ΗΛΕΚΤΡΟΝΙΚΟ ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ

Ένας «άϋλος» υπόκοσμος

Τάσσος Συμεωνίδης
(RIEAS Academic Advisor)

Publication date: 29 November 2018

Έστιν ο πόλεμος ουχ όπλων το πλέον, αλλά δαπάνης

Θουκυδίδης

Το ηλεκτρονικό έγκλημα (cyber crime) έχει πάρει διαστάσεις χιονοστιβάδας παγκοσμίως με ιδιαίτερους στόχους τις ανεπτυγμένες χώρες. Μια απ' τις μορφές του που αναπτύσσεται με γεωμετρική πρόοδο είναι η εκμετάλλευση του διαδικτύου για κάθε είδους εγκληματική παράβαση με *οικονομικό στόχο*.

Μια απλή περιήγηση σε ιστοχώρους της Ευρώπης και των ΗΠΑ μας δίνει άφθονα παραδείγματα: από απλές απάτες μέσω ηλεκτρονικού ταχυδρομείου (email scam) και υποκλοπή προσωπικών δεδομένων για πρόσβαση σε τραπεζικούς λογαριασμούς μέχρι καταχρήσεις, ξέπλυμα εκατομμυρίων και παράνομη διείσδυση (hacking) σε βάσεις δεδομένων υψηλής ασφάλειας με σκοπό την κλοπή εκατομμυρίων δεδομένων πιστωτικών καρτών και άλλων ευαίσθητων πληροφοριών.

Δυστυχώς η Ελλάδα δεν αποτελεί εξαίρεση στον ανωτέρω κανόνα. Αν και η κλίμακα του φαινομένου είναι μικρότερη απ' ότι σε άλλες μεγαλύτερες χώρες, τα τελευταία χρόνια έχουν γίνει μάρτυρες της ταχύτατα αυξανόμενης γενικότερης εγκληματικής χρήσης του Διαδικτύου όπως αποδεικνύουν και πρόσφατα στοιχεία της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος.

Ένας μάλιστα ιδιαίτερος χώρος που απασχολεί πιεστικά τις διωκτικές αρχές είναι αυτός της ηλεκτρονικής απάτης με στόχο το Δημόσιο που μπορεί να πάρει πολλές μορφές όπως φοροδιαφυγή, «ηλεκτρονική» πλαστογράφηση στοιχείων με σκοπό την απόκρυψη κερδών, «διευκολύνσεις» πολλαπλών μεταβιβάσεων χρήματος με κατεύθυνση φορολογικούς παραδείσους και στόχο την εξαφάνιση των ιχνών των ροών αυτών, δημιουργία πλασματικών

εταιρικών σχημάτων online με σκοπό την εξαπάτηση του Δημοσίου ή και διευκόλυνση δωροδοκίας κ.ο.κ.

Είναι πλέον κοινή διαπίστωση ότι το αιώνιο ελληνικό πρόβλημα της φοροδιαφυγής / φοραποφυγής, αλλά και η εφευρετικότητα των παρανόμων κυκλωμάτων που εκμεταλλεύονται τις online υπηρεσίες, θα συνεχίσουν να αναπτύσσονται και να μεταλλάσσονται ταχύτατα. Η διεθνής πείρα μάλιστα αποδεικνύει ότι οι υπηρεσίες για την πάταξη του ηλεκτρονικού εγκλήματος βρίσκονται συνεχώς ένα τουλάχιστον βήμα πίσω από την εφευρετικότητα των «ηλεκτρονικών» εγκληματιών. Οι υφιστάμενες ειδικές ελληνικές υπηρεσίες δεν αποτελούν εξαίρεση σ' αυτόν τον κανόνα σε εποχή μάλιστα που η βελτίωση των υποδομών και η απόκτηση τεχνικών μέσων τελευταίας τεχνολογίας συχνά προσκρούει στην οικονομική στενότητα και στις αιώνιες γραφειοκρατικές αγκυλώσεις.

Είναι λοιπόν αναγκαίο να υπάρξουν πρωτοβουλίες οι οποίες (α) θα επικεντρωθούν αποκλειστικά στο ηλεκτρονικό οικονομικό έγκλημα και (β) να αναπτύξουν ερευνητικές μεθόδους οι οποίες θα συμβαδίζουν με τις εξελίξεις στην τεχνολογία και την τελευταία λέξη των διεθνών ανακριτικών και καταδιωκτικών μεθόδων (leading edge adjustment).

Η δημιουργία ενός *οργανισμού αποκλειστικής σκόπευσης* (dedicated targeted agency) αποτελεί μια επιλογή που θα πρέπει να αντιμετωπισθεί επειγόντως. Ένα cyber «ΣΔΟΕ» θα πρέπει στηριχθεί σε νομοθετικές ρυθμίσεις με έμφαση στην ανεξαρτησία ενεργειών και στην διασυνδεσιμότητα (interconnectivity) με άλλες συγγενείς υπηρεσίες υπουργείων, ανεξαρτήτων αρχών κλπ.

Η επάνδρωση του οργανισμού με εξιδεικευμένο προσωπικό θα πρέπει να προσεγγισθεί με αυστηρά επιστημονικά κριτήρια καθ' όσον, όπως έχει ήδη αναγνωρισθεί στο εξωτερικό, το cyber έγκλημα οιασδήποτε μορφής απαιτεί προωθημένες μεθόδους που ξεφεύγουν από τις κλασικές «αστυνομικές» τακτικές.

Το cyber ΣΔΟΕ θα αντιμετωπίσει έναν χώρο που έχει περιορισμένη (ή και καμιά) σχέση με το λεγόμενο «κοινό» έγκλημα. Οι σημερινές διαδικτυωμένες οικονομικές και τραπεζικές υπηρεσίες π.χ. προσφέρουν αναρίθμητες επιλογές *νομιμοποίησης* εγκληματικών ενεργειών. Σε συνδυασμό με την στιγμιαία άϋλη κίνηση κεφαλαίων διεθνώς (push-button transfer) ο οικονομικός παραβάτης διαθέτει σχεδόν πάντοτε την πρωτοβουλία της άνετης διεξαγωγής μπαράζ κινήσεων και μεταβιβάσεων που είναι σχεδόν αδύνατο να ελεγχθούν για την νομιμότητα τους.

Ένα πρόσθετο σημαντικό εμπόδιο είναι επίσης το ό,τι σε πληθώρα περιπτώσεων η παράνομη ενέργεια καλύπτεται από το πέπλο κατά τ'άλλα νόμιμων επιχειρηματικών δραστηριοτήτων που σπανίως προκαλούν υποψίες, ιδιαιτέρως μάλιστα όταν ο εμπλεκόμενος οργανισμός έχει υψηλά εχέγγυα αποδεδειγμένης επιχειρηματικής τιμιότητας.

Στις δυσκολίες αυτές πρέπει να προστεθεί η απόλυτη ανεξαρτησία του παραβάτη στην επιλογή χώρου και χρόνου αλλά και στην χρήση των πλέον σύγχρονων τεχνολογιών λογισμικού και υλικών υποδομών που του επιτρέπει την θωράκιση της ανωνυμίας του. Και ενώ

η μακρά αστυνομική πείρα με «κοινούς» ποινικούς εγκληματίες βοηθά τις διωκτικές αρχές στην σταδιακή απομόνωση υπόπτων που ανταποκρίνονται σε κλασικά κριτήρια εγκληματικής δραστηριότητας, ο οικονομικός εγκληματίας δεν ανταποκρίνεται σε τέτοια «προφίλ» κάτι που τον καθιστά πρακτικά αόρατο καθώς είτε είναι τελείως άγνωστος στις διωκτικές αρχές είτε εμφανίζεται ως άτομο υπεράνω πάσης υποψίας.

Δειγματοληπτικά, το cyber ΣΔΟΕ θα πρέπει να αποκτήσει ανεπτυγμένες δεξιότητες αιχμής σε κατηγορίες όπως ακολούθως:

1. Νομικές υπηρεσίες με αυξημένη συναίσθηση του γεγονότος ότι η αποκατάσταση των θυμάτων οικονομικού εγκλήματος απαιτεί την συνεργασία του παραβάτη ο οποίος, σχεδόν πάντα, είναι η *μοναδική πηγή πληροφοριών* για το πώς τα κλαπέντα ή μέρος αυτών μπορούν να επιστραφούν στο θύμα ή θύματα.
2. Ενδελεχή και συνεχή ενημέρωση γύρω από την οργάνωση εταιρικών τμημάτων πληροφορικής και των τεχνολογιών που χρησιμοποιούνται ώστε ύποπτα ίχνη να ενεργοποιούν τις διαδικασίες έρευνας αμέσως.
3. Εντατική συνεργασία με ανώτερα στελέχη επιχειρήσεων για συνεχή τους ενημέρωση εξελίξεων στον τομέα του cyber εγκλήματος και στις προόδους της τεχνολογίας.
4. Ανάπτυξη συστήματος επικοινωνίας μόνιμης διπλής κατεύθυνσης με τις αστυνομικές αρχές που θα διευκολύνει την ροή πληροφοριών από και προς αυτές με αντικειμενικό σκοπό την παρακολούθηση καταγγελιών από θύματα και την κατά περίπτωση εμπλοκή του cyber ΣΔΟΕ ως κυρίου ανακριτικού/διερευνητικού οργάνου.
5. Ίδρυση και λειτουργεία τμήματος *διαρκούς εκπαίδευσης* (continuing education) για στελέχη της υπηρεσίας αλλά και άλλων στελεχών-επισκεπτών από τον δημόσιο αλλά και τον ιδιωτικό τομέα.
6. Μόνιμη συνεργασία με ειδικές υπηρεσίες του εξωτερικού και εισαγωγή και εφαρμογή νέων προτύπων στην ανίχνευση και αντιμετώπιση του cyber εγκλήματος.
7. Δημιουργία ειδικού σκέλους με αντικείμενο την εκπαίδευση προσωπικού στην διεθνή διακίνηση κεφαλαίων μέσω τραπεζών και επενδυτικών εταιρικών σχημάτων και στην επεξεργασία ερευνών από υπηρεσίες μεγέθους του εξωτερικού με στόχο την ανάπτυξη νέων μεθόδων και στρατηγικών.

Η δημιουργία του cyber ΣΔΟΕ επείγει λόγω της συνεχώς αυξανόμενης πολυεπίπεδης παραβατικότητας και της οικονομικής ζημίας που αυτή προκαλεί. Μια σοβαρή νομοθετική πρωτοβουλία έχει ήδη γίνει με στόχο το ***μεγάλο οικονομικό έγκλημα*** αρμοδιότητας Υπουργείου Οικονομικών**.** Ένα cyber ΣΔΟΕ θα αποτελέσει το απαραίτητο εκείνο συμπληρωματικό σχήμα που θα ***σκοπεύσει ειδικά το «μικρότερο ευρείας κατανάλωσης» οικονομικό έγκλημα που αυξάνεται με ρυθμούς πλημμυρίδας*** και του οποίου το *συνολικό μέγεθος* αποτελεί ιδιαίτερη απειλή για την εύνομη και ασφαλή λειτουργία και την ισορροπία του γενικότερου οικονομικού συστήματος.