Πανεπιστήμιο Κύπρου
Υπηρεσία Πληροφορικής Υποδομής

Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών

(Incident Response Procedure)

Έκδοση: 1.0
Τομέας Ασφάλειας Πληροφοριών
Υπηρεσία Πληροφορικής Υποδομής
Οκτώβριος 2025

Περιεχόμενα

Σκοπός

Η διαδικασία αυτή καθορίζει τα βήματα που πρέπει να ακολουθούνται για την έγκαιρη επικύρωση και αντιμετώπιση των περιστατικών ασφάλειας πληροφοριών που προκύπτουν στο Πανεπιστήμιο Κύπρου.

Ρόλοι

- Ομάδα Αντιμετώπισης Περιστατικών (Incidence Response Team)
  - Λήδα Φιούρη, Τομέας Ασφάλειας Πληροφοριών
  - Φώτια Παναγιώτου, Τομέας Ασφάλειας Πληροφοριών
  - Μάριος Φωκάς, Επικεφαλής Τομέα Δικτύων
  - Μάριος Κωνσταντίνου, Επικεφαλής Τομέα Πληροφορικής Υποστήριξης
  - Ευτύχιος Ευτυχίου, Επικεφαλής Τομέα Συστημάτων
  - Χρίστος Χαραλάμπους, Αν. Προϊστάμενος Υπηρεσίας Πληροφορικής Υποδομής

- Τομέας Ασφάλειας Πληροφοριών Υπηρεσίας Πληροφορικής Υποδομής

- Τομέας Συστημάτων ΥΠΥ, Τομέας Δικτύων ΥΠΥ, Διαχειριστές Υπηρεσιών / Εξυπηρετητών, Τοπικές Ομάδες Υποστήριξης Πληροφορικής

Διαδικασία

1. Αναγνώριση – Παραλαβή & Επιβεβαίωση περιστατικού

Υπεύθυνοι: Τομέας Ασφάλειας Πληροφοριών

Ενέργειες:

- Παραλαβή email/ticket από το εξωτερικό SOC, ή αναφορά χρήστη.
- Επιβεβαίωση παραλαβής περιστατικού.

Σημ.: Για περιστατικά υψηλής ή κρίσιμης σημασίας, το SOC επικοινωνεί απευθείας με την Ομάδα Αντιμετώπισης Περιστατικών.

2. Αρχική Επισκόπηση

Υπεύθυνοι: Ομάδα Αντιμετώπισης Περιστατικών

Ενέργειες:

- Επισκόπηση της περίληψης ειδοποίησης και των παρεχόμενων αρχείων.
- Επιβεβαίωση του επιπέδου σοβαρότητας (severity alert): Κρίσιμη, Υψηλή, Μεσαία, Χαμηλή.
- Ανάθεση περιστατικού στην κατάλληλη ομάδα (Τομέας Συστημάτων, Τομέας Δικτύων, Τοπική Υποστήριξη, ή Helpdesk εάν σχετίζεται με χρήστη/τερματικό) μέσω Service Desk (OTRS) ticket.
- Σε περίπτωση υψηλού/κρίσιμου περιστατικού, άμεση τηλεφωνική επικοινωνία με τον αρμόδιο διαχειριστή.

3. Έρευνα & Συλλογή Πληροφοριών, Περιορισμός & Αντιμετώπιση

Υπεύθυνοι: Λειτουργοί Συστημάτων/Δικτύων ΥΠΥ, Διαχειριστές Εξυπηρετητών, Ομάδες Υποστήριξης (Τοπικές/Helpdesk)

Ενέργειες:

- Διερεύνηση και λήψη κατάλληλων ενεργειών:
    - Ανάλυση δεδομένων και έλεγχος αρχείων καταγραφής (logs).
    - Έλεγχος δραστηριότητας χρήστη και συμπεριφοράς συστήματος.
    - Έλεγχος ιστορικού και εξαγωγή στοιχείων επικοινωνίας επηρεαζόμενου χρήστη.
- Πιθανές ενέργειες (υποδείξεις SOC και Ομάδας Αντιμετώπισης Περιστατικών):
    - Παρακολούθηση και επικοινωνία με τον χρήστη.
    - Απομόνωση επηρεαζόμενων τερματικών ή κλείδωμα λογαριασμών.
    - Μπλοκάρισμα IOCs (IPs, domains, file hashes).
    - Εφαρμογή ενημερώσεων ή αλλαγών ρυθμίσεων.
    - Format υπολογιστή.
    - Επαναφορά κωδικών ή ανάκληση πρόσβασης.

- Ενημέρωση του Service Desk (OTRS) ticket με όλες τις ενέργειες.
- Ενημέρωση της Ομάδας Αντιμετώπισης Περιστατικών για περαιτέρω ενέργειες ή κλιμάκωση.

Για όλα τα περιστατικά, εάν δεν ληφθεί ενέργεια (ή δοθεί σχετική ανατροφοδότηση) εντός των καθορισμένων χρονικών ορίων από τον υπεύθυνο διαχειριστή, η Ομάδα Αντιμετώπισης Περιστατικών δύναται να προχωρήσει σε **απομόνωση ή απενεργοποίηση της δικτυακής σύνδεσης του επηρεαζόμενου συστήματος** (π.χ. φορητού υπολογιστή, εξυπηρετητή, εικονικής μηχανής κ.λπ.).

Καθορισμένα Χρονικά Όρια (SLA):

Σοβαρότητα Περιστατικού	Ενέργεια
Κρίσιμη	Εντός 2 ωρών από την ειδοποίηση
Υψηλή	Εντός 1 εργάσιμης ημέρας
Μεσαία	Εντός 3 εργάσιμων ημερών
Χαμηλή	Εντός 5 εργάσιμων ημερών

4. Κλιμάκωση

Υπεύθυνοι: Ομάδα Αντιμετώπισης Περιστατικών

Ενέργειες:

- Εάν το περιστατικό εμπεριέχει κίνδυνο για το σύνολο του Πανεπιστημίου, η Ομάδα Διαχείρισης Κρίσεων έχει την εξουσιοδότηση να **απομονώσει άμεσα το επηρεαζόμενο σύστημα, ενημερώνοντας τη Διοίκηση του ΠΚ**.
- Κλιμάκωση στην Ομάδα Διαχείρισης Κρίσεων ή/και στη Διοίκηση.
- Συνεχής ενημέρωση εμπλεκομένων μερών.

5. Αποκατάσταση & Κλείσιμο

Υπεύθυνοι: Λειτουργοί Συστημάτων/Δικτύων ΥΠΥ, Διαχειριστές Εξυπηρετητών, Ομάδες Υποστήριξης (Τοπικές/Helpdesk)

Ενέργειες:

- Επαναφορά από backup, εάν απαιτείτε.
- Έλεγχος λειτουργικότητας συστήματος/υπολογιστή/εξυπηρετητή.

- Επιβεβαίωση ότι η απειλή έχει εξαλειφθεί.
- Καταγραφή πλήρους χρονολογίου, ενεργειών και τελικής ταξινόμησης (True/False Positive).
- Αποστολή επιβεβαίωσης κλεισίματος στην Ομάδα Αντιμετώπισης Περιστατικών.
- Κλείσιμο ticket στο Service Desk (OTRS) και στο SOC.

Έγκριση πολιτικής

Η πολιτική αυτή έχει εγκριθεί από το πιο κάτω αρμόδιο όργανο, και θα αναθεωρείται όταν κρίνεται αναγκαίο.

Αρμόδιο Όργανο:

Ημερομηνία Έγκρισης: