Επιθέσεις κατά συστημάτων πληροφοριών

Η νέα οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου[1]

Ιωάννης Δ. Ιγγλεζάκης, *Επίκ. Καθηγητής Νομικής Σχολής ΑΠΘ, Δικηγόρος Θεσσαλονίκης*

I. Εισαγωγή

Οι επιθέσεις σε η/υ και συστήματα η/υ αποτελούν πλέον καθημερινή πραγματικότητα για τις μεγάλες επιχειρήσεις που δραστηριοποιούνται στο Διαδίκτυο (π.χ. Microsoft, Apple, Facebook κ.ά.[2]), όπως και για τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) του τομέα της πληροφορικής, καθώς και γενικά για τις επιχειρήσεις που στηρίζονται στις τεχνολογίες πληροφορικής και επικοινωνιών (ΤΠΕ), όπως είναι, λ.χ., οι χρηματοπιστωτικοί οργανισμοί, ενώ, σημαντικό μέρος των επιθέσεων στρέφονται και κατά των κυβερνήσεων διαφόρων κρατών ανά την υφήλιο[3]. Έτσι, λ.χ., σε έρευνα που διενήργησε η εταιρία Kaspersky Lab's τον Οκτώβριο του 2012 μετά από μια σειρά επιθέσεις που είχαν ως στόχο διεθνείς διπλωματικές αποστολές, κυβερνητικούς φορείς και επιστημονικούς οργανισμούς, διαπίστωσε την ύπαρξη ενός εκτεταμένου δικτύου κυβερνοκατασκοπείας που πήρε το όνομα «Κόκκινος Οκτώβρης» (Red October). Το εν λόγω δίκτυο λειτουργούσε από το 2007 και στόχευε την περιοχή της Ανατολικής Ευρώπης, τις χώρες της πρώην Σοβιετικής Ένωσης και της Κεντρικής Ασίας[4].

Ιδιαίτερα προβεβλημένο είναι, επίσης, το παράδειγμα της Εσθονίας που δέχθηκε μια σειρά κυβερνοεπιθέσεων επί τρεις εβδομάδες, μετά από την ένταση που προκλήθηκε με τη Ρωσία σχετικά με την απομάκρυνση ενός μνημείου της σοβιετικής εποχής από την πρωτεύουσα Ταλίν. Οι επιθέσεις αυτές ήταν κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS attacks)[5] και είχαν ως στόχο πολλούς κρατικούς φορείς, όπως το Κοινοβούλιο, τράπεζες, υπουργεία, ΜΜΕ κ.ά[6].

Εδώ θα πρέπει να σημειωθεί ότι οι τέτοιου τύπου επιθέσεις μπορούν να θέσουν σε κίνδυνο τη λειτουργία κρίσιμων υποδομών, όπως συνέβη, λ.χ. στην περίπτωση ενός εργοστασίου παραγωγής ηλεκτρικής ενέργειας στη Γερμανία, που δέχθηκε επίθεση, με τη χρήση δικτύου υπολογιστών ρομπότ (botnet) και είχε ως αποτέλεσμα τη διακοπή επικοινωνίας του εργοστάσιου με το Διαδίκτυο[7].

Γενικότερα, οι κακόβουλες επιθέσεις αυξάνονται εκθετικά, όπως τεκμηριώνεται στην έρευνα της εταιρίας Symantec για το έτος 2012, στην οποία σημειώνεται αύξηση 42% σε αυτές, με τον αριθμό των μολυσμένων η/υ (bot zombies) να ανέρχεται σε 3,4 εκατομμύρια και ένα μεγάλο μέρος των επιθέσεων (50%) να στρέφονται κατά ΜΜΕ, αλλά και κατά των ιδιωτών που υφίστανται κλοπή ταυτότητας, σε μεγάλη κλίμακα[8].

Το περιβάλλον στο οποίο διεξάγονται οι εν λόγω επιθέσεις είναι, ασφαλώς, ιδιαίτερα περίπλοκο, καθ' ότι η υποδομή του Διαδικτύου ανήκει στην ιδιοκτησία ιδιωτικών επιχειρήσεων που βρίσκονται σε πολλές χώρες του κόσμου και το ίδιο το δίκτυο διαθέτει ανοικτή αρχιτεκτονική. Το γεγονός δε ότι το Διαδίκτυο είναι ένα παγκοσμιοποιημένο δίκτυο δικτύων η/υ σημαίνει ότι μια επίθεση σε έναν τομέα έχει επίδραση και σε άλλους τομείς, διεθνώς και όχι μόνο σε μία χώρα[9]. Η ποινική αντιμετώπιση του φαινομένου αυτού στο πλαίσιο ενός υπερεθνικού οργανισμού, όπως είναι η ΕΕ, αποκτά, συνεπώς, εξαιρετική σημασία.

II. Η απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της 24ης Φεβρουαρίου 2005 σχετικά με τις επιθέσεις κατά των συστημάτων πληροφοριών

Στο πλαίσιο της ΕΕ εκδόθηκε η απόφαση-πλαίσιο 2005/222/ΔΕΥ, η οποία είχε ως στόχο την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο και την προώθηση της ασφάλειας πληροφοριών σε ό,τι αφορά τη νέα μορφή διεθνικής εγκληματικότητας που συνιστούν οι επιθέσεις κατά συστημάτων πληροφοριών. Όπως αναφέρεται στο προοίμιο της απόφασης – πλαίσιο, οι επιθέσεις κατά των συστημάτων πληροφοριών οφείλονται ιδίως στην απειλή που αντιπροσωπεύει το οργανωμένο έγκλημα, ενώ υπάρχει και αυξημένη ανησυχία για το ενδεχόμενο τρομοκρατικών επιθέσεων κατά των συστημάτων πληροφοριών που αποτελούν μέρος της ζωτικής σημασίας υποδομής των κρατών μελών[10].

Η απόφαση - πλαίσιο προβλέπει την ποινικοποίηση των εξής πράξεων:

α) παράνομη πρόσβαση σε σύστημα πληροφοριών

β) παράνομη παρεμβολή σε σύστημα και

γ) παράνομη παρεμβολή σε δεδομένα.

Ακόμα, η απόφαση - πλαίσιο προβλέπει ρυθμίσεις για την ηθική αυτουργία, υποβοήθηση, συνέργεια και απόπειρα, σε σχέση με τα παραπάνω αδικήματα, καθώς και επιβαρυντικές περιστάσεις, όπως είναι ιδίως η διάπραξη των εν λόγω πράξεων στα πλαίσια εγκληματικής οργάνωσης. Επιπλέον, ρυθμίζεται η ευθύνη νομικών πρόσωπων, όταν τα αδικήματα αυτά τελούνται από εκπροσώπους τους, τέλος δε, >

ρυθμίζονται ζητήματα δικαιοδοσίας, ενώ προβλέπεται και η υποχρέωση των κρατών μελών της Ένωσης για την ανταλλαγή πληροφοριών.

Η άνω πράξη δεν μεταφέρθηκε πλήρως στα κράτη μέλη, σύμφωνα με την από 14.7.2008 Έκθεση της Επιτροπής[11], στην οποία διαπιστώθηκε ότι σημειώθηκε αξιοσημείωτη πρόοδος στην πλειοψηφία των κρατών μελών, με εξαίρεση επτά κράτη μέλη, μεταξύ των οποίων και η Ελλάδα, τα οποία δεν κοινοποίησαν στην Επιτροπή τα μέτρα εφαρμογής της απόφασης - πλαίσιο. Στην Έκθεση γίνεται αναφορά στις μελλοντικές εξελίξεις και συγκεκριμένα, στην ανάδειξη νέων απειλών, όπως είναι η εμφάνιση μαζικών ταυτόχρονων επιθέσεων κατά συστημάτων πληροφοριών και η αυξημένη εγκληματική χρήση του δικτύου προγραμμάτων ρομπότ (botnet), η οποία δεν δύναται να αντιμετωπισθεί από την απόφαση - πλαίσιο. Επίσης, συστήνεται η ανάληψη δράσης για την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών και τον καλύτερο συντονισμό τους και σε συνεργασία με ιδιωτικούς φορείς, σε διεθνές επίπεδο, για την αντιμετώπιση μαζικών επιθέσεων κατά των συστημάτων πληροφοριών.

Αξίζει να σημειωθεί ότι η Χώρα μας υπέγραψε, αλλά δεν κύρωσε τη Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα της 23.11.2001[12], η οποία αποτελεί σημείο αναφοράς όσον αφορά τη ρύθμιση του κυβερνοεγκλήματος, διεθνώς. Η εν λόγω Σύμβαση περιέχει αντίστοιχες διατάξεις με αυτές της απόφασης-πλαισίου.

Η ανάγκη για περαιτέρω δράση στην αντιμετώπιση της ηλεκτρονικής εγκληματικότητας, στο πλαίσιο της ΕΕ, διαπιστώθηκε και στο πρόγραμμα της Χάγης για την ενίσχυση της ελευθερίας, της ασφάλειας και της δικαιοσύνης στην ΕΕ[14], το πρόγραμμα της Στοκχόλμης[15], αλλά και το ψηφιακό θεματολόγιο για την Ευρώπη[16]. Για το λόγο αυτό, κατατέθηκε από την Επιτροπή το 2010 πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου[17], η οποία εγκρίθηκε σε πρώτη ανάγνωση από το Ευρωπαϊκό Κοινοβούλιο στις 4.7.2013.

III. Η οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών

1. Νομική θεμελίωση της οδηγίας

Η αναγκαιότητα θέσπισης μέτρων για την αντιμετώπιση του φαινομένου των επιθέ-

σεων κατά συστημάτων πληροφοριών στο επίπεδο της ΕΕ προκύπτει από το προοίμιο της οδηγίας. Καταρχάς, σημειώνεται ότι ενώ η ομαλή λειτουργία και ασφάλεια των συστημάτων πληροφοριών στην Ένωση είναι ζωτικής σημασίας για την ανάπτυξη της εσωτερικής αγοράς και μιας ανταγωνιστικής και καινοτόμου οικονομίας, οι επιθέσεις κατά των συστημάτων πληροφοριών και ιδίως εκείνες που συνδέονται με το οργανωμένο έγκλημα αποτελούν αυξανόμενη απειλή τόσο στην ΕΕ όσο και παγκόσμια, αλλά και για την επίτευξη ασφαλέστερης κοινωνίας της πληροφορίας[18]. Ειδική αναφορά γίνεται στο γεγονός ότι στην Ένωση υπάρχουν υποδομές ζωτικής σημασίας των οποίων η βλάβη ή καταστροφή θα μπορούσε να έχει σημαντικό διασυνοριακό αντίκτυπο[19].

Παραπέρα, σημειώνεται ότι επιθέσεις μεγάλης κλίμακας μπορούν να προξενήσουν σημαντικές οικονομικές ζημίες τόσο λόγω της διακοπής λειτουργίας των συστημάτων ΤΠΕ όσο και λόγω της απώλειας ή αλλοίωσης σημαντικών εμπορικών εμπιστευτικών πληροφοριών ή άλλων δεδομένων, σημαντικό αντίκτυπο μπορεί δε να έχουν οι επιθέσεις αυτές στις καινοτόμες ΜΜΕ[20].

Σύμφωνα με τον κοινοτικό νομοθέτη, υπάρχουν στοιχεία που δείχνουν μια τάση διάπραξης όλο και πιο επικίνδυνων και επαναλαμβανόμενων επιθέσεων μεγάλης κλίμακας κατά συστημάτων πληροφοριών που συχνά μπορεί να έχουν ζωτική σημασία για τα κράτη ή για ειδικές δραστηριότητες του δημόσιου ή ιδιωτικού τομέα, η οποία (τάση) συνοδεύεται από την ανάπτυξη όλο και πιο εξελιγμένων μεθόδων, όπως η δημιουργία και χρήση δικτύων προγραμμάτων ρομπότ (botnet)[21].

Με βάση αυτές τις παρατηρήσεις, καθίσταται σαφής η αρμοδιότητα του κοινοτικού νομοθέτη, βάσει του άρθρου 83 ΣΛΕΕ, να θεσπίσει ελάχιστους κανόνες για την προσέγγιση της ποινικής νομοθεσίας των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών. Η οδηγία 2013/40/ΕΕ, σύμφωνα με το άρθρο 1 αυτής, καθιερώνει κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των κυρώσεων στον τομέα αυτό, στοχεύει δε και στη διευκόλυνση της πρόληψης των αδικημάτων αυτών και τη βελτίωση της συνεργασίας μεταξύ δικαστικών και άλλων αρμόδιων αρχών.

2. Τα δίκτυα προγραμμάτων ρομπότ (botnets)

Ένας σημαντικός νεωτερισμός της οδηγίας σε σχέση με την απόφαση - πλαίσιο 2005/222/ΔΕΥ είναι ότι λαμβάνει υπόψη και ποινικοποιεί τη χρήση νέων μεθόδων για τη διάπραξη κυβερνοεγκλημάτων, όπως είναι η χρήση δικτύων προγραμμάτων ρομπότ (botnets), στα οποία πρέπει να γίνει ακολούθως αναφορά. Ειδικότερα, με τον όρο αυτό δηλώνεται ένα δίκτυο η/υ που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται από έναν άλλο η/υ, συχνά δίχως να το γνωρίζει ο κάτοχός τους (υπολογιστές «ζόμπι»). Τα δίκτυα αυτά μπορεί να ενεργοποιηθούν προκειμένου να εκτελέσουν συγκεκριμένες ενέργειες, όπως π.χ. να επιτεθούν σε συστήματα πληροφοριών. Ενίοτε, τα δίκτυα botnets εκτελούν επιθέσεις μεγάλης κλίμακας, δηλ. επιθέσεις σε μεγάλο αριθμό συστημάτων η/υ ή επιθέσεις που προκαλούν μεγάλες ζημίες, επιφέροντας άρνηση υπηρεσίας και διακοπή λειτουργίας των συστημάτων, οικονομική ζημία, κλοπή ή καταστροφή προσωπικών δεδομένων κ.λπ. Ένα μεγάλο τέτοιο δίκτυο μπορεί να έχει μεταξύ 40.000 και 100.000 συνδέσεων[22].

Ένα δίκτυο προγραμμάτων ρομπότ μπορεί να χρησιμοποιηθεί για την αποστολή ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, για την αλίευση προσωπικών δεδομένων (phishing) ή την κλοπή τέτοιων στοιχείων από τους η/υ των χρηστών, την αποστολή και καταφόρτωση κακόβουλου λογισμικού κ.λπ.[23] Βεβαίως, η χρησιμότητά της έγκειται κυρίως στην εκτέλεση επιθέσεων άρνησης υπηρεσίας (Denial-of-Service (DoS Attacks). Οι επιθέσεις αυτές συνίστανται στην υπερφόρτωση ενός συστήματος με την αποστολή υπερβολικά μεγάλου αριθμού πακέτων δεδομένων, ώστε να καταναλώνεται μνήμη υπολογιστή, ισχύς και εύρος ζώνης (bandwidth) του συστήματος, με αποτέλεσμα να μη μπορεί πλέον αυτό να εξυπηρετήσει τους κανονικούς χρήστες του και να διακόπτει τη λειτουργία του[24].

3. Οι διατάξεις της οδηγίας

Η οδηγία περιέχει στο άρθρο 2 ορισμούς των όρων που χρησιμοποιούνται στο κείμενό της, από τους οποίους ενδιαφέρον παρουσιάζει ο ορισμός του «συστήματος πληροφοριών». Ειδικότερα, ως ένα τέτοιο σύστημα νοείται «η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με

ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους» (άρθρο 2 περ. α).

Περαιτέρω, η οδηγία περιέχει διατάξεις για αδικήματα που θίγουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων συστημάτων η/υ. Όπως και η απόφαση-πλαίσιο 2005/222/ΔΕΥ, κυρώνει την παράνομη πρόσβαση σε συστήματα πληροφοριών (άρθρο 3), την παράνομη παρεμβολή σε σύστημα (άρθρο 4) και την παράνομη παρεμβολή σε δεδομένα (άρθρο 5). Ειδικότερα, για τις πράξεις αυτές προβλέπονται τα εξής:

Σύμφωνα με το άρθρο 3 της οδηγίας, τα κράτη μέλη πρέπει να λάβουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

Σύμφωνα με το άρθρο 4, τα κράτη μέλη πρέπει να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

Και ακόμα, σύμφωνα με το άρθρο 5, τα κράτη μέλη πρέπει να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

Οι παραπάνω διατάξεις εφαρμόζονται στα δίκτυα προγραμμάτων ρομπότ και συγκεκριμένα, κατά το στάδιο της δημιουργίας τους, όπου αποκτάται ο από απόσταση έλεγχος η/υ με τη μόλυνσή τους με κακόβουλο λογισμικό, βρίσκει εφαρμογή το άρθρο 3, ενώ το άρθρο 4 βρίσκει εφαρμογή κατά το στάδιο της εξαπόλυσης κυβερνοεπιθέσεων και το άρθρο 5 όταν προκαλούνται ζημίες από αυτές.

Περαιτέρω, στο άρθρο 6 προβλέπεται ότι πρέπει να τιμωρείται η παράνομη υποκλοπή. Συγκεκριμένα, ορίζεται ότι η υποκλοπή με τεχνικά μέσα μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, περιλαμβανομένων των ηλεκτρονικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις. Η υποκλοπή περιλαμβάνει, ενδεικτικά, την ακρόαση, έλεγχο ή επιτήρηση του περιεχομένου των επικοινωνιών και παροχή του περιεχομένου των δεδομένων είτε άμεσα, με πρόσβαση και χρήση των συστημάτων πληροφοριών, είτε έμμεσα με τη χρήση ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα[25].

Πιο πέρα, ποινικοποιείται η χρήση εργαλείων λογισμικού για τη διάπραξη των ως άνω αδικημάτων, η οποία είχε προκαλέσει μεγάλη συζήτηση στη θεωρία[26]. Συγκεκριμένα, στο άρθρο 7, προβλέπεται ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός από τα ακόλουθα εργαλεία χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε από τα αδικήματα που αναφέρονται στα άρθρα 3 έως 6, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις:

α) πρόγραμμα υπολογιστή που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε από τα αδικήματα που αναφέρονται στα άρθρα 3 έως 6·

β) συνθηματικό κωδικού η/υ, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών[27].

Τα εργαλεία στα οποία αναφέρεται η οδηγία είναι το κακόβουλο λογισμικό που χρησιμοποιείται, μεταξύ άλλων, για τη διάπραξη κυβερνοεπιθέσεων με τη δημιουργία botnet. Προς αποφυγή, ωστόσο, της ποινικοποίησης της έρευνας στον τομέα της ασφάλειας πληροφοριών και της ανάπτυξης λογισμικού, προβλέπεται ότι τιμωρείται η παραγωγή και διάθεση των εν λόγω εργαλείων, αλλά εκτός από τη γενική υποχρέωση της πρόθεσης θα πρέπει να υφίσταται και άμεση πρόθεση να χρησιμοποιηθούν τα εργαλεία αυτά για τη διάπραξη κάποιου από τα αδικήματα των άρθρων 3 έως 6[28]. Συνακόλουθα, δεν θα πληρούται η υποκειμενική υπόσταση του αδικήματος όταν οι παραπάνω πράξεις διαπράττονται χωρίς πρόθεση, όπως όταν το πρόσωπο που τις διενεργεί δεν γνώριζε ότι απαγορεύεται η πρόσβαση ή στην περίπτωση εξουσιοδοτημένης δοκιμής ή προστασίας συστημάτων πληροφοριών, π.χ. όταν ένας ειδικός ελέγχει την ισχύ του συστήματος ασφάλειας πληροφοριών μιας επιχείρησης[29].

Όπως στην απόφαση-πλαίσιο 2005/222/ΔΕΥ, έτσι και η οδηγία προβλέπει στο άρθρο 8 ότι πρέπει να τιμωρείται η ηθική αυτουργία, η υποβοήθηση και η συνέργεια προς διάπραξη αδικήματος που αναφέρεται στα άρθρα 3 έως 7, αλλά και η απόπειρα διάπραξης αδικήματος που αναφέρεται στα άρθρα 4 έως 5.

Στο άρθρο 9 της οδηγίας προβλέπεται το πλαίσιο ποινών για τα αδικήματα που τυποποιούνται στα άρθρα 3 έως 8. Ως γενικός κανόνας προβλέπεται στην παρ. 1 ότι οι κυρώσεις θα πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές και να περιλαμβάνουν φυλάκιση και/ή χρηματικές ποινές. Επίσης, τα κράτη μέλη πρέπει να προβλέψουν ποιες περιπτώσεις θεωρούνται ως ήσσονος σημασίας και μένουν ατιμώρητες. Αυτό μπορεί να συμβαίνει, π.χ., όταν οι ζημίες που προκαλεί το αδίκημα και/ή ο κίνδυνος που συνεπάγεται για το δημόσιο ή το ιδιωτικό συμφέρον (όπως η ακεραιότητα ενός συστήματος η/υ ή ηλεκτρονικών δεδομένων, η σωματική ακεραιότητα, τα δικαιώματα και άλλα συμφέροντα ενός πρόσωπου) είναι αμελητέα ή τέτοιας φύσεως ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης[30]. Στην παρ. 2 του ίδιου άρθρου προβλέπεται το πλαίσιο της ποινής για τα ανωτέρω αδικήματα. Συγκεκριμένα, ορίζεται ότι αυτά τιμωρούνται με μέγιστη ποινή φυλάκισης τουλάχιστον δύο ετών, τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας.

Περαιτέρω, ρυθμίζονται ορισμένες επιβαρυντικές περιπτώσεις. Η πρώτη αφορά τις επιθέσεις μεγάλης κλίμακας που πλήττουν σημαντικό αριθμό συστημάτων πληροφοριών ή προκαλούν σοβαρές ζημίες και η δεύτερη, τη διάπραξη μιας επίθεσης από εγκληματική οργάνωση. Συγκεκριμένα, προβλέπεται ότι τα αδικήματα που αναφέρονται στα άρθρα 4 έως 5 τιμωρούνται με μέγιστη ποινή φυλάκισης τουλάχιστον τριών ετών όταν τα αδικήματα διαπράττονται εκ προθέσεως και εφόσον έχει πληγεί σημαντικός αριθμός συστημάτων πληροφοριών μέσω της χρήσης εργαλείου αναφερόμενου στο άρθρο 7 (άρθρο 9 παρ. 3).

Ακόμα, προβλέπεται ότι τα αδικήματα που αναφέρονται στα άρθρα 4 έως 5 τιμωρούνται με μέγιστη ποινή φυλάκισης τουλάχιστον >

Επιθέσεις κατά συστημάτων πληροφοριών (συνέχεια)

πέντε ετών, εφόσον: α) διαπράττονται στο πλαίσιο εγκληματικής οργάνωσης, κατά την έννοια της απόφασης - πλαισίου 2008/814/ΔΕΥ, ανεξαρτήτως της κύρωσης που ορίζεται σε αυτή, β) προκαλούν σημαντικές ζημίες, ή γ) διαπράττονται κατά συστημάτων πληροφοριών που αποτελεί μέρος ζωτικής σημασίας υποδομής (άρθρο 9 παρ. 4).

Μια τρίτη επιβαρυντική περίπτωση είναι αυτή που αφορά τη διάπραξη αδικημάτων με απόκτηση εμπιστοσύνης τρίτων (social engineering). Συγκεκριμένα, ορίζεται ότι τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν ότι όταν τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται με υφαρπαγή προσωπικών δεδομένων άλλου ατόμου, προκείμενου να αποκτηθεί η εμπιστοσύνη τρίτων, και προκαλούν ζημία στον νόμιμο δικαιούχο της ταυτότητας, αυτό μπορεί, σύμφωνα με τις σχετικές διατάξεις της εσωτερικής νομοθεσίας, να θεωρείται ως επιβαρυντική περίσταση, εκτός εάν οι περιστάσεις αυτές καλύπτονται ήδη από άλλο αδίκημα που τιμωρείται σύμφωνα με την εθνική νομοθεσία (άρθρο 9 παρ. 5).

Ακολούθως, η οδηγία περιλαμβάνει διατάξεις σχετικά με την ευθύνη και τις ποινές κατά νομικών πρόσωπων. Τα νομικά πρόσωπα μπορούν να θεωρούνται υπεύθυνα για τα αδικήματα των άρθρων 3 έως 8 όταν διαπράττονται προς όφελός τους από πρόσωπο που κατέχει την εξουσία εκπροσώπησης του νομικού προσώπου, την εξουσία λήψης αποφάσεων για λογαριασμό του ή την εξουσία άσκησης ελέγχου εντός αυτού (άρθρο 10). Οι ποινές που τους επιβάλλονται πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές και σε αυτές περιλαμβάνονται χρηματικές ποινές ή πρόστιμα και ενδεχομένως και άλλες κυρώσεις, όπως: α) αποκλεισμός από δημόσιες παροχές ή ενισχύσεις, β) προσωρινή ή οριστική απαγόρευση της άσκησης εμπορικών δραστηριοτήτων, γ) θέση υπό δικαστική εποπτεία, δ) δικαστική εκκαθάριση, ε) προσωρινό ή οριστικό κλείσιμο των εγκαταστάσεων που χρησιμοποιήθηκαν για τη διάπραξη του αδικήματος (άρθρο 11).

Η οδηγία περιέχει, ακόμα, κανόνες δικαιοδοσίας για τα αδικήματα των άρθρων 3 έως 8, στο άρθρο 12. Συγκεκριμένα, προβλέπει ότι θεμελιώνεται η δικαιοδοσία ενός κράτους μέλους εφόσον το αδίκημα έχει διαπραχθεί: εν όλω ή εν μέρει στο έδαφος του οικείου κράτους μέλους ή από υπηκόους τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται ποινικό αδίκημα στον τόπο όπου έχει διαπραχθεί.

Διευκρινιστικά αναφέρεται στην ίδια διάταξη ότι δικαιοδοσία θεμελιώνεται και στις περιπτώσεις όπου ο δράστης διέπραξε το αδίκημα ενώ βρισκόταν στο έδαφος του οικείου κράτους μέλους, ασχέτως εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός του ή όταν το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδαφος του οικείου κράτους μέλους, ανεξάρτητα αν ο δράστης διαπράττει το αδίκημα ευρισκόμενος στο έδαφός του. Ωστόσο, ένα κράτος μέλος που αποφασίζει να θεμελιώσει δικαιοδοσία για αδίκημα που αναφέρεται στα άρθρα 3 έως 8 που διαπράττεται εκτός του εδάφους του, όταν ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφός του, ή το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφός του, πρέπει να ενημερώνει σχετικά την Επιτροπή.

Κεντρική σημασία αποδίδεται από τον κοινοτικό νομοθέτη στην ανταλλαγή πληροφοριών μέσω εθνικών δικτύων επαφής, τα οποία θα πρέπει να είναι σε θέση να προσφέρουν αποτελεσματική βοήθεια διευκολύνοντας, λ.χ., την ανταλλαγή διαθέσιμων σχετικών πληροφοριών ή την παροχή τεχνικών συμβουλών ή νομικών πληροφοριών για έρευνας ή διαδικασίες σχετικές με ποινικά αδικήματα που συνδέονται με συστήματα πληροφοριών και συναφή δεδομένα που αφορούν το κράτος μέλος το οποίο υποβάλλει την αίτηση[31]. Έτσι, το άρθρο 13 ορίζει ότι για τους σκοπούς της ανταλλαγής πληροφοριών σχετικά με τα αδικήματα των άρθρων 3 έως 8, τα κράτη μέλη διασφαλίζουν ότι διαθέτουν ένα λειτουργικό σημείο επαφής και κάνουν χρήση του υφιστάμενου δικτύου επιχειρησιακών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και επτά ημέρες την εβδομάδα.

Δεδομένου ότι οι κυβερνοεπιθέσεις πραγματοποιούνται με μεγάλη ταχύτητα, πρέπει και ο χρόνος ανταπόκρισης να είναι σύντομος. Έτσι, προβλέπεται στην ίδια διάταξη η υποχρέωση των κρατών μελών να θεσπίζουν διαδικασίες που να τους επιτρέπουν σε περιπτώσεις επειγουσών αιτήσεων συνδρομής, η αρμόδια αρχή να μπορεί να δηλώσει εντός 8 ωρών από την παραλαβή, τουλάχιστον εάν θα απαντήσει στην αίτηση συνδρομής, καθώς και τη μορφή και τον εκτιμώμενος χρόνος της απάντησης αυτής.

Για την αρτιότερη αντιμετώπιση των αδικημάτων που τυποποιούνται στην οδηγία κρίθηκε αναγκαία η συλλογή συγκρίσιμων στοιχείων. Για αυτό ορίζεται στο άρθρο 14 ότι τα κράτη μέλη πρέπει να θεσπίσουν σύστημα για την καταγραφή, παραγωγή και παροχή στατιστικών στοιχείων για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7. Τα στοιχεία αυτά καλύπτουν τουλάχιστον τα δεδομένα για τον αριθμό των αδικημάτων που καταγράφονται, καθώς και τον αριθμό των προσώπων που διώχθηκαν και καταδικάσθηκαν.

Τέλος, με το άρθρο 15 προβλέπεται η αντικατάσταση της απόφασης-πλαίσιο 2005/222/ΔΕΥ όσον αφορά τα κράτη μέλη που συμμετέχουν στην έκδοση της οδηγίας, με την επιφύλαξη των υποχρεώσεων όσον αφορά τις προθεσμίες μεταφοράς της απόφασης-πλαισίου στο εθνικό τους δίκαιο, ενώ η προθεσμία μεταφοράς της οδηγίας στο εθνικό δίκαιο καθορίζεται στο άρθρο 16.

4. Μεταφορά της οδηγίας στο ελληνικό δίκαιο

Με δεδομένο ότι η Χώρα μας δεν έχει κυρώσει τη Σύμβαση για το Κυβερνοέγκλημα ούτε έχει ενσωματώσει τις διατάξεις της απόφασης-πλαίσιο 2005/222/ΔΕΥ στο ελληνικό δίκαιο, θα χρειασθεί να μεταφέρει το σύνολο των διατάξεων της οδηγίας. Βεβαίως, στο νέο σχέδιο Ποινικού Κώδικα ενσωματώνονται οι σχετικές διατάξεις και πιο συγκεκριμένα, τυποποιούνται τα αδικήματα της παράνομης πρόσβασης σε σύστημα πληροφοριών ή σε δεδομένα (άρθρο 274), της παρακώλυσης λειτουργίας συστήματος πληροφοριών (άρθρο 275), της φθοράς ηλεκτρονικών δεδομένων (άρθρο 276) και της υποκλοπής ηλεκτρονικών δεδομένων (άρθρο 277), καθώς και η απαγόρευση του λογισμικού για την τέλεση των ως άνω αδικημάτων. Ωστόσο, ενόψει του ότι η οδηγία περιέχει αρκετές νέες ρυθμίσεις, θα πρέπει να ληφθεί μέριμνα για την πλήρη ενσωμάτωσή της στο ελληνικό δίκαιο.

IV. Επίμετρο

Η οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών θα συμβάλλει ουσιαστικά στην εναρμόνιση του ποινικού δικαίου των κρατών μελών της ΕΕ στον κρίσιμο αυτό τομέα. Παρόλο που πρόκειται για μια οδηγία ελάχιστης εναρμόνισης, θα συμβάλλει σε μεγαλύτερο βαθμό στην προσέγγιση του ποινικού δικαίου απ' ό,τι η απόφαση-πλαίσιο 2005/222/ΔΕΥ, διότι η νομική μορφή της οδηγίας είναι πιο κατάλληλη για το σκοπό αυτό.

Ακόμα, η ως άνω οδηγία λαμβάνει υπόψη τα σύγχρονα τεχνολογικά δεδομένα και περιέχει σαφείς κυρωτικούς κανόνες κατά των δραστών επιθέσεων κατά συστημάτων πληροφοριών, ιδίως όσον χρησιμοποιούν δίκτυα προγραμμάτων ρομπότ (botnet) ή προβαίνουν σε επιθέσεις μεγάλης κλίμακας κατά συστημάτων πληροφοριών. Και πιο πέρα, ποινικοποιεί την παραγωγή, χρήση και διάθεση των εργαλείων που χρησιμοποιούνται για τη διάπραξη αδικημάτων που αναφέρονται στην οδηγία

και τα οποία είναι απολύτως απαραίτητα για το σκοπό αυτό. Για το λόγο δε αυτό, δεν είναι άστοχη η ποινικοποίησή τους, όπως έχει υποστηριχθεί στη θεωρία. Τέλος, η οδηγία αποδίδει σημασία στα δίκτυα συνεργασίας μεταξύ των κρατών μελών, όπως και στη συνεργασία μεταξύ των δημόσιων αρχών και του ιδιωτικού τομέα και της κοινωνίας των πολιτών.

Παράλληλα με την οδηγία, αξίζει να σημειωθεί ότι η Ευρωπαϊκή Επιτροπή δημοσίευσε στις 7.2.2013 τη στρατηγική για την ασφάλεια στον κυβερνοχώρο[32], καθώς και πρόταση οδηγίας για μέτρα με σκοπό τη διασφάλιση ενός υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών στην ΕΕ[33]. Επιπλέον, θεσμοθέτησε το Κέντρο για το Κυβερνοέγκλημα στα πλαίσια της Europol[34], το οποίο θα αποτελέσει σημείο αναφοράς για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Με τις δράσεις αυτές, επιδιώκεται η ενίσχυση της ασφάλειας στον κυβερνοχώρο, στο πλαίσιο της ΕΕ και ειδικότερα, η πρόληψη και αντιμετώπιση διαταραχών και επιθέσεων στον κυβερνοχώρο, με στόχο την προώθηση των αξιών της ελευθερίας και της δημοκρατίας και τη διασφάλιση της ανάπτυξης της ψηφιακής οικονομίας με ασφάλεια. Σ

ΥΠΟΣΗΜΕΙΩΣΕΙΣ

1. With the financial support of the Prevention of and Fight against Crime Programme European Commission - Directorate General Home Affairs. This project has been funded from the European Commission. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

2. Βλ. Microsoft Gets Hacked; Siilar to Attacks on Apple, facebook, CNBC, 22.2.2013, διαθέσιμο στην ηλ. διεύθυνση: http://www.cnbc.com/id/100486700
3. Βλ. *J. Hiller/R. Russell*, The challenge and imperative of private sector cybersecurity: An international comparison, CLSR 2013, σελ. 236 επ.
4. Βλ. «Red October» Diplomatic Cyber Attacks Investigation, διαθέσιμο στην ηλ. διεύθυνση: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation
5. Για τις επιθέσεις άρνησης υπηρεσίας βλ. *S. Furnell*, Κυβερνοέγκλημα. Καταστρέφοντας την κοινωνία της πληροφορίας, 2006, σελ. 36 επ.
6. Για την εν λόγω επίθεση κατηγορήθηκε η Ρωσία, βλ. Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17.5.2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia
7. Βλ. Euractiv, European renewable power grid rocked by cyber-attack, 10.12.2012, διαθέσιμο στην ηλ. διεύθυνση: http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541
8. Βλ. Symantec, Internet Security Threat Report 2013, διαθέσιμο στην ηλ. διεύθυνση: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
9. Βλ. *J. Hiller/R. Russell*, The challenge and imperative of private sector cybersecurity: An international comparison, ό.π., σελ. 237.
10. Βλ. αιτιολογ. σκέψη αρ. 2.
11. COM(2008) 448 τελικό.
12. Βλ. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
13. Σημειώνεται ότι η πλειοψηφία των κρατών μελών της ΕΕ υπέγραψε και κύρωσε τη Σύμβαση, βλ. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
14. Βλ. 2005/C 53/01.
15. Βλ. Ανακοίνωση της Επιτροπής, Για ένα χώρο ελευθερίας, ασφάλειας και δικαιοσύνης στην υπηρεσία των πολιτών της Ευρώπης. Σχέδιο δράσης για την εφαρμογή του προγράμματος της Στοκχόλμης, COM (2010) 171, 20.4.2010.
16. COM (2010) 245 τελικό.
17. COM (2010) 0517 - C7-0293/2010 - 2010/0273 (COD).
18. Βλ. αιτιολογ. σκέψη αρ. 3.
19. Βλ. αιτιολογ. σκέψη αρ. 4.
20. Βλ. αιτιολογ. σκέψη αρ. 6.
21. Βλ. αιτιολογ. σκέψη αρ. 5.
22. Βλ. για τα παραπάνω Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010) 517, σελ. 3.
23. Βλ. Microsoft Security Intelligence Report, Battling Botnets for Control of computers, vol. 9 (2010), σελ. 12 επ.
24. Βλ. Microsoft, ό.π., σελ. 13, Βικιπαίδεια, επιθέσεις άρνησης υπηρεσιών, http://el.wikipedia.org/
25. Βλ. αιτιολογ. σκέψη αρ. 9.
26. Βλ. *K. Chatziioannou,* The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data, Paper presented in the 4th International Conference on Information Law, http://conferences.ionio.gr/icil2011
27. Βλ. αντίστοιχα τη διάταξη του άρθρου 6 της Σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
28. Βλ. αιτιολογ. σκέψη αρ. 16 της οδηγίας. Αντίστοιχα, για τη Σύμβαση για το Κυβερνοέγκλημα βλ. *U. Sieber*, Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes, in: *D. Spinellis* (Ed.), Computer crimes, Cyber-terrorism, child pornography and financial crimes 2004, σελ. 26.
29. Βλ. αιτιολογ. σκέψη αρ. 17 της οδηγίας.
30. Βλ. αιτιολογ. σκέψη αρ. 11 της οδηγίας.
31. Βλ. αιτιολογ. σκέψη αρ. 11.
32. Βλ. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final.
33. COM (20130) 48 final.
34. Βλ. https://www.europol.europa.eu/ec3