ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΕΙΔΙΚΑ ΘΕΜΑΤΑ ΔΙΚΑΙΟΥ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Ενότητα 4: ΟΔΗΓΙΑ ΓΙΑ ΕΠΙΘΕΣΕΙΣ ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Λίλιαν Μήτρου, Αναπληρώτρια Καθηγήτρια

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΟΔΗΓΙΑ 2013/40/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 12ης Αυγούστου 2013

για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 83 παράγραφος 1,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ([1]),

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ([2]),

Εκτιμώντας τα ακόλουθα:

(1) Οι στόχοι της παρούσας οδηγίας είναι η προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων, και η βελτίωση της συνεργασίας μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, καθώς και των αρμόδιων ειδικευμένων οργανισμών της Ένωσης και φορέων της Ένωσης, όπως η Eurojust, η Ευρωπόλ και το Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος, καθώς και ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια δικτύων και Πληροφοριών (ENISA).

(2) Τα συστήματα πληροφοριών είναι βασικό στοιχείο για την πολιτική, κοινωνική και οικονομική αλληλεπίδραση στην Ένωση. Η κοινωνία εξαρτάται σε υψηλό και αυξανόμενο βαθμό από τέτοια συστήματα. Η ομαλή λειτουργία και η ασφάλεια αυτών των συστημάτων στην Ένωση είναι ζωτικής σημασίας για την ανάπτυξη της εσωτερικής αγοράς και μιας ανταγωνιστικής και καινοτόμου οικονομίας. Η εξασφάλιση κατάλληλων επιπέδων προστασίας των συστημάτων πληροφοριών θα πρέπει να αποτελεί μέρος ενός αποτελεσματικού ολοκληρωμένου πλαισίου από μέτρα πρόληψης τα οποία συνοδεύουν τις απαντήσεις του ποινικού δικαίου στον κυβερνοχώρο.

(3) Οι επιθέσεις κατά των συστημάτων πληροφοριών, και ιδίως οι επιθέσεις που συνδέονται με το οργανωμένο έγκλημα, αποτελούν συνεχώς αυξανόμενη απειλή, τόσο στην Ένωση όσο και παγκοσμίως, και εντείνουν τις ανησυχίες για το ενδεχόμενο τρομοκρατικών επιθέσεων ή επιθέσεων με πολιτικά κίνητρα κατά των συστημάτων πληροφοριών που αποτελούν μέρος των υποδομών ζωτικής σημασίας των κρατών μελών και της Ένωσης. Αυτό αποτελεί απειλή για την επίτευξη μιας ασφαλέστερης κοινωνίας της πληροφορίας και ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, και, επομένως, απαιτείται απάντηση στο επίπεδο της Ένωσης και βελτιωμένη συνεργασία και συντονισμός σε διεθνές επίπεδο.

(4) Υπάρχουν ορισμένες υποδομές ζωτικής σημασίας στην Ένωση, η διακοπή ή η καταστροφή των οποίων θα μπορούσε να έχει σημαντικό διασυνοριακό αντίκτυπο. Έχει καταστεί προφανές, λόγω της ανάγκης να ενισχυθεί η προστασία των υποδομών ζωτικής σημασίας στην Ένωση, ότι τα μέτρα κατά των επιθέσεων στον κυβερνοχώρο θα πρέπει να συμπληρώνονται με αυστηρές ποινικές κυρώσεις που να αντανακλούν τη σοβαρότητα των επιθέσεων αυτών. Ως υποδομές ζωτικής σημασίας μπορούν να νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που ευρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των ζωτικών κοινωνιακών λειτουργιών, της υγείας, της ασφάλειας, της προστασίας της οικονομικής ή κοινωνικής ευημερίας, όπως εγκαταστάσεις παραγωγής ενεργείας, μεταφορικά δίκτυα ή κυβερνητικά δίκτυα, και η διακοπή ή η καταστροφή των οποίων θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών.

(5) Υπάρχουν στοιχεία που δείχνουν μια τάση διάπραξης όλο και πιο επικίνδυνων και επαναλαμβανόμενων επιθέσεων μεγάλης κλίμακας κατά συστημάτων πληροφοριών που συχνά μπορούν να έχουν ζωτική σημασία για τα κράτη μέλη ή για ειδικές δραστηριότητες του δημόσιου ή του ιδιωτικού τομέα. Η τάση αυτή συνοδεύεται από την ανάπτυξη όλο και πιο εξελιγμένων μεθόδων, όπως η δημιουργία και η χρήση των αποκαλούμενων «botnet» (δίκτυα προγραμμάτων ρομπότ), η οποία περιλαμβάνει διάφορα στάδια της αξιόποινης πράξης, καθένα από τα οποία μπορεί από μόνο του να θέσει σε σοβαρό κίνδυνο το δημόσιο συμφέρον. Η παρούσα οδηγία σκοπεύει, μεταξύ άλλων, στην εισαγωγή ποινικών κυρώσεων για τη δημιουργία των «botnet», ήτοι πράξη της απόκτησης εξ αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών διά της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο. Μόλις δημιουργηθεί, το προσβεβλημένο δίκτυο υπολογιστών, που συνιστά το «botnet», μπορεί να ενεργοποιείται εν αγνοία των χρηστών των εν λόγω υπολογιστών, με σκοπό την εξαπόλυση επιθέσεων στον κυβερνοχώρο μεγάλης κλίμακας, η οποία συνήθως μπορεί να προκαλέσει σοβαρές ζημίες, όπως αναφέρεται στην παρούσα οδηγία. Τα κράτη μέλη θα πρέπει να μπορούν να ορίσουν τι συνιστά σοβαρή ζημιά σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές, όπως διακοπή της λειτουργίας συστημάτων μεγάλης δημόσιας σημασίας ή σημαντική οικονομική ζημιά ή απώλεια δεδομένων προσωπικού χαρακτήρα ή ευαίσθητων πληροφοριών.

(6) Επιθέσεις στον κυβερνοχώρο μεγάλης κλίμακας μπορούν να προξενήσουν σημαντικές οικονομικές ζημίες, τόσο μέσω της διακοπής της λειτουργίας των συστημάτων πληροφοριών και των επικοινωνιών όσο και μέσω της απώλειας ή αλλοίωσης σημαντικών εμπορικών εμπιστευτικών πληροφοριών ή άλλων δεδομένων. Θα πρέπει να αποδίδεται ιδιαίτερη προσοχή στην αύξηση της ευαισθητοποίησης των καινοτόμων μικρών και μεσαίων επιχειρήσεων για απειλές σχετικές με αυτές τις επιθέσεις και για την ευπάθειά τους σε αυτές τις επιθέσεις, επειδή εξαρτώνται, σε μεγάλο βαθμό, από την ορθή λειτουργία και τη διαθεσιμότητα πληροφοριακών συστημάτων και συχνά έχουν περιορισμένους πόρους για την ασφάλεια των πληροφοριών.

([1]) ΕΕ C 218 της 23.7.2011, σ. 130.

([2]) Θέση του Ευρωπαϊκού Κοινοβουλίου της 4ης Ιουλίου 2013 (δεν έχει ακόμα δημοσιευθεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 22ας Ιουλίου 2013.

(7) Είναι σημαντικό να υπάρχουν κοινοί ορισμοί στον τομέα αυτό ώστε να διασφαλισθεί η συνεκτική προσέγγιση μεταξύ των κρατών μελών κατά την εφαρμογή της παρούσας οδηγίας.

(8) Είναι ανάγκη να επιτευχθεί κοινή προσέγγιση για τα στοιχεία της αντικειμενικής υπόστασης των ποινικών αδικημάτων, με την πρόβλεψη των κοινών αδικημάτων της παράνομης πρόσβασης σε σύστημα πληροφοριών, της παράνομης παρεμβολής σε σύστημα, της παράνομης παρεμβολής σε δεδομένα και της παράνομης υποκλοπής.

(9) Η υποκλοπή περιλαμβάνει, ενδεικτικά και όχι εξαντλητικά, την ακρόαση, έλεγχο ή επιτήρηση του περιεχομένου των επικοινωνιών και την παροχή του περιεχομένου των δεδομένων είτε άμεσα, μέσω της πρόσβασης και χρήσης των συστημάτων πληροφοριών, είτε έμμεσα μέσω της χρήσης ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα.

(10) Τα κράτη μέλη θα πρέπει να προβλέπουν κυρώσεις για τις επιθέσεις κατά συστημάτων πληροφοριών. Οι εν λόγω κυρώσεις θα πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές και να περιλαμβάνουν φυλάκιση και/ή χρηματικές ποινές.

(11) Η παρούσα οδηγία προβλέπει ποινικές κυρώσεις, τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας. Τα κράτη μέλη θα πρέπει να μπορούν να καθορίζουν τι συνιστά περίπτωση ήσσονος σημασίας σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές. Η περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν, παραδείγματος χάριν, οι ζημίες που προκαλεί το αδίκημα και/ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον, όπως η ακεραιότητα ενός συστήματος υπολογιστών ή ηλεκτρονικών δεδομένων, ή η σωματική ακεραιότητα, τα δικαιώματά ή άλλα συμφέροντα ενός προσώπου, είναι αμελητέα ή τέτοιας φύσης ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης.

(12) Ο προσδιορισμός και η αναφορά απειλών και κινδύνων που προκύπτουν από επιθέσεις στον κυβερνοχώρο και της συναφούς ευπάθειας των συστημάτων πληροφοριών, είναι σχετικές με την αποτελεσματική πρόληψη και αντιμετώπιση των επιθέσεων στον κυβερνοχώρο και τη βελτίωση της ασφάλειας των συστημάτων πληροφοριών. Η παροχή κινήτρων για την αναφορά κενών ασφαλείας θα μπορούσε να συμβάλει προς τον σκοπό αυτό. Τα κράτη μέλη θα πρέπει να προσπαθούν να παρέχουν δυνατότητες για τη νομική ανίχνευση και αναφορά των κενών ασφαλείας.

(13) Είναι σκόπιμο να προβλεφθούν αυστηρότερες κυρώσεις όταν μια επίθεση κατά συστήματος πληροφοριών διαπράττεται από εγκληματική οργάνωση, όπως ορίζεται στην απόφαση-πλαίσιο 2008/841/ΔΕΥ του Συμβουλίου, της 24ης Οκτωβρίου 2008, για την καταπολέμηση του οργανωμένου εγκλήματος ([1]), όταν η επίθεση στον κυβερνοχώρο διαπράττεται σε μεγάλη κλίμακα και πλήττει έτσι σημαντικό αριθμό συστημάτων πληροφοριών, συμπεριλαμβανομένης της επίθεσης που έχει ως στόχο τη δημιουργία «botnet» ή όταν η επίθεση στον κυβερνοχώρο προκαλεί σοβαρές ζημίες, μεταξύ άλλων όταν η επίθεση εκτελείται μέσω «botnet». Είναι επίσης σκόπιμο να προβλεφθούν αυστηρότερες κυρώσεις, όταν η επίθεση διεξάγεται κατά υποδομής ζωτικής σημασίας των κρατών μελών ή της Ένωσης.

(14) Η θέσπιση αποτελεσματικών μέτρων κατά της κλοπής ταυτότητας και άλλων αδικημάτων σχετικών με την ταυτότητα αποτελεί ένα άλλο σημαντικό στοιχείο μιας ολοκληρωμένης προσέγγισης του εγκλήματος στον κυβερνοχώρο. Η τυχόν ανάγκη για δράση της Ένωσης σχετικά με αυτό το είδος εγκληματικής συμπεριφοράς θα μπορούσε επίσης να εξετάζεται στο πλαίσιο της αξιολόγησης της ανάγκης για μια συνολική οριζόντια πράξη της Ένωσης.

(15) Τα συμπεράσματα του Συμβουλίου της 27ης και 28ης Νοεμβρίου 2008 ανέφεραν ότι τα κράτη μέλη και η Επιτροπή θα πρέπει να αναπτύξουν νέα στρατηγική, λαμβάνοντας υπόψη το περιεχόμενο της σύμβασης του Συμβουλίου της Ευρώπης του 2001 για το έγκλημα στον κυβερνοχώρο. Η σύμβαση αυτή είναι το νομικό πλαίσιο αναφοράς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών. Η παρούσα οδηγία στηρίζεται στην εν λόγω σύμβαση. Η ολοκλήρωση της διαδικασίας επικύρωσης της εν λόγω σύμβασης από όλα τα κράτη μέλη, το συντομότερο δυνατόν, θα πρέπει να θεωρηθεί προτεραιότητα.

(16) Λαμβανομένων υπόψη των διαφορετικών τρόπων με τους οποίους μπορούν να πραγματοποιηθούν οι επιθέσεις και της ταχείας εξέλιξης του υλισμικού και του λογισμικού, η παρούσα οδηγία αναφέρεται σε εργαλεία που μπορούν να χρησιμοποιηθούν για τη διάπραξη των αδικημάτων που απαριθμούνται στην παρούσα οδηγία. Τέτοια εργαλεία μπορούν να περιλαμβάνουν το κακόβουλο λογισμικό —συμπεριλαμβανομένων των εργαλείων που μπορούν να δημιουργούν «botnet»— το οποίο χρησιμοποιείται για τη διάπραξη επιθέσεων στον κυβερνοχώρο. Ακόμη και όταν ένα τέτοιο εργαλείο είναι κατάλληλο ή ιδιαιτέρως κατάλληλο για τη διάπραξη ενός εκ των αδικημάτων που ορίζονται στην παρούσα οδηγία, είναι πιθανό το εργαλείο να έχει παραχθεί για νόμιμο σκοπό. Με αιτιολογία την ανάγκη να αποφευχθεί η ποινικοποίηση οσάκις τα εν λόγω εργαλεία παράγονται και διατίθενται στην αγορά για νόμιμους σκοπούς, όπως για τον έλεγχο της αξιοπιστίας των προϊόντων της τεχνολογίας πληροφοριών ή της ασφάλειας των συστημάτων πληροφοριών, εκτός από τη γενική απαίτηση της πρόθεσης, μια απαίτηση άμεσης πρόθεσης να χρησιμοποιήσει τα εργαλεία αυτά για να διαπράξει ένα ή περισσότερα εκ των αδικημάτων που ορίζονται στην παρούσα οδηγία, πρέπει επίσης να πληρούται.

(17) Η παρούσα οδηγία δεν αποδίδει ποινική ευθύνη όταν πληρούνται τα αντικειμενικά κριτήρια των αδικημάτων που ορίζονται στην παρούσα οδηγία, αλλά οι πράξεις διαπράττονται χωρίς εγκληματική πρόθεση, παραδείγματος χάριν όταν το πρόσωπο δεν γνωρίζει ότι απαγορεύεται η πρόσβαση ή στην περίπτωση εξουσιοδοτημένης δοκιμής ή προστασίας συστημάτων πληροφοριών, όπως όταν μια εταιρεία ή ένας πωλητής αναθέτει σε ένα πρόσωπο να ελέγξει την ισχύ του συστήματος ασφαλείας του. Στο πλαίσιο της παρούσας οδηγίας, συμβατικές υποχρεώσεις ή συμφωνίες να περιορισθεί η πρόσβαση σε συστήματα πληροφοριών με τη μέθοδο της πολιτικής χρηστών ή όρων παροχής υπηρεσίας, καθώς και εργατικές διαφορές όσον αφορά την πρόσβαση και τη χρήση συστημάτων πληροφοριών του εργοδότη για ιδιωτικούς σκοπούς, δεν θα πρέπει να συνεπάγονται ποινική ευθύνη, όταν η πρόσβαση, υπ' αυτές τις συνθήκες, θα κρινόταν απαγορευμένη και, συνεπώς, θα αποτελούσε τη μοναδική βάση για ποινική διαδικασία. Η παρούσα οδηγία δεν θίγει το δικαίωμα της πρόσβασης σε πληροφορίες, όπως ορίζεται στο εθνικό και στο ενωσιακό δίκαιο, ενώ την ίδια στιγμή δεν μπορεί να χρησιμεύσει ως αιτιολογία για παράνομη ή αυθαίρετη πρόσβαση σε πληροφορίες.

([1]) ΕΕ L 300 της 11.11.2008, σ. 42.

(18) Οι επιθέσεις στον κυβερνοχώρο μπορούν να διευκολύνονται από διάφορες περιστάσεις, όπως όταν ο δράστης έχει πρόσβαση στα συστήματα ασφαλείας που ενυπάρχουν στα προσβαλλόμενα συστήματα πληροφοριών, μέσα στο πλαίσιο των καθηκόντων του. Στο πλαίσιο του εθνικού δικαίου, τέτοιες περιστάσεις θα πρέπει να λαμβάνονται υπόψη καταλλήλως κατά τη διεξαγωγή ποινικών διαδικασιών.

(19) Τα κράτη μέλη θα πρέπει να προβλέπουν στο εθνικό τους δίκαιο επιβαρυντικές περιστάσεις, σύμφωνα με τους εφαρμοστέους κανόνες περί επιβαρυντικών περιστάσεων που προβλέπονται στα νομικά τους συστήματα. Θα πρέπει να μεριμνούν ώστε αυτές οι επιβαρυντικές περιστάσεις να μπορούν να εξετάζονται από τους δικαστές κατά την επιμέτρηση της ποινής των δραστών. Εμπίπτει στη διακριτική ευχέρεια του δικαστή να αξιολογεί τις εν λόγω περιστάσεις, μαζί με τα άλλα γεγονότα της συγκεκριμένης υπόθεσης.

(20) Η παρούσα οδηγία δεν διέπει τις προϋποθέσεις κατά την άσκηση δικαιοδοσίας για οποιοδήποτε από τα αδικήματα που αναφέρονται σε αυτή, όπως η κατάθεση από το θύμα στον τόπο όπου διαπράχθηκε το αδίκημα, η καταγγελία από το κράτος στο οποίο διαπράχθηκε το αδίκημα ή η μη άσκηση δίωξης σε βάρος του δράστη στον τόπο όπου διαπράχθηκε το αδίκημα.

(21) Στο πλαίσιο της παρούσας οδηγίας, κράτη και δημόσιοι φορείς, παραμένουν πλήρως υποχρεωμένα να εγγυώνται τον σεβασμό των ανθρώπινων δικαιωμάτων και των θεμελιωδών ελευθεριών, σύμφωνα με τις υπάρχουσες διεθνείς υποχρεώσεις.

(22) Η παρούσα οδηγία ενισχύει τη σημασία των δικτύων, όπως το δίκτυο των σημείων επαφής της ομάδας G8 ή του Συμβουλίου της Ευρώπης, που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες την εβδομάδα. Τα εν λόγω σημεία επαφής θα πρέπει να είναι σε θέση να προσφέρουν αποτελεσματική βοήθεια, παραδείγματος χάριν διευκολύνοντας την ανταλλαγή διαθέσιμων σχετικών πληροφοριών και την παροχή τεχνικών συμβουλών ή νομικών πληροφοριών για έρευνες ή διαδικασίες σχετικές με ποινικά αδικήματα που συνδέονται με συστήματα πληροφοριών και συναφή δεδομένα που αφορούν το κράτος μέλος το οποίο υποβάλλει την αίτηση. Προκειμένου να διασφαλισθεί η ομαλή λειτουργία των δικτύων, κάθε σημείο επαφής θα πρέπει να διαθέτει την ικανότητα να επικοινωνεί με τα σημεία επαφής των άλλων κρατών μελών, βάσει επείγουσας διαδικασίας, με την υποστήριξη, μεταξύ άλλων, εκπαιδευμένου και εξοπλισμένου προσωπικού. Δεδομένης της ταχύτητας με την οποία μπορούν να πραγματοποιηθούν επιθέσεις στον κυβερνοχώρο μεγάλης κλίμακας, τα κράτη μέλη θα πρέπει να είναι σε θέση να ανταποκρίνονται αμέσως σε επείγουσες αιτήσεις που προέρχονται από το εν λόγω δίκτυο σημείων επαφής. Στις περιπτώσεις αυτές, μπορεί να είναι σκόπιμο η αίτηση πληροφοριών να συνοδεύεται από τηλεφωνικό αριθμό επαφής, ώστε να διασφαλίζεται ότι η αίτηση θα διεκπεραιώνεται σύντομα από το κράτος μέλος στο οποίο υποβάλλεται η αίτηση και να δίνεται απάντηση εντός οκτώ ωρών.

(23) Η συνεργασία μεταξύ των δημόσιων αρχών αφενός, και του ιδιωτικού τομέα και της κοινωνίας των πολιτών αφετέρου, έχει μεγάλη σημασία για την αποτροπή και την καταπολέμηση των επιθέσεων κατά των συστημάτων πληροφοριών. Είναι αναγκαίο να ενισχυθεί και να βελτιωθεί η συνεργασία μεταξύ των παρόχων υπηρεσιών, παραγωγών, οργάνων επιβολής του νόμου και δικαστικών αρχών, με εκ παραλλήλου πλήρη σεβασμό του κράτους δικαίου. Τέτοια συνεργασία θα μπορούσε να περιλαμβάνει υποστήριξη από παρόχους υπηρεσιών υπό μορφή βοήθειας για τη διατήρηση πιθανών αποδεικτικών στοιχείων, παροχής στοιχείων που βοηθούν στον εντοπισμό των δραστών και, ως τελευταία επιλογή, πλήρους ή μερικής παύσης της λειτουργίας παρανόμων συστημάτων ή λειτουργιών που έχουν δεχτεί επίθεση ή έχουν χρησιμοποιηθεί για παράνομους σκοπούς, σύμφωνα με το εθνικό δίκαιο και τις εθνικές πρακτικές. Τα κράτη μέλη θα πρέπει επίσης να εξετάσουν τη δημιουργία δικτύων εταιρικής σχέσης και συνεργασίας με τους παρόχους υπηρεσιών και τους παραγωγούς για την ανταλλαγή πληροφοριών σε σχέση με τα αδικήματα που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

(24) Υπάρχει ανάγκη συλλογής συγκρίσιμων δεδομένων σχετικά με τα αδικήματα που ορίζονται στην παρούσα οδηγία. Τα σχετικά δεδομένα θα πρέπει να τίθενται στη διάθεση των αρμόδιων ειδικευμένων οργανισμών και φορέων της Ένωσης, όπως η Ευρωπόλ και ο ENISA, σύμφωνα με τα καθήκοντά τους και τις ανάγκες πληροφόρησης, ώστε να αποκτούν μια πιο ολοκληρωμένη εικόνα του προβλήματος της εγκληματικότητας στον κυβερνοχώρο και την ασφάλεια δικτύων και πληροφοριών στο επίπεδο της Ένωσης, συμβάλλοντας έτσι στη διαμόρφωση πιο αποτελεσματικής απάντησης. Τα κράτη μέλη θα πρέπει να υποβάλλουν πληροφορίες σχετικά με το modus operandi που χρησιμοποιείται από τους δράστες στην Ευρωπόλ και το Ευρωπαϊκό Κέντρο Ηλεκτρονικού εγκλήματος ώστε να προβαίνουν σε αξιολογήσεις περί των απειλών και στρατηγικές αναλύσεις του εγκλήματος στον κυβερνοχώρο σύμφωνα με την απόφαση 2009/371/ΔΕΥ του Συμβουλίου, της 6ης Απριλίου 2009, για την ίδρυση Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Ευρωπόλ) [1]. Η παροχή πληροφοριών μπορεί να διευκολύνει την καλύτερη κατανόηση των σημερινών και μελλοντικών απειλών και να συμβάλει έτσι στη λήψη καταλληλότερων και στοχευμένων αποφάσεων για την καταπολέμηση και την πρόληψη των επιθέσεων κατά των συστημάτων πληροφοριών.

(25) Η Επιτροπή θα πρέπει να υποβάλει έκθεση σχετικά με την εφαρμογή της παρούσας οδηγίας καθώς και τις αναγκαίες νομοθετικές προτάσεις οι οποίες θα μπορούσαν να οδηγήσουν στη διεύρυνση του πεδίου εφαρμογής της, λαμβάνοντας υπόψη τυχόν εξελίξεις στον τομέα του εγκλήματος στον κυβερνοχώρο. Οι εξελίξεις αυτές μπορούν να περιλαμβάνουν τεχνολογικές εξελίξεις, παραδείγματος χάριν αυτές που επιτρέπουν την αποτελεσματικότερη επιβολή της εφαρμογής του νόμου όσον αφορά τις επιθέσεις εναντίον συστημάτων πληροφοριών ή διευκολύνουν την πρόληψη ή την άμβλυνση των επιπτώσεων αυτών των επιθέσεων. Για τον σκοπό αυτό, η Επιτροπή θα πρέπει να λαμβάνει υπόψη τις διαθέσιμες αναλύσεις και εκθέσεις που συντάσσονται από τους αρμόδιους φορείς και ιδίως την Ευρωπόλ και τον ENISA.

(26) Προκειμένου να καταπολεμηθεί αποτελεσματικά το έγκλημα στον κυβερνοχώρο, είναι αναγκαίο να αυξηθεί η ανθεκτικότητα των συστημάτων πληροφοριών με τη λήψη των ενδεδειγμένων μέτρων για να προστατεύονται αποτελεσματικότερα από επιθέσεις στον κυβερνοχώρο. Τα κράτη μέλη θα πρέπει να λαμβάνουν τα απαραίτητα μέτρα για την προστασία των πληροφοριακών τους συστημάτων που αποτελούν μέρος των υποδομών ζωτικής σημασίας από επιθέσεις στον κυβερνοχώρο, ως μέρος των οποίων θα πρέπει να εξετάζουν

[1] ΕΕ L 121 της 15.5.2009, σ. 37.

την προστασία των πληροφοριακών τους συστημάτων και των συναφών δεδομένων. Η εξασφάλιση κατάλληλου επιπέδου προστασίας και ασφάλειας των συστημάτων πληροφοριών από νομικά πρόσωπα, παραδείγματος χάριν σε συνάρτηση με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό σύμφωνα με την ισχύουσα νομοθεσία της Ένωσης περί ιδιωτικής ζωής, ηλεκτρονικών επικοινωνιών και προστασίας δεδομένων, αποτελεί ουσιώδες μέρος μιας συνεκτικής προσέγγισης για την αποτελεσματική καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Θα πρέπει να παρέχονται κατάλληλα επίπεδα προστασίας έναντι ευλόγως εντοπίσιμων απειλών και ευπαθειών σύμφωνα με την «τελευταία λέξη» της τεχνικής για συγκεκριμένους τομείς και συγκεκριμένες καταστάσεις επεξεργασίας δεδομένων. Το κόστος και ο φόρτος της εν λόγω προστασίας θα πρέπει να αναλογούν με τη βλάβη που είναι πιθανό να προκαλέσει μια επίθεση στον κυβερνοχώρο στα θύματά της. Τα κράτη μέλη παροτρύνονται να προβλέπουν σχετικά μέτρα αναλαμβάνοντας υποχρεώσεις στο πλαίσιο του εθνικού τους δικαίου στις περιπτώσεις που ένα νομικό πρόσωπο σαφώς δεν έχει προβλέψει κατάλληλο επίπεδο προστασίας ενάντια σε επιθέσεις στον κυβερνοχώρο.

(27) Τα σημαντικά κενά και οι διαφορές ανάμεσα στα δίκαια και τις ποινικές διαδικασίες των κρατών μελών στον τομέα των επιθέσεων κατά των συστημάτων πληροφοριών μπορούν να παρεμποδίσουν την καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας και να περιπλέξουν την αποτελεσματική αστυνομική και δικαστική συνεργασία στον τομέα αυτό. Ο διεθνικός και χωρίς σύνορα χαρακτήρας των σύγχρονων συστημάτων πληροφοριών σημαίνει ότι, οι επιθέσεις κατά των συστημάτων αυτών, έχουν διασυνοριακή διάσταση, υπογραμμίζοντας έτσι την επείγουσα ανάγκη να ληφθούν περαιτέρω μέτρα για την προσέγγιση του ποινικού δικαίου στον συγκεκριμένο τομέα. Επιπλέον, ο συντονισμός της δίωξης όσον αφορά επιθέσεις κατά συστημάτων πληροφοριών θα πρέπει να διευκολυνθεί με την προσήκουσα υλοποίηση και εφαρμογή της οδηγίας-πλαισίου 2009/948/ΔΕΥ του Συμβουλίου, της 30ής Νοεμβρίου 2009, για την πρόληψη και τον διακανονισμό συγκρούσεων δικαιοδοσίας σε ποινικές υποθέσεις ([1]). Τα κράτη μέλη, σε συνεργασία με την Ένωση, θα πρέπει επίσης να επιδιώξουν να βελτιώσουν τη διεθνή συνεργασία που αφορά την ασφάλεια των συστημάτων πληροφοριών και των υπολογιστικών δικτύων και δεδομένων. Σε κάθε διεθνή συμφωνία που άπτεται της ανταλλαγής δεδομένων θα πρέπει να λαμβάνεται δεόντως υπόψη η ασφάλεια της μεταφοράς και της αποθήκευσης δεδομένων.

(28) Η βελτιωμένη συνεργασία μεταξύ των αρμόδιων οργάνων επιβολής του νόμου και των δικαστικών αρχών, στο σύνολο της Ένωσης, είναι ουσιώδους σημασίας για την αποτελεσματική καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Στο πλαίσιο αυτό, θα πρέπει να ενθαρρυνθεί η επιτάχυνση των προσπαθειών να παρασχεθεί η κατάλληλη κατάρτιση στις αρμόδιες αρχές, προκειμένου να αυξηθεί η κατανόησή τους για το έγκλημα στον κυβερνοχώρο και τις επιπτώσεις του και να ενισχυθεί η συνεργασία και η ανταλλαγή βέλτιστων πρακτικών, παραδείγματος χάριν μέσω των αρμόδιων ειδικευμένων οργανισμών και φορέων της Ένωσης. Η κατάρτιση αυτή θα πρέπει, μεταξύ άλλων, να στοχεύει στην αύξηση της ευαισθητοποίησης σχετικά με τα διάφορα εθνικά νομικά συστήματα, τις ενδεχόμενες νομικές και τεχνικές προκλήσεις που προκύπτουν στις ποινικές έρευνες και την κατανομή αρμοδιοτήτων μεταξύ των αρμόδιων εθνικών αρχών.

(29) Η παρούσα οδηγία σέβεται τα ανθρώπινα δικαιώματα και τις θεμελιώδεις ελευθερίες και τηρεί τις αρχές που αναγνωρίζονται, ιδίως από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και την Ευρωπαϊκή σύμβαση περί προάσπισης των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, συμπεριλαμβανομένων της προστασίας των δεδομένων προσωπικού χαρακτήρα, της ιδιωτικής ζωής, της ελευθερίας έκφρασης και πληροφόρησης, του δικαιώματος δίκαιης δίκης, του τεκμηρίου αθωότητας και των δικαιωμάτων της υπεράσπισης, καθώς και των αρχών της νομιμότητας και αναλογικότητας των ποινικών αδικημάτων και κυρώσεων. Ειδικότερα, η παρούσα οδηγία επιδιώκει να εξασφαλίσει την πλήρη τήρηση των εν λόγω δικαιωμάτων και των αρχών και πρέπει να εφαρμόζεται αναλόγως.

(30) Η προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί θεμελιώδες δικαίωμα σύμφωνα με το άρθρο 16 παράγραφος 1 ΣΛΕΕ και το άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Συνεπώς, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της εφαρμογής της παρούσας οδηγίας θα πρέπει να συμμορφώνεται πλήρως με το σχετικό δίκαιο της Ένωσης περί προστασίας δεδομένων.

(31) Σύμφωνα με το άρθρο 3 του πρωτοκόλλου για τη θέση του Ηνωμένου Βασιλείου και της Ιρλανδίας όσον αφορά τον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης, το οποίο έχει προσαρτηθεί στη Συνθήκη για την Ευρωπαϊκή Ένωση και στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, τα εν λόγω κράτη μέλη γνωστοποίησαν την επιθυμία τους να συμμετάσχουν στην έκδοση και την εφαρμογή της παρούσας οδηγίας.

(32) Σύμφωνα με τα άρθρα 1 και 2 του πρωτοκόλλου σχετικά με τη θέση της Δανίας, το οποίο έχει προσαρτηθεί στη Συνθήκη για την Ευρωπαϊκή Ένωση και στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, η Δανία δεν συμμετέχει στην έκδοση της παρούσας οδηγίας και δεν δεσμεύεται από αυτή ούτε υπόκειται στην εφαρμογή της.

(33) Δεδομένου ότι οι στόχοι της παρούσας οδηγίας —ήτοι να υπόκεινται οι επιθέσεις κατά των συστημάτων πληροφοριών, σε όλα τα κράτη μέλη, σε αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις και να βελτιωθεί και να ενθαρρυνθεί η συνεργασία μεταξύ δικαστικών και άλλων αρμοδίων αρχών—, δεν μπορούν να επιτευχθούν επαρκώς από τα κράτη μέλη, και δύνανται, συνεπώς, λόγω της κλίμακας και των αποτελεσμάτων τους, να επιτευχθούν καλύτερα στο επίπεδο της Ένωσης, η Ένωση δύναται να θεσπίζει μέτρα, σύμφωνα με την αρχή της επικουρικότητας, όπως ορίζεται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας, όπως ορίζεται στο άρθρο αυτό, η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών.

(34) Σκοπός της παρούσας οδηγίας είναι η τροποποίηση και επέκταση των διατάξεων της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, της 24ης Φεβρουαρίου 2005, για τις επιθέσεις κατά των συστημάτων πληροφοριών ([2]). Επειδή οι τροποποιήσεις που πρέπει να επέλθουν είναι ουσιαστικές ως προς τον αριθμό και τη φύση τους, η απόφαση-πλαίσιο 2005/222/ΔΕΥ θα πρέπει, για λόγους σαφήνειας, να αντικατασταθεί στο σύνολό της σε σχέση με τα κράτη μέλη που συμμετέχουν στην έκδοση της παρούσας οδηγίας,

([1]) ΕΕ L 328 της 15.12.2009, σ. 42.

([2]) ΕΕ L 69 της 16.3.2005, σ. 67.

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

Άρθρο 1

Αντικείμενο

Η παρούσα οδηγία θεσπίζει ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των κυρώσεων στον τομέα των επιθέσεων κατά των συστημάτων πληροφοριών. Σκοπεύει επίσης να διευκολύνει την πρόληψη των αδικημάτων αυτών και να βελτιώσει τη συνεργασία μεταξύ δικαστικών και άλλων αρμόδιων αρχών.

Άρθρο 2

Ορισμοί

Για τους σκοπούς της παρούσας οδηγίας, εφαρμόζονται οι ακόλουθοι ορισμοί:

α) «σύστημα πληροφοριών»: 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·

β) «ηλεκτρονικά δεδομένα»: η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία·

γ) «νομικό πρόσωπο»: κάθε οντότητα που έχει το καθεστώς του νομικού προσώπου βάσει του εφαρμοστέου δικαίου, αλλά δεν περιλαμβάνει κράτη, ή δημόσιους φορείς κατά την άσκηση της εξουσίας τους ή δημόσιους διεθνείς οργανισμούς·

δ) «χωρίς δικαίωμα»: η αναφερόμενη στην παρούσα οδηγία συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου.

Άρθρο 3

Παράνομη πρόσβαση σε συστήματα πληροφοριών

Τα κράτη μέλη λαμβάνουν 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.

Άρθρο 4

Παράνομη παρεμβολή σε σύστημα

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, 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.

Άρθρο 5

Παράνομη παρεμβολή σε δεδομένα

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για 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.

Άρθρο 6

Παράνομη υποκλοπή

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών 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.

Άρθρο 7

Εργαλεία που χρησιμοποιούνται για τη διάπραξη των αδικημάτων

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλουθων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε εκ των αδικημάτων 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 εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6·

β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών.

Άρθρο 8

Ηθική αυτουργία, υποβοήθηση και συνέργεια και απόπειρα

1. Τα κράτη μέλη εξασφαλίζουν ότι η ηθική αυτουργία, ή η υποβοήθηση και η συνέργεια, προς διάπραξη αδικήματος που αναφέρεται στα άρθρα 3 έως 7 τιμωρείται ως ποινικό αδίκημα.

2. Τα κράτη μέλη εξασφαλίζουν ότι η απόπειρα διάπραξης αδικήματος που αναφέρεται στα άρθρα 4 και 5 να τιμωρείται ως ποινικό αδίκημα.

Άρθρο 9

Κυρώσεις

1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8 τιμωρούνται με αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις.

2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7 τιμωρούνται με στερητική της ελευθερίας ποινή, το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον δύο έτη, τουλάχιστον για περιπτώσεις που δεν είναι ήσσονος σημασίας.

3. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, οσάκις τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται εκ προθέσεως, και εφόσον έχει πληγεί σημαντικός αριθμός συστημάτων πληροφοριών μέσω της χρήσης εργαλείου αναφερομένου στο άρθρο 7, το οποίο έχει σχεδιασθεί ή

προσαρμοσθεί πρωτίστως για τον σκοπό αυτό, τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον τρία έτη.

4. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον πέντε έτη, εφόσον:

α) διαπράττονται στο πλαίσιο εγκληματικής οργάνωσης κατά την έννοια της απόφασης-πλαισίου 2008/841/ΔΕΥ, ανεξαρτήτως της κύρωσης που ορίζεται σε αυτή·

β) προκαλούν σημαντικές ζημίες, ή

γ) διαπράττονται κατά συστήματος πληροφοριών που αποτελεί μέρος ζωτικής σημασίας υποδομής.

5. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν ότι εφόσον τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται με υφαρπαγή δεδομένων προσωπικού χαρακτήρα άλλου προσώπου, προκειμένου να αποκτηθεί η εμπιστοσύνη τρίτων, και, ως εκ τούτου, προκαλούν ζημία στον νόμιμο δικαιούχο της ταυτότητας, το γεγονός αυτό μπορεί, σύμφωνα με το εθνικό δίκαιο, να εκλαμβάνεται ως επιβαρυντική περίσταση, εκτός εάν οι εν λόγω περιστάσεις καλύπτονται ήδη από άλλο αδίκημα που τιμωρείται σύμφωνα με το εθνικό δίκαιο.

Άρθρο 10

Ευθύνη νομικών προσώπων

1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι νομικά πρόσωπα είναι δυνατόν να υπέχουν ευθύνη για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8 τα οποία έχουν τελεσθεί προς όφελός τους από οιοδήποτε πρόσωπο, ενεργώντας είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου και το οποίο κατέχει ιθύνουσα θέση εντός του νομικού αυτού προσώπου, βάσει μιας από τις ακόλουθες εξουσίες:

α) εξουσία εκπροσώπησης του νομικού προσώπου·

β) εξουσία λήψης αποφάσεων για λογαριασμό του νομικού προσώπου·

γ) εξουσία άσκησης ελέγχου εντός του νομικού προσώπου.

2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι νομικά πρόσωπα μπορούν να θεωρούνται υπεύθυνα οσάκις η έλλειψη εποπτείας ή ελέγχου εκ μέρους ενός από τα πρόσωπα που αναφέρονται στην παράγραφο 1 έχει επιτρέψει τη διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 8 προς όφελος του εν λόγω νομικού προσώπου από πρόσωπο που τελεί υπό την εξουσία του.

3. Η ευθύνη των νομικών προσώπων δυνάμει των παραγράφων 1 και 2 δεν αποκλείει την ποινική δίωξη φυσικών προσώπων που είναι αυτουργοί ή ηθικοί αυτουργοί ή συνεργοί στη διάπραξη αδικημάτων που αναφέρονται στα άρθρα 3 έως 8.

Άρθρο 11

Κυρώσεις κατά νομικών προσώπων

1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι το νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 10 παράγραφος 1 τιμωρείται με αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις, στις οποίες περιλαμβάνονται χρηματικές ποινές ή πρόστιμα και οι οποίες μπορούν να περιλαμβάνουν και άλλες κυρώσεις, όπως:

α) αποκλεισμό 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.

2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι το νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 10 παράγραφος 2 τιμωρείται με αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις ή άλλα μέτρα.

Άρθρο 12

Δικαιοδοσία

1. Τα κράτη μέλη θεμελιώνουν τη δικαιοδοσία τους για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8, εφόσον το αδίκημα έχει διαπραχθεί:

α) εν όλω ή εν μέρει στο έδαφος τους· ή

β) από υπήκοό τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται αδίκημα στον τόπο όπου έχει διαπραχθεί.

2. Κράτος μέλος, κατά τη θεμελίωση της δικαιοδοσίας του σύμφωνα με την παράγραφο 1 στοιχείο α), εξασφαλίζει ότι διαθέτει δικαιοδοσία, οσάκις:

α) ο δράστης διέπραξε το αδίκημα, όταν ευρίσκετο στο έδαφός του, ανεξάρτητα από το εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός του· ή

β) το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδαφός του ανεξάρτητα από το εάν όταν ο δράστης διέπραξε το αδίκημα ευρίσκετο στο έδαφός του.

3. Το κράτος μέλος ενημερώνει σχετικά την Επιτροπή οσάκις αποφασίζει να θεμελιώσει δικαιοδοσία για αδίκημα που αναφέρεται στα άρθρα 3 έως 8, το οποίο διαπράττεται εκτός του εδάφους του, οσάκις, μεταξύ άλλων:

α) ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφος του, ή

β) το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφος του.

Άρθρο 13

Ανταλλαγή πληροφοριών

1. Για τους σκοπούς της ανταλλαγής πληροφοριών σχετικά με τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8, τα κράτη μέλη εξασφαλίζουν ότι διαθέτουν ένα λειτουργικό εθνικό σημείο επαφής και κάνουν χρήση του υφιστάμενου δικτύου επιχειρησιακών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας. Τα κράτη μέλη εξασφαλίζουν επίσης ότι διαθέτουν διαδικασίες ώστε, σε περιπτώσεις επειγουσών αιτήσεων συνδρομής, η αρμόδια αρχή να μπορεί να δηλώσει, εντός οκτώ ωρών από την παραλαβή, τουλάχιστον εάν θα απαντήσει στην αίτηση, καθώς και τη μορφή και τον εκτιμώμενο χρόνο της απάντησης αυτής.

2. Τα κράτη μέλη ενημερώνουν την Επιτροπή για το σημείο επαφής που έχουν ορίσει κατά τα αναφερόμενα στην παράγραφο 1. Η Επιτροπή διαβιβάζει αυτές τις πληροφορίες στα άλλα κράτη μέλη και τους αρμόδιους ειδικευμένους οργανισμούς και φορείς της Ένωσης.

3. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να εξασφαλίσουν ότι διατίθενται οι κατάλληλοι δίαυλοι αναφοράς προκειμένου να διευκολυνθεί η υποβολή αναφορών χωρίς αδικαιολόγητη καθυστέρηση σχετικά με αδικήματα που αναφέρονται στα άρθρα 3 έως 6 στις αρμόδιες εθνικές τους αρχές.

Άρθρο 14

Παρακολούθηση και στατιστικές

1. Τα κράτη μέλη εξασφαλίζουν ότι ένα σύστημα ευρίσκεται σε ετοιμότητα για την καταγραφή, την παραγωγή και την παροχή στατιστικών στοιχείων για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7.

2. Τα αναφερόμενα στην παράγραφο 1 στατιστικά στοιχεία καλύπτουν κατ' ελάχιστον τα υφιστάμενα δεδομένα ως προς τον αριθμό των αδικημάτων που αναφέρονται στα άρθρα 3 έως 7, τα οποία καταγράφονται από τα κράτη μέλη, καθώς και τον αριθμό των προσώπων τα οποία διώχθηκαν και καταδικάστηκαν για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7.

3. Τα κράτη μέλη διαβιβάζουν στην Επιτροπή τα στοιχεία που συγκεντρώνουν σύμφωνα με το παρόν άρθρο. Η Επιτροπή μεριμνά ώστε να δημοσιεύεται και να υποβάλλεται στους αρμόδιους ειδικευμένους οργανισμούς και φορείς της Ένωσης συγκεντρωτική επισκόπηση αυτών των στατιστικών εκθέσεων.

Άρθρο 15

Αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ

Η απόφαση-πλαίσιο 2005/222/ΔΕΥαντικαθίσταται όσον αφορά τα κράτη μέλη που συμμετέχουν στην έκδοση της παρούσας οδηγίας, με την επιφύλαξη των υποχρεώσεων των κρατών μελών ως προς τις προθεσμίες μεταφοράς της απόφασης-πλαισίου στο εθνικό τους δίκαιο.

Όσον αφορά τα κράτη μέλη που συμμετέχουν στην έκδοση της παρούσας οδηγίας, οι παραπομπές στην απόφαση-πλαίσιο 2005/222/ΔΕΥ θεωρούνται ως παραπομπές στην παρούσα οδηγία.

Άρθρο 16

Μεταφορά στο εθνικό δίκαιο

1. Τα κράτη μέλη θέτουν σε ισχύ τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για συμμορφωθούν με την παρούσα οδηγία έως τις 4 Σεπτεμβρίου 2015.

2. Τα κράτη μέλη διαβιβάζουν στην Επιτροπή το κείμενο των μέτρων με τα οποία μεταφέρουν στο εθνικό τους δίκαιο τις υποχρεώσεις που υπέχουν δυνάμει της παρούσας οδηγίας.

3. Τα εν λόγω μέτρα, όταν θεσπίζονται από τα κράτη μέλη, περιέχουν αναφορά στην παρούσα οδηγία ή συνοδεύονται από παρόμοια αναφορά κατά την επίσημη δημοσίευσή τους. Ο τρόπος πραγματοποίησης της αναφοράς αυτής καθορίζεται από τα κράτη μέλη.

Άρθρο 17

Υποβολή εκθέσεων

Η Επιτροπή υποβάλλει, μέχρι τις 4 Σεπτεμβρίου 2017, έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο με την οποία αξιολογείται κατά πόσον τα κράτη μέλη έχουν λάβει τα αναγκαία μέτρα για να συμμορφωθούν προς την παρούσα οδηγία, συνοδευόμενη, εφόσον απαιτείται, από νομοθετικές προτάσεις. Η Επιτροπή λαμβάνει επίσης υπόψη τις τεχνικές και νομικές εξελίξεις στον τομέα του εγκλήματος στον κυβερνοχώρο, ιδίως σε σχέση με το πεδίο εφαρμογής της παρούσας οδηγίας.

Άρθρο 18

Έναρξη ισχύος

Η παρούσα οδηγία αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Άρθρο 19

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη σύμφωνα με τις Συνθήκες.

Βρυξέλλες, 12 Αυγούστου 2013.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Ο Πρόεδρος	*Ο Πρόεδρος*
M. SCHULZ	L. LINKEVIČIUS