ΠΑΝΟΠΤΗΣ 2014
CYBER EUROPE 2014

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

Τχης (ΜΧ) Μονογιούδης Ισίδωρος

Αντικειμενικοί Σκοποί

1. *Η δοκιμασία των διαδικασιών έγκαιρης προειδοποίησης, συνεργασίας και ανταλλαγής πληροφοριών μεταξύ των υπεύθυνων εθνικών αρχών για περιστατικά κυβερνοάμυνας.*
2. *Η δυνατότητα δοκιμής των εθνικών σχεδίων και των τεχνικών δυνατοτήτων σε εθνικό επίπεδο*
3. *Η διερεύνηση της αποτελεσματικότητας της ανταλλαγής πληροφοριών μεταξύ δημόσιου και ιδιωτικού τομέα.*
4. *Η διερεύνηση των διαδικασιών αντιμετώπισης περιστατικών καθώς και η κλιμάκωση ή αποκλιμάκωσή τους σε τεχνικό, επιχειρησιακό και στρατηγικό επίπεδο.*
5. *Η διερεύνηση του χειρισμού των δημοσίων σχέσεων σε μεγάλης κλίμακας περιστατικά κυνερνοάμυνας.*

Διεξαγωγή

- Οργάνωση σε επίπεδο ΕΕ: **ENISA**
- Οργάνωση σε εθνικό επίπεδο: **ΓΕΕΘΑ/ΔΙΚΥΒ**
- ΠΑΝΟΠΤΗΣ 2014
  - 28 -30 Απρ 2-14

- CE2014-TLEx: Technical-level Exercise
  - 28 – 29 Απρ 2014
  - Collaboration with GR National Cyber Defence Exercise “Panoptis 2014”
- CE2014-OLEx: Operational-level Exercise
  - Oct 2014 – TBC
- CE2014-SLE/PLEx: Strategic/Political-level Exercise
  - Nov-Dec 2014 – TBC
  - Workshop/table-top: walk through ‘what-if’ scenarios

CE 2014 - Εκτέλεση

- 1η φάση: Ασκηση σε τακτικό επίπεδο (τεχνικά επεισόδια)
- Εθνικός φορέας εκπροσώπησης: Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων
- Καθορισμός ομάδων αντιμετώπισης από κάθε ασκούμενο.
- Επιλογή επεισοδίων
- Εγγραφή στον ιστότοπο του ENISA (Cyber Exercises Platform)
- Συμμετοχή από τις έδρες τους:
  - Cyber Security Agencies, CERTs, IT Sec teams from ministries and public Institutions, Academia
  - Private sector
- Setup:
  - Πλήρως κατανεμημένο στους ασκούμενους -
  - ENISA συντονισμός – έλεγχος ασκήσεως
- Σενάριο:
  - Τεχνικά επεισόδια βασισμένα σε προκαθορισμένο σενάριο που θα προσομοιάζει την δημιουργία μεγάλης κλίμακος κρίσης σε επίπεδο ΕΕ

ΠΑΝΟΠΤΗΣ 2014 - Εκτέλεση

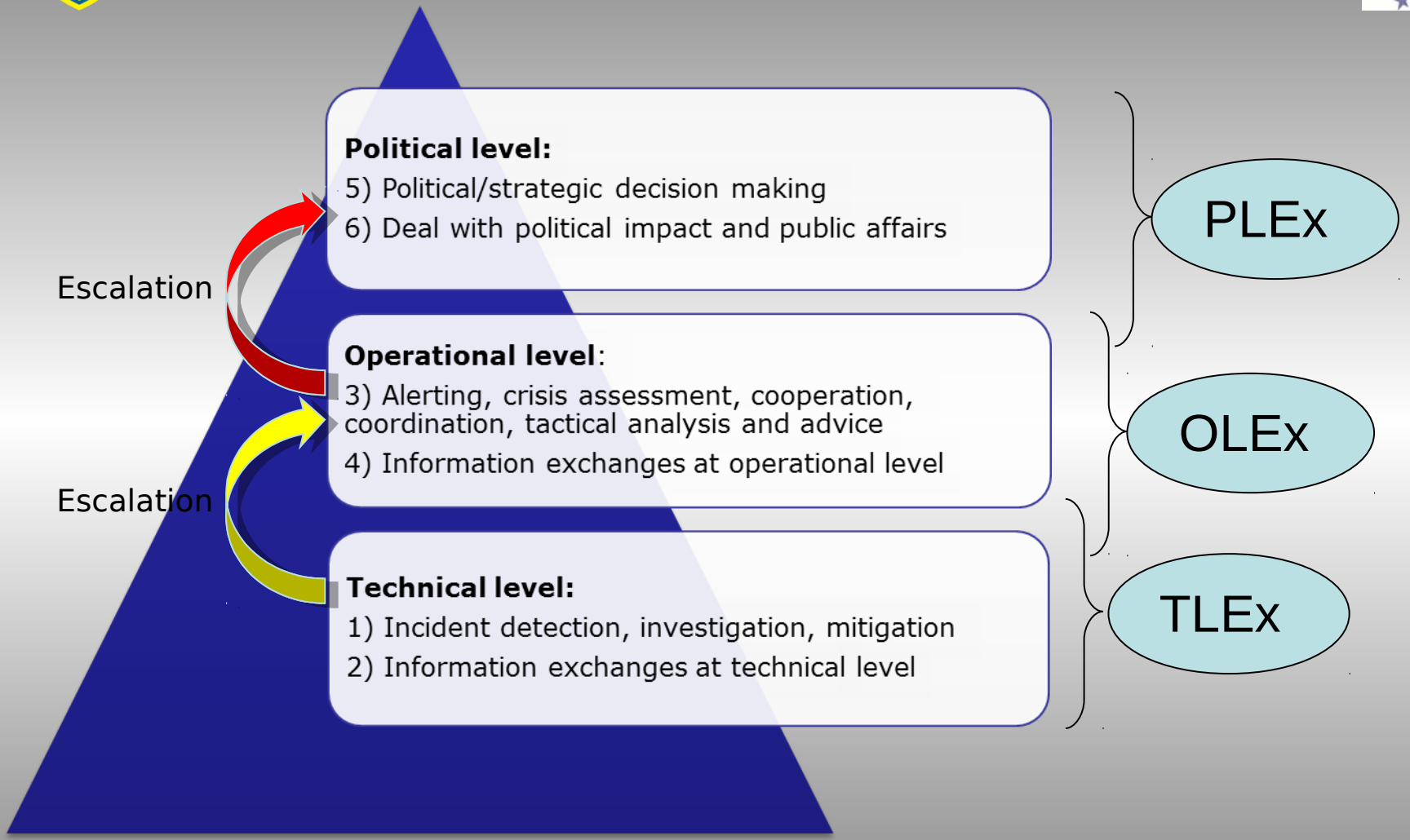
- Ασκηση σε τακτικό και επιχειρησιακό επίπεδο (τεχνικά επεισόδια και διαδικασίες)
- Εθνικός φορέας συντονισμού: ΓΕΕΘΑ/Διεύθυνση Κυβερνοάμυνας
- Καθορισμός ομάδων αντιμετώπισης(κοινή με CE) και εκπροσώπησης σε διαδικαστικά θέματα από κάθε ασκούμενο.
- Επιλογή τεχνικών επεισοδίων
- Επεισόδια σε επιχειρησιακό επίπεδο (διαδικασίες) σε μορφή συμβάντων.
- Εγγραφή στην ΔΙΚΥΒ (ηλεκτρονικό μήνυμα).
- Συμμετοχή από τις έδρες τους
  - Εκπρόσωπος Φορέα/Σημείο Επαφής (Επιχειρησιακό επίπεδο)
  - Ομάδα Αντιμετώπισης/Σημείο Επαφής (Τακτικό επίπεδο)
- Setup:
  - Πλήρως κατανεμημένο στους ασκούμενους
  - ΔΙΚΥΒ συντονισμός – έλεγχος ασκήσεως
- Σενάριο:
  - Υιοθέτηση σεναρίου Cyber Europe με εθνικές προεκτάσεις.
  - Τεχνικά επεισόδια της CE 2014.

Τεχνικά Επεισόδια Ασκήσεων

- Technical Challenges
  1. Log analysis of a DDOS Attack
  2. Forensics Investigation of a compromised web server
  3. Infected web site investigation and malware analysis
  4. Mobile (Android) malware analysis.
  5. Infected SCADA system analysis
  6. APT Trojan malware analysis
  7. Defaced web site analysis
  8. Insider information leakage investigation
  9. Compromised workstation network traffic analysis
  10. Cyber attack coordination via social media identification

- Ανταλλαγή πληροφοριών επί των αποτελασμάτων (attack patterns, IDS rules, Indicators of Compromise etc.)
- Συμμετοχή σε εθελοντική βάση ανά επεισόδιο και ανάλογα με τις δυνατότητες σε αριθμό και τεχνογνωσία.

CE 2014 - Overview



CYBER EUROPE 2014

- **Χρονοδιάγραμμα**
  - Διεξαγωγή: 28-30 Απρ 2014
  - Δήλωση συμμετοχής μέχρι 14 Φεβ 2014
  - Κύρια Σύσκεψη Ασκήσεως: 12 Μαρ 2014
  - Τελική Σύσκεψη Ασκήσεως: 10 Απρ 2014
  - Προάσκηση – Δοκιμή Επικοινωνιών: 25 Απρ 2014
  - Σημεία Επαφής/Δηλώσεις Συμμετοχής:
    - ΓΕΕΘΑ/ΔΙΚΥΒ: imonogioudis@mil.gr
    - NCERT: cert@nis.gr
  - Απαιτούμενα Στοιχεία:
    - Εκπρόσωπος Φορέα/ Σημείο Επαφής (Τακτικό, Επιχειρησιακό)
    - Επιλογή επεισοδίων
    - Αριθμός ατόμων

ΠΑΝΟΠΤΗΣ 2014 - CYBER EUROPE 2014

enisa

Questions?