσει και να πραγματοποιήσει την πιο ολοκληρωμένη και ενημερωμένη ανάλυση αυτού που συνέβη σε ένα συγκεκριμένο σύστημα. Η ομάδα CSIRT συσχετίζει τη δραστηριότητα μεταξύ περιστατικών, προκειμένου να εντοπίσει οποιονδήποτε συσχετισμό, οποιαδήποτε τάση, οποιοδήποτε επαναλαμβανόμενο μοντέλο ή υπογραφές εισβολέων. Δύο επιμέρους υπηρεσίες που μπορούν να πραγματοποιηθούν στο πλαίσιο της ανάλυσης περιστατικών, ανάλογα με την αποστολή, τους στόχους και τις διαδικασίες της ομάδας CSIRT, είναι οι εξής:

Συλλογή αποδεικτικών στοιχείων

Η συλλογή, η διατήρηση, η τεκμηρίωση και η ανάλυση των αποδεικτικών στοιχείων από ένα υπολογιστικό σύστημα που έχει προσβληθεί, προκειμένου να εντοπιστούν οι μεταβολές στο σύστημα και να διευκολυνθεί η αναπαράσταση των συμβάντων που οδήγησαν στην προσβολή. Η εν λόγω συλλογή πληροφοριών και αποδεικτικών στοιχείων θα πρέπει να πραγματοποιείται με τρόπο ώστε να τεκμηριώνεται ένα αποδείξιμο σύστημα διασύνδεσης, το οποίο μπορεί να γίνει δεκτό σε δικαστήριο σύμφωνα με τους κανόνες αποδείξεως. Οι εργασίες που περιλαμβάνονται στη συλλογή αποδεικτικών στοιχείων περιλαμβάνουν (δίχως να περιορίζονται σε αυτές) τη δημιουργία

ενός αντιγράφου του σκληρού δίσκου του συστήματος που έχει προσβληθεί με τη μορφή εικόνας bit, τον έλεγχο για αλλαγές στο σύστημα, όπως νέα προγράμματα, αρχεία, υπηρεσίες και χρήστες, την αναζήτηση εκτελούμενων διεργασιών και ανοικτών θυρών και τον έλεγχο για προγράμματα ''δούρειους ίππους'' και εργαλειοθήκες. Το προσωπικό της ομάδας CSIRT το οποίο επιτελεί την εν λόγω λειτουργία μπορεί να πρέπει να είναι έτοιμο να ενεργήσει και με την ιδιότητα του εξειδικευμένου μάρτυρα σε περίπτωση προσφυγής στο δικαστήριο.

Εντοπισμός ή ανίχνευση

Η ανίχνευση της προέλευσης ενός εισβολέα ή ο εντοπισμός των συστημάτων στα οποία είχε πρόσβαση ο εισβολέας. Η εν λόγω δραστηριότητα μπορεί να περιλαμβάνει τον εντοπισμό ή την ανίχνευση του τρόπου με τον οποίο ο εισβολέας εισήλθε στα συστήματα που προσβλήθηκαν και τα συναφή δίκτυα, των συστημάτων τα οποία χρησιμοποιήθηκαν για την απόκτηση της εν λόγω πρόσβασης, του σημείου από το οποίο ξεκίνησε η επίθεση και των υπόλοιπων συστημάτων και δικτύων που χρησιμοποιήθηκαν στο πλαίσιο της επίθεσης. Επίσης, μπορεί να περιλαμβάνει τη προσπάθεια καθορισμού της ταυτότητας του εισβολέα. Η εν λόγω εργασία μπορεί να πραγματοποιηθεί μεμονωμένα, αλλά συνήθως προϋποθέτει τη συνεργασία με το προσωπικό της επιβολής του νόμου, τους παρόχους υπηρεσιών Διαδικτύου ή άλλους εμπλεκόμενους οργανισμούς.

Επιτόπια απόκριση σε περιστατικά

Η ομάδα CSIRT παρέχει άμεση ηλεκτρονική υποστήριξη προκειμένου να βοηθήσει τους αποδέκτες να επανέλθουν μετά από ένα περιστατικό. Η ίδια η ομάδα CSIRT αναλύει το υλικό των συστημάτων που έχουν προσβληθεί και πραγματοποιεί την επιδιόρθωση και την αποκατάσταση των συστημάτων, αντί να παρέχει απλώς υποστήριξη μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου για την αντιμετώπιση ενός περιστατικού (βλέπε παρακάτω). Η εν λόγω υπηρεσία περιλαμβάνει όλες τις ενέργειες που πραγματοποιούνται σε τοπικό επίπεδο και οι οποίες είναι απαραίτητες σε περίπτωση που υπάρχει υποψία ή προκύπτει ένα περιστατικό. Εάν η ομάδα CSIRT δεν βρίσκεται στο σημείο που έχει προσβληθεί, τα μέλη της ομάδας μεταβαίνουν στο εν λόγω σημείο και αντιμετωπίζουν το περιστατικό. Σε άλλες περιπτώσεις, μπορεί να βρίσκεται σε ετοιμότητα μια τοπική ομάδα, η οποία αντιμετωπίζει το περιστατικό στο πλαίσιο της καθημερινής της εργασίας. Αυτό ισχύει ιδιαίτερα εάν το περιστατικό αντιμετωπίζεται στο πλαίσιο της συνήθους εργασίας των διαχειριστών του συστήματος, του δικτύου ή των υπευθύνων ασφαλείας αντί μιας καθιερωμένης ομάδας CSIRT.

Υποστήριξη απόκρισης σε περιστατικά

Η ομάδα CSIRT υποστηρίζει και καθοδηγεί το ή τα θύματα της επίθεσης, ώστε να επανέλθουν μετά από ένα περιστατικό, μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου, φαξ ή τεκμηρίωσης. Αυτό μπορεί να περιλαμβάνει την τεχνική υποστήριξη στην ερμηνεία των δεδομένων που έχουν συλλεχθεί, την παροχή στοιχείων επικοινωνίας ή την παροχή καθοδήγησης για τις στρατηγικές μετριασμού και αποκατάστασης. Δεν περιλαμβάνει τις ενέργειες άμεσης, επιτόπιας αντιμετώπισης περιστατικού που περιγράφηκαν παραπάνω. Αντ' αυτού, η ομάδα CSIRT παρέχει καθοδήγηση εξ αποστάσεως, ώστε το τοπικό προσωπικό να μπορεί από μόνο του να προχωρήσει στην αποκατάσταση.

Συντονισμός απόκρισης σε περιστατικά

Η ομάδα CSIRT συντονίζει την προσπάθεια αντιμετώπισης του περιστατικού μεταξύ των φορέων που εμπλέκονται σε αυτό. Σε αυτούς συνήθως περιλαμβάνεται το θύμα της επίθεσης, άλλα σημεία που εμπλέκονται στην επίθεση και οποιοδήποτε σημείο απαιτεί υποστήριξης για την ανάλυση της επίθεσης. Μπορεί επίσης να περιλαμβάνει τους φορείς που παρέχουν πληροφοριακή υποστήριξη στο θύμα, όπως οι πάροχοι υπηρεσιών Διαδικτύου, άλλες ομάδες CSIRT και οι επιτόπιοι διαχειριστές συστήματος και δικτύου. Η εργασία συντονισμού μπορεί να περιλαμβάνει τη συλλογή στοιχείων επικοινωνίας, την ενημέρωση τοποθεσιών για την πιθανή εμπλοκή τους (ως θύματα ή ως πηγές μιας επίθεσης), τη συλλογή στατιστικών στοιχείων για τον αριθμό των εμπλεκόμενων τοποθεσιών και τη διευκόλυνση της ανταλλαγής πληροφοριών και της ανάλυσης. Μέρος της εργασίας συντονισμού μπορεί να περιλαμβάνει την ενημέρωση και τη συνεργασία με τον νομικό σύμβουλο ενός οργανισμού ή με τα τμήματα δημοσίων σχέσεων. Θα μπορούσε επίσης να περιλαμβάνει το συντονισμό με τις υπηρεσίες επιβολής του νόμου. Η εν λόγω υπηρεσία δεν περιλαμβάνει ενέργειες άμεσης επιτόπιας αντιμετώπισης περιστατικού.

Αντιμετώπιση αδυναμιών

Η αντιμετώπιση αδυναμιών περιλαμβάνει τη λήψη πληροφοριών και αναφορών σχετικά με αδυναμίες του υλικού και του λογισμικού, την ανάλυση της φύσης, των μηχανισμών και των αποτελεσμάτων των αδυναμιών, καθώς και την ανάπτυξη των στρατηγικών αντιμετώπισης για τον εντοπισμό και την επιδιόρθωση των αδυναμιών. Εφόσον οι δραστηριότητες αντιμετώπισης αδυναμιών εφαρμόζονται με διαφορετικούς τρόπους από τις διαφόρων ειδών ομάδες CSIRT, η εν λόγω υπηρεσία χωρίζεται σε περαιτέρω κατηγορίες με βάση τον τύπο των δραστηριοτήτων που πραγματοποιούνται και τον τύπο της υποστήριξης που παρέχεται ως εξής:

Ανάλυση αδυναμιών

Η ομάδα CSIRT πραγματοποιεί την τεχνική ανάλυση και την εξέταση των αδυναμιών του υλικού ή του λογισμικού. Σε αυτήν περιλαμβάνεται η επαλήθευση των ύποπτων αδυναμιών και η τεχνική εξέταση της αδυναμίας του υλικού ή του λογισμικού, προκειμένου να εντοπισθεί πού βρίσκεται και πώς μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης. Η ανάλυση μπορεί να περιλαμβάνει την εξέταση του πηγαίου κώδικα, χρησιμοποιώντας πρόγραμμα αποσφαλμάτωσης, προκειμένου να εντοπισθεί πού βρίσκεται η αδυναμία ή επιχειρώντας την αναπαραγωγή του προβλήματος σε ένα δοκιμαστικό σύστημα.

Απόκριση σε αδυναμίες

Η εν λόγω υπηρεσία περιλαμβάνει τον καθορισμό της κατάλληλης απόκρισης για τον μετριασμό ή την επιδιόρθωση της αδυναμίας. Σε αυτή την υπηρεσία μπορεί να περιλαμβάνεται η ανάπτυξη ή αναζήτηση προσωρινών ή μόνιμων διορθωτικών προγραμμάτων και παρακάμψεων. Επίσης, περιλαμβάνει την ενημέρωση άλλων για τη στρατηγική μετριασμού, ενδεχομένως δημιουργώντας και διανέμοντας συμβουλευτικά ή συναγερμούς. Η εν λόγω υπηρεσία μπορεί να περιλαμβάνει απόκριση μέσω της εγκατάστασης προσωρινών ή διορθωτικών προγραμμάτων ή παρακάμψεων.

Συντονισμός απόκρισης σε αδυναμίες

Η ομάδα CSIRT ενημερώνει τα διάφορα τμήματα της εταιρείας ή την κοινότητα αποδεκτών για την αδυναμία και ανταλλάσσει πληροφορίες για τον τρόπο επιδιόρθωσης ή μετριασμού της αδυναμίας. Η ομάδα CSIRT επαληθεύει ότι η στρατηγική αντιμετώπισης της αδυναμίας εφαρμόσθηκε επιτυχώς. Η εν λόγω υπηρεσία μπορεί να περιλαμβάνει την επικοινωνία με προμηθευτές, άλλες ομάδες CSIRT, ειδικούς τεχνικούς, μέλη της κοινότητας αποδεκτών και τα άτομα ή τις ομάδες που εντόπισαν ή ανέφεραν αρχικά την αδυναμία. Οι δραστηριότητες περιλαμβάνουν τη διευκόλυνση της ανάλυσης μιας αδυναμίας ή αναφοράς αδυναμίας, τον συντονισμό των χρονοδιαγραμμάτων έκδοσης των αντίστοιχων εγγράφων, διορθωτικών προγραμμάτων ή παρακάμψεων και τη σύνθεση της τεχνικής ανάλυσης που πραγματοποιείται από διάφορους φορείς. Η εν λόγω υπηρεσία μπορεί επίσης να περιλαμβάνει τη διατήρηση ενός δημόσιου ή ιδιωτικού αρχείου ή μιας βάσης γνώσεων με πληροφορίες σχετικά με την αδυναμία και τις αντίστοιχες στρατηγικές αντιμετώπισης.

Αντιμετώπιση ευρημάτων

Εύρημα είναι οποιοδήποτε αρχείο ή αντικείμενο εντοπίζεται σε ένα σύστημα, το οποίο μπορεί να εμπλέκεται στη διερεύνηση ή την προσβολή συστημάτων και δικτύων ή το οποίο χρησιμοποιείται για την ανατροπή των μέτρων ασφαλείας. Τα ευρήματα μπορεί να περιλαμβάνουν, μεταξύ άλλων, ιούς υπολογιστών, προγράμματα ''δούρειους ίππους'', σκουλήκια, σενάρια επίθεσης και εργαλειοθήκες.
Η αντιμετώπιση ευρημάτων περιλαμβάνει τη λήψη πληροφοριών και αντιγράφων των ευρημάτων που χρησιμοποιούνται στις επιθέσεις των εισβολέων, τις αναγνωρίσεις και άλλες μη εξουσιοδοτημένες ή επιζήμιες δραστηριότητες. Μόλις ληφθεί το εύρημα, εξετάζεται. Η εν λόγω εξέταση περιλαμβάνει την ανάλυση της φύσης, των μηχανισμών, της έκδοσης και της χρήσης των ευρημάτων και την ανάπτυξη (ή την πρόταση) στρατηγικών αντιμετώπισης για τον εντοπισμό, την απομάκρυνση και την υπεράσπιση έναντι των εν λόγω ευρημάτων. Εφόσον οι δραστηριότητες αντιμετώπισης ευρημάτων εφαρμόζονται με διαφορετικούς τρόπους από τις διαφόρων ειδών ομάδες CSIRT, η εν λόγω υπηρεσία χωρίζεται σε περαιτέρω κατηγορίες με βάση τον τύπο των δραστηριοτήτων που πραγματοποιούνται και τον τύπο της υποστήριξης που παρέχεται ως εξής:

Ανάλυση ευρημάτων

Η ομάδα CSIRT πραγματοποιεί τεχνική εξέταση και ανάλυση οποιουδήποτε ευρήματος εντοπίζεται σε ένα σύστημα. Η ανάλυση που πραγματοποιείται μπορεί να περιλαμβάνει τον εντοπισμό του τύπου του αρχείου και της δομής του ευρήματος, τη σύγκριση ενός νέου ευρήματος έναντι υφιστάμενων ευρημάτων ή άλλων εκδοχών του ίδιου ευρήματος προκειμένου να διαπιστωθούν οι ομοιότητες και οι διαφορές, ή την ανάστροφη μηχανική ή την αποσύνθεση του κώδικα προκειμένου να διαπιστωθεί ο σκοπός και η λειτουργία του ευρήματος.

Απόκριση σε ευρήματα

Η εν λόγω υπηρεσία περιλαμβάνει τον καθορισμό των κατάλληλων ενεργειών για τον εντοπισμό και την απομάκρυνση των ευρημάτων από ένα σύστημα, καθώς και των ενεργειών για την αποφυγή της εγκατάστασης των ευρημάτων. Η εν λόγω υπηρεσία μπορεί να περιλαμβάνει τη δημιουργία υπογραφών που μπορούν να προστεθούν σε αντιβιοτικό λογισμικό ή IDS.

Συντονισμός απόκρισης σε ευρήματα

Η εν λόγω υπηρεσία περιλαμβάνει την ανταλλαγή και τη σύνθεση των αποτελεσμάτων της ανάλυσης και των στρατηγικών αντιμετώπισης σε σχέση με ένα εύρημα με άλλους ερευνητές, άλλες ομάδες CSIRT, προμηθευτές και άλλους ειδικούς ασφαλείας. Στις δραστηριότητες περιλαμβάνεται η ενημέρωση άλλων φορέων και η σύνθεση της τεχνικής ανάλυσης από μια πληθώρα πηγών. Επίσης, στις δραστηριότητες περιλαμβάνεται η διατήρηση ενός δημόσιου ή ιδιωτικού αρχείου αποδεκτών με τα γνωστά ευρήματα, τον αντίκτυπό τους, καθώς και τις αντίστοιχες στρατηγικές αντιμετώπισης.

Υπηρεσίες Πρόληψης

Οι υπηρεσίες πρόληψης είναι σχεδιασμένες με τρόπο ώστε να βελτιώνεται η υποδομή και οι διαδικασίες ασφαλείας της κοινότητας αποδεκτών προτού πραγματοποιηθεί ή εντοπιστεί οποιοδήποτε περιστατικό ή συμβάν. Οι κύριοι στόχοι είναι να αποφεύγονται τα περιστατικά και να μειώνεται ο αντίκτυπος και το εύρος τους όταν πραγματοποιούνται.

Ανακοινώσεις

Σε αυτές περιλαμβάνονται, μεταξύ άλλων, οι συναγερμοί για εισβολές, οι προειδοποιήσεις για αδυναμίες και τα συμβουλευτικά ασφαλείας. Τέτοιου είδους ανακοινώσεις ενημερώνουν τους αποδέκτες για νέες εξελίξεις με μεσο-μακροπρόθεσμο αντίκτυπο, όπως αδυναμίες ή εργαλεία εισβολέων που μόλις έχουν εντοπισθεί. Οι ανακοινώσεις επιτρέπουν στους αποδέκτες να προστατεύσουν τα συστήματα και τα δίκτυά τους έναντι προβλημάτων που μόλις έχουν εντοπιστεί προτού γίνουν αντικείμενο εκμετάλλευσης.

Παρακολούθηση Τεχνολογίας

Η ομάδα CSIRT παρακολουθεί τις νέες τεχνολογικές εξελίξεις, τις δραστηριότητες των εισβολέων και συναφείς τάσεις προκειμένου να βοηθήσει στον εντοπισμό μελλοντικών απειλών. Τα θέματα που εξετάζονται μπορεί να επεκτείνονται ώστε να περιλαμβάνουν και νομικούς και νομοθετικούς κανονισμούς, κοινωνικές ή πολιτικές απειλές και αναδυόμενες τεχνολογίες. Η εν λόγω υπηρεσία περιλαμβάνει την ανάγνωση των καταλόγων αλληλογραφίας που σχετίζονται με την ασφάλεια, των ιστοσελίδων για την ασφάλεια, καθώς και των υφιστάμενων ειδήσεων και δημοσιογραφικών άρθρων στον τομέα της επιστήμης, της τεχνολογίας, της πολιτικής και της διακυβέρνησης, για εξαγωγή πληροφοριών αναφορικά με την ασφάλεια των συστημάτων και των δικτύων των αποδεκτών. Η εν λόγω δραστηριότητα μπορεί να περιλαμβάνει την επικοινωνία με άλλες αρχές των εν λόγω πεδίων, προκειμένου να διασφαλιστεί ότι λαμβάνονται οι καλύτερες και πιο ακριβείς πληροφορίες ή ερμηνείες. Το αποτέλεσμα αυτής της υπηρεσίες μπορεί να έχει τη μορφή ανακοίνωσης, οδηγιών ή συστάσεων που εστιάζουν σε πιο μεσο-μακροπρόθεσμα ζητήματα ασφαλείας.

Έλεγχοι ή Αξιολογήσεις Ασφαλείας

Η εν λόγω υπηρεσία περιλαμβάνει μια λεπτομερή ανασκόπηση και ανάλυση της πληροφοριακής υποδομής ενός οργανισμού με βάση τις απαιτήσεις που ορίζονται από τον οργανισμό ή άλλα ισχύοντα πρότυπα του τομέα. Μπορεί επίσης να περιλαμβάνει την ανασκόπηση των πρακτικών ασφαλείας του οργανισμού. Υπάρχουν πολλά διαφορετικά είδη ελέγχων ή αξιολογήσεων που μπορούν να παρασχεθούν, συμπεριλαμβανομένων των εξής:

Ανασκόπηση υποδομής

Χειρωνακτική εξέταση της διαμόρφωσης του υλικού και του λογισμικού, των δρομολογητών, των τειχών προστασίας, των διακομιστών και των περιφερειακών συσκευών, προκειμένου να διασφαλισθεί ότι ταιριάζουν με τη βέλτιστη πρακτική στις πολιτικές ασφαλείας του οργανισμού ή του τομέα και τις τυπικές διαμορφώσεις.

Ανασκόπηση βέλτιστης πρακτικής

Πραγματοποίηση συνεντεύξεων με υπαλλήλους και διαχειριστές του συστήματος και του δικτύου, προκειμένου να διαπιστωθεί εάν οι πρακτικές ασφαλείας τους ταιριάζουν με την καθορισμένη πολιτική ασφαλείας του οργανισμού ή συγκεκριμένα πρότυπα του τομέα.

Σάρωση

Χρήση σαρωτών αδυναμιών ή ιών, προκειμένου να διαπιστωθεί ποια συστήματα και ποια δίκτυα είναι ευπαθή.

Δοκιμή διείσδυσης

Δοκιμή ασφαλείας μιας τοποθεσίας πραγματοποιώντας σκόπιμη επίθεση στα συστήματα και τα δίκτυά της.
Απαιτείται η λήψη της έγκρισης της ανώτερης διοίκησης πριν από την πραγματοποίηση τέτοιων ελέγχων ή αξιολογήσεων. Ορισμένες από τις εν λόγω προσεγγίσεις μπορεί να απαγορεύονται από την πολιτική του οργανισμού. Η παροχή της εν λόγω υπηρεσίας μπορεί να περιλαμβάνει την ανάπτυξη μιας κοινής ομάδας πρακτικών, έναντι των οποίων διεξάγονται οι δοκιμές ή οι αξιολογήσεις, σε συνδυασμό με την ανάπτυξη μιας ομάδας απαιτούμενων δεξιοτήτων ή προϋποθέσεων πιστοποίησης για το προσωπικό που πραγματοποιεί τη δοκιμή, τις αξιολογήσεις, τους ελέγχους ή την ανασκόπηση. Η εν λόγω υπηρεσία θα μπορούσε επίσης να ανατεθεί σε τρίτο ανάδοχο ή σε παροχέα υπηρεσιών διαχείρισης ασφαλείας με την κατάλληλη εξειδίκευση στη διεξαγωγή ελέγχων και αξιολογήσεων.

Διαμόρφωση και Συντήρηση Εργαλείων, Εφαρμογών, Υποδομών και Υπηρεσιών Ασφαλείας

Η εν λόγω υπηρεσία αναγνωρίζει ή παρέχει τις κατάλληλες οδηγίες για τον τρόπο ασφαλούς διαμόρφωσης και συντήρησης των εργαλείων, των εφαρμογών και της γενικής υπολογιστικής υποδομής που χρησιμοποιείται από την κοινότητα αποδεκτών της CSIRT ή την ίδια την ομάδα CSIRT. Εκτός από την παροχή καθοδήγησης, η ομάδα CSIRT μπορεί να πραγματοποιεί ενημερώσεις στη διαμόρφωση και να προβαίνει στη συντήρηση εργαλείων και υπηρεσιών, όπως IDS, συστήματα σάρωσης ή παρακολούθησης δικτύων, φίλτρα, τείχη προστασίας, εικονικά ιδιωτικά δίκτυα (VPN), ή και μηχανισμοί πιστοποίησης ταυτότητας. Η ομάδα CSIRT μπορεί ακόμη να παρέχει τις εν λόγω υπηρεσίες στο πλαίσιο της κύριας λειτουργίας της. Επίσης, η ομάδα CSIRT μπορεί να προβαίνει σε διαμόρφωση και συντήρηση διακομιστών, επιτραπέζιων υπολογιστών, φορητών υπολογιστών, προσωπικών ψηφιακών βοηθών (PDA) και άλλων ασύρματων συσκευών σύμφωνα με τις οδηγίες ασφαλείας. Η εν λόγω υπηρεσία περιλαμβάνει την διαβίβαση στη διοίκηση οποιουδήποτε ζητήματος ή προβλήματος σχετικά με τη διαμόρφωση ή τη χρήση εργαλείων και εφαρμογών που η ομάδα CSIRT θεωρεί ότι μπορεί να επιτρέψουν επίθεση ενάντια στο σύστημα.

Ανάπτυξη Εργαλείων Ασφαλείας

Η εν λόγω υπηρεσία περιλαμβάνει την ανάπτυξη νέων εργαλείων ειδικά για τους αποδέκτες που απαιτεί ή επιθυμεί η κοινότητα αποδεκτών ή η ίδια η ομάδα CSIRT. Μπορεί, για παράδειγμα, να περιλαμβάνει την ανάπτυξη διορθωτικών προγραμμάτων ασφαλείας για προσαρμοσμένο λογισμικό που χρησιμοποιείται από την κοινότητα αποδεκτών ή τη διανομή ασφαλούς λογισμικού, το οποίο μπορεί να χρησιμοποιηθεί για την αναδόμηση κεντρικών υπολογιστών που έχουν προσβληθεί. Επίσης, μπορεί να περιλαμβάνει την ανάπτυξη εργαλείων ή σεναρίων που επεκτείνουν τη λειτουργικότητα των υφιστάμενων εργαλείων ασφαλείας, όπως ένα νέο πρόσθετο (plug-in) για μια αδυναμία ή ένας νέος σαρωτής δικτύου, σενάρια τα οποία διευκολύνουν τη χρήση τεχνολογίας κρυπτογράφησης ή μηχανισμοί αυτοματοποιημένης διανομής διορθωτικών προγραμμάτων.

Υπηρεσίες Εντοπισμού Εισβολής

Οι ομάδες CSIRT που παρέχουν την εν λόγω υπηρεσία εξετάζουν τα υφιστάμενα ημερολόγια IDS, αναλύουν και προτείνουν μια αντιμετώπιση για οποιοδήποτε συμβάν ικανοποιεί το κατώφλι που έχουν ορίσει ή διαβιβάζουν οποιονδήποτε συναγερμό σύμφωνα με μια προκαθορισμένη συμφωνία επιπέδου υπηρεσιών ή μια στρατηγική κλιμάκωσης. Ο εντοπισμός της εισβολής και η ανάλυση των υφιστάμενων ημερολογίων ασφαλείας μπορεί να αποτελεί πρόκληση - όχι μόνο ως προς τον καθορισμό του σημείου στο οποίο εντοπίζονται οι ανιχνευτές στο περιβάλλον, αλλά και ως προς τη συλλογή και κατόπιν την ανάλυση της μεγάλης ποσότητας των δεδομένων που συλλέγονται. Σε πολλές περιπτώσεις, απαιτούνται ειδικά εργαλεία ή εξειδίκευση για τη σύνθεση και την ερμηνεία των πληροφοριών, προκειμένου να εντοπισθούν οι εσφαλμένοι συναγερμοί, οι επιθέσεις ή τα δικτυακά συμβάντα και να εφαρμοσθούν στρατηγικές για την εξάλειψη ή την ελαχιστοποίηση τέτοιων συμβάντων. Ορισμένοι οργανισμοί επιλέγουν να αναθέτουν εξωτερικά την εν λόγω δραστηριότητα σε άλλους, οι οποίοι είναι πιο εξειδικευμένοι στην παροχή των εν λόγω υπηρεσιών, όπως οι παροχείς υπηρεσιών διαχείρισης ασφαλείας.

Διάχυση Πληροφοριών για την Ασφάλεια

Η εν λόγω υπηρεσία παρέχει στους αποδέκτες μια ολοκληρωμένη και εύκολα προσβάσιμη συλλογή χρήσιμων πληροφοριών που συμβάλλει στη βελτίωση της ασφάλειας. Στις εν λόγω πληροφορίες μπορεί να περιλαμβάνονται τα εξής:

- οδηγίες σύνταξης αναφορών και στοιχεία επικοινωνίας για την ομάδα CSIRT,
- αρχεία συναγερμών, προειδοποιήσεων και άλλων ανακοινώσεων,
- τεκμηρίωση σχετικά με τις υφιστάμενες βέλτιστες πρακτικές,
- γενικές οδηγίες ασφαλείας για υπολογιστές,
- πολιτικές, διαδικασίες και καταλόγους ελέγχου,
- πληροφορίες για την ανάπτυξη και τη διανομή διορθωτικών προγραμμάτων,
- σύνδεσμοι προμηθευτών,
- υφιστάμενες στατιστικές και τάσεις στις αναφορές περιστατικών,
- άλλες πληροφορίες που μπορούν να βελτιώσουν τις συνολικές πρακτικές ασφαλείας.

Οι εν λόγω πληροφορίες μπορεί να αναπτύσσονται και να δημοσιεύονται από την ομάδα CSIRT ή από άλλο τμήμα του οργανισμού (IT, ανθρωπίνων πόρων ή δημοσίων σχέσεων) και μπορούν να περιλαμβάνουν πληροφορίες από εξωτερικούς πόρους, όπως άλλες ομάδες CSIRT, προμηθευτές και ειδικοί ασφαλείας.

Υπηρεσίες Διαχείρισης Ποιότητας Ασφαλείας

Οι υπηρεσίες που εμπίπτουν σε αυτή την κατηγορία δεν αφορούν αποκλειστικά την αντιμετώπιση περιστατικών ή τις ομάδες CSIRT. Είναι γνωστές καθιερωμένες υπηρεσίες που έχουν σχεδιαστεί για τη βελτίωση της συνολικής ασφάλειας ενός οργανισμού. Αξιοποιώντας τις εμπειρίες που έχει αποκομίσει από την παροχή των υπηρεσιών αντίδρασης και πρόληψης που περιγράφηκαν παραπάνω, μια ομάδα CSIRT μπορεί να προσφέρει μοναδικές προοπτικές στις εν λόγω υπηρεσίες διαχείρισης ποιότητας που σε διαφορετική περίπτωση μπορεί να μην ήταν διαθέσιμες. Οι εν λόγω υπηρεσίες είναι σχεδιασμένες με τρόπο ώστε να ενσωματώνεται το υλικό ανατροφοδότησης και τα διδάγματα με βάση τη γνώση που αποκτήθηκε κατά την αντιμετώπιση περιστατικών, αδυναμιών και επιθέσεων. Η τροφοδότηση τέτοιων εμπειριών στις καθιερωμένες παραδοσιακές υπηρεσίες (περιγράφονται παρακάτω) στο πλαίσιο μιας διαδικασίας διαχείρισης ποιότητας ασφάλειας μπορεί να βελτιώσει τις μακροπρόθεσμες προσπάθειες για την ασφάλεια ενός οργανισμού. Ανάλογα με τις οργανωτικές δομές και τις αρμοδιότητες, μια ομάδα CSIRT μπορεί να παρέχει τις εν λόγω υπηρεσίες ή να συμμετέχει στο πλαίσιο της προσπάθειας μιας ευρύτερης οργανωτικής ομάδας.
Οι παρακάτω περιγραφές εξηγούν τον τρόπο με τον οποίο η εξειδίκευση της ομάδας CSIRT μπορεί να ωφελήσει καθεμιά από τις εν λόγω υπηρεσίες διαχείρισης ποιότητας ασφαλείας.

Ανάλυση Κινδύνου

Οι ομάδες CSIRT μπορεί να είναι σε θέση να συμβάλλουν στην ανάλυση και τις εκτιμήσεις κινδύνου. Αυτό μπορεί να βελτιώσει τη δυνατότητα του οργανισμού να εκτιμά τις πραγματικές απειλές, να παρέχει ρεαλιστικές ποιοτικές και ποσοτικές εκτιμήσεις των κινδύνων για τους πληροφοριακούς πόρους και να αξιολογεί τις στρατηγικές προστασίας και αντίδρασης. Οι ομάδες CSIRT που παρέχουν την εν λόγω υπηρεσία θα διεξάγουν δραστηριότητες ανάλυσης του κινδύνου ασφαλείας των πληροφοριών, θα τις υποστηρίζουν για νέα συστήματα και επιχειρηματικές διαδικασίες ή θα αξιολογούν απειλές και επιθέσεις ενάντια σε πόρους και συστήματα των αποδεκτών.

Σχεδιασμός Επιχειρηματικής Συνέχειας και Ανάκαμψης μετά από Καταστροφή

Σύμφωνα με προηγούμενα περιστατικά και μελλοντικές προβλέψεις για αναδυόμενα περιστατικά ή τάσεις στον τομέα της ασφάλειας, ολοένα και περισσότερα περιστατικά μπορεί να οδηγήσουν σε σοβαρή υποβάθμιση των επιχειρηματικών λειτουργιών. Επομένως, οι προσπάθειες σχεδιασμού θα πρέπει να λαμβάνουν υπόψη την εμπειρία και τις συστάσεις της ομάδας CSIRT, προκειμένου να καθορισθεί ποιος είναι ο βέλτιστος τρόπος αντιμετώπισης των εν λόγω περιστατικών ώστε να διασφαλίζεται η συνέχεια των επιχειρηματικών λειτουργιών. Οι ομάδες CSIRT που παρέχουν την εν λόγω υπηρεσία συμμετέχουν στο σχεδιασμό της επιχειρηματικής συνέχειας και της ανάκαμψης από καταστροφές για συμβάντα που σχετίζονται με τις απειλές και τις επιθέσεις ασφαλείας σε υπολογιστές.

Συμβουλευτικές Υπηρεσίες Ασφαλείας

Οι ομάδες CSIRT μπορούν να χρησιμοποιηθούν για την παροχή συμβουλών και καθοδήγησης σχετικά με τις βέλτιστες πρακτικές ασφαλείας που θα πρέπει να εφαρμόζονται στις επιχειρηματικές λειτουργίες των αποδεκτών. Μια ομάδα CSIRT που παρέχει την εν λόγω υπηρεσία συμμετέχει στη σύνταξη συστάσεων ή στον καθορισμό των απαιτήσεων για την αγορά, την εγκατάσταση ή τη θωράκιση νέων συστημάτων,

συσκευών δικτύου, εφαρμογών λογισμικού ή επιχειρηματικών διαδικασιών ολόκληρης της εταιρείας. Η εν λόγω υπηρεσία περιλαμβάνει την παροχή καθοδήγησης και υποστήριξης στην ανάπτυξη πολιτικών ασφαλείας για τον οργανισμό ή την κοινότητα αποδεκτών. Μπορεί επίσης να περιλαμβάνει την παροχή μαρτυρίας ή συμβουλών σε νομοθετικούς ή άλλους κυβερνητικούς φορείς.

Ενίσχυση Ευαισθητοποίησης

Οι ομάδες CSIRT μπορεί να είναι σε θέση να αναγνωρίσουν ποιοι αποδέκτες απαιτούν περισσότερες πληροφορίες και καθοδήγηση, ώστε να συμμορφώνονται σε μεγαλύτερο βαθμό με τις αποδεκτές πρακτικές ασφαλείας και τις πολιτικές ασφαλείας του οργανισμού. Αυξάνοντας τη γενική ευαισθητοποίηση των αποδεκτών σε θέματα ασφαλείας, όχι μόνο βελτιώνεται η κατανόησή τους σε θέματα ασφαλείας, αλλά διευκολύνονται και στην επιτέλεση των καθημερινών λειτουργιών τους με ασφαλέστερο τρόπο. Κατ' αυτόν τον τρόπο μπορεί να μειωθεί η εμφάνιση επιτυχημένων επιθέσεων και να αυξηθεί η πιθανότητα εντοπισμού και αναφοράς επιθέσεων από τους αποδέκτες, μειώνοντας έτσι τους χρόνους απόκρισης ή ελαχιστοποιώντας τις απώλειες.
Οι ομάδες CSIRT που παρέχουν την εν λόγω υπηρεσία αναζητούν ευκαιρίες για την αύξηση της ευαισθητοποίησης σε θέματα ασφαλείας μέσω της δημιουργίας άρθρων, αφισών, ενημερωτικών δελτίων, ιστοτόπων ή άλλων ενημερωτικών πόρων που εξηγούν τις βέλτιστες πρακτικές ασφαλείας και παρέχουν συμβουλές ή οδηγίες προφύλαξης. Στις δραστηριότητες μπορεί να περιλαμβάνεται η διοργάνωση συναντήσεων και σεμιναρίων, ώστε να ενημερώνονται οι αποδέκτες για τις εξελισσόμενες διαδικασίες ασφαλείας και τις πιθανές απειλές στα συστήματα του οργανισμού.

Εκπαίδευση/κατάρτιση

Η εν λόγω υπηρεσία σχετίζεται με την παροχή πληροφοριών στους αποδέκτες για θέματα ασφάλειας των υπολογιστών μέσω σεμιναρίων, εργαστηρίων, μαθημάτων και προγραμμάτων εκμάθησης. Τα θέματα μπορεί να περιλαμβάνουν οδηγίες σύνταξης αναφορών περιστατικών, κατάλληλες μεθόδους αντίδρασης, εργαλεία αντιμετώπισης περιστατικών, μεθόδους πρόληψης περιστατικών και άλλες πληροφορίες που είναι απαραίτητες για την προστασία, τον εντοπισμό, την αναφορά και την αντίδραση σε περιστατικά ασφάλειας σε υπολογιστές.

Αξιολόγηση ή Πιστοποίηση Προϊόντος

Για την εν λόγω υπηρεσία, η ομάδα CSIRT μπορεί να πραγματοποιεί αξιολογήσεις προϊόντων σε εργαλεία, εφαρμογές ή άλλες υπηρεσίες προκειμένου να διασφαλίζει την ασφάλεια των προϊόντων και τη συμμόρφωσή τους με τις αποδεκτές πρακτικές ασφαλείας της ομάδας CSIRT ή του οργανισμού. Τα εργαλεία κι οι εφαρμογές που εξετάζονται μπορεί να είναι ανοικτού κώδικα ή εμπορικά προϊόντα. Η εν λόγω υπηρεσία μπορεί να παρέχεται ως αξιολόγηση ή μέσω ενός προγράμματος πιστοποίησης, ανάλογα με το πρότυπα που εφαρμόζονται από τον οργανισμό ή την ομάδα CSIRT.

A.3 Τα παραδείγματα

Εικονική Ομάδα CSIRT

Βήμα 0: Κατανοώντας τι είναι μια ομάδα CSIRT

Η δοκιμαστική ομάδα CSIRT θα πρέπει να εξυπηρετεί έναν οργανισμό μεσαίου μεγέθους που αποτελείται από προσωπικό 200 μελών. Ο οργανισμός διαθέτει το δικό του τμήμα πληροφοριακών συστημάτων και δύο άλλα υποκαταστήματα στην ίδια χώρα. Τα πληροφοριακά συστήματα παίζουν βασικό ρόλο για την εταιρεία, επειδή χρησιμοποιούνται για την εσωτερική επικοινωνία, το δίκτυο δεδομένων και τη διεξαγωγή ηλεκτρονικών επιχειρηματικών συναλλαγών 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα. Ο οργανισμός διαθέτει το δικό του δίκτυο και μια ταχύτατη σύνδεση στο διαδίκτυο μέσω δύο διαφορετικών Παροχέων Υπηρεσιών Διαδικτύου (ISP).

- -

Βήμα 1: Φάση έναρξης

Κατά τη φάση έναρξης η νέα ομάδα CSIRT σχεδιάζεται ως Εσωτερική Ομάδα CSIRT, παρέχοντας τις υπηρεσίες της στην εταιρεία στην οποία εντάσσεται, στο τοπικό τμήμα πληροφοριακών συστημάτων και στο προσωπικό. Επίσης, υποστηρίζει και συντονίζει την αντιμετώπιση περιστατικών σχετικών με την ασφάλεια πληροφοριακών συστημάτων μεταξύ των διαφόρων υποκαταστημάτων.

- -

Βήμα 2: Επιλέγοντας τις κατάλληλες υπηρεσίες

Κατά τη φάση έναρξης αποφασίζεται ότι η νέα ομάδα CSIRT θα εστιάσει κυρίως στην παροχή ορισμένων από τις βασικές υπηρεσίες στους υπαλλήλους.

Αποφασίζεται ότι μετά από την πιλοτική φάση μπορεί να εξετασθεί η επέκταση του χαρτοφυλακίου υπηρεσιών και ενδέχεται να προστεθούν ορισμένες Υπηρεσίες Διαχείρισης Ασφαλείας. Η εν λόγω απόφαση θα ληφθεί με βάση το υλικό ανατροφοδότησης από τους πιλοτικούς αποδέκτες και σε στενή συνεργασία με το Τμήμα Διασφάλισης Ποιότητας.

- -

Βήμα 3: Πραγματοποίηση ανάλυσης της κοινότητας αποδεκτών και των κατάλληλων επικοινωνιακών διαύλων

Μια σύσκεψη ανταλλαγής ιδεών με μερικά βασικά στελέχη της διοίκησης και εκπροσώπους της κοινότητας αποδεκτών είχε ως αποτέλεσμα τη δημιουργία επαρκούς υλικού για μια ανάλυση SWOT. Η εν λόγω διαδικασία οδήγησε στο συμπέρασμα ότι υφίσταται ανάγκη για τις βασικές υπηρεσίες:

- συναγερμοί και προειδοποιήσεις,
- αντιμετώπιση περιστατικών (ανάλυση, υποστήριξη απόκρισης και συντονισμός απόκρισης),
- ανακοινώσεις.

Θα πρέπει να διασφαλισθεί ότι οι πληροφορίες διανέμονται σωστά και με οργανωμένο τρόπο, ώστε να απευθύνονται σε όσο το δυνατόν μεγαλύτερο τμήμα της κοινότητας αποδεκτών. Επομένως, λαμβάνεται η απόφαση να δημοσιευτούν συναγερμοί, προειδοποιήσεις και ανακοινώσεις με τη μορφή συμβουλευτικών ασφαλείας σε έναν εξειδικευμένο ιστότοπο και να διανεμηθούν μέσω ενός καταλόγου αλληλογραφίας. Η ομάδα CSIRT διαθέτει ηλεκτρονικό ταχυδρομείο, τηλέφωνο και φαξ για τη λήψη των αναφορών περιστατικών. Ένα ενιαίο ηλεκτρονικό έντυπο σχεδιάζεται για το επόμενο βήμα.

- -

Βήμα 4: Δήλωση Αποστολής

Η διοίκηση της εικονικής ομάδας CSIRT συνέταξε την παρακάτω δήλωση αποστολής:
"Η Εικονική Ομάδα CSIRT παρέχει πληροφορίες και υποστήριξη στο προσωπικό της εταιρείας στην οποία εντάσσεται προκειμένου να μειωθούν οι κίνδυνοι που παρέχονται από περιστατικά ασφαλείας σε υπολογιστές, καθώς και να αντιμετωπίζονται τα εν λόγω περιστατικά όταν προκύπτουν."

Μέσω αυτού, η εικονική ομάδα CSIRT διευκρινίζει ότι αποτελεί εσωτερική ομάδα CSIRT και ότι η κύρια δραστηριότητά της είναι να αντιμετωπίζει τα ζητήματα ασφαλείας πληροφοριακών συστημάτων.

- -

Βήμα 5: Καθορίζοντας το Επιχειρηματικό Σχέδιο

Οικονομικό μοντέλο
Εξαιτίας του γεγονότος ότι η εταιρεία πραγματοποιεί ηλεκτρονικές συναλλαγές 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα και διαθέτει επίσης τμήμα πληροφοριακών συστημάτων που λειτουργεί τις ίδιες ώρες και ημέρες, αποφασίστηκε να παρέχεται πλήρης εξυπηρέτηση κατά τις ώρες γραφείου και εξυπηρέτηση κατόπιν κλήσης εκτός ωρών γραφείου. Οι υπηρεσίες θα παρέχονται δωρεάν στην κοινότητα αποδεκτών, αλλά η πιθανότητα παροχής υπηρεσιών σε εξωτερικούς πελάτες θα εξετάζεται κατά την πιλοτική φάση και τη φάση αξιολόγησης.

Μοντέλο εσόδων
Κατά τη φάση έναρξης και την πιλοτική φάση, η ομάδα CSIRT θα χρηματοδοτείται μέσω της εταιρείας στην οποία εντάσσεται. Κατά την πιλοτική φάση και τη φάση αξιολόγησης, θα συζητηθεί η τυχόν επιπρόσθετη χρηματοδότηση, συμπεριλαμβανομένης της πιθιανότητας πώλησης υπηρεσιών σε εξωτερικούς πελάτες.

Οργανωτικό μοντέλο
Ο οργανισμός είναι μια μικρή εταιρεία και επομένως επιλέγεται το ενσωματωμένο μοντέλο.
Κατά τις ώρες γραφείου προσωπικό τριών ατόμων θα παρέχει τις βασικές υπηρεσίες (διανομή συμβουλευτικών ασφαλείας και αντιμετώπιση περιστατικών/συντονισμός).

Το τμήμα πληροφοριακών συστημάτων της εταιρείας απασχολεί ήδη άτομα με τα κατάλληλα προσόντα. Έχει συναφθεί μια συμφωνία με το εν λόγω τμήμα, ώστε η νέα ομάδα CSIRT να μπορεί να ζητήσει υποστήριξη κατά περίπτωση όταν απαιτείται. Επίσης μπορεί να χρησιμοποιηθεί η 2^{η} σειρά των τεχνικών που βρίσκονται σε επαγρύπνηση.
Θα υπάρχει μια βασική ομάδα CSIRT με τέσσερα μέλη πλήρους απασχόλησης και πέντε επιπρόσθετα μέλη της ομάδας CSIRT. Ένα από αυτά θα είναι επίσης διαθέσιμο σε κυκλική βάρδια.

Προσωπικό
Ο επικεφαλής της ομάδας CSIRT διαθέτει προηγούμενη εμπειρία σε θέματα ασφάλειας και υποστήριξης 1^{ου} και 2^{ου} επιπέδου και έχει εργασθεί στο πεδίο της διαχείρισης κρίσης αντοχής. Τα άλλα τρία μέλη της ομάδας είναι ειδικοί σε θέματα ασφάλειας. Τα μέλη της ομάδας CSIRT με καθεστώς μερικής απασχόλησης από το τμήμα πληροφοριακών συστημάτων είναι ειδικοί ο καθένας στο δικό του τμήμα της υποδομής της εταιρείας.

- -

Βήμα 6: Αξιοποίηση του γραφείου και της πολιτικής ασφάλειας πληροφοριών.
Εξοπλισμός και τοποθεσία γραφείου
Εξαιτίας του γεγονότος ότι η εταιρεία διαθέτει ήδη επαρκή υλική ασφάλεια στον χώρο, η νέα ομάδα CSIRT είναι απολύτως καλυμμένη από αυτή την άποψη. Παρέχεται μια αποκαλούμενη “αίθουσα μάχης”, ώστε να διευκολύνεται ο συντονισμός σε περίπτωση έκτακτου περιστατικού. Αγοράζεται ένα χρηματοκιβώτιο για το υλικό κρυπτογράφησης και τα ευαίσθητα έγγραφα. Εγκαταστάθηκε ξεχωριστή τηλεφωνική γραμμή συμπεριλαμβανομένου ενός κεντρικού πίνακα για τη διευκόλυνση της γραμμής επικοινωνίας κατά τις ώρες γραφείου και τη βάρδια "κατόπιν κλήσης" σε κινητό τηλέφωνο εκτός ωρών γραφείου με τον ίδιο τηλεφωνικό αριθμό.

Μπορεί επίσης να χρησιμοποιηθεί ο υφιστάμενος εξοπλισμός και ο εταιρικός ιστότοπος για την ανακοίνωση πληροφοριών σχετικά με την ομάδα CSIRT. Έχει εγκατασταθεί και διατηρείται μια λίστα αλληλογραφίας με μια ενότητα περιορισμένης πρόσβασης για την επικοινωνία μεταξύ των μελών της ομάδας και άλλες ομάδες. Όλα τα στοιχεία επικοινωνίας των μελών του προσωπικού έχουν αποθηκευθεί σε μια βάση δεδομένων, ενώ μια εκτύπωσή τους φυλάσσεται στο χρηματοκιβώτιο.

Κανονισμός
Εξαιτίας του γεγονότος ότι η ομάδα CSIRT είναι ενσωματωμένη σε μια εταιρεία με υφιστάμενες πολιτικές ασφάλειας πληροφοριών, οι αντίστοιχες πολιτικές για την ομάδα CSIRT έχουν διαμορφωθεί με τη βοήθεια του νομικού συμβούλου της εταιρείας.
- -

Βήμα 7: Αναζήτηση συνεργασίας
Χρησιμοποιώντας τον Κατάλογο του ENISA βρέθηκαν γρήγορα ορισμένες ομάδες CSIRT στην ίδια χώρα και πραγματοποιήθηκε επικοινωνία μαζί τους. Προγραμματίστηκε μια επιτόπια επίσκεψη σε μια από αυτές από τον νεοπροσληφθέντα επικεφαλής της ομάδας. Έμαθε για τις εθνικές δραστηριότητες CSIRT και παρακολούθησε μια συνάντηση.
Η συνάντηση ήταν κάτι παραπάνω από χρήσιμη για τη συλλογή παραδειγμάτων μεθόδων εργασίας και την εξασφάλιση της υποστήριξης από μερικές άλλες ομάδες.- -

Βήμα 8: Προώθηση του Επιχειρηματικού Σχεδίου
Αποφασίστηκε να συλλεχθούν δεδομένα και αριθμητικά στοιχεία από το ιστορικό της εταιρείας. Αυτό είναι κάτι παραπάνω από χρήσιμο για μια στατιστική επισκόπηση της κατάστασης της ασφάλειας των πληροφοριακών συστημάτων. Η εν λόγω συλλογή δεδομένων θα πρέπει να συνεχισθεί όταν έχει ολοκληρωθεί η δημιουργία και έχει ξεκινήσει η λειτουργία της ομάδας CSIRT, ώστε να ενημερώνονται τα στατιστικά στοιχεία.

Πραγματοποιήθηκε επικοινωνία και συνεντεύξεις με άλλες εθνικές ομάδες CSIRT σχετικά με τις επιχειρηματικές τους πρακτικές. Παρείχαν υποστήριξη συγκεντρώνοντας μερικές διαφάνειες με στοιχεία σχετικά με τις πρόσφατες εξελίξεις στα περιστατικά ασφαλείας των πληροφοριακών συστημάτων και τις δαπάνες των περιστατικών.

Σε αυτό το παράδειγμα πρακτικής της Εικονικής Ομάδας CSIRT δεν υπήρχε πιεστική ανάγκη να πεισθεί η διοίκηση για τη σημασία των πληροφοριακών συστημάτων και επομένως δεν ήταν δύσκολο να ληφθεί η έγκριση για το πρώτο βήμα. Ετοιμάστηκε η επιχειρηματική πρακτική και το σχέδιο έργου, συμπεριλαμβανομένης μιας εκτίμησης των δαπανών έναρξης και του κόστους λειτουργίας.
- -

Βήμα 9: Καθορισμός ροών διεργασιών και λειτουργικών και τεχνικών διαδικασιών
Η Εικονική Ομάδα CSIRT εστιάζει στην παροχή των βασικών υπηρεσιών CSIRT:

- συναγερμοί και προειδοποιήσεις,
- ανακοινώσεις,
- αντιμετώπιση περιστατικών.

Η ομάδα ανέπτυξε διαδικασίες που λειτουργούν σωστά και είναι εύκολα κατανοητές από κάθε μέλος της ομάδας. Η Εικονική Ομάδα CSIRT προσέλαβε επίσης έναν νομικό σύμβουλο για την αντιμετώπιση της αστικής ευθύνης και τη διαμόρφωση της πολιτικής ασφάλειας πληροφοριών. Η ομάδα υιοθέτησε ορισμένα χρήσιμα εργαλεία και βρήκε χρήσιμες πληροφορίες για λειτουργικά ζητήματα συζητώντας με άλλες ομάδες CSIRT.

Δημιουργήθηκε ένα προκαθορισμένο πρότυπο συμβουλευτικών ασφαλείας και αναφορών περιστατικών. Η ομάδα χρησιμοποιεί το RTIR για την αντιμετώπιση περιστατικών.

- -

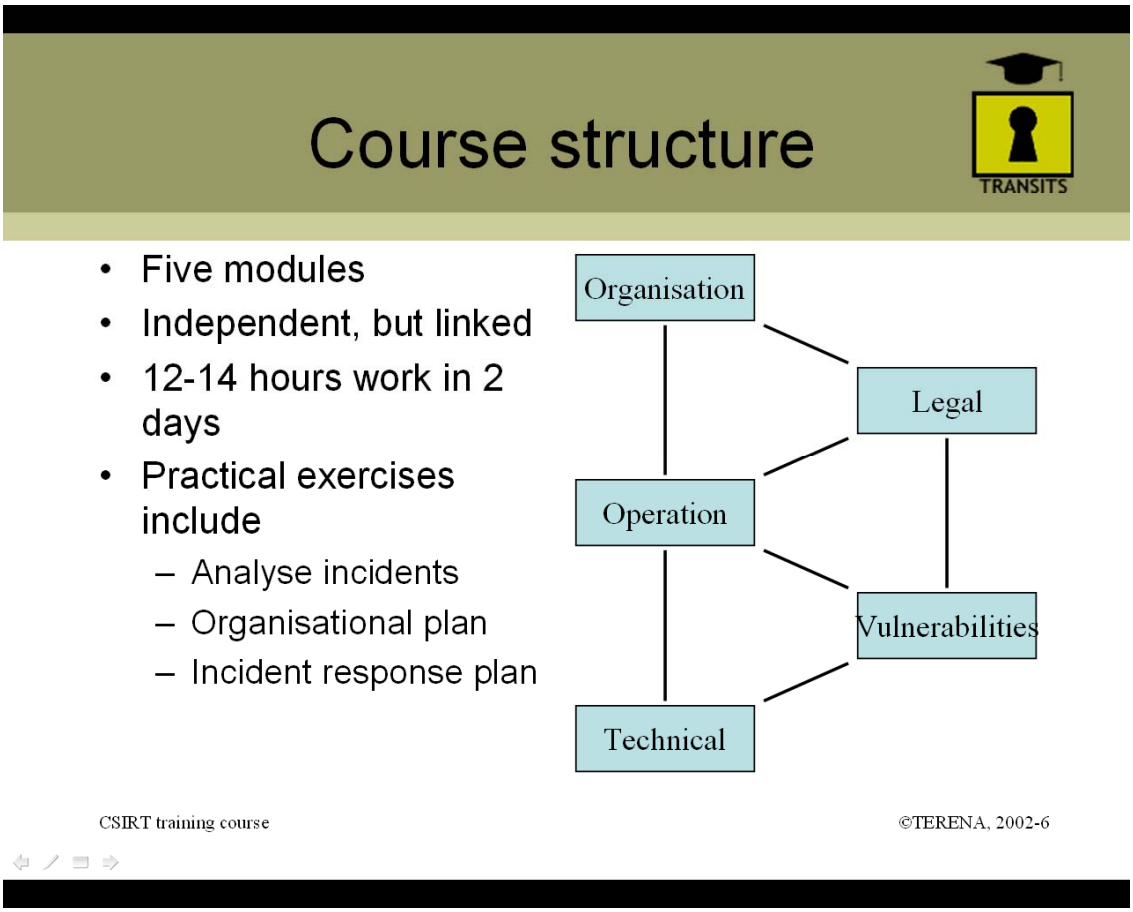
Βήμα 10: Εκπαίδευση του προσωπικού
Η Εικονική Ομάδα CSIRT αποφασίζει να στείλει όλο το τεχνικό προσωπικό της στα επόμενα διαθέσιμα μαθήματα TRANSITS. Επιπροσθέτως, ο επικεφαλής της ομάδας παρακολουθεί το μάθημα *Διαχείριση ομάδας* CSIRT του CERT/CC.

- -

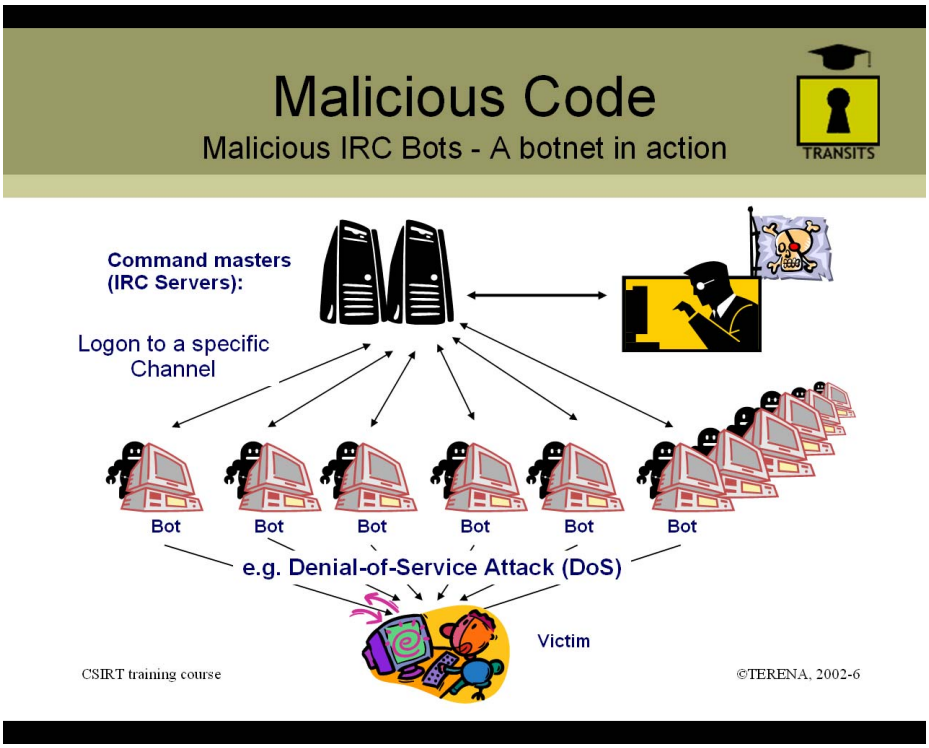
Βήμα 11: Εξάσκηση
Κατά τις πρώτες εβδομάδες λειτουργίας, η Εικονική Ομάδα CSIRT χρησιμοποίησε διάφορες εικονικές πρακτικές (που έλαβε ως παράδειγμα από άλλες ομάδες CSIRT) εν είδει εξάσκησης. Επιπλέον, εξέδωσε μερικά συμβουλευτικά ασφαλείας με βάση τις πραγματικές πληροφορίες αδυναμιών που διανεμήθηκαν από προμηθευτές υλικού και λογισμικού, οι οποίες ρυθμίστηκαν και προσαρμόστηκαν στις ανάγκες της κοινότητας αποδεκτών.

A.4 Δείγμα υλικού από τα Μαθήματα CSIRT

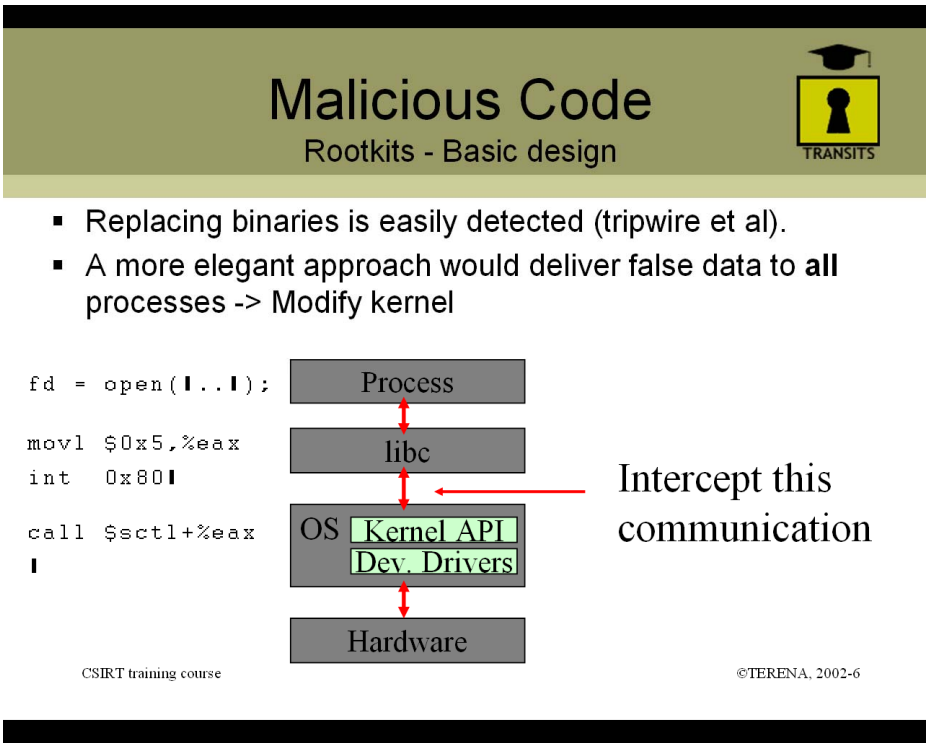
TRANSITS (με την ευγενή παραχώρηση του Terena, http://www.terena.nl)



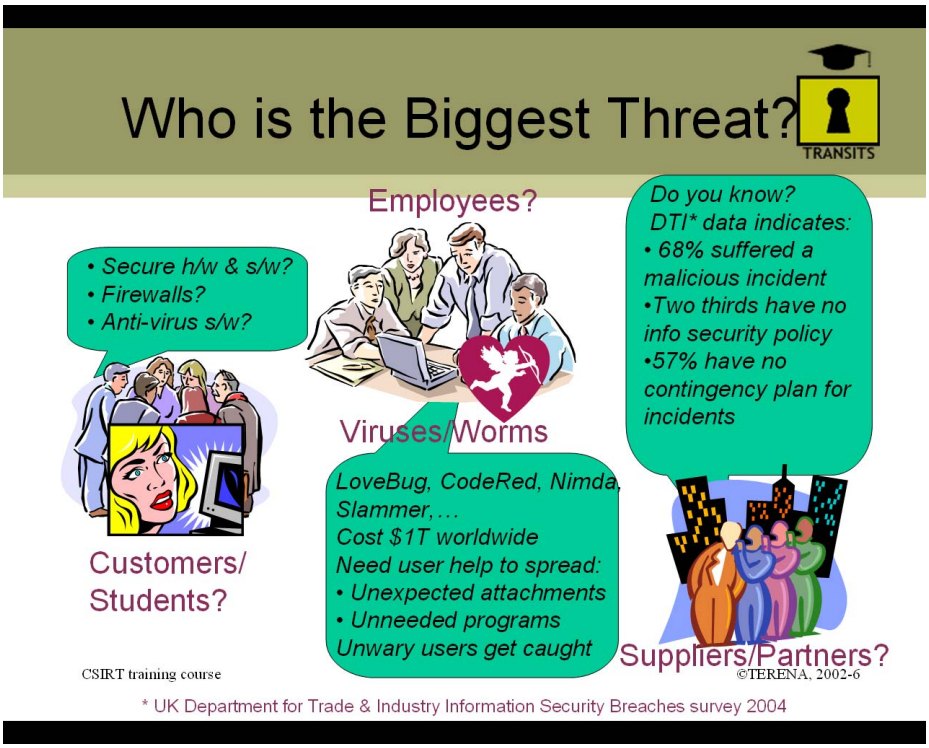
Επισκόπηση: Η δομή του μαθήματος



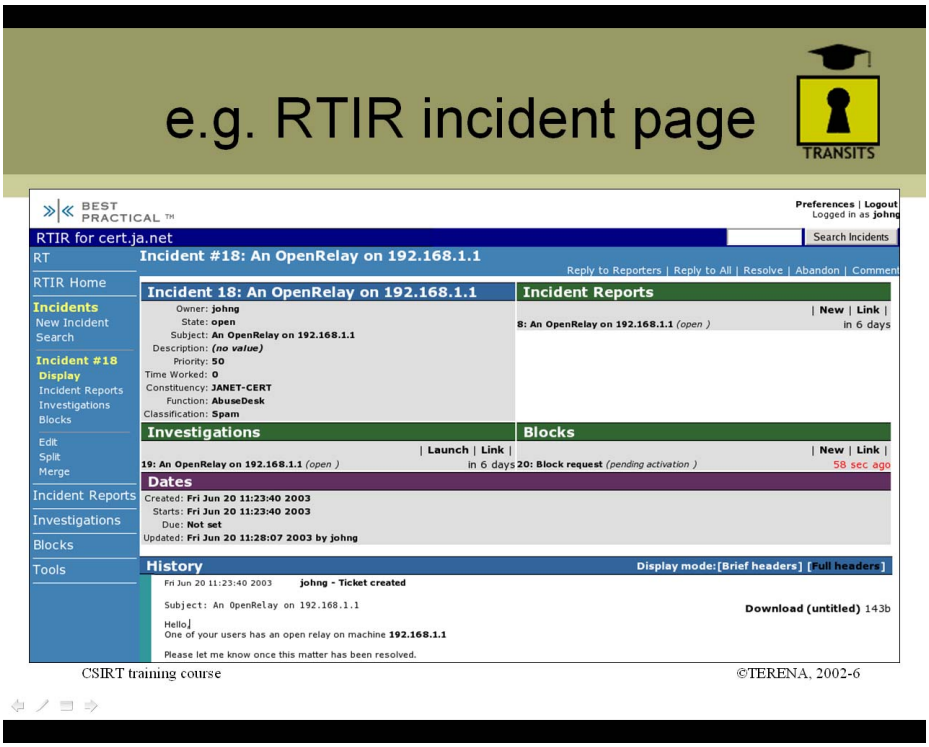
Από το *Τεχνικό μάθημα*: Περιγραφή ενός Botnet



Από το *Τεχνικό μάθημα*: Βασικός σχεδιασμός ενός rootkit



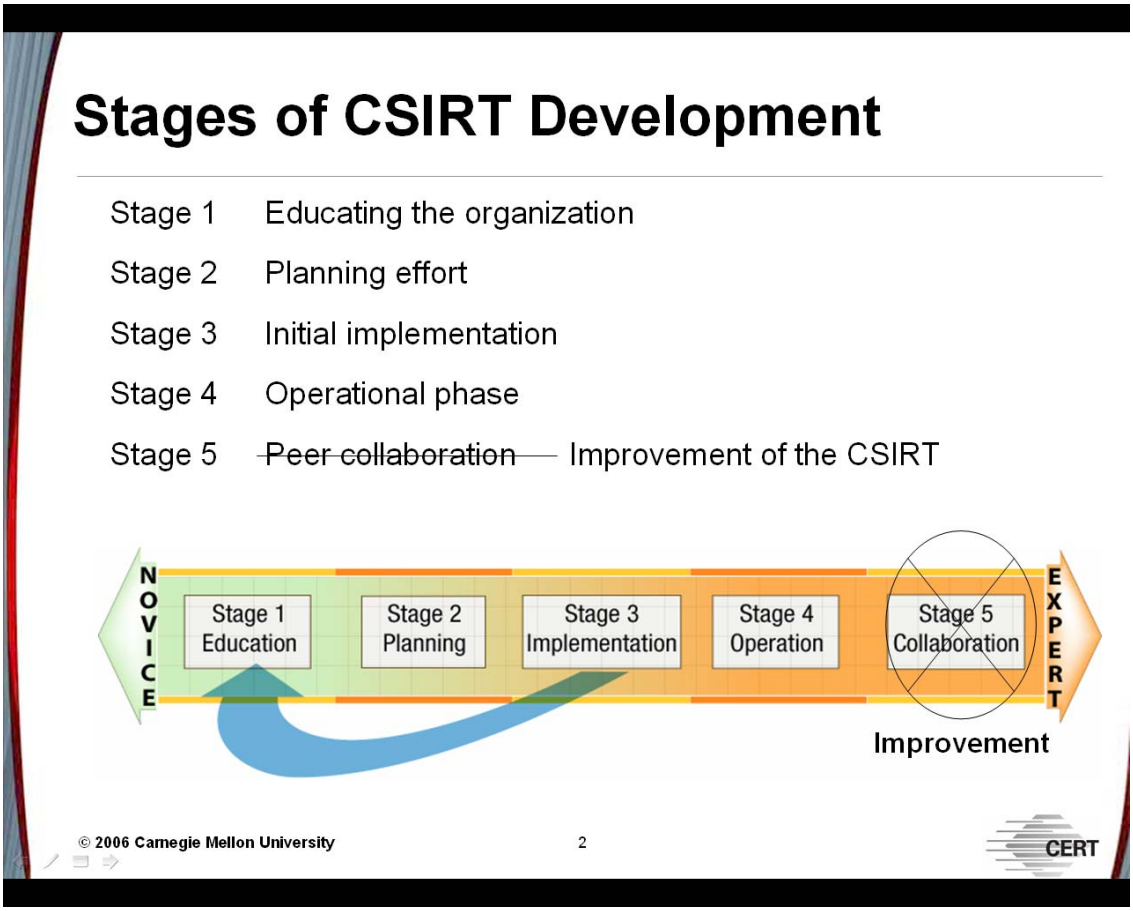
Από το *Οργανωτικό μάθημα*: Εισβολέας ή παρείσακτος - Πού έγκειται η μεγαλύτερη απειλή;



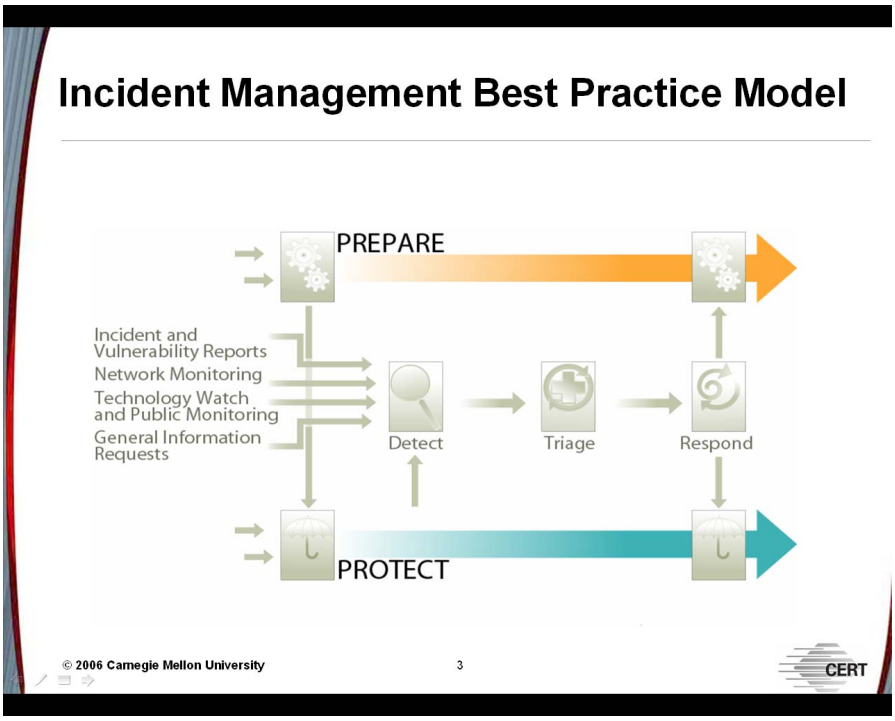
Από το *Οργανωτικό μάθημα*: Αίτημα Εντοπιστή για Αντιμετώπιση Περιστατικού (RTIR)

"Δημιουργία ομάδων CSIRT" (με την ευγενή παραχώρηση του CERT/CC, http://www.cert.org)

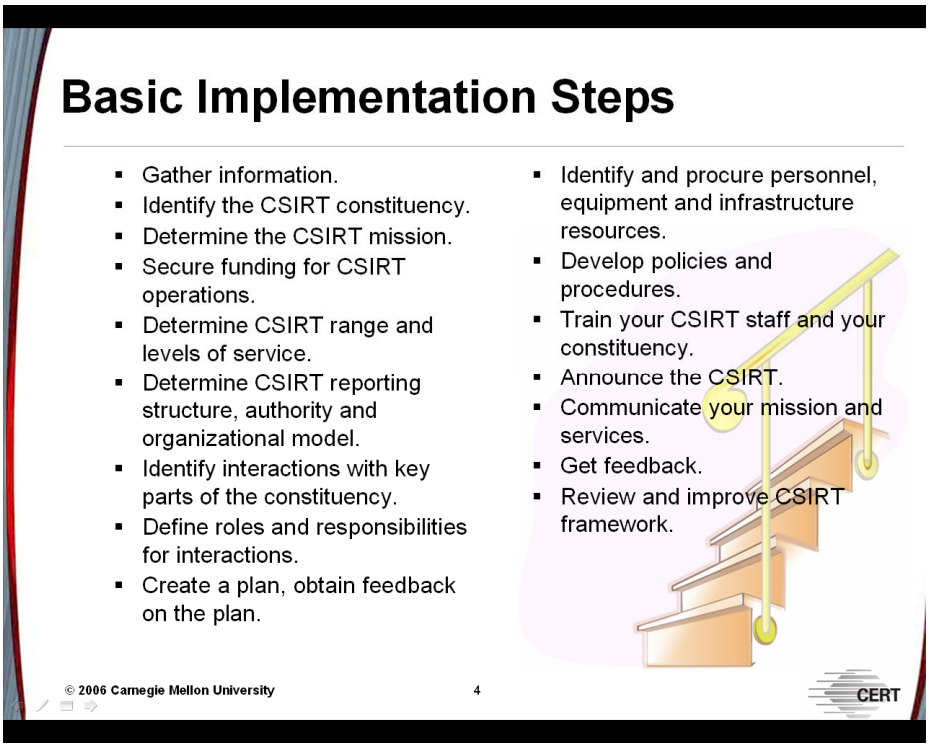
Ο ENISA ευχαριστεί από καρδίας την Ομάδα Ανάπτυξης CSIRT του Προγράμματος CERT που μας επέτρεψε να χρησιμοποιήσουμε το περιεχόμενο των εκπαιδευτικών μαθημάτων του!



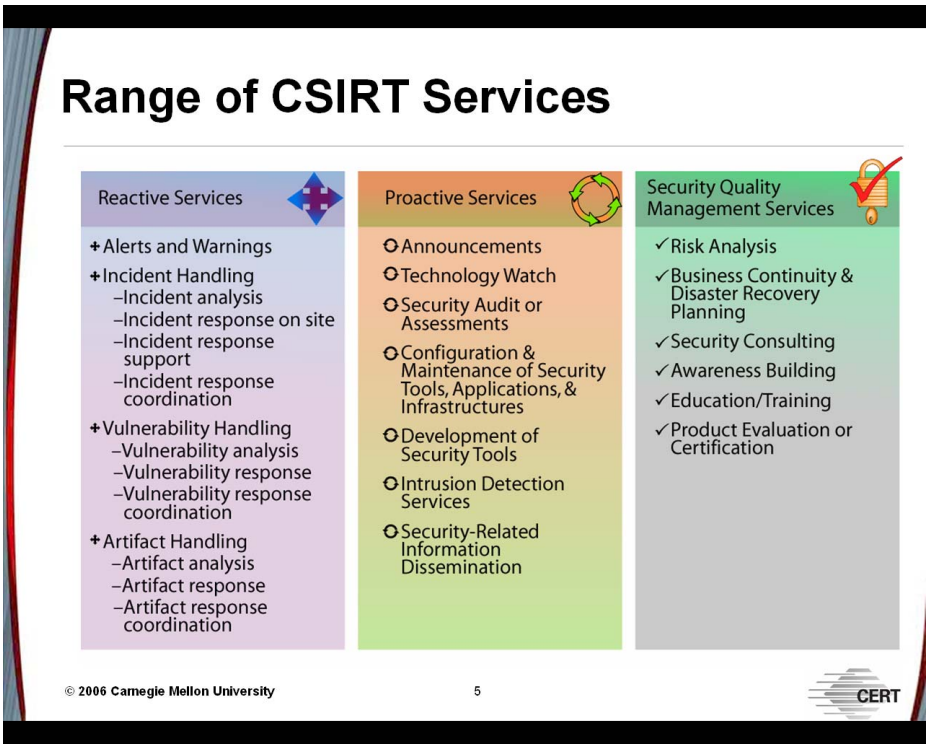
Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Στάδια ανάπτυξης CSIRT



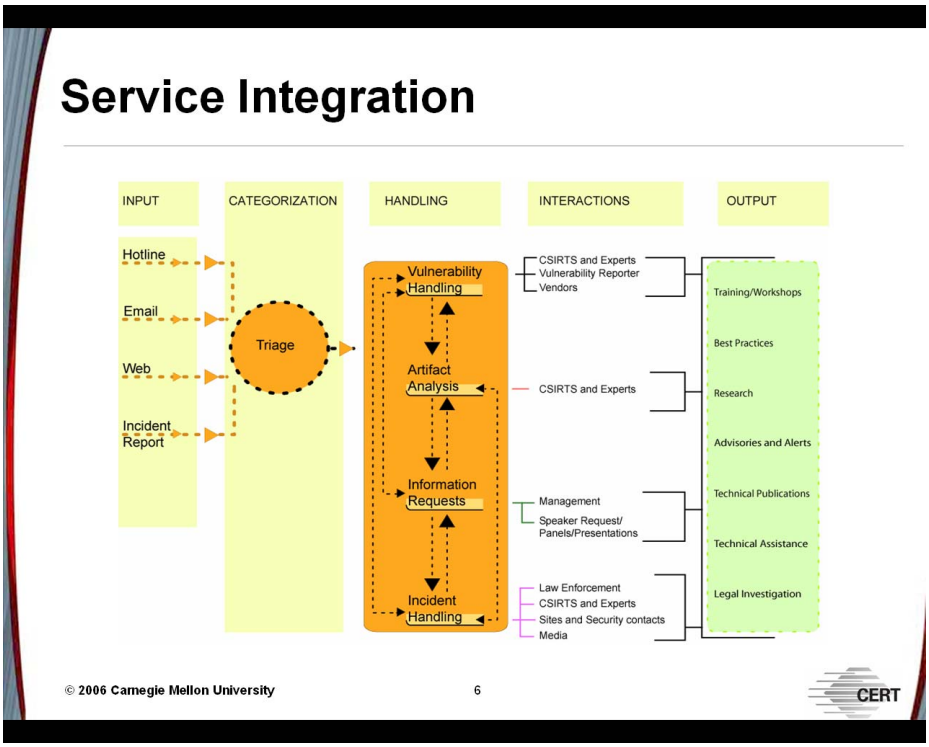
Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Βέλτιστη πρακτική στη διαχείριση περιστατικών



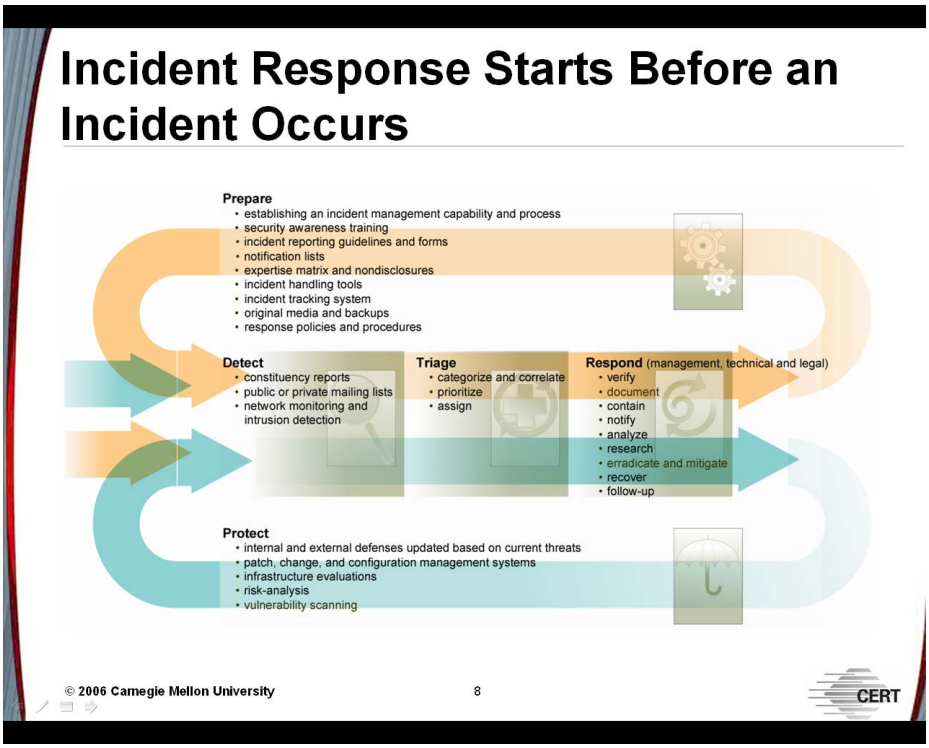
Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Βήματα για τη δημιουργία μιας ομάδας CSIRT



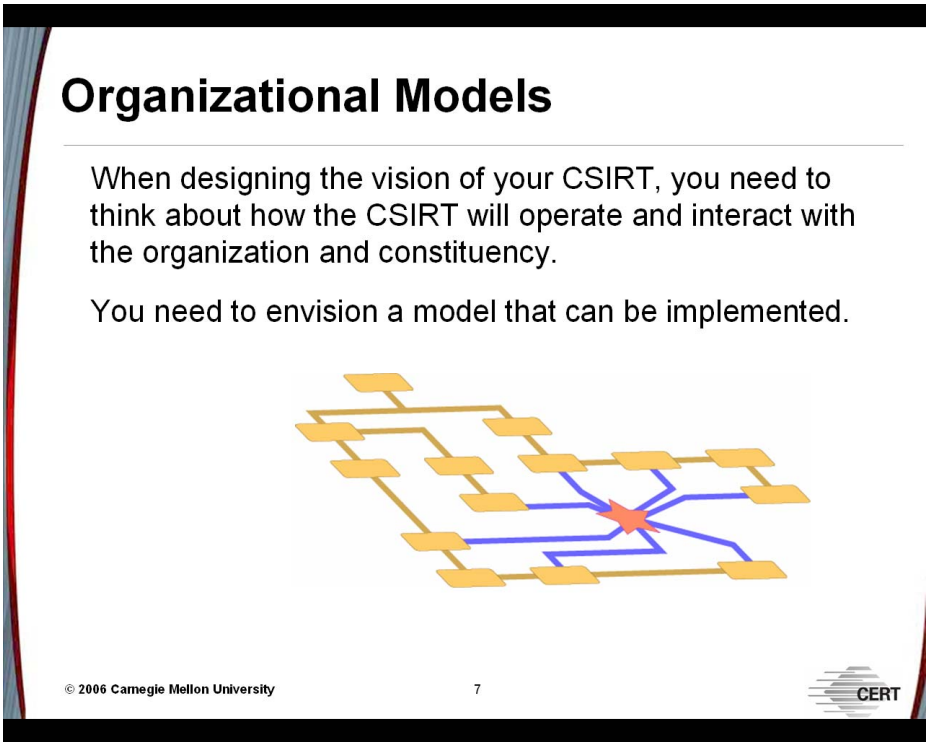
Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Οι υπηρεσίες που μπορεί να παράσχει μια ομάδα CSIRT



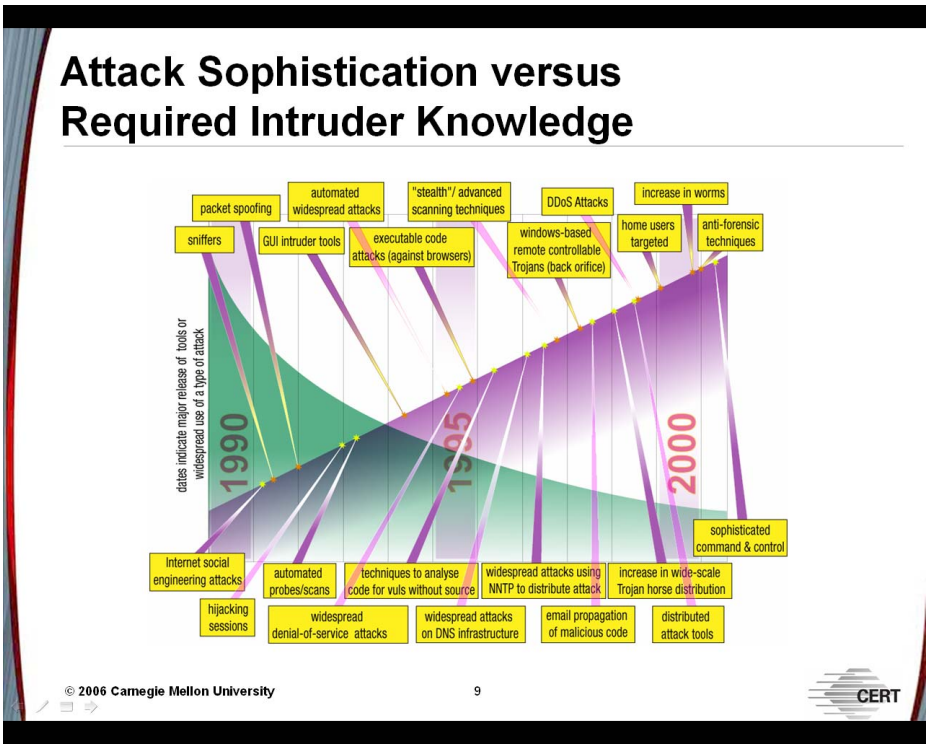
Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Η ροή εργασιών διαχείρισης περιστατικών



Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Αντιμετώπιση περιστατικών



Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Πώς θα οργανωθεί η ομάδα CSIRT;



Από το *Εκπαιδευτικό μάθημα* του CERT/CC: Λιγότερη γνώση, περισσότερη ζημία