Εθνική άσκηση Κυβερνοάμυνας “ΠΑΝΟΠΤΗΣ” 2014-Cyber Europe

Αντχος (Μ) Σ. Παπαγεωργίου Π.Ν. Δ/ΔΙΚΥΒ
spapageorgiou@mil.gr

περιεχόμενα

- Γενικά
- Άσκηση blue-red team
- ΠΑΝΟΠΤΗΣ 2014
- Cyber Europe
- Εθνική στρατηγική
- Εθνικό δίκτυο honeynet
- Μητρώο ειδικών

Δράσεις ΔΙΚΥΒ

- Στρατιωτική Στρατηγική Κυβερνοάμυνας
- Δόγμα επιχειρήσεων Κυβερνοχώρου
- Πολιτική Κυβερνοάμυνας
- Τεχνικό σχέδιο δράσεως ανάπτυξης κυβερνοάμυνας στις ΕΔ.
- Τεχνικό εγχειρίδιο ασφαλείας
- 10ημερο σχολείο κυβερνοάμυνας
- Mailing list --> **cd@lists.grnet.gr** (Ελεύθερη λίστα για όλους)

Δράσεις σε εξέλιξη

- Εφαρμογή του σχεδίου δράσης
- Διαδραστικό σχολείο ενημέρωσης σε θέματα Κυβερνοάμυνας-κυβερνοασφάλειας.
- Επικαιροποίηση τεχνικού εγχειριδίου ασφαλείας προσωπικού υπολογιστή
- Ενεργοποίηση διακλαδικού κέντρου αντιμετώπισης κυβερνοπεριστατικών
- Μετασχηματισμός της ΔΙΚΥΒ σε ΔΙΔΕΚ (Διακλαδική Διοίκηση Επιχειρήσεων Κυβερνοχώρου).
- Ευρωπαικό συνέδριο κυβερνοάμυνας 6-7 Μαρτίου
- Cyber Europe 28-29 Απρ.
- ΠΑΝΟΠΤΗΣ 2014 28-30 Απρ.

Κυβερνοάμυνα-ορισμός

Η Κυβερνοάμυνα απαιτεί μία σειρά από μηχανισμούς, διαδικασίες και συνεχώς ανεπτυγμένες και δοκιμασμένες δυνατότητες, με σκοπό την **πρόληψη**, τον **εντοπισμό**, την **αξιολόγηση**, την **αντιμετώπιση**, την **αποκατάσταση** και την **εξαγωγή συμπερασμάτων**, στην περίπτωση των κυβενροεπιθέσεων, που έχουν σαν στόχο να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριακών υποδομών.

Γιατί συμμετέχουμε στις ασκήσεις

- Συμμετέχουμε για την προσωπική μας προστασία, για την προστασία του οργανισμού μας και την προστασία της χώρας μας από κυβερνοεπιθέσεις.
- Να βοηθήσουμε να αναπτυχθεί μία πολιτική κυβερνο-ασφάλειας (πολιτική ορθής χρήσης), σε προσωπικό επίπεδο, σε επίπεδο οργανισμού και σε Εθνικό επίπεδο.
- Γιατί θέλουμε να εκπαιδευτούμε εμείς προσωπικά, αλλά και το σύνολο των χρηστών του οργανισμού μας.

Προϋποθέσεις-Δοκιμή

Τι δοκιμάζουμε (τι πρέπει να έχουμε) στην άσκηση:

- Πολιτική κυβερνοασφάλειας
- Κατάλληλη υποδομή ασφαλείας οργανισμού
- Εκπαίδευση ειδικών, ενημέρωση - επαγρύπνηση χρηστών
- Σύστημα επιτήρησης δικτύου (εντοπισμός-αξιολόγηση-αντιμετώπιση)
- Πολιτική κυβερνοάμυνας
- Διαδικασίες αναφοράς και αντιμετώπισης περιστατικών κυβερνοχώρου, τόσο σε επίπεδο οργανισμού, όσο και σε Εθνικό και διεθνές.

Ιδιαιτερότητα των ασκήσεων --> offline αντιμετώπιση, όχι real time αντιμετώπιση.

Επιπλέον οφέλη των ασκήσεων

- Να γνωριστούμε (νέα πρόσωπα κάθε φορά)
- Να συνεργαστούμε, γνωρίζοντας ο καθένας την δράση και τις ικανότητες-δυνατότητες του άλλου.
- Να έχουμε συνεχή επικοινωνία μέσα απο την mailing list.
- Να προσφέρουμε βοήθεια όταν χρειαστεί
- Να ενημερωθούμε για τις νέες μορφές επίθεσης και τις νέες δυνατότητες του “εχθρού”.
- Να εκπαιδευτούμε, όλοι μας.
- Να έχουμε ετοιμότητα, σε περίπτωση κρίσης στον εθνικό κυβερνοχώρο

Όλα αυτά έχουν ως στόχο να πετύχουμε σε Εθνικό επίπεδο δυνατότητες διαχείρισης και αντιμετώπισης κυβερνοπεριστατικών.

Πρέπει να Να πετύχουμε την επαγρύπνηση σε Εθνικό επίπεδο.

Ιδιαιτερότητα των ασκήσεων

- Είναι υπό την μορφή των εξετάσεων.
- Για να αντιμετωπίσουμε ένα περιστατικό θα πρέπει να έχει πάρει πρόσβαση ο “κακός”.
- Θα πρέπει να είμαστε σε θέση να εντοπίζουμε τις επιθέσεις ακόμα και από το επίπεδο ανίχνευσης.
- Συγκεντρώνουμε στοιχεία που μας παρέχουν τρίτοι. να συνεργαστούμε με όλους τους φορείς να έχουμε δυνατότητα σε Εθνικό επίπεδο να αντιμετωπίζουμε botnets (sinkhole).
- Επόμενος ΠΑΝΟΠΤΗΣ να γίνει διπλής ενεργείας. Χρειαζόμαστε την υποδομή του GRNET.

Επιπλέον Στόχοι- πρόταση

Η άσκηση επαναλαμβάνεται κάθε χρόνο. Θα γίνεται κάθε Μάιο.

Πρόταση: **να θέτουμε στόχους και να τους πετυχαίνουμε**

Προτείνουμε να εστιαστούμε αυτή την φορά στην **επαγρύπνηση των χρηστών**

Να ετοιμάσουμε λύσεις και προγράμματα για αυτό το σκοπό.

Με λίγα λόγια προτείνουμε:

Να ετοιμάσουμε ένα διαδραστικό σχολείο κυβερνοασφάλειας και κυβερνοάμυνας online. Να το φιλοξενήσουμε σε διάφορες ιστοσελίδες.

Σκοπός να ενημερώσουμε τον απλό πολίτη για τους κινδύνους και πως μπορεί να προστατευτεί. Να προβάλουμε μια εθνική κουλτούρα κυβερνοασφάλειας.

Να επικαιροποιήσουμε και να βελτιώσουμε το τεχνικό εγχειρίδιο ασφαλείας προσωπικού υπολογιστή.

Να ξεκινήσουμε μία εκστρατεία ενημέρωσης, από απλά μηνύματα μέχρι ουσιαστικά τεχνικά μηνύματα.

Άσκηση διπλής ενεργείας (Red-blue team exercise)

- Πρόταση από ειδικούς συμβούλους για μία άσκηση χωρίς κόστος, τέλος Μαρτίου.
- Οκτώ ομάδες, από οκτώ ως δέκα μέλη.
- Red Team επιθετικοί, θα είναι άγνωστη σε εμάς ομάδα.
- Blue team, οι οκτώ αμυνόμενες ομάδες.

Συμμετοχή

Πρόταση:

- Ομάδες δημοσίου με επικεφαλής τα CERT
- Ομάδες με συνεργασίες με Πανεπιστήμια
- Στρατιωτικό CERT
- Δήλωση στο cd1@cd.mil.gr

ΠΑΝΟΠΤΗΣ-Cyber Europe

- Ταυτόχρονη διεξαγωγή “ΠΑΝΟΠΤΗ” και Cyber Europe
- Δήλωση συμμετοχής στην Cyber Europe μέσω ΕΥΠ.
- Ίδια επεισόδια και στις δύο ασκήσεις
- Επιπλέον επεισόδια αν θέλει κάποιος να προτείνει
- Δήλωση συμμετοχής για όσους θέλουν να εκπονήσουν νέα επεισόδια.

Επικοινωνία-εκτέλεση άσκησης

- Επικοινωνία κυρίως με υπηρεσιακά email (και προσωπικά)
  - Ανταλλαγή κλειδιών
- Τηλέφωνο
- Χρήση web server για “κατέβασμα” των επεισοδίων (τουλάχιστον μία εβδομάδα νωρίτερα).
- Mailing list

Εθνική στρατηγική

- Δημιουργία ομάδας εργασίας
- Συμμετοχή όλων
- Εκπόνηση ενός “ζωντανού” κειμένου
- Στόχος ένα προσχέδιο αρχές Μαρτίου

Εθνική Αρχή κυβερνοάμυνας

- Πρόταση για Εθνική Αρχή κυβερνοάμυνας.
- Όλα να γίνονται οργανωμένα από την αρχή και όχι απλά με πρωτοβουλίες
- Το ΓΕΕΘΑ λαμβάνει πρωτοβουλίες, δεν είμαστε Εθνική Αρχή.

Εθνικό δίκτυο έγκαιρης προειδοποίησης (Honeynet)

- Ποιο λογισμικό θα χρησιμοποιήσουμε?
  - Πρόταση για αυτό του **FORTH-CERT**.
- Εθελοντική φιλοξενία
- Τα δεδομένα σε όλους
- Να ετοιμάσουμε και εδώ ομάδα εργασίας

Μητρώο Ειδικών Επιστημόνων Ασφάλειας Κυβερνοχώρου.

- Βρίσκεται στην διαδικασία ανάπτυξης της βάσης.

Άλλες προτάσεις

- Μνημόνια συνεργασίας με όλους τους φορείς
- Να μελετήσουμε τον τρόπο παρακολούθησης από τις μυστικές υπηρεσίες και να βγάλουμε οδηγούς προστασίας.
- Να μελετήσουμε τις νέες μορφές επιθέσεων και να ετοιμάσουμε τον δικό μας τρόπο αντίδρασης.
- Να συνεργαζόμαστε με Πανεπιστήμια, να δίνουμε διπλωματικές που να είναι στην διάθεση όλων (πρακτικές-τεχνικές διπλωματικές-εργασίες)
- Προτάσεις να προστατέψουμε τα email μας
- Εθνικό λειτουργικό σύστημα (Linux)
- Να αναλύσουμε το τεχνικό σχέδιο δράσης ανάπτυξης κυβερνοασφάλειας-κυβερνοάμυνας και να αναπτύξουμε δικά μας εργαλεία

Στοιχεία επικοινωνίας

Στρατιωτικό CERT mcirc@cd.mil.gr 210-6574242

(Ασχος (Ι) Ν. Σταματελάτος)

Αντχος (Μ) Σ. Παπαγεωργίου Π.Ν. spapageorgiou@mil.gr 210-6576220

Τχης (ΜΗΧ) Ι. Μονογιούδης imonogioudis@mil.gr 210-6576273

Ερωτήσεις;

Εθνική άσκηση Κυβερνοάμυνας “ΠΑΝΟΠΤΗΣ” 2014-
Cyber Europe

Αντχος (Μ) Σ. Παπαγεωργίου Π.Ν. Δ/ΔΙΚΥΒ
spapageorgiou@mil.gr

περιεχόμενα

- Γενικά
- Άσκηση blue-red team
- ΠΑΝΟΠΤΗΣ 2014
- Cyber Europe
- Εθνική στρατηγική
- Εθνικό δίκτυο honeynet
- Μητρώο ειδικών

Δράσεις ΔΙΚΥΒ

- Στρατιωτική Στρατηγική Κυβερνοάμυνας
- Δόγμα επιχειρήσεων Κυβερνοχώρου
- Πολιτική Κυβερνοάμυνας
- Τεχνικό σχέδιο δράσεως ανάπτυξης κυβερνοάμυνας στις ΕΔ.
- Τεχνικό εγχειρίδιο ασφαλείας
- 10ημερο σχολείο κυβερνοάμυνας
- Mailing list --> **cd@lists.grnet.gr** (Ελεύθερη λίστα για όλους)

Δράσεις σε εξέλιξη

- Εφαρμογή του σχεδίου δράσης
- Διαδραστικό σχολείο ενημέρωσης σε θέματα Κυβερνοάμυνας-κυβερνοασφάλειας.
- Επικαιροποίηση τεχνικού εγχειριδίου ασφαλείας προσωπικού υπολογιστή
- Ενεργοποίηση διακλαδικού κέντρου αντιμετώπισης κυβερνοπεριστατικών
- Μετασχηματισμός της ΔΙΚΥΒ σε ΔΙΔΕΚ (Διακλαδική Διοίκηση Επιχειρήσεων Κυβερνοχώρου).
- Ευρωπαικό συνέδριο κυβερνοάμυνας 6-7 Μαρτίου
- Cyber Europe 28-29 Απρ.
- ΠΑΝΟΠΤΗΣ 2014 28-30 Απρ.

Κυβερνοάμυνα-ορισμός

Η Κυβερνοάμυνα απαιτεί μία σειρά από μηχανισμούς, διαδικασίες και συνεχώς ανεπτυγμένες και δοκιμασμένες δυνατότητες, με σκοπό την **πρόληψη**, τον **εντοπισμό**, την **αξιολόγηση**, την **αντιμετώπιση**, την **αποκατάσταση** και την **εξαγωγή συμπερασμάτων**, στην περίπτωση των κυβενροεπιθέσεων, που έχουν σαν στόχο να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριακών υποδομών.

Γιατί συμμετέχουμε στις ασκήσεις

- Συμμετέχουμε για την προσωπική μας προστασία, για την προστασία του οργανισμού μας και την προστασία της χώρας μας από κυβερνοεπιθέσεις.
- Να βοηθήσουμε να αναπτυχθεί μία πολιτική κυβερνο-ασφάλειας (πολιτική ορθής χρήσης), σε προσωπικό επίπεδο, σε επίπεδο οργανισμού και σε Εθνικό επίπεδο.
- Γιατί θέλουμε να εκπαιδευτούμε εμείς προσωπικά, αλλά και το σύνολο των χρηστών του οργανισμού μας.

Προϋποθέσεις-Δοκιμή

Τι δοκιμάζουμε (τι πρέπει να έχουμε) στην άσκηση:

- Πολιτική κυβερνοασφάλειας
- Κατάλληλη υποδομή ασφαλείας οργανισμού
- Εκπαίδευση ειδικών, ενημέρωση - επαγρύπνηση χρηστών
- Σύστημα επιτήρησης δικτύου (εντοπισμός-αξιολόγηση-αντιμετώπιση)
- Πολιτική κυβερνοάμυνας
- Διαδικασίες αναφοράς και αντιμετώπισης περιστατικών κυβερνοχώρου, τόσο σε επίπεδο οργανισμού, όσο και σε Εθνικό και διεθνές.

Ιδιαιτερότητα των ασκήσεων --> offline αντιμετώπιση, όχι real time αντιμετώπιση.

Επιπλέον οφέλη των ασκήσεων

- Να γνωριστούμε (νέα πρόσωπα κάθε φορά)
- Να συνεργαστούμε, γνωρίζοντας ο καθένας την δράση και τις ικανότητες-δυνατότητες του άλλου.
- Να έχουμε συνεχή επικοινωνία μέσα απο την mailing list.
- Να προσφέρουμε βοήθεια όταν χρειαστεί
- Να ενημερωθούμε για τις νέες μορφές επίθεσης και τις νέες δυνατότητες του “εχθρού”.
- Να εκπαιδευτούμε, όλοι μας.
- Να έχουμε ετοιμότητα, σε περίπτωση κρίσης στον εθνικό κυβερνοχώρο

Όλα αυτά έχουν ως στόχο να πετύχουμε σε Εθνικό επίπεδο δυνατότητες διαχείρισης και αντιμετώπισης κυβερνοπεριστατικών.

Πρέπει να Να πετύχουμε την επαγρύπνηση σε Εθνικό επίπεδο.

Ιδιαιτερότητα των ασκήσεων

- Είναι υπό την μορφή των εξετάσεων.
- Για να αντιμετωπίσουμε ένα περιστατικό θα πρέπει να έχει πάρει πρόσβαση ο “κακός”.
- Θα πρέπει να είμαστε σε θέση να εντοπίζουμε τις επιθέσεις ακόμα και από το επίπεδο ανίχνευσης.
- Συγκεντρώνουμε στοιχεία που μας παρέχουν τρίτοι. να συνεργαστούμε με όλους τους φορείς να έχουμε δυνατότητα σε Εθνικό επίπεδο να αντιμετωπίζουμε botnets (sinkhole).
- Επόμενος ΠΑΝΟΠΤΗΣ να γίνει διπλής ενεργείας. Χρειαζόμαστε την υποδομή του GRNET.

Επιπλέον Στόχοι- πρόταση

Η άσκηση επαναλαμβάνεται κάθε χρόνο. Θα γίνεται κάθε Μάιο.

Πρόταση: **να θέτουμε στόχους και να τους πετυχαίνουμε**

Προτείνουμε να εστιαστούμε αυτή την φορά στην **επαγρύπνηση των χρηστών**

Να ετοιμάσουμε λύσεις και προγράμματα για αυτό το σκοπό.

Με λίγα λόγια προτείνουμε:

Να ετοιμάσουμε ένα διαδραστικό σχολείο κυβερνοασφάλειας και κυβερνοάμυνας online. Να το φιλοξενήσουμε σε διάφορες ιστοσελίδες.

Σκοπός να ενημερώσουμε τον απλό πολίτη για τους κινδύνους και πως μπορεί να προστατευτεί. Να προβάλουμε μια εθνική κουλτούρα κυβερνοασφάλειας.

Να επικαιροποιήσουμε και να βελτιώσουμε το τεχνικό εγχειρίδιο ασφαλείας προσωπικού υπολογιστή.

Να ξεκινήσουμε μία εκστρατεία ενημέρωσης, από απλά μηνύματα μέχρι ουσιαστικά τεχνικά μηνύματα.

Άσκηση διπλής ενεργείας (Red-blue team exercise)

- Πρόταση από ειδικούς συμβούλους για μία άσκηση χωρίς κόστος, τέλος Μαρτίου.
- Οκτώ ομάδες, από οκτώ ως δέκα μέλη.
- Red Team επιθετικοί, θα είναι άγνωστη σε εμάς ομάδα.
- Blue team, οι οκτώ αμυνόμενες ομάδες.

Συμμετοχή

Πρόταση:

- Ομάδες δημοσίου με επικεφαλής τα CERT
- Ομάδες με συνεργασίες με Πανεπιστήμια
- Στρατιωτικό CERT
- Δήλωση στο cd1@cd.mil.gr

ΠΑΝΟΠΤΗΣ-Cyber Europe

- Ταυτόχρονη διεξαγωγή “ΠΑΝΟΠΤΗ” και Cyber Europe
- Δήλωση συμμετοχής στην Cyber Europe μέσω ΕΥΠ.
- Ίδια επεισόδια και στις δύο ασκήσεις
- Επιπλέον επεισόδια αν θέλει κάποιος να προτείνει
- Δήλωση συμμετοχής για όσους θέλουν να εκπονήσουν νέα επεισόδια.

Επικοινωνία-εκτέλεση άσκησης

- Επικοινωνία κυρίως με υπηρεσιακά email (και προσωπικά)
  - Ανταλλαγή κλειδιών
- Τηλέφωνο
- Χρήση web server για “κατέβασμα” των επεισοδίων (τουλάχιστον μία εβδομάδα νωρίτερα).
- Mailing list

Εθνική στρατηγική

- Δημιουργία ομάδας εργασίας
- Συμμετοχή όλων
- Εκπόνηση ενός “ζωντανού” κειμένου
- Στόχος ένα προσχέδιο αρχές Μαρτίου

Εθνική Αρχή κυβερνοάμυνας

- Πρόταση για Εθνική Αρχή κυβερνοάμυνας.
- Όλα να γίνονται οργανωμένα από την αρχή και όχι απλά με πρωτοβουλίες
- Το ΓΕΕΘΑ λαμβάνει πρωτοβουλίες, δεν είμαστε Εθνική Αρχή.

Εθνικό δίκτυο έγκαιρης προειδοποίησης (Honeynet)

- Ποιο λογισμικό θα χρησιμοποιήσουμε?
  - Πρόταση για αυτό του **FORTH-CERT**.
- Εθελοντική φιλοξενία
- Τα δεδομένα σε όλους
- Να ετοιμάσουμε και εδώ ομάδα εργασίας

Μητρώο Ειδικών Επιστημόνων Ασφάλειας Κυβερνοχώρου.

- Βρίσκεται στην διαδικασία ανάπτυξης της βάσης.

Άλλες προτάσεις

- Μνημόνια συνεργασίας με όλους τους φορείς
- Να μελετήσουμε τον τρόπο παρακολούθησης από τις μυστικές υπηρεσίες και να βγάλουμε οδηγούς προστασίας.
- Να μελετήσουμε τις νέες μορφές επιθέσεων και να ετοιμάσουμε τον δικό μας τρόπο αντίδρασης.
- Να συνεργαζόμαστε με Πανεπιστήμια, να δίνουμε διπλωματικές που να είναι στην διάθεση όλων (πρακτικές-τεχνικές διπλωματικές-εργασίες)
- Προτάσεις να προστατέψουμε τα email μας
- Εθνικό λειτουργικό σύστημα (Linux)
- Να αναλύσουμε το τεχνικό σχέδιο δράσης ανάπτυξης κυβερνοασφάλειας-κυβερνοάμυνας και να αναπτύξουμε δικά μας εργαλεία

Στοιχεία επικοινωνίας

Στρατιωτικό CERT mcirc@cd.mil.gr 210-6574242

(Ασχος (Ι) Ν. Σταματελάτος)

Αντχος (Μ) Σ. Παπαγεωργίου Π.Ν. spapageorgiou@mil.gr 210-6576220

Τχης (ΜΗΧ) Ι. Μονογιούδης imonogioudis@mil.gr 210-6576273

Ερωτήσεις;