ΟΜΙΛΙΑ ΔΝΤΗ ΚΕΜΕΑ «GCC: Ελληνικό Κέντρο Αριστείας για την Εκπαίδευση και την Έρευνα του Κυβερνοεγκλήματος»

14 Οκτωβρίου 2015

Αξιότιμε κύριε Υπουργέ,

Αξιότιμοι ομιλητές και συμμετέχοντες,

Καλησπέρα σας,

Σας καλωσορίζω στο τρίτο διήμερο σεμινάριο στο πλαίσιο του ευρωπαϊκού ερευνητικού έργου «GCC: Ελληνικό Κέντρο Αριστείας για την Εκπαίδευση και την Έρευνα του Κυβερνοεγκλήματος» που διοργανώνει το Κέντρο Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α.) σε συνεργασία με το Ίδρυμα Τεχνολογίας και Έρευνας (Ι.Τ.Ε.), το Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Internet (Safenet) και το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (Α.Π.Θ.). Το έργο εντάσσεται στο Ευρωπαϊκό Πρόγραμμα «Πρόληψη και Αντιμετώπιση του Εγκλήματος» (ISEC 2011), χρηματοδοτείται από τη Διεύθυνση Εσωτερικών Υποθέσεων της Ευρωπαϊκής Επιτροπής, και αφορά το κρίσιμο ζήτημα της πρόληψης και της καταπολέμησης του Ηλεκτρονικού Εγκλήματος.

Η πρωτοβουλία είναι εναρμονισμένη τόσο με το Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα της Europol, το οποίο αποτελεί κομβικό εργαλείο της Ευρωπαϊκής Ένωσης στην προσπάθεια της για την άμεση και συντονισμένη πρόληψη και αντιμετώπιση μίας από τις σημαντικότερες απειλές για την ασφάλεια σήμερα, του κυβερνοεγκλήματος, όσο και με τα εννέα αντίστοιχα εθνικά κέντρα που λειτουργούν στο Βέλγιο, στη Μεγάλη Βρετανία, στην Ιρλανδία, στην Κύπρο, στη Γαλλία, στη Βουλγαρία, στην Εσθονία, στη Ρουμανία και στην Ισπανία.

Το σημερινό σεμινάριο υλοποιείται σε συνεχεία των δύο ιδιαιτέρως επιτυχημένων διημέρων που πραγματοποιήθηκε τον Ιανουάριο του 2013 και το Νοέμβριο του 2014 με τη συμμετοχή εκπροσώπων του Ευρωπαϊκού Κέντρου για το Κυβερνοέγκλημα, του Ευρωπαϊκού Οργανισμού για την Ασφάλεια των Δικτύων και Πληροφοριών, εισαγγελικών και δικαστικών λειτουργών, στελεχών των Διευθύνσεων Δίωξης Ηλεκτρονικού Εγκλήματος, Εγκληματολογικών Ερευνών και Πληροφορικής της Ελληνικής Αστυνομίας,

καθώς και στελεχών της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και του Υπουργείου Εσωτερικών.

Το έγκλημα στον κυβερνοχώρο αποτελεί παγκόσμια, τεχνική, διασυνοριακή και ανώνυμη απειλή των συστημάτων πληροφοριών και ως εκ τούτου, δημιουργεί πολλές επιπρόσθετες προκλήσεις για τις υπηρεσίες επιβολής του νόμου-

Είναι ένας από τους ταχύτερα αναπτυσσόμενους τομείς της οργανωμένης και διασυνοριακής εγκληματικότητας. Η καθημερινή μας ζωή, η ασφάλεια μας και η οικονομική ανάπτυξη εξαρτώνται από ένα σταθερό, ασφαλές και ανθεκτικό διαδίκτυο, καθώς στηριζόμαστε σε αυτό για να επικοινωνούμε και να διαχειριζόμαστε την ζωή μας. Έχει παρατηρηθεί ότι τα εγκλήματα στον κυβερνοχώρο έχουν αυξηθεί την τελευταία δεκαετία, εκθέτοντας προσωπικές ευαίσθητες, εμπορικές και εθνικές πληροφορίες. Βάσει ερευνών που πραγματοποιήθηκαν την τελευταία διετία, το κυβερνοέγκλημα είναι υπεύθυνο για την απώλεια 300 δισεκατομμυρίων έως και 1 τρισεκατομμυρίου δολαρίων κάθε χρόνο, το οποίο αντιστοιχεί στο 0.4 έως 1.4% του παγκοσμίου ΑΕΠ. Πέρα από το οικονομικό αντίκτυπο, οι κυβερνοεπιθέσεις μπορούν να θέσουν σε κίνδυνο ανθρώπινες ζωές μέσω επιθέσεων σε κρίσιμες υποδομές όπως Δίκτυα Μεταφοράς Ηλεκτρικής Ενέργειες και Υδροδότησης, Εργοστάσια Πυρηνικής Ενέργειας, Δίκτυα Συντονισμού Φωτεινών Σηματοδοτών κ.α.

Χαρακτηριστικό παράδειγμα του μεγέθους και της δριμύτητας της απειλής είναι οι κυβερνοεπιθέσεις του 2007 στην Εσθονία που είχαν ως στόχο το κοινοβούλιο, τις τράπεζες, τα υπουργεία, τις εφημερίδες και τα μέσα μαζικής ενημέρωσης και είχαν σοβαρές επιπτώσεις και σε διεθνές επίπεδο. Κατά τη διάρκεια των δύο εβδομάδων που διήρκησαν οι επιθέσεις:

α) δεν λειτουργούσαν τα μηχανήματα αυτόματης ανάληψης,

β) τα ξενοδοχεία και οι επιχειρήσεις δεν μπορούσαν να δεχτούν πληρωμές μέσω πιστωτικών/χρεωστικών καρτών,

γ) οι διακομιστές αλληλογραφίας, τραπεζών, εταιριών, εθνικών αρχών και ΜΜΕ ήταν εκτός λειτουργίας.

Η καταπολέμηση του εγκλήματος στον κυβερνοχώρο απαιτεί μια διαφορετική προσέγγιση, από ότι έχει παραδοσιακά υιοθετηθεί έως τώρα, για τις περισσότερες εγκληματικές ενέργειες. Σε αντίθεση με τον κόσμο εκτός διαδικτύου όπου οι εγκληματίες κανονικά πρέπει να είναι σωματικά παρόντες στη σκηνή του εγκλήματος και τυπικά δύνανται να πραγματοποιήσουν μόνο ένα αδίκημα σε μία δεδομένη χρονική στιγμή (δηλαδή ληστεία μια τράπεζας ή διάρρηξη σε ένα σπίτι σε μία δεδομένη χρονική στιγμή), οι εγκληματίες του κυβερνοχώρου δεν χρειάζεται να βρίσκονται κοντά στον τόπο του εγκλήματος, ενδεχομένως δεν χρειάζεται καν να ταξιδέψουν στη χώρα-στόχο, ενώ παράλληλα είναι σε θέση να προκαλέσουν μεγάλο αριθμό θυμάτων σε παγκόσμιο επίπεδο, με ελάχιστη προσπάθεια και κίνδυνο, αποκρύπτοντας την ταυτότητά τους.

Στην πράξη, η ανάγκη για μια διαφορετική προσέγγιση για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο, φέρει αντιμέτωπες τις αστυνομικές δυνάμεις με νέες προκλήσεις. Αυτό απαιτεί πολύ ισχυρότερη διασυνοριακή συνεργασία και καθοδήγηση. Πρέπει να βρεθούν νέοι συνεργάτες και να ενσωματωθούν στα υφιστάμενα πλαίσια συνεργασίας, όπως έχουμε δει να γίνεται με το Ευρωπαϊκό Κέντρο για την Αντιμετώπιση του Εγκλήματος στον Κυβερνοχώρο (EC3) της Europol. Σε πολλές χώρες εκτός της ΕΕ, δεν υπάρχουν, ωστόσο, επαρκή νομικά πλαίσια που θα προσφέρουν το έδαφος για δικαστική συνεργασία. Ουσιαστικά, το σχέδιο δράσης για διακρατικές ερευνητικές προσεγγίσεις, έρχεται σε σύγκρουση με τη φύση του διαδικτυακού εγκλήματος που δεν έχει σύνορα.

Ακόμη και στο εσωτερικό της ΕΕ, οι διαφορές στη νομοθεσία και στα νομικά όργανα για τον εντοπισμό, τη διάδοση και την ανταλλαγή πληροφοριών για τα εγκλήματα στον κυβερνοχώρο προκαλούν σοβαρά εμπόδια. Το τελευταίο δεν ισχύει μόνο για τη διαδικασία επιβολής του νόμου, αλλά και στο πεδίο συνεργασίας με τον ιδιωτικό τομέα.

Το ίδιο το έγκλημα στον κυβερνοχώρο αποτελεί πρόβλημα το οποίο λαμβάνει διαρκώς μεγαλύτερες διαστάσεις. Οι τάσεις δείχνουν σημαντική αύξηση στο πεδίο εφαρμογής, στην καινοτομία, στον αριθμό και το είδος των επιθέσεων, καθώς επίσης και στον αριθμό των θυμάτων και τις οικονομικές επιπτώσεις.

Ειδικότερα:

- Η έλευση του ¨Internet of Everything (OIE)¨ σε συνδυασμό με τον διαρκώς αυξανόμενο αριθμό των χρηστών του Διαδικτύου παγκοσμίως, δημιουργεί ένα διευρυμένο πεδίο επιθέσεων και περισσότερα σημεία εισόδου προς εκμετάλλευση από τη μεριά των εγκληματιών.

- Η ΕΕ θα εξακολουθήσει να αποτελεί βασικό στόχο για ηλεκτρονικές εγκληματικές δραστηριότητες λόγω του υψηλού βαθμού χρήσης του Διαδικτύου και των διαρκώς εξαρτώμενων από το Διαδίκτυο οικονομιών και συστημάτων πληρωμών.

- Οι επιθέσεις προέρχονται κατά κύριο λόγο από χώρες εκτός της ΕΕ, και ιδιαίτερα από χώρες όπου οι εισπράξεις από το ηλεκτρονικό έγκλημα, υπερτερούν των εσόδων που προέρχονται από νόμιμες δραστηριότητες.

- Σε γενικές γραμμές το έγκλημα στον κυβερνοχώρο αυξάνεται σε μέγεθος και αντίκτυπο· ενώ υπάρχει έλλειψη αξιόπιστων στοιχείων, παράλληλα οι τάσεις δείχνουν σημαντική αύξηση στο πεδίο εφαρμογής, μεγέθυνση του αριθμού και εξέλιξη του είδους των επιθέσεων, αύξηση του αριθμού των θυμάτων και των οικονομικών επιπτώσεων.

- Οι εγκληματίες του κυβερνοχώρου είναι σε θέση να διαπράττουν εγκλήματα εναντίον μεγάλου αριθμού θυμάτων, παράλληλα σε διάφορες χώρες με ελάχιστη προσπάθεια και κίνδυνο.

- Η διακρατική φύση του διαδικτυακού/ηλεκτρονικού εγκλήματος, δημιουργεί
  προκλήσεις για την επίτευξη της διασφάλισης και της ανάλυσης ηλεκτρονικών αποδεικτικών στοιχείων από τα αρμόδια όργανα επιβολής του νόμου.

- Οι παραδοσιακές ομάδες οργανωμένου εγκλήματος αρχίζουν να χρησιμοποιούν το ηλεκτρονικό όπλο, με σκοπό τα εγκλήματα που διαπράττουν να διαθέτουν πιο εξελιγμένη μορφή.

- Το κακόβουλο λογισμικό ¨malware¨ γίνεται ολοένα και πιο εξελιγμένο, έξυπνο, ευέλικτο, διαθέσιμο και επηρεάζει ένα ευρύτερο φάσμα στόχων και συσκευών.

- Το ηλεκτρονικό εμπόριο που σχετίζεται με απάτες, έχει αυξηθεί παράλληλα με τον αυξανόμενο αριθμό των ηλεκτρονικών πληρωμών, επηρεάζοντας μεγάλες βιομηχανικές μονάδες, όπως αεροπορικές εταιρείες και ξενοδοχεία.

- Τα ¨Σκοτεινά Δίκτυα Darknets¨και άλλα πεδία που προσφέρουν υψηλό βαθμό ανωνυμίας, ¨φιλοξενούν¨ όλο και περισσότερες αγορές ταγμένες σε παραδοσιακές μορφές εγκλήματος, όπως το εμπόριο ναρκωτικών, η πώληση κλοπιμαίων, όπλων, επικίνδυνα στοιχεία πιστωτικών καρτών, πλαστά έγγραφα, πλαστές ταυτότητες, και εμπορία ανθρώπων.

- Οι δράστες σεξουαλικής κακοποίησης παιδιών χρησιμοποιούν όλο και περισσότερο τα ¨σκοτεινά δίκτυα Darknet¨ και άλλα πεδία δράσης .
- Νέες μορφές σεξουαλικής κακοποίησης παιδιών σε απευθείας σύνδεση όπως μέσω ¨live streaming¨, αποτελούν νέες προκλήσεις για τα νομοθετικά όργανα.

- Μέσω της ευρείας χρήσης των μέσων μαζικής δικτύωσης και της διαθεσιμότητας των συσκευών που συνδέονται στο Διαδίκτυο, τα φαινόμενα της διαδικτυακής παραγωγής και διάδοσης σεξουαλικών εικόνων, οι οποίες σε ορισμένες περιπτώσεις είναι αυτοδημιούργητες, και η χρήση αυτών των εικόνων με σκοπό τον σεξουαλικό εκβιασμό, αυξάνονται όλο και περισσότερο.

Καταληκτικά, θα αναφερθώ στο ζήτημα της «κυβερνοάμυνας». Σε αυτή την περίπτωση κάνουμε λόγο για τρεις κατηγορίες απειλών:

1. Απειλές με τη μορφή ψυχολογικών επιχειρήσεων. Κρατικοί ή παρακρατικοί φορείς, μη κρατικοί δρώντες, τρομοκρατικές ομάδες κτλ. χρησιμοποιούν το διαδίκτυο και τα ηλεκτρονικά Μέσα για τη χειραγώγηση της κοινής γνώμης, τη στρατολόγηση μελών και τη διαμόρφωση συνειδήσεων.
2. Η απειλή του κυβερνοπολέμου. Η διείσδυση στα αυτοματοποιημένα συστήματα των οργανισμών κοινής ωφελείας και στα μηχανογραφικά συστήματα Υπουργείων και κυβερνητικών φορέων, με σκοπό την παραπλάνηση ή αλλοίωση στοιχείων ή ακόμη και την καταστροφή αρχείων.

3. Απειλές με τη μορφή επιχειρήσεων Ηλεκτρονικού Πολέμου. Η απειλή αφορά κυρίως της Ένοπλες Δυνάμεις και τα Σώματα Ασφάλεια με τη μορφή της υποκλοπής και των παρεμβολών.

Στις εργασίες του 3ου Σεμιναρίου έχουμε την τιμή και χαρά να φιλοξενούμε διακεκριμένους και καταξιωμένους επιστήμονες, τόσο από τον Ελληνικό όσο και από τον Ευρωπαϊκό χώρο, που αποδέχτηκαν με χαρά την πρόσκλησή μας να συμμετάσχουν σε αυτή την προσπάθεια. Ευελπιστώ ότι το συγκεκριμένο σεμινάριο θα αποτελέσει για μία ακόμα φορά αρωγό σε θέματα πρόληψης και αντιμετώπισης του Κυβερνοεγκλήματος.

Σας ευχαριστώ πολύ όλους για την παρουσία σας και τη συμμετοχή σας και εύχομαι καλή επιτυχία στις εργασίες σας.