ΓΕΡΗΕΤ
Γραφείο Επιτρόπου Ρυθμίσεως
Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων
Ηλιουπόλεως 12, 1101 Λευκωσία

Γ.Ε.Ρ.Η.Ε.Τ. 04.02.010.008 16.08.009.002.
Τηλ.: +357 22 693000
Φαξ: +357 22 693070
Email: info@ocecpr.org.cy

7 Ιουλίου 2009

ΕΛΗΦΘΗ ΑΡΧΕΙΟ
Ημερ. 7/7
Υπογρ.

Έντιμο

Υπουργό Συγκοινωνιών και Έργων

κ. Νίκο Νικολαΐδη

Θέμα: <u>Εισηγητικό Έγγραφο Πολιτικής για τη δημιουργία φορέων Άμεσης Ανταπόκρισης για περιστατικά/συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRT) στην Κύπρο</u>

Με βάση το πλαίσιο πολιτικής σχετικά με την Ασφάλεια Δικτύων και Πληροφοριών το οποίο εγκρίθηκε από το Υπουργείο Συγκοινωνιών και Έργων στις 5/10/2006 το ΓΕΡΗΕΤ προχώρησε με συγκεκριμένες δράσεις για την προώθηση των θεμάτων ασφάλειας δικτύων και πληροφοριών στην Κύπρο.

Μια βασική δραστηριότητα του Γραφείου επί του θέματος είναι η ετοιμασία σχεδίου πολιτικής για την ίδρυση φορέων CSIRTs στην Κυπριακή Δημοκρατία. Κατόπιν εντολής του Υπουργού Συγκοινωνιών και Έργων ετοιμάστηκε το εισηγητικό έγγραφο πολιτικής που επισυνάπτεται στο Παράρτημα 1. Για την ετοιμασία του εγγράφου προηγήθηκαν διαβουλεύσεις με τις δύο υπηρεσίες τις οποίες το ΓΕΡΗΕΤ εισηγείται όπως αναλάβουν το συγκεκριμένο ρόλο, δηλαδή το Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ) του Υπουργείου Οικονομικών και το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο (ΚΕΑΔ). Με τις δύο υπηρεσίες έχουν συμφωνηθεί οι βασικές αρχές λειτουργίας των συγκεκριμένων φορέων όπως καταγράφονται στο σχετικό έγγραφο.

Για την οριστικοποίηση του σχεδίου πολιτικής το ΓΕΡΗΕΤ είχε διαβουλεύσεις με άλλους φορείς στην αγορά και συνεργάστηκε με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) από τον οποίο ζήτησε επίσημη γνωμοδότηση η οποία επισυνάπτεται στο Παράρτημα 2. Η πολιτική την οποία προτείνει το ΓΕΡΗΕΤ βασίζεται στις κατευθυντήριες[1] γραμμές που έχει δημοσιεύσει ο ENISA. Στην γραπτή αξιολόγηση του ο οργανισμός ENISA έχει τοποθετηθεί θετικά σε σχέση με το σχεδιασμό που εισηγείται το ΓΕΡΗΕΤ και ενισχύει τις προτάσεις του Γραφείου. Το ΓΕΡΗΕΤ έχει εξασφαλίσει επίσης τη βοήθεια του ENISA σε σχέση με την υλοποίηση του προτεινόμενου σχεδιασμού κυρίως σε θέματα μεταφοράς τεχνογνωσίας.

Η ίδρυση των φορέων CSIRT στην Κύπρο, η οποία είναι μία από τα τελευταία κράτη μέλη που δεν έχει υιοθετήσει το θεσμό σε εθνικό επίπεδο, κρίνεται ιδιαίτερα σημαντική για την προώθηση των θεμάτων ασφάλειας δικτύων και πληροφοριών στη χώρα μας αλλά και για την ισότιμη συμμετοχή της Κύπρου στα αρμόδια ευρωπαϊκά όργανα. Η Ευρωπαϊκή Επιτροπή στα

[1] Έγγραφο ENISA "A step-by-step approach on how to setup a CSIRT"

πλαίσια των δραστηριοτήτων του Οργανισμού ENISA αλλά και του ευρύτερου πολιτικού σχεδιασμού για την ασφάλεια δικτύων και πληροφοριών (NIS) σε επίπεδο Ευρωπαϊκής Ένωσης προωθεί την ίδρυση φορέων CSIRT σε όλα τα κράτη μέλη με έμφαση στην κάλυψη του κυβερνητικού τομέα. Στα πλαίσια του εν λόγω πολιτικού σχεδιασμού η Ευρωπαϊκή Επιτροπή σχεδιάζει από το 2010 τη διοργάνωση πανευρωπαϊκών ασκήσεων που εντάσσονται στις δραστηριότητες για την προστασία των κρίσιμων υποδομών πληροφοριών στα κράτη μέλη. Οι φορείς CSIRT σε όλα τα κράτη μέλη αναμένεται να διαδραματίσουν σημαντικό ρόλο στις συγκεκριμένες δραστηριότητες.

Η ίδρυση των φορέων CSIRTS, προϋποθέτει την κατάλληλη στελέχωση και την εγκατάσταση υποδομής. Το σχετικό κόστος θα καλύπτεται από τον προϋπολογισμό του ΤΥΠ και του ΚΕΑΔ αντίστοιχα, οπότε και πρέπει να γίνουν σχετικές πρόνοιες στο προϋπολογισμό τους.

Παρακαλώ όπως οι αποφάσεις επί του προτεινόμενου πλαισίου πολιτικής προχωρήσουν το συντομότερο δυνατό ώστε το ΓΕΡΗΕΤ να προχωρήσει αμέσως με τις Υπηρεσίες που προτείνονται να αναλάβουν τις σχετικές αρμοδιότητες, στη φάση υλοποίησης.

Είμαστε στη διάθεση σας για οποιεσδήποτε περαιτέρω πληροφορίες ή διευκρινίσεις.

Με εκτίμηση

Φώτης Αγαστάση

Βοηθός Επίτροπος Ρυθμίσεως

Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων

Παράρτημα 1

Εισηγητικό Έγγραφο Πολιτικής για τη δημιουργία φορέα CSIRT στην Κύπρο

1. Εισαγωγή

Το παρόν εισηγητικό έγγραφο ετοιμάστηκε μετά από την ειλλημένη απόφαση του αξιότιμου κ. Υπουργού Συγκοινωνιών και Έργων με την οποία έδωσε εντολή στον Επίτροπο για την ανάπτυξη πλαισίου πολιτικής σχετικά με την Ασφάλεια Δικτύων και Πληροφοριών και την έγκριση του γενικότερου πλαισίου πολιτικής όπως αυτό κατατέθηκε από το ΓΕΡΗΕΤ στον Υπουργό Συγκοινωνιών και Έργων την 22α Αυγούστου 2006 και εγκρίθηκε την 5η Οκτωβρίου 2006.

Το ΓΕΡΗΕΤ έχει την ευθύνη για την δημιουργία και τον συντονισμό των ενεργειών *αρμόδιων φορέων για* τον καταρτισμό φορέα/φορέων CSIRT στην Κύπρο.

Το παρόν έγγραφο πολιτικής εστιάζεται στις ενέργειες που απαιτούνται για τον καθορισμό τέτοιου φορέα, τον ρόλο που θα διαδραματίζει στο ευρύτερο έργο της Ασφάλειας Δικτύων και Πληροφοριών καθώς και τις ευθύνες, βασικές λειτουργείες και μηχανισμούς ενημέρωσης των «πελατών/χρηστών» του φορέα αυτού προς το σύνολο των Κυπρίων Πολιτών.

2. Νομική Βάση

Το ΓΕΡΗΕΤ είναι το κατά νόμο υπεύθυνο Γραφείο όσον αφορά τον συντονισμό των θεμάτων της ασφάλειας δικτύων ηλεκτρονικών επικοινωνιών και πληροφοριών στην επικράτεια της Κυπριακής Δημοκρατίας. Η σχετική αρμοδιότητα πηγάζει από το Νόμο 112(Ι)/2004 (άρθρα 2(2)(ζ)&(ι), 2(3), 18(3)(στ) 19(1), 37(5), 39(2)(ιστ), 42(7), 55(2)(β), 80(α), 97, 98), και την αρμοδιότητα του ΓΕΡΗΕΤ να εκπροσωπεί την Κύπρο στο Διοικητικό Συμβούλιο του ENISA[1] και να ενεργεί ως κεντρικός σύνδεσμος επικοινωνίας και συντονισμού στην Κύπρο με την υπηρεσία. Στα πλαίσια των αρμοδιοτήτων του αυτών συντονίζει την αμφίδρομη ενημέρωση των κυπριακών αρχών, των ενδιαφερομένων μερών και των καταναλωτών εντός της Κυπριακής Δημοκρατίας, με τις αρμόδιες υπηρεσίες της *Ευρωπαϊκής Ένωσης για θέματα και* δραστηριότητες που αφορούν την ασφάλεια δικτύων και πληροφοριών.

3. Ορισμοί

Computer Security Incident Response Team-CSIRT: σημαίνει «Ομάδα Άμεσης Ανταπόκρισης για Περιστατικά/συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών *και αποτελείται από* μια ομάδα ειδικών, επί των θεμάτων ασφαλείας πληροφοριών που διακινούνται σε δίκτυα ηλεκτρονικών επικοινωνιών, των οποίων η εργασία επικεντρώνεται στην ανταπόκριση προς τους «πελάτες/χρήστες» τους σχετικά με θέματα ασφάλειας πληροφοριών.

CSIRT: Computer Security Incident Response Team είναι το σύνηθες πλέον ακρώνυμο που χρησιμοποιείται για αυτού του τύπου τους φορείς/σώματα στην Ευρώπη ενώ το ακρώνυμο CERT χρησιμοποείται ευρέως στην Αμερική.

[1] **E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency

4. Τύποι CSIRT/Ρόλοι CSIRT:

Ο τύπος/κατηγορία CSIRT είναι άμεσα συνδεδεμένος με τους πελάτες/χρήστες τους οποίους θα κληθεί να εξυπηρετήσει.

Οι ανάγκες του «πελατολογίου» του CSIRT θα καθορίσουν τον τύπο και σε τελική ανάλυση τις ευθύνες/λειτουργία του CSIRT.

Ως εκ των πιο πάνω τα CSIRTs διακρίνονται σε κατηγορίες ως ακολούθως:

- Ακαδημαϊκό CSIRT
- Εμπορικό CSIRT
- Κυβερνητικό CSIRT
- Εσωτερικό CSIRT για εταιρείες με λειτουργικό διαχωρισμό
- Στρατιωτικής Ευθύνης CSIRT
- Εθνικό CSIRT
- CSIRT Κατασκευαστών Υλισμικού ή Λογισμικού

5. Κατηγορίες Υπηρεσιών που μπορεί να προσφέρει ένα CSIRT

Οι υπηρεσίες που μπορούν να προσφερθούν από ένα φορέα CSIRT χωρίζονται σε τέσσερεις μεγάλες κατηγορίες οι οποίες κατά βάση καθορίζουν το μέγεθος και την πληρότητα σε υπηρεσίες ενός CSIRT:

- Υπηρεσίες Αποκατάστασης μετά από Καταστροφικά περιστατικά/συμβάντα απώλειας πληροφοριών,
- Υπηρεσίες Πρόληψης Καταστροφικών ενδεχομένων,
- Υπηρεσίες Ανάλυσης/Forensics μετά από Καταστροφικά περιστατικά
- Υπηρεσίες Διαχείρισης Ποιότητας Ασφαλείας Πληροφοριών.

Οι πιο πάνω υπηρεσίες υπό-κατηγοριοποιούνται στα ακόλουθα:

i. Υπηρεσίες Αποκατάστασης μετά από καταστροφικά περιστατικά/ενδεχόμενα- Reactive Services

- **Alerts and Warnings**
- **Incident Handling**
- **Incident analysis**
- **Incident response**
- **support**
- **Incident response coordination**
- Incident response on site
- Vulnerability Handling
- Vulnerability analysis
- Vulnerability response
- Vulnerability response coordination

ii. **Υπηρεσίες Πρόληψης Καταστροφικών ενδεχομένων- Proactive Services**

- **Announcements**
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security
- Development of Security Tools
- Intrusion Detection
- Services
- Security-Related Information
- Dissemination

iii. **Artifact Handling**

- Artifact analysis
- Artifact response
- Artifact response coordination

iv. ***Security Quality Management***

- Risk Analysis
- Business Continuity and
- Disaster Recovery
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or
- Certification

Οι βασικές υπηρεσίες εμαφανίζονται με τονισμένο χρώμα και αυτές καθορίζουν τον βασικό/ελάχιστο βαθμό λειτουργίας ενός CSIRT. Οι βασικές υπηρεσίες χωρίζονται σε υπηρεσίες αποκατάστασης μετά από καταστροφικό ενδεχόμενο με την διαχείριση της κρίσης που δημιουργείται και την προσπάθεια ελαχιστοποίησης/περιορισμού της έκτασης της ζημιάς που προκαλεί το καταστροφικό περιστατικό.

6. Επιλογή καταλληλότερου τύπου CSIRT για την ικανοποίηση των αναγκών της Κυπριακής Δημοκρατίας

Το ΓΕΡΗΕΤ μέσα από τη συλλογή πληροφοριών από διάφορους τόσο δημόσιους όσο και ιδιωτικούς φορείς σχετικά με την δυνατότητα τους να εκπληρώσουν τον ρόλο ενός φορέα CSIRT στην Κύπρο προχώρησε σε επί μέρους διαβούλευση με τους δύο επικρατέστερους φορείς σύμφωνα με τα κριτήρια που έθεσε το ΓΕΡΗΕΤ σε σχέση με την ανάθεση καθηκόντων CSIRT για την Κύπρο.

Οι δύο φορείς οι οποίοι συγκέντρωσαν τις μεγαλύτερες πιθανότητες να αναλάβουν την δημιουργία/λειτουργία φορέα CSIRT στην Κύπρο ήταν το Τμήμα Υπηρεσιών Πληροφορικής της Κυβέρνησης-ΤΥΠ και το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο (ΚΕΑΔ).

Το Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ) είναι ο αρμόδιος κυβερνητικός φορέας για θέματα μηχανογράφησης στη Δημόσια Υπηρεσία. Δημιουργήθηκε το 1980 μέσα στα πλαίσια της αναδιοργάνωσης/αναδιάρθρωσης της Δημόσιας Υπηρεσίας αρχικά ως Τμήμα Μηχανογραφικών Υπηρεσιών και μετονομάστηκε το 1997 σε Τμήμα Υπηρεσιών Πληροφορικής, ονομασία που διατηρεί μέχρι σήμερα. Το Τμήμα Υπηρεσιών Πληροφορικής υπάγεται διοικητικά στο Υπουργείο Οικονομικών.

Αρμοδιότητες του ΤΥΠ περιλαμβάνουν:

- Την παροχή συμβουλευτικών υπηρεσιών σε θέματα της αρμοδιότητάς του στο Δημόσιο και ορισμένες φορές στον Ημικρατικό Τομέα,
- Την μελέτη και υποβολή εισηγήσεων *και εφαρμογή της πολιτικής και στρατηγικής* σε θέματα Πληροφορικής στο Δημόσιο Τομέα,
- Την εξασφάλιση, μέσω προσφορών, μηχανογραφικό εξοπλισμό, προγράμματα και υπηρεσίες για ανάπτυξη συστημάτων για όλο τον Δημόσιο Τομέα,
- Την διευθύνση και εφαρμογή του Προγράμματος Μηχανογράφησης (Βραχυπρόθεσμου και Γενικού Στρατηγικού Σχεδίου) και επιμέρους έργα,
- Την ανάπτυξη των συστημάτων των εφαρμογών όλου του Προγράμματος Μηχανογράφησης (είτε από μόνο του είτε με τη βοήθεια του *Ιδιωτικού Τομέα*),
- Την λειτουργία, συντήρηση και υποστήριξη των συστημάτων αυτών μετά την παράδοσή τους,
- Την υποστήριξη όλων τα μικροϋπολογιστικών συστημάτων και έτοιμων προγραμμάτων που αγοράζονται για τα Υπουργεία/Τμήματα/Υπηρεσίες,
- Την εκπροσώπηση της Κύπρου σε διάφορα διεθνή συνέδρια για θέματα Πληροφορικής.

Το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο- ΚΕΑΔ παρέχει την υποδομή δικτύου για την Κυπριακή Ερευνητική και Ακαδημαϊκή Κοινότητα και συνδέει οργανισμούς τριτοβάθμιας εκπαίδευσης και ερευνητικούς οργανισμούς. Η υποδομή του ΚΕΑΔ είναι συνδεδεμένη με το Ευρωπαϊκό δίκτυο GEANT2 το οποίο αποτελεί μέρος της παγκόσμιας κοινότητας ερευνητικών και ακαδημαϊκών δικτύων. Μέσω αυτής της σύνδεσης το δίκτυο του ΚΕΑΔ είναι επίσης συνδεδεμένο με το Διαδίκτυο.

Αρμοδιότητες του ΚΕΑΔ περιλαμβάνουν:

- Την Διασύνδεση οργανισμών τριτοβάθμιας εκπαίδευσης με το Ευρωπαϊκό Δίκτυο και το Διαδίκτυο
- Την ενημέρωση των χρηστών των διασυνδεδεμένων με αυτό οργανισμών και φορέων σχετικά με κινδύνους στο διαδίκτυο
- Την υποστήριξη κατόπιν αναφοράς χρηστών/οργανισμών που αντιμετωπίζουν διακοπή ή/και απώλεια *υπηρεσιών μετά από καταστροφικά συμβάντα.*

Το ΚΕΑΔ παρέχει ήδη τις βασικές υπηρεσίες φορέα CSIRT για τα ακαδημαϊκά ιδρύματα τα οποία έχουν διασυνδέσει τα δίκτυα τους με την υποδομή του ΚΕΑΔ.

Μέσα από την επιλογή του ΚΕΑΔ υπάρχει η δυνατότητα κατανομής της δραστηριότητας του φορέα CSIRT μεταξύ των ακαδημαϊκών ιδρυμάτων που διασυνδέονται με το δίκτυο του στη βάση του μοντέλου ακαδημαϊκού CSIRT που παρουσιάζεται στη σελίδα 8 του παρόντος εγγράφου.

Σημαντικό ρόλο στην κατάληξη του ΓΕΡΗΕΤ σε δύο υποψήφιους φορείς ήταν η τεχνική υποδομή για υποστήριξη ενός φορέα CSIRT που διαθέτουν καθώς και η τεχνογνωσία του προσωπικού που στο πρώτο στάδιο λειτουργίας θα αποβεί καθοριστική για τη σωστή λειτουργία του φορέα.

Πρώτιστο ρόλο στην επιλογή ΓΕΡΗΕΤ διαδραμάτισε και η «επαφή» των δύο φορέων με μεγάλο αριθμό χρηστών όπως οι χρήστες της μηχανογραφικής υποδομής της Κυβέρνησης και οι χρήστες του ακαδημαϊκού δικτύου Κύπρου.

Το ΓΕΡΗΕΤ καλείται να απαντήσει στην ερώτηση γιατί δεν τάσσεται υπέρ της δημιουργίας Παγκύπριου/Εθνικού τύπου CSIRT που θα λειτουργεί σαν κεντρικό σημείο εξυπηρέτησης όλων των τομέων της Κυπριακής κοινωνίας και οικονομίας και αντίθετα επιλέγει να δημιουργήσει δύο παράλληλα/αυτοδύναμα CSIRTs, ένα για την υποστήριξη κυρίως των χρηστών της κυβερνητικής

μηχανογραφικής υποδομής και άλλο ένα για την υποστήριξη του όγκου των χρηστών της υποδομής των ακαδημαϊκών ιδρυμάτων.

Στην αρχική φάση της δημιουργίας φορέα CSIRT η δημιουργία εθνικού CSIRT εκτιμήθηκε ότι δεν θα επιφέρει την ομαλή διείσδυση του θεσμού του CSIRT στον Κυπριακό κοινωνικό-οικονομικό χώρο. Οι *πελάτες αυτού του τύπου* CSIRT προέρχονται από διαφορετικό υπόβαθρο σε ότι αφορά την χρήση ICT υποδομής οπότε και οι ανάγκες τους τόσο σε πρόληψη/ενημέρωση όσο και σε αποκατάσταση μετά από καταστροφικά ενδεχόμενα ποικίλουν. Ως εκ τούτου και με γνώμονα την συντομότερη το δυνατόν εισαγωγή του θεσμού και εγκαθίδρυση του CSIRT στην Κύπρο το μοντέλο του εθνικού CSIRT και ο τεράστιος όγκος χρηστών με διαφορετικές ανάγκες κρίθηκε ότι δεν θα μπορούσε να υποστηριχθεί στην παρούσα φάση αλλά σε μελλοντικότερο στάδιο με την ωρίμανση του θεσμού.

Η επιλογή του **Τμήματος Υπηρεσιών Πληροφορικής της Κυβέρνησης- ΤΥΠ** έγινε στη βάση πρώτιστα της αξιολόγησης της δυνατότητας να παρέχει υποστηρικτικές και προληπτικές υπηρεσίες σε μεγάλο όγκο χρηστών— ήδη υποστηρίζουν τους χρήστες των κυβερνητικών υπηρεσιών και στη βάση του ότι υπάρχουν έτοιμες οι διαδικασίες για ενσωμάτωση του φορέα CSIRT κάτω από την υποδομή (τεχνική υποδομή και ανθρώπινο δυναμικό) του ΤΥΠ[2] στα πλαίσια των αρμοδιοτήτων του.

Η επιλογή του **Κυπριακού Ερευνητικού και Ακαδημαϊκού Δικτύου-ΚΕΑΔ** έγινε στην ίδια βάση αφού οι χρήστες της ακαδημαϊκής κοινότητας είναι πολυπληθείς και έχουν διαφορετικές ανάγκες από τους προαναφερθέντες χρήστες της μηχανογραφικής υποδομής της Κυβέρνησης.

Αποτελεί επίσης συνήθη πρακτική στις χώρες της Ευρωπαϊκής Ένωσης ένα εκ των CSIRT που πιθανό να υπάρχουν εγκαθιδρυμένα σε μια χώρα να υποστηρίζει τα δίκτυα και χρήστες των ακαδημαϊκών ιδρυμάτων.

Αναμένεται ότι εντός μιας τριετίας από τη λειτουργία των δύο (2) CSIRTS τουλάχιστον το ένα θα είναι σε θέση να διευρύνει το φάσμα των υπηρεσιών που θα προσφέρει και σε άλλους τομείς της Κυπριακής οικονομίας π.χ. στον επιχειρηματικό τομέα.

7. Υπηρεσίες που θα πρέπει να υποστηρίζουν τα δύο CSIRTs— ΤΥΠ και ΚΕΑΔ.

Στην αρχική φάση της δημιουργίας των CSIRTs και για σκοπούς μείωσης του αρχικού προυπολογισμού που απαιτεί η δημιουργία φορέα CSIRT συστήνεται όπως η λειτουργία των CSIRTS περιοριστεί στις βασικές λειτουργίες που δίνονται πιο πάνω και αφορούν λειτουργίες αποκατάστασης μετά από καταστροφικά συμβάντα όπως:

- Αποστολή σημάνσεων κινδύνου και προειδοποιήσεις για κινδύνους προς τους χρήστες
- Διαχείριση Κρίσεων μετά και κατά την διάρκεια καταστροφικών ενδεχομένων
- Ανάλυση των ενδεχομένων
- Ανταπόκριση/Υποστήριξη *των χρηστών για αποκατάσταση των συστημάτων* τους μετά από καταστροφικά συμβάντα
- Συντονισμός Ενεργειών των αρμόδιων φορέων/τμημάτων για αποκατάσταση κρίσιμων υπηρεσιών των χρηστών μετά από καταστροφικά συμβάντα.

[2] Βλ. Σελ. 7 του παρόντος εγγράφου

Περαιτέρω, η λειτουργία του φορέα CSIRT θα πρέπει να ικανοποιεί τις βασικές λειτουργίες σχετικά με υπηρεσίες πρόληψης καταστροφικών συμβάντων όπως ανακοινώσεις και ενημέρωση των «πελατών» του CSIRT για νέα κακόβουλα λογισμικά που πιθανό να προκαλέσουν καταστροφές όπως π.χ. Denial of service attacks.

8. Επικοινωνία του CIRT με τους «πελάτες/χρήστες» των υπηρεσιών τους- Κανάλια/οδοί επικοινωνίας

Για να επιτευχθεί ο στόχος των CSIRT όσον αφορά τις υπηρεσίες κυρίως της πρόληψης και της αποκατάστασης μετά από καταστροφικά συμβάντα/περιστατικά συστήνεται όπως τα CSIRTS δημιουργήσουν/διατηρούν τα ακόλουθα κανάλια επικοινωνίας με το κοινό τους:

- Δημόσια διαθέσιμές πληροφορίες στο κοινό μέσω δημόσιας ιστοσελίδας την οποία οι πελάτες/χρήστες θα χρησιμοποιούν για να λαμβάνουν πρωτίστως ενημέρωση για πιθανούς κινδύνους που μπορούν να προκαλέσουν κυρίως απώλεια των δεδομένων και της υπηρεσίας τους καθώς και ενημερωτικά λογισμικά (software updates) ανάλογα με το λειτουργικό σύστημα (operating system) και λογισμικές εφαρμογές που χρησιμοποιούν καθώς και ενημερωμένες εκδόσεις virus definitions για τα «λογισμικά προστασίας από ιούς/αντι-ικά/antivirus» λογισμικά που χρησιμοποιούν.

- Πληροφορίες οι οποίες μπορούν να διαβαθμιστούν ως μη δημόσια διαθέσιμες για όλους τους χρήστες/πελάτες και μπορούν να γίνουν προσβάσιμες μετά την εξασφάλιση σχετικού κωδικού ασφαλείας από τους διαχειριστές της ιστοσελίδας και του περιεχομένου της. Οι χρήστες μπορούν να χωριστούν σε κατηγορίες (οικιακός χρήστης, χρήστης με πρόσβαση σε ευαίσθητες πληροφορίες, επιχειρηματικός χρήστης, διαχειριστής συστημάτων κλπ) και ανάλογα με την κατηγορία στην οποία ανήκουν να έχουν πρόσβαση σε αποκλειστικά μέρη του περιεχομένου της ιστοσελίδας – Members' areas.

- Στους χρήστες/επισκέπτες της ιστοσελίδας του CSIRT θα πρέπει να παρέχεται η δυνατότητα να συμπληρώσουν ηλεκτρονικά σε χρόνο πραγματικής πρόσβασης-online access- σχετικές φόρμες επικοινωνίας με τους διαχειριστές της ιστοσελίδας και μέσω αυτής της φόρμας να μπορούν να ενημερώσουν το CSIRT για διάφορα περιστατικά/κινδύνους για τα οποία θα ήθελαν να λάβουν περισσότερη ενημέρωση.

- Οι διαχειριστές του CSIRT θα πρέπει να διατηρούν σχετικές λίστες με τις ηλεκτρονικές διευθύνσεις και αριθμούς κινητής τηλεφωνίας των χρηστών/πελατών τους ούτως ώστε να επιτυγχάνουν άμεση ενημέρωση όλων των ομάδων των χρηστών οι οποίοι πιθανό να είναι ευάλωτοι σε συγκεκριμένη απειλή. Η ενημέρωση δύναται να γίνεται πέραν της αποστολής ηλεκτρονικού μηνύματος και με την αποστολή σχετικού σύντομου μηνύματος SMS. Οι διαχειριστές του CSIRT θα έχουν την ευθύνη για την ομαδοποίηση των χρηστών σύμφωνα με κριτήρια όπως το λειτουργικό σύστημα που χρησιμοποιούν, οι λογισμικές εφαρμογές, τα ενδιαφέροντα τους και άρα οι ιστοσελίδες που επισκέπτονται στο διαδίκτυο και γενικότερα το προφίλ τους.

- Παραδοσιακούς τρόπους επικοινωνίας των CSIRTs με τους πελάτες/χρήστες αποτελούν η επικοινωνία μέσω τηλεφώνου, τηλεομοιοτύπου ή αποστολή αλληλογραφίας μέσω ταχυδρομείου.

- Ενημέρωση των χρηστών μπορεί να γίνεται επίσης με την δημοσίευση από το CSIRT μηναίων ή τριμηνιαίων ενημερωτικών φυλλαδίων σχετικά με την δραστηριότητα τους και τις απειλές για τους χρήστες οι οποίες αντιμετωπίστηκαν ή πιθανό να προκύψουν.

9. Mission Statements

Το «Τμήμα Υπηρεσιών Πληροφορικής της Κυβέρνησης» θα παρέχει πληροφόρηση/ενημέρωση σε όλους τους χρήστες μηχανογραφικής υποδομής των Κυβερνητικών Τμημάτων καθώς και όλους τους Κύπριους πολίτες που θα τυγχάνουν εξυπηρέτησης από την Υπηρεσία καθώς και υποστήριξη πρώτου βαθμού-τηλεφωνική υποστήριξη[3]- σε όλους τους Κύπριους πολίτες που θα τυγχάνουν εξυπηρέτησης από την Υπηρεσία και οι οποίοι αντιμετωπίζουν απώλεια υπηρεσίας λόγω καταστροφικού συμβάντος.

Η ενημέρωση δεν θα περιορίζεται μόνο στην αποστολή ενημερωτικών ηλεκτρονικών μηνυμάτων αλλά και σε δημοσίευση στην ιστοσελίδα του ΤΥΠ διαφόρων τεχνικών εγγράφων/white papers και στη παροχή της δυνατότητας λήψης από την ιστοσελίδα αναβαθμίσεων για διάφορα λογισμικά. Η ενημέρωση είναι δυνατόν να παρέχεται και σε συνεργασία με του παροχείς υπηρεσιών ηλεκτρονικών επικοινωνιών π.χ. παροχείς υπηρεσιών διαδικτύου (ISPs).

Ο βαθμός της τεχνικής υποστήριξης για τους χρήστες των μηχανογραφικών συστημάτων της Κυβέρνησης δεν αναλύεται στο παρόν έγγραφο αφού αποτελεί δραστηριότητα του ΤΥΠ που πηγάζει από το καταστατικό σύστασης του.

Το «Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο» θα παρέχει πληροφόρηση/ενημέρωση σε όλους τους χρήστες μηχανογραφικής υποδομής των πανεπιστημιακών ιδρυμάτων καθώς και όλους τους Κύπριους πολίτες που θα τυγχάνουν εξυπηρέτησης από την Υπηρεσία καθώς και υποστήριξη πρώτου βαθμού-τηλεφωνική υποστήριξη- σε όλους τους Κύπριους πολίτες που θα τυγχάνουν εξυπηρέτησης από την Υπηρεσία και οι οποίοι αντιμετωπίζουν απώλεια υπηρεσίας λόγω καταστροφικού συμβάντος.

Η ενημέρωση δεν θα περιορίζεται μόνο στην αποστολή ενημερωτικών ηλεκτρονικών μηνυμάτων αλλά και *σε δημοσίευση* στην ιστοσελίδα του ΤΥΠ διαφόρων τεχνικών εγγράφων/white papers και στη παροχη της δυνατότητας λήψης από την ιστοσελίδα αναβαθμίσεων για διάφορα λογισμικά. Η ενημέρωση είναι δυνατόν να παρέχεται και σε συνεργασία με του παροχείς υπηρεσιών ηλεκτρονικών επικοινωνιών π.χ. παροχείς υπηρεσιών διαδικτύου (ISPs).

10. Μοντέλα Οργάνωσης CSIRT

Τα δύο επικρατέστερα μοντέλα οργάνωσης CSIRT τα οποία ανταποκρίνονται στα χαρακτηριστικά τα οποία έχουν οι δύο υποψήφιοι/επιλεγμένοι φορείς ΤΥΠ και ΚΕΑΔ είναι τα ακόλουθα:

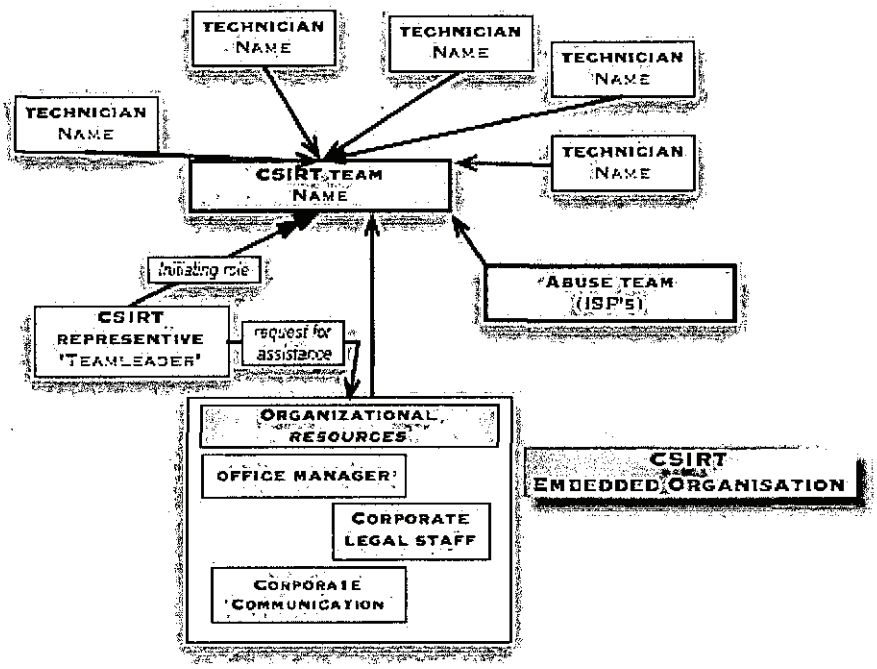
1. Η δημιουργία φορέα CSIRT εντός της οργανωτικής δομής ενός υφιστάμενου τμήματος/φορέα

Το Τμήμα Υπηρεσιών Πληροφορικής φέρεται να πληροί το συγκεκριμένο μοντέλο φορέα CSIRT αφού υπάρχει ήδη η οργανωτική του δομή και μηχανογραφική υποδομή η οποία μπορεί να διευκολύνει την ταχεία δημιουργία φορέα CSIRT.

Στα αρχικά στάδια της δημιουργίας του CSIRT υποδομή όπως κτίρια, μηχανογραφικός εξοπλισμός και δίκτυο είναι διαθέσιμα καθώς και προσωπικό το οποίο μπορεί εύκολα να αποσπαστεί ή να λειτουργεί παράλληλα και τα καθήκοντα που εκπηγάζουν από τη λειτουργία ενός φορέα CSIRT.

[3] Σε περιπτώσεις μεγάλου αριθμού τηλεφωνικών κλήσεων προς το κέντρο υποστήριξης των χρηστών και για αποφυγή υπερφόρτωσης του τηλεφωνικού συστήματος, παρέχεται η δυνατότητα ενεργοποίησης της αποδοχής «μέγιστου αριθμού τηλεφωνημάτων» και απόρριψη των κλήσεων εφόσον ξεπεραστεί αυτός ο αριθμός κλήσεων.

Σχετικό σχηματικό παρουσιάζεται πιο κάτω.

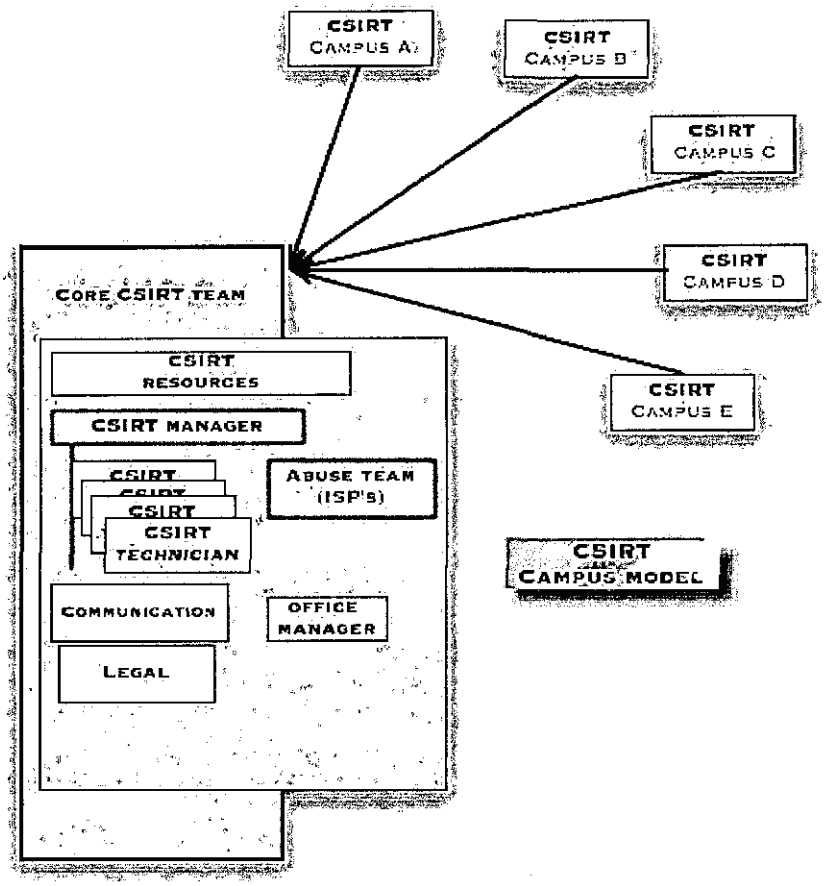


2. Το ακαδημαϊκό μοντέλο φορέα CSIRT

Αυτό το μοντέλο οργανωτικής δομής χρησιμοποιείται κυρίως για ακαδημαϊκά ιδρύματα τα οποία λειτουργούν ανεξάρτητα και υπό την «ομπρέλα» ενός κεντρικού CSIRT το οποίο αποτελεί ένα μοναδικό σημείο επαφής με άλλους αρμόδιους φορείς. Οι πληροφορίες διακινούνται από και προς τα ακαδημαϊκά ιδρύματα μέσω του κεντρικού CSIRT.

Το ΚΕΑΔ φέρεται να μπορεί να διεκπεραιώσει αυτή την δραστηριότητα για τα ακαδημαϊκά ιδρύματα της Κύπρου.

Σχετικό σχηματικό παρουσιάζεται πιο κάτω.



11. Ωράριο Λειτουργίας Φορέα CSIRT

Το ωράριο λειτουργίας του φορέα CSIRT καθώς και το πλήθος των υπηρεσιών που προσφέρει στους «πελάτες» του καθορίζουν τον αριθμό του προσωπικού που θα εργοδοτεί καθώς και τα προσόντα τα οποία θα κατέχουν με άμεσο αντίκτυπο στο ύψος του προϋπολογισμού που θα αφορά τη λειτουργία του.

Οι επιλογές για το ωράριο λειτουργίας καθορίζουν άμεσα και τον αριθμό των εργοδοτούμενων αφού εφόσον επιλεχθεί το CSIRT να παρέχει υπηρεσίες 24ώρη υπηρεσίες για 7 ημέρες την βδομάδα, με το προσωπικό να εργάζεται με σύστημα βάρδιας τότε το ελάχιστο που απαιτείται και συστήνεται για ορθή λειτουργία του CSIRT είναι δώδεκα (12) άτομα πλήρους απασχόλησης.

Εφόσον απαιτείται το CSIRT να παρέχει την βασική δέσμη υπηρεσιών- Πρόληψης και Αποκατάστασης μετά από καταστροφικά συμβάντα- και να ακολουθεί ωράριο λειτουργίας ωρών γραφείου – 0730 πμ - 1430 μμ και 1430 μμ-1730 μμ- τότε ο αριθμός προσωπικού που απαιτείται κυμαίνεται μεταξύ 6-8 άτομα πλήρους απασχόλησης.

Εναλλακτικά το προσωπικό του CSIRT μπορεί να εργάζεται από τις 0730πμ -1430μμ και για τις απογευματινές ώρες να υπάρχει προσωπικό σε επιφυλακή έτσι να μπορεί να ειδοποιείται εφόσον προκύψει η ανάγκη για αποκατάσταση/συντονισμό ενεργειών για αποκατάσταση μετά από καταστροφικά συμβάντα.

Σε αυτή την περίπτωση τότε το CSIRT μπορεί να έχει μέγιστο ανθρώπινο δυναμικό της τάξεως των έξι (6) ατόμων.

Λαμβάνοντας υπόψη την δομή και το ωράριο εργασίας των δύο φορέων- ΤΥΠ και ΚΕΑΑΔ- που έχουν επιλεγεί για να διεκπεραιώσουν δραστηριότητες φορέα CSIRT- καθώς και τις βασικές υπηρεσίες *που θα* προσφέρουν καταρχάς οι δύο φορείς CSIRTs τότε το καταλληλότερο μοντέλο ωρών εργασίας του προσωπικού είναι, η εργασία εντός ωραρίου 0730 -1430 καθημερινά εκτός από μια μέρα την εβδομάδα κατά την οποία η υπηρεσία θα λειτουργεί με βάση το ωράριο 0730- 1800, ή το εκάστοτε ωράριο της Δημόσιας Υπηρεσίας..

Τις υπόλοιπες ημέρες- τις απογευματινές ώρες- οι χρήστες/πελάτες του κάθε φορέα μπορούν να εξυπηρετούνται από προσωπικό σε επιφυλακή.

12. Χαρακτηριστικά προσωπικού CSIRT

Το προσωπικό του CSIRT συστήνεται όπως έχει την ακόλουθη τεχνική γνώση/εμπειρία:

- Ευρεία γνώση της τεχνολογίας και πρωτοκόλλων του Διαδικτύου
- Γνώση λειτουργικών συστημάτων όπως UNIX και LINUX ανάλογα με τα λειτουργικά συστήματα τα οποία χρησιμοποιούν οι πελάτες/χρήστες του CSIRT.
- Γνώση λειτουργικών συστημάτων Windows (server versions + home/professional versions)
- Γνώση επιμέρους εφαρμογών που χρησιμοποιούν ευρέως οι πελάτες/χρήστες του CSIRT
- Γνώση εξοπλισμού και τεχνολογιών/πρωτοκόλλων δικτύωσης (Δρομολογητές, Διακόπτες, Διακομιστές Ονοματοδοσίας- DNS, Proxy servers, Mail servers, CISCO IOS κλπ)
- Γνώση εφαρμογών διαδικτύου (SMTP, HTTP, HTTPS, FTP, TELNET, SSH κλπ).
- Γνώση απειλών Ασφαλείας Δικτύων και Πληροφοριών (DdoS, Phishing, Defacing, Sniffing κλπ)
- Γνώση σχετικά με αξιολόγηση των απειλών-Risk Assessment και πρακτικές εφαρμογές.
- Επιπρόσθετα πρόσληψη προσωπικού που να έχει πιστοποιηθεί ως CISSP- Certified Information Systems Security Professional μπορεί να θεωρηθεί πλεονέκτημα για την λειτουργία του φορέα.

Όσον αφορά την απόκτηση από το προσωπικό επαγγελματικών τίτλων και συναφών πιστοποιητικών (π.χ. MSCE, CISCO και CISSP), οι δύο φορείς CSIRT θα πρέπει - εντός δύο (2) ετών από την λειτουργία τους - να εντάξουν στον προυπολογισμό τους σχετικό κονδύλι εκπαίδευσης που θα επιτρέψει στο προσωπικό να αποκτήσει τα πιο πάνω πιστοποιητικά.

13. Εκτίμηση Κόστους για Δημιουργία Φορέα/Φορέων CSIRT στην Κύπρο

Στην παρούσα φάση του έργου δεν μπορούν να γίνουν ασφαλείς υπολογισμοί σχετικά με το κόστος που απαιτείται για την δημιουργία φορέων CSIRT στην Κύπρο. Η επιλογή των υπηρεσιών, κατά κύριο λόγο, που θα παρέχει στο κοινό του ο φορέας CSIRT καθώς και η επιλογή του ωραρίου λειτουργίας του φορέα αποτελούν σημαντικές παραμέτρους στη σύνθεση του τελικού κόστους που απαιτείται.

Το κόστος της υποδομής/δικτύου που θα πρέπει να διαθέτει ο φορέας CSIRT συνδέεται άμεσα με τον αριθμό των υπηρεσιών που θα προσφέρονται από το CSIRT και επηρεάζει σε μεγάλο βαθμό το κόστος σύστασης των φορέων.

Το ΓΕΡΗΕΤ προτού καταλήξει σε τελική οικονομική πρόταση σχετικά με το κόστος δημιουργίας των φορέων CSIRT στην Κύπρο θα διαβουλευθεί εκ νέου με το ΤΥΠ και το ΚΕΑΔ αφού έχει ήδη διαβουλευθεί και λάβει τα θετικά σχόλια του ENISA.

Στη βάση των πιο πάνω αποφάσεων σχετικά με τον τύπο των υπηρεσιών που θα παρέχει, το ωράριο λειτουργίας και τον αριθμό του ανθρώπινου δυναμικού και που θα επανδρώνει τον φορέα CSIRT το κόστος της δημιουργίας τέτοιων φορέων δύναται να συνοψιστεί ως ακολούθως:

I. Κόστος Υποδομής:

Εφόσον προκύπτουν πρόσθετες οικονομικές απαιτήσεις σε υποδομή/μηχανογραφικό εξοπλισμό που θα χρησιμοποιηθεί για να καλύψει τις επιπρόσθετες ανάγκες που δημιουργούνται με την παροχή βασικών υπηρεσιών κυρίως της αποκατάστασης των υπηρεσιών των «πελατών/constituents», αυτές αναμένεται να καλυφθούν από τους ετήσιους προϋπολογισμούς του ΤΥΠ και του ΚΕΑΔ.

II. Κόστος Επάνδρωσης Φορέα/ Οργανική Δομή και Μισθολόγιο Προσωπικού:

Στη βάση της απόφασης σχετικά με το ωράριο και τον τύπο των υπηρεσιών που θα παρέχουν αυτού του τύπου οι φορείς οι ανάγκες των δύο φορέων σε προσωπικό μπορεί να είναι της τάξεως των έξι (6) ατόμων (μέγιστος αριθμός).

Η σύνθεση της ομάδας των έξι (6) ατόμων του προσωπικού συστήνεται να έχει ως πιο κάτω:

1 x βαθμός Ανώτερου Λειτουργού – Κλίμακα Εισδοχής Α13

2 x βαθμός Λειτουργού- Κλίμακα Εισδοχής Α8 και

3 x βαθμός Τεχνικού- Κλίμακα Εισδοχής Α5

Το συνολικό ετήσιο ακαθάριστο κόστος επάνδρωσης σε Ευρώ ανά φορέα ανέρχεται σε (1x 4286 € x 13) (2x 1971 € x 13) + (3 x 1303 € x 13) = 55718+ 51246 + 50817 = 157,781 Euro

14. Συνεργασία μεταξύ των φορέων CSIRTs

Οι δύο φορείς CSIRT που θα δημιουργηθούν στην Κύπρο θα λειτουργούν παράλληλα και με στόχο το κάθε CSIRT να εξυπηρετεί πρωτίστως τους πελάτες/χρήστες του. Οι δύο φορείς θα πρέπει να συνεργάζονται στα θέματα ενημέρωσης των πελατών τους ανάλογα με το προφίλ του κάθε χρήστη/πελάτη καθώς και στα θέματα υποστήριξης των χρηστών.

Στις περιπτώσεις όπου απαιτείται συντονισμός μεταξύ των δύο CSIRT για αποκατάσταση λειτουργίας/υπηρεσιών που λαμβάνουν οι χρήστες μετά από καταστροφικό συμβάν τότε το προσωπικό των δύο φορέων θα καταβάλει προσπάθειες για αλληλοβοήθεια στο μέγιστο δυνατό βαθμό.

Στην πιθανότητα που το ένα από τα δύο CSIRTs αντιμετωπίζει προβλήματα με την υποδομή του σε βαθμό που δεν μπορεί να παρέχει υπηρεσίες στους δικούς του πελάτες, οι δύο φορείς θα πρέπει να συνεργάζονται και έχουν σε θέση μηχανισμούς έτσι ώστε η διακοπή υπηρεσίας του ενός να μπορεί να ξεπεραστεί το συντομότερο και με τις λιγότερες επιπτώσεις στους πελάτες/χρήστες.

Σημειώνεται ότι ο σχεδιασμός της υποδομής του CSIRT θα πρέπει να βασίζεται στην εφεδρικότητα συστημάτων και ζεύξεων έτσι ώστε να μπορεί να προσφέρει απρόσκοπτη υπηρεσία.

Τα θέματα συνεργασίας, διαδικασιών συντονισμού, εκπροσώπησης και επίλυσης τυχόν προβλημάτων/διαφορών θα τυγχάνουν συντονισμού από το συντονιστικό φορέα που είναι το ΓΕΡΗΕΤ. Λεπτομέρειες για τα συγκεριμένα θέματα μπορούν να καθοριστούν στην απόφαση διορισμού τους από τον ΕΡΗΕΤ.

15. Συμμετοχή σε Διεθνείς Ομάδες Εργασίας/*Οργανισμούς* CSIRT

Οι δύο φορείς CSIRT θα πρέπει να είναι μέλη σε δύο διεθνή σώματα:

- TF-CSIRT Task Force[4]: πρωταρχικός στόχος της Ομάδας Εργασίας είναι να παρέχει την βάση για ανταλλαγή εμπειριών και πληροφοριών μεταξύ των φορέων CSIRT των Ευρωπαϊκών χωρών καθώς επίσης και να παρέχει υποστήριξη/βοήθεια στην δημιουργία καινούργιων φορέων CSIRT.
- Global CSIRT Initiative-FIRST[5]: η συμμετοχή δίνει την δυνατότητα στα μέλη να ανταποκρίνονται γρηγορότερα και με μεγαλύτερη αποδοτικότητα σε καταστροφικά συμβάντα σχετικά με την ασφάλεια πληροφοριών- τόσο για υπηρεσίες πρόληψης όσο και για υπηρεσίες αποκατάστασης μετά από τέτοια συμβάντα.

[4] http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

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

Παράρτημα 2

enisa
European Network and Information Security Agency

November | 2008

Response to request from Cyprus

Opinion on the development plan for Cyprus' national CSIRT

(Ref. ENISA/REG/REQ/16) (Ref. OCECPR 04.05.002)

Marco Thorbruegge, Andrea Dufkova

General remarks

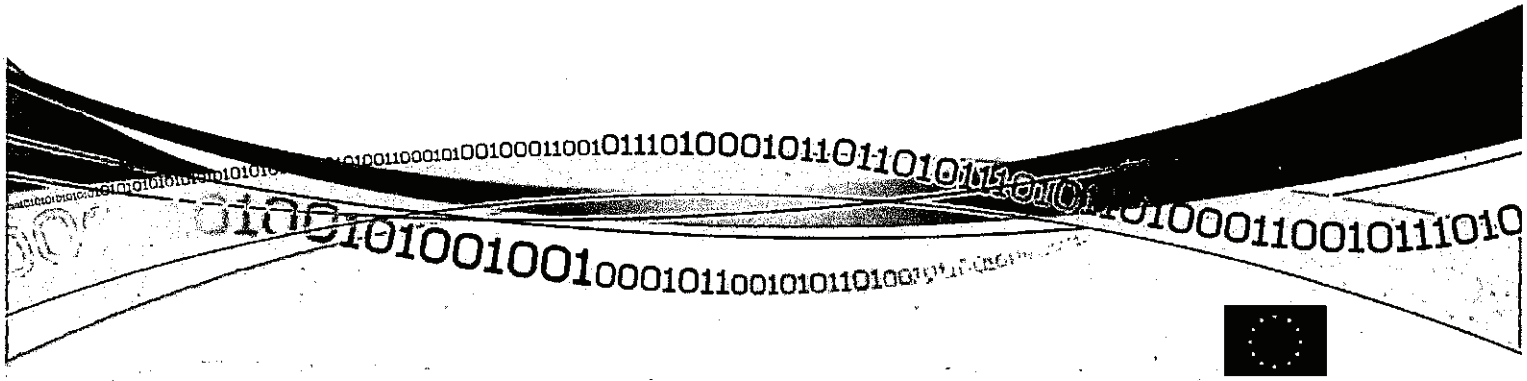
The submitted draft of a project plan for the establishment of national CSIRTs in Cyprus outlines a throughout **reasonable** approach that testifies **profound knowledge** of the underlying matter. The draft is suited, in all parts, to be built upon when creating the detailed final project plan.

Hence ENISAs response mainly consists of **remarks, tips** and outlines for potential **next steps.**

Outline of the request

Cyprus submitted a draft project plan for the setting-up of national incident response capabilities and requested ENISA's input on the following steps:

- General decision to have two national CSIRTs (sections 5 and 6)
- CSIRT services to be provided (section 7)
- Communication channels between CSIRTs and constituency (section 8)
- Mission statements of the two CSIRTs (section 9)
- Organisational structure (section 10)
- CSIRT working hours (section 11)
- Expected qualification of CSIRT staff (section 12)
- Cost calculation and CSIRT budget (section 13)
- Cooperation between the two national CSIRTs and with others (section 14)



Detailed response

General decision to have two national CSIRTs (sections 5 and 6)

AGREE: in the given situation and also taking into account experiences from other Member States, the proposed scenario of having two separate teams working for different constituencies, but under auspices of the government is plausible. Both hosting organisations (DITS and CyNET) seem to be capable of hosting a CSIRT and providing the outlined service. The CyNET CSIRT, according to the ENISA inventory of CERT activities in Europe, was already established in 2001, so the team members should dispose of profound skills and expertise, which is very *valuable* for the whole project.

REMARKS: in the case of setting-up of two separate entities the segmentation of roles and responsibilities must be made perfectly clear. Especially the separation of the constituents (which CSIRT is responsible for which networks) and the question which entity finally plays the role of "National point of contact (PoC)" to foreign CSIRTs should be clarified very soon in the process. Overlaps of constituencies should be avoided. In the setting-up phase a single project manager should be in charge, and emancipated representatives (sub-leaders) of both envisaged CSIRTs should report to him. It is crucial that, from the very beginning, all involved parties closely work together and communicate with each other on a regular basis!

OUTLOOK: ENISA is prepared to depute CSIRT experts to a kickoff meeting with all involved parties, in order to discuss starting issues in more details. ENISA is also prepared to accompany the setting-up process, to answer questions and give advice on an "ad-hoc" basis.

CSIRT services to be provided (section 7)

AGREE: experience shows that the "start small, but think big" approach is the most suitable for new CSIRTs. The proposed set of services outlined in section 7 of the draft project plan is (almost) exactly the right set to start with.

REMARKS: it may be gainful to add the service of "Announcements" to the portfolio of both CSIRTs, regular information to the constituents that bear a lower priority than alerts or warnings. Most of the known CSIRTs supply their constituents with regular flowing information in order to raise security awareness but also to reassure the constituents that "their" CSIRT constantly works in order to protect their networks. This reassurance must (!) also be given when incidents are reported: incident reports must always be acknowledged. Please also refer to "expected skills of CSIRT staff" later in this paragraph.

There should be a review of services on a regular basis (approx. twice a year) where the existing services and an expansion of the service portfolio are assessed.

OUTLOOK: ENISA is prepared to facilitate training for the CSIRT staff members on request. Furthermore ENISA provides exercise material that can be used to train the CSIRT staff members in various facets of service provision. A list with trusted publicly available sources of NIS information can be provided by ENISA on request.

Communication channels between CSIRTs and constituency (section 8)

AGREE: as for services, the proposed communication channels (public and restricted website, mailing list) are most suitable to communicate with the constituents (in both directions).

REMARKS: after some time of operation there should be a review of the communication channels, that includes feedback by users (i.e. in form of a survey). Experience shows that especially inexperienced users may require additional communication channels (like SMS alerts or similar) in order to reach out to them. An analysis of the composition of the constituency (including the IT systems in use), that is constantly reviewed, is necessary in order to successfully reach out to a majority of users (experience also shows that a reach-out to all single users is almost impossible to achieve). Make sure that some communication channels are also suited to receive feedback from users (therefore a discussion-mailing list besides the one for the distribution of warnings and alerts should be installed). In addition it is absolutely necessary that both CSIRTs agree on a common set of terminology that is used consequently when communicating with the constituency (i.e. both should have a clear understanding of a "security incident" or have the same names for attack vectors). For incident reporting a hotline / helpdesk function realised with telephones (landline and mobile) is furthermore necessary, also to provide an "out-of-band" communication during times when internet is not available (therefore VoIP telephones for the hotline / helpdesk should be avoided!) and the development of a triage mechanism for peak times should be developed or adopted from other teams.

OUTLOOK: ENISA is prepared to provide further input on that matter on request.

Mission statements of the two CSIRTs (section 9)

AGREE: the proposed mission statements are suitable for the two new CSIRTs.

REMARKS: the mission statements should be reviewed again before they are published, as mission statements should not be changed once they are communicated to the constituency.

Organisational structure (section 10)

AGREE: the proposed operation models ("embedded model" for the DITS CSIRT, the "campus model" for the CyNET CSIRT) seem to be the most appropriate in the given situation, as most of known CSIRTs with similar constituencies chose the same models (there are differences when CSIRT services are provided by a private company).

REMARKS: the most suitable model is also highly depending on the revenue model chosen for the operation of the two CSIRTs, i.e. how is operation financed. For the CyNET CSIRT the establishment of security points of contacts at the served institutes (universities, schools, etc.) will be necessary on the long run, but should probably already be initiated in the setting-up phase of CyNET CSIRT.

OUTLOOK: ENISA is prepared to make contact to CSIRTs in Europe with similar constituencies on request, in order to initiate target-oriented information sharing (see also paragraph "Cooperation between the two national CSIRTs and with others").

CSIRT working hours (section 11)

AGREE: the proposed working hours are appropriate for the two proposed CSIRTs.

REMARKS: academic CSIRTs usually operate during "normal business hours", but provide means to contact them out of these times, like answering machines or mailing lists. For CSIRTs that are responsible for public administration or even CIIP a 24/7 including a "security officer on call" is the most appropriate setting that most of the CSIRTs with national responsibilities choose.

OUTLOOK: ENISA is prepared to make contact to CSIRTs in Europe with similar constituencies on request, in order to initiate target-oriented information sharing (see also paragraph "Cooperation between the two national CSIRTs and with others").

Expected qualification of CSIRT staff (section 12)

AGREE: the proposed expected qualifications for CSIRT staff members are derived from the ENISA "CSIRT setting-up guide" and therefore already proved to be the most essential skills CSIRT staff should have.

REMARKS: clearly the team leader for both CSIRTs must furthermore dispose of profound social and management skills. The CSIRT staff members that will have direct contact to constituents (i.e. via the hotline / helpdesk) should be monitored closely concerning their attitude towards inexperienced users; experience shows that (often) the more technically skilled a person is, the lower is preparedness to communicate with inexperienced users. In addition, required technical skills (like in operating systems) are also dependant on the infrastructure and IT systems in place. The whole topic of staff recruitment is probably the most complex one in the whole process of setting-up of CSIRTs, and information that goes beyond chapter 6.3 in the ENISA "CSIRT setting-up" guide is impossible to give beforehand. It may be gainful to include CSIRT experts from other teams or an experienced external consultant in the hiring process.

OUTLOOK: ENISA is prepared to facilitate training for the CSIRT staff members on request. Furthermore ENISA provides exercise material that can be used to train the CSIRT staff members in various facets of service provision (including the recruitment process).

Cost calculation and CSIRT budget (section 13)

No competent remark can be given by ENISA on that topic.

Cooperation between the two national CSIRTs and with others (section 14)

AGREE: the proposed way of communication between the two CSIRTs is appropriate. The future plans to get involved in the international CSIRT communicates make sense. The availability of both teams to serve as a fall-back mechanism for the respective other teams to a high extend facilitates the resilience and sustainability of the national incident response capabilities.

REMARKS: both teams need to meet in a regular basis in order to share information, at least once a month in the beginning of operation. On a longer term the inclusion of other relevant (incident response providing) parties (like ISPs, vendors, law enforcement, etc.) may be gainful. Example models of a regional cooperation initiatives can be found for example in Germany (CERT Verbund), UK or The Netherlands.

For the international cooperation it may be useful to send one or more representatives that will play a role in the planned two CSIRTs to the next joint TF-CSIRT/FIRST meeting end of January 2009 in Riga/Latvia, in order to initiate contact to other teams and to potential sponsors for a FIRST membership (it may be too early for the latter). FIRST membership and listing by the Trusted Introducer service definitely is a desirable goal.

OUTLOOK: ENISA is prepared to provide further input on that matter on request and make contact to other CSIRTs in the communities. ENISA representatives will also be in Riga.

Summary and outlook

As stated in the beginning ENISA can fully support the chosen approach and the submitted draft project plan. However, the input given on the draft project plan does not get into detail of specific problems or tasks that may occur during the implementation. So Cyprus may consider to also requesting ENISA support in the future, when a detailed project plan is developed and the setting-up process of the two new CSIRTs is started. Once the CSIRT staff is hired, an initial training can be organised with the help of ENISA. In addition Cyprus may consider being involved in the pilot of the

CSIRT exercise material that is planned in 2009, or in subsequent exercises ENISA may facilitate in the future, depending of the success of the pilot.

ENISA welcomes the initiative of planning Cyprus' national incident response capabilities and is prepared to further facilitate it in the future on request!

Additional material

The ENISA inventory of CERT activities in Europe

URL: http://www.enisa.europa.eu/cert_inventory

A constantly updated overview of known CSIRTs, cooperation-, standardisation- and support initiatives in Europe and beyond. Once the two teams are established in Cyprus, they will be listed in this inventory.

The ENISA CSIRT setting-up guide

URL: http://www.enisa.europa.eu/cert_guide/

The de-facto standard guide for project managers that need to set-up incident response capabilities. All advice, input and answers to questions are given on the basis of this guide. The contained project plan template was already used in a couple of similar cases where Member States planned their national CSIRTs.

The ENISA report on CERT cooperation

URL: http://www.enisa.europa.eu/cert_cooperation/

Another standard guide that especially deals with all the various aspects cooperation and communication. As Cyprus plans to have two separate CSIRTs this guide gives valuable insight in the "secrets" of successful communication on national and international level, including "real world" examples.

ENISA basic collection of good practice for running CSIRTs

URL: http://www.enisa.europa.eu/cert_goodPractices/

Quasi the successor to the setting-up guides this document provides tips, tricks and good practice for "surviving the first year" of operation. The project manager responsible for the setting-up of the two CSIRTs may already now take this material into account.

End of 2008 ENISA will also make available exercise material.

As annex to this document ENISA will include a report on the status quo of national incident response capabilities in the Member States that the agency produced on request by the European Commission.

ANNEX: Overview of national incident response capabilities in the EU Member States (Status: 11/2008)

The following list is an excerpt of ENISAs inventory of "CERT activities in Europe" that shows the coverage with CERT services in the Member States and other countries in Europe. The information is based on publicly available data and collected and presented to the best of our knowledge. ENISA does not take any responsibility concerning the up-to-datedness of the presented data.

Please take into account that the term "national CSIRT" is at the moment not clearly defined and some of the CSIRTs mentioned in this list may not consider themselves as "national CSIRT".

CERT.AT (Austria)

Established: 1Q 2008

Team info: http://www.trusted-introducer.nl/teams/certat.html

Constituency: IT security teams in Austria. This includes bodies of public interest such as IT security teams from the medical field, the chamber of commerce, ISPs, etc. Through their GovCERT.at function CERT.at also serves IT security teams for all bodies of the Austrian government.

More Info: http://www.cert.at/

BELNET CERT (Belgium)

Established: 3Q 2004

Team info: http://www.trusted-introducer.nl/teams/belnet-cert.html

Constituency: BELNET's customers (Belgian universities, public administrations, high schools and research centres connected to BELNET's network). Not official national CSIRT!

More Info: http://cert.belnet.be

DK-CERT (Denmark)

Established: 3Q 1991

Team info: http://www.trusted-introducer.nl/teams/dk-cert.html

Constituency: The national organisation UNI-C, the Danish research- and educational networks, Sektornet and Forskningsnet. The entire Danish it-community (coordination, support and information). Not

More Info: http://www.cert.dk

CERT-EE Estonia (Estonia)

Established: 2Q 2006

Team info: http://www.trusted-introducer.nl/teams/teams-c.html#CERT-EE

Constituency: Estonian National CERT.

More Info: http://www.cert.ee/

CERT-FI (Finland)

Established: 1Q 2002

Team info: http://www.trusted-introducer.nl/teams/cert-fi.html

Constituency: The whole country of Finland, with emphasis on telecommunications network operators, service providers and critical infrastructure.

More Info: http://www.cert.fi

CERTA (France)

Established: 4Q 1999

Team info: http://www.trusted-introducer.nl/teams/certa.html

Constituency: French administration community: All French public offices and services as well as local territorial offices.

More Info: http://www.certa.ssi.gouv.fr

CERT-BUND (Germany)

Established: 3Q 2001

Team info: http://www.trusted-introducer.nl/teams/teams-c.html#CERT-BUND

Constituency: Federal government departments in Germany.

More Info: http://www.bsi.bund.de/certbund/

GRNET-CERT (Greece)

Established: 2Q 2000

Team info: http://www.trusted-introducer.nl/teams/grnet-cert.html

Constituency: All users connected to the Greek Research and Technology Network. De facto point of contact for Greece related incidents. Not official national CSIRT!

More Info: http://cert.grnet.gr

CERT-Hungary (Hungary)

Established: 2004

Team info: http://www.trusted-introducer.nl/teams/cert-hungary.html

Constituency: Users of systems of the Hungarian government, municipalities, and businesses, with special attention to the security of the government's computer systems.

More Info: http://www.cert-hungary.hu/

(Ireland)

No national CSIRT so far, but at least a (recently established) PoC to report incidents to (privately organised, no official governmental mandate).

GOVCERT.IT (Italy)

Established: 2004

Constituency: Central public administration in Italy and 21 ministries and national government agencies of Italy comprising CERT-AM (21).

More Info: http://www.govcert.it/

DDIRV (Latvia)

Established: 1Q2007

Team info: http://www.trusted-introducer.nl/teams/teams-d.html#DDIRV

Constituency: State and municipal institutions in Latvia (Government & Military).

More Info: http://www.ddirv.lv, http:// www.vita.gov.lv

CERT-LT (Lithuania)

Established: 4Q/2006

Team info: http://www.trusted-introducer.nl/teams/teams-d.html#DDIRV

Constituency: CERT-LT is the Lithuanian national CERT and its scope of activity are the networks of telecommunication operators and Internet service providers in Lithuania.

More Info: http://www.cert.lt/en/

mtCERT (Malta)

Established: 3Q 2002

Team info: http://www.trusted-introducer.nl/teams/mtcert.html

Constituency: All Government employees.

More Info: http://www.mtcert.gov.mt/

NorCERT (Norway)

Established: 2Q 2004

Team info: http://www.trusted-introducer.nl/teams/teams-n.html#NORCERT

Constituency: Norwegian Organisations with critical national infrastructure and information.

More Info: http://www.cert.no/

CERT GOV PL (Poland)

Established: 2008

Team info: http://www.cert.gov.pl/

Constituency: Government sector

More Info: http://www.cert.pl/english.html

CERT.PT (Portugal)

Established: 3Q 2002

Team info: http://www.trusted-introducer.nl/teams/cert-pt.html

Constituency: Users of systems connected to the Portugal National Research and Education Network. De facto point of contact for Portugal related incidents. Not official national CSIRT!

More Info: http://www.cert.pt

SI-CERT (Slovenia)

Established: 4Q 1994

Team info: http://www.trusted-introducer.nl/teams/si-cert.html

Constituency: Customers of ARNES (primary), users of systems inside the .si namespace (secondary). Not official national CSIRT!

More Info: http://www.arnes.si/english/si-cert/

CCN-CERT (Spain)

Established: 4Q 2006

Team Info: http://www.trusted-introducer.nl/teams/teams-c.html#CCN-CERT

Constituency: Spanish Public Civil Service (Central Government, Regional and Local Institutions).

More Info: http://www.ccn-cert.cni.es

SITIC (Sweden)

Established: 1Q 2003

Team info: http://www.trusted-introducer.nl/teams/sitic.html

Constituency: Members of Swedish government organisations, additional target groups outside the government organisations.

More Info: http://www.sitic.se

GOVCERT.NL (The Netherlands)

Established: 2Q 2002

Team info: http://www.trusted-introducer.nl/teams/govcert-nl.html

Constituency: Members of governmental institutions of The Netherlands

More Info: http://www.govcert.nl

GovCertUK (United Kingdom)

Established: 1Q 2007

Team info: http://www.trusted-introducer.nl/teams/teams-g.html#GOVCERTUK

Constituency: Government community, public sector organisations.

More Info: http://www.govcertuk.gov.uk/

CSIRTUK (United Kingdom)

Established: 1992

Team info: http://www.trusted-introducer.nl/teams/csirtuk.html

Constituency: Organisations that form part of the UK National Infrastructure.

Specified .co.uk, .org.uk and .com domains.

More Info: http://www.cpni.gov.uk/

CARNet CERT (Croatia)

Established: 3Q 1996

Team info: http://www.trusted-introducer.nl/teams/carnet-cert.html

Constituency: Users of systems inside the .hr namespace. Not official national CSIRT!

More Info: http://www.cert.hr

CYPRUS (Cyprus)

Established: 1Q 2001

Team info: http://www.trusted-introducer.nl/teams/teams-c.html#CYPRUS

Constituency: Users of systems connected to CYNET, the Cyprus Academic and Research Network. Not official national CSIRT!

CSIRT.CZ (Czech Republic)

Established: 3Q 2007

Team info: http://www.trusted-introducer.nl/teams/teams-c.html#CSIRTCZ

Constituency: The Czech Republic. CSIRT.CZ is the "Last Resort CSIRT" for the Czech Republic, effectively taking over this task from the CESNET-CERTS team. Not (yet) official national CSIRT!

More Info: http://www.csirt.cz/en/

RHnet CERT (Iceland)

Established: 4Q 2003

Team info: http://www.trusted-introducer.nl/teams/teams-r.html#RHNET-CERT

Constituency: Users of RHnet Iceland University Research Network. Not official national CSIRT!

CIRCL (Luxembourg)

Team info: http://www.trusted-introducer.nl/teams/teams-c.html#CIRCL

Constituency: The administrations and ministries of the Grand-Duchy of Luxembourg (this includes government and local government agencies). Not official national CSIRT!

More Info: http://www.circl.lu/

RoCSIRT (Romania)

Team info: http://www.trusted-introducer.nl/teams/teams-r.html#ROCSIRT

Constituency: All institutions connected to RoEduNet. Not official national CSIRT!

More Info: http://www.csirt.ro/index.html

RU-CERT (Russia)

Established: 1998

Team info: http://www.trusted-introducer.nl/teams/ru-cert.html

Constituency: Customers of RBNET, general services for the entire Russian IT community.

More Info: http://www.cert.ru

UNKNOWN (Switzerland)

Newly built up team unknown to ENISA so far.

TR-CERT (Turkey)

Established: 2Q 2007

Team info: http://www.trusted-introducer.nl/teams/teams-t.html#TR-CERT

Constituency: Members of governmental organisations.

More Info: http://www.tr-cert.gov.tr