ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ

ΥΠΑΤΗ ΕΚΠΡΟΣΩΠΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΘΕΜΑΤΑ ΚΟΙΝΗΣ ΕΞΩΤΕΡΙΚΗΣ ΠΟΛΙΤΙΚΗΣ ΚΑΙ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Βρυξέλλες, 7.2.2013
JOIN(2013) 1 final

ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο

Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο

ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο

Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο

1. ΕΙΣΑΓΩΓΗ

1.1. Πλαίσιο

Κατά τις δύο τελευταίες δεκαετίες, το διαδίκτυο και γενικότερα ο κυβερνοχώρος είχαν τεράστια επίδραση όλα τα τμήματα της κοινωνίας. Η καθημερινή μας ζωή, τα θεμελιώδη δικαιώματα, οι κοινωνικές αλληλεπιδράσεις και οι οικονομίες εξαρτώνται από την ομαλή λειτουργία της τεχνολογίας πληροφοριών και επικοινωνιών. Ο ανοικτός και ελεύθερος κυβερνοχώρος προώθησε την πολιτική και κοινωνική ένταξη παγκοσμίως, κατάργησε τα σύνορα μεταξύ χωρών, κοινοτήτων και πολιτών και κατέστησε δυνατή την αλληλεπίδραση και την κοινή χρήση πληροφοριών και ιδεών ανά την υφήλιο, εξασφάλισε ένα βήμα ελευθερίας της έκφρασης και άσκησης των θεμελιωδών δικαιωμάτων και ενδυνάμωσε τους λαϊκούς αγώνες για δημοκρατικότερες και δικαιότερες κοινωνίες – με τον πλέον εντυπωσιακό τρόπο κατά την Αραβική Άνοιξη.

Για να παραμείνει ανοικτός και ελεύθερος ο κυβερνοχώρος, πρέπει να ισχύσουν διαδικτυακά τα ίδια πρότυπα, αρχές και αξίες που προβάλλει η ΕΕ και εκτός διαδικτύου. Τα θεμελιώδη δικαιώματα, η δημοκρατία και το κράτος δικαίου πρέπει να προστατευθούν και στον κυβερνοχώρο. Η ελευθερία και η ευημερία μας εξαρτώνται όλο και περισσότερο από ένα σταθερό και καινοτόμο διαδίκτυο, το οποίο θα συνεχίσει να ανθίζει εάν η ανάπτυξή του προωθείται από την καινοτομία του ιδιωτικού τομέα και από την κοινωνία των πολιτών. Όμως η διαδικτυακή ελευθερία απαιτεί επίσης ασφάλεια και προστασία από έκνομες ενέργειες. Ο κυβερνοχώρος πρέπει να προστατευτεί από συμβάντα, κακόβουλες δραστηριότητες και καταχρήσεις· και οι κυβερνήσεις θα διαδραματίσουν σημαντικό ρόλο όσον αφορά την εξασφάλιση ελεύθερου και ασφαλούς κυβερνοχώρου. Οι κυβερνήσεις έχουν αρκετά καθήκοντα: να διασφαλίσουν την πρόσβαση και το άνοιγμα, να σεβαστούν και να προστατεύσουν τα θεμελιώδη δικαιώματα διαδικτυακά και να διατηρήσουν την αξιοπιστία και την διαλειτουργικότητα του διαδικτύου. Ωστόσο, ο ιδιωτικός τομέας κατέχει και εξασφαλίζει τη λειτουργία σημαντικών τμημάτων του κυβερνοχώρου και κατά συνέπεια προκειμένου να πετύχει κάθε πρωτοβουλία στον εν λόγω τομέα οφείλει να αναγνωρίσει τον ηγετικό του ρόλο.

Οι τεχνολογίες πληροφοριών και επικοινωνιών έχουν καταστεί η ραχοκοκαλιά της οικονομικής μας μεγέθυνσης και αποτελούν πόρο κρίσιμης σημασίας από τον οποίο εξαρτώνται όλοι οι κλάδοι της οικονομίας. Αποτελούν τη βάση των πολύπλοκων συστημάτων που στηρίζουν τη λειτουργία των οικονομιών μας σε κλάδους ζωτικής σημασίας, όπως ο χρηματοπιστωτικός, η υγεία, η ενέργεια και οι μεταφορές· παράλληλα πολλά επιχειρηματικά μοντέλα στηρίζονται στην αδιάλειπτη διαθεσιμότητα του διαδικτύου και στην απρόσκοπτη λειτουργία των συστημάτων πληροφορικής.

Με την ολοκλήρωση της ψηφιακής εσωτερικής αγοράς της, η Ευρώπη θα μπορούσε να αυξήσει το ΑΕΠ της κατά σχεδόν 500 δισ. ευρώ ετησίως[1]· ποσό που αντιστοιχεί σε 1.000 ευρώ ανά άτομο. Προκειμένου να απογειωθεί η χρήση των νέων συνδεδεμένων τεχνολογιών που περιλαμβάνουν τις ηλε-πληρωμές, το υπολογιστικό νέφος ή την επικοινωνία μεταξύ μηχανών[2], οι πολίτες χρειάζονται αξιοπιστία και εμπιστοσύνη. Δυστυχώς, από μια έρευνα του Ευρωβαρομέτρου το 2012[3] προέκυψε ότι σχεδόν το ένα τρίτο των Ευρωπαίων δεν εμπιστεύονται την ικανότητά τους να χρησιμοποιήσουν το διαδίκτυο για τραπεζικές συναλλαγές ή για αγορές. Η συντριπτική πλειοψηφία δήλωσαν επίσης ότι αποφεύγουν να κοινοποιούν προσωπικά δεδομένα στο διαδίκτυο λόγω επιφυλάξεων όσον αφορά την ασφάλεια. Ανά την ΕΕ, περισσότεροι από ένας στους δέκα χρήστες του διαδικτύου έχουν πέσει θύματα διαδικτυακής απάτης.

Τα τελευταία χρόνια έχει αποδειχτεί ότι παράλληλα με το τεράστιο όφελος που επιφέρει, ο ψηφιακός κόσμος είναι και ευάλωτος. Τα σχετικά με την ασφάλεια συμβάντα στον κυβερνοχώρο[4], ανεξάρτητα αν είναι εκ προθέσεως ή εξ αμελείας, αυξάνονται με ανησυχητικό ρυθμό και ενδέχεται να διαταράξουν την παροχή βασικών υπηρεσιών που θεωρούμε αυτονόητες, όπως η ύδρευση, η ιατρική περίθαλψη και η παροχή ηλεκτρικής ενέργειας ή κινητών υπηρεσιών. Οι απειλές είναι δυνατόν να προέρχονται από διάφορες πηγές – εγκληματικές, πολιτικά υποκινούμενες, τρομοκρατικές ή κρατικά υποκινούμενες επιθέσεις, καθώς και φυσικές καταστροφές και ακούσια σφάλματα.

Η οικονομία της ΕΕ επηρεάζεται ήδη από δραστηριότητες ηλεκτρονικού εγκλήματος[5] κατά του ιδιωτικού τομέα και των μεμονωμένων ατόμων. Οι ηλεκτρονικοί εγκληματίες χρησιμοποιούν όλο και πολυπλοκότερες μεθόδους για να διεισδύσουν στα πληροφοριακά συστήματα, να υποκλέψουν δεδομένα ζωτικής σημασίας ή να εκβιάσουν επιχειρήσεις. Η αύξηση της οικονομικής κατασκοπείας και των κρατικά υποκινούμενων δραστηριοτήτων στον κυβερνοχώρο δημιουργεί μια νέα κατηγορία απειλών για τις κυβερνήσεις και τις επιχειρήσεις της ΕΕ.

Σε χώρες εκτός ΕΕ οι κυβερνήσεις είναι δυνατόν να χρησιμοποιήσουν καταχρηστικά τον κυβερνοχώρο για επιτήρηση και έλεγχο των ίδιων των πολιτών τους. Η ΕΕ μπορεί να αντιταχθεί στην εν λόγω κατάσταση προωθώντας την διαδικτυακή ελευθερία και εξασφαλίζοντας τον σεβασμό των θεμελιωδών δικαιωμάτων στο διαδίκτυο.

Όλοι οι προαναφερθέντες παράγοντες εξηγούν γιατί οι κυβερνήσεις ανά την υφήλιο έχουν αρχίσει να καταστρώνουν στρατηγικές για την ασφάλεια στον κυβερνοχώρο και να θεωρούν

---

1 http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

2 Για παράδειγμα, φυτά εξοπλισμένα με αισθητήρες που επικοινωνούν με το σύστημα ψεκασμού όταν έλθει η στιγμή που απαιτούν πότισμα.

3 Ειδικό Ευρωβαρόμεντρο 390 του 2012 σχετικά με την Ασφάλεια στον κυβερνοχώρο

4 Ο όρος ασφάλεια στον κυβερνοχώρο αναφέρεται συνήθως στις διασφαλίσεις και τα μέτρα που μπορούν να χρησιμοποιηθούν για να προστατευθεί ο κυβερνοχώρος, για στρατιωτικές και πολιτικές χρήσεις ταυτόχρονα, από τις απειλές εκείνες που συνδέονται με ή που μπορεί να βλάψουν τα ανεξάρτητα δίκτυα και τις πληροφοριακές υποδομές του. Ο κλάδος της ασφάλειας στην κυβερνοχώρο επιδιώκει να διατηρήσει την διαθεσιμότητα και την ακεραιότητα των δικτύων και της υποδομής και την εμπιστευτικότητα των πληροφοριών που περιέχονται σε αυτά.

5 Ο όρος ηλεκτρονικό έγκλημα καλύπτει συνήθως μεγάλο εύρος διαφορετικών εγκληματικών δραστηριοτήτων στις οποίες χρησιμοποιούνται υπολογιστές και πληροφοριακά συστήματα ως πρωτογενή εργαλεία ή ως πρωτογενείς στόχοι. Το ηλεκτρονικό έγκλημα περιλαμβάνει συνήθεις αξιόποινες πράξεις (π.χ. απάτη, πλαστογραφία και κλοπή ταυτότητας), εγκλήματα που αφορούν το περιεχόμενο (π.χ. διαδικτυακή διανομή παιδικής πορνογραφίας ή προτροπή σε φυλετικό μίσος) και αξιόποινες πράξεις που αφορούν συγκεκριμένα υπολογιστές και πληροφοριακά συστήματα (π.χ. επιθέσεις κατά πληροφοριακών συστημάτων, άρνηση υπηρεσίας και κακόβουλο λογισμικό).

τον κυβερνοχώρο ως όλο και σημαντικότερο διεθνές ζήτημα. Έφτασε η στιγμή να αναβαθμίσει τις δράσεις της στον υπόψη τομέα και η ΕΕ. Η παρούσα πρόταση για μια στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο που υποβάλλει η Επιτροπή και η Ύπατη Εκπρόσωπος της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας (εφεξής Ύπατη Εκπρόσωπος) περιγράφει το όραμα της ΕΕ στον υπόψη τομέα, αποσαφηνίζει τους ρόλους και τις αρμοδιότητες και προσδιορίζει τα απαιτούμενα μέτρα με βάση την αυστηρή και αποτελεσματική προστασία των δικαιωμάτων των πολιτών έτσι ώστε το διαδικτυακό περιβάλλον της ΕΕ να καταστεί το ασφαλέστερο παγκοσμίως.

1.2. Αρχές της ασφάλειας στην κυβερνοχώρο

Το χωρίς σύνορα και πολυεπίπεδο διαδίκτυο έχει καταστεί ένα από τα ισχυρότερα εργαλεία παγκόσμιας προόδου χωρίς κυβερνητική επιτήρηση ή κανονιστική ρύθμιση. Ο ιδιωτικός τομέας πρέπει να συνεχίσει να διαδραματίζει ηγετικό ρόλο στην οικοδόμηση και καθημερινή διαχείριση του διαδικτύου, αλλά, παράλληλα, η ανάγκη για διαφάνεια, λογοδοσία και ασφάλεια καθίσταται όλο και εμφανέστερη. Η παρούσα στρατηγική αποσαφηνίζει τις αρχές που πρέπει να καθοδηγούν την πολιτική ασφάλειας στον κυβερνοχώρο στην ΕΕ και διεθνώς.

Οι βασικές αρχές της ΕΕ ισχύουν τόσο στον ψηφιακό όσο και στον πραγματικό κόσμο

Οι νόμοι και τα πρότυπα που ισχύουν σε άλλους τομείς της καθημερινής μας ζωής ισχύουν και στον κυβερνοχώρο.

Προστασία των θεμελιωδών δικαιωμάτων, της ελευθερίας της έκφρασης, των προσωπικών δεδομένων και της ιδιωτικότητας

Η ασφάλεια στον κυβερνοχώρο μπορεί να είναι ορθή και αποτελεσματική εάν βασίζεται στα θεμελιώδη δικαιώματα και τις ελευθερίες, όπως κατοχυρώνονται στον Χάρτη των θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης και στις βασικές αρχές της ΕΕ. Αντίστροφα, τα ατομικά δικαιώματα δεν μπορούν να εξασφαλιστούν χωρίς ασφαλή δίκτυα και συστήματα. Κάθε ανταλλαγή πληροφοριών για τους σκοπούς της ασφάλειας στον κυβερνοχώρο, πρέπει – εφόσον εμπλέκονται προσωπικά δεδομένα – να συνάδει με το ενωσιακό δίκαιο προστασίας των δεδομένων και να λαμβάνει πλήρως υπόψη τα ατομικά δικαιώματα στον εν λόγω τομέα.

Προσβασιμότητα για όλους

Η περιορισμένη ή η έλλειψη πρόσβασης στο διαδίκτυο και ο ψηφιακός αναλφαβητισμός αποτελούν μειονεκτήματα για τους πολίτες με δεδομένη την έκταση στην οποία έχει διεισδύσει στην κοινωνία ο ψηφιακός κόσμος. Όλοι θα πρέπει να έχουν δυνατότητα πρόσβασης στο διαδίκτυο και ανεμπόδιστη ροή πληροφοριών. Η ακεραιότητα και η ασφάλεια του διαδικτύου πρέπει να διασφαλίζονται ώστε να είναι δυνατή η ασφαλής πρόσβαση από όλους.

Δημοκρατική και αποτελεσματική πολυμερής διακυβέρνηση

Ο ψηφιακός κόσμος δεν ελέγχεται από μια μοναδική οντότητα. Σήμερα υπάρχουν αρκετοί ενδιαφερόμενοι, εκ των οποίων πολλοί είναι εμπορικές και μη κυβερνητικές οντότητες, που εμπλέκονται στην καθημερινή διαχείριση των πόρων, των πρωτοκόλλων και των προτύπων του διαδικτύου και στην μελλοντική του ανάπτυξη. Η ΕΕ επανεπιβεβαιώνει την σημασία

όλων των εμπλεκόμενων στο σημερινό μοντέλο διακυβέρνησης του διαδικτύου και υποστηρίζει αυτήν την πολυμερή προσέγγιση διακυβέρνησης[6].

Συναρμοδιότητα για να κατοχυρωθεί η ασφάλεια

Η αυξανόμενη εξάρτηση από τις τεχνολογίες πληροφοριών και επικοινωνιών σε όλους του τομείς της ανθρώπινης ζωής έχει οδηγήσει σε τρωτά σημεία που πρέπει να οριστούν σωστά, να αναλυθούν ενδελεχώς και να διορθωθούν ή να περιοριστούν. Όλοι οι συναφείς φορείς, ήτοι οι δημόσιες αρχές, ο ιδιωτικός τομέας ή οι μεμονωμένοι πολίτες, πρέπει να αναγνωρίσουν αυτήν την συνυπευθυνότητα, να αναλάβουν δράση για να αυτοπροστατευθούν και εάν χρειαστεί να εξασφαλίσουν συντονισμένη αντίδραση για ενίσχυση της ασφάλειας του κυβερνοχώρου.

2. ΣΤΡΑΤΗΓΙΚΕΣ ΠΡΟΤΕΡΑΙΟΤΗΤΕΣ ΚΑΙ ΜΕΤΡΑ

Η ΕΕ οφείλει να διασφαλίσει ένα διαδικτυακό περιβάλλον που να παρέχει την μέγιστη δυνατή ελευθερία και ασφάλεια προς όφελος των πάντων. Παρόλο που αναγνωρίζεται πως αυτό αποτελεί κυρίως καθήκον των κρατών μελών που πρέπει να αντιμετωπίσουν τις προκλήσεις ασφάλειας στον κυβερνοχώρο, με την παρούσα στρατηγική προτείνονται συγκεκριμένες δράσεις με τις οποίες είναι δυνατόν να ενισχυθούν οι συνολικές επιδόσεις της ΕΕ. Οι εν λόγω δράσεις πρέπει να είναι βραχυ- και μακροπρόθεσμες, περιλαμβάνουν ποικιλία εργαλείων πολιτικής[7] και αφορούν φορείς διαφόρων τύπων, ανεξάρτητα αν είναι θεσμικά όργανα της ΕΕ, κράτη μέλη ή επιχειρήσεις του κλάδου.

Το όραμα της ΕΕ που παρουσιάζεται στην παρούσα στρατηγική διαρθρώνεται σε πέντε στρατηγικές προτεραιότητες, με τις οποίες αντιμετωπίζονται οι προκλήσεις που υπογραμμίστηκαν ανωτέρω:

- Επίτευξη ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο
- Δραστική μείωση του ηλεκτρονικού εγκλήματος
- Ανάπτυξη πολιτικής και ικανοτήτων για την άμυνα στον κυβερνοχώρο σε σχέση με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ)
- Ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο
- Θέσπιση συνεκτικής διεθνούς πολιτικής κυβερνοχώρου για την Ευρωπαϊκή Ένωση και προώθηση των βασικών αξιών της ΕΕ

2.1. Επίτευξη ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο

Για την προώθηση της ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο στην ΕΕ, τόσο οι δημόσιες αρχές όσο και ο ιδιωτικός τομέας πρέπει να αναπτύξουν ικανότητες και να συνεργαστούν αποτελεσματικά. Αξιοποιώντας τα θετικά αποτελέσματα που έχουν επιτευχθεί μέσω των δραστηριοτήτων που έχουν υλοποιηθεί μέχρι σήμερα[8], οι περαιτέρω δράσεις της ΕΕ είναι δυνατόν να συμβάλλουν ιδίως στην αντιμετώπιση των κινδύνων και των

---

6 Βλέπε επίσης COM(2009) 277, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο - Διακυβέρνηση του Ίντερνετ : τα επόμενα βήματα

7 Οι δράσεις που σχετίζονται με την ανταλλαγή πληροφοριών, όταν διακυβεύονται προσωπικά δεδομένα, πρέπει να συνάδουν με την ενωσιακή νομοθεσία για την προστασία των δεδομένων.

8 Βλέπε τα παραπομπές στην παρούσα ανακοίνωση καθώς και το έγγραφο εργασίας των υπηρεσιών της Επιτροπής με την έκθεση εκτίμησης επιπτώσεων που συνοδεύει την πρόταση της Επιτροπής για οδηγία σχετικά με την ασφάλεια δικτύων και πληροφοριών, ιδίως τα τμήματα 4.1.4 και 5.2 καθώς και τα παραρτήματα 2, 6 και 8

απειλών στον κυβερνοχώρο με διασυνοριακή διάσταση και να συμβάλλουν στην συντονισμένη αντίδραση σε καταστάσεις έκτακτης ανάγκης. Αυτό θα στηρίξει ιδιαίτερα την σωστή λειτουργία της εσωτερικής αγοράς και θα ενισχύσει την εσωτερική ασφάλεια της ΕΕ.

Η Ευρώπη θα παραμείνει ευάλωτη χωρίς σημαντική προσπάθεια βελτίωσης των ικανοτήτων, των πόρων και των διαδικασιών του δημόσιου και του ιδιωτικού τομέα για την πρόληψη, την ανίχνευση και την αντιμετώπιση των συμβάντων ασφάλειας στον κυβερνοχώρο. Για τον λόγο αυτό η Επιτροπή κατάρτισε πολιτική σχετικά με την ασφάλεια δικτύων και πληροφοριών (ΑΔΠ)[9]. Ο **Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών ENISA** ιδρύθηκε το 2004[10] και ένας νέος κανονισμός για την ενίσχυση του ENISA και τον εκσυγχρονισμό της αποστολής του αποτελεί αντικείμενο διαπραγματεύσεων μεταξύ Συμβουλίου και Κοινοβουλίου[11]. Επιπλέον, η οδηγία πλαίσιο για τις ηλεκτρονικές επικοινωνίες[12] απαιτεί από τους παρόχους ηλεκτρονικών επικοινωνιών να διαχειρίζονται με κατάλληλο τρόπο τους κινδύνους που απειλούν τα δίκτυά τους και να αναφέρουν τις σημαντικές παραβιάσεις ασφάλειας. Εξάλλου, η ενωσιακή νομοθεσία προστασίας δεδομένων[13], απαιτεί από τους υπεύθυνους επεξεργασίας δεδομένων να εξασφαλίζουν την τήρηση των απαιτήσεων και των διασφαλίσεων περί προστασίας των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων μέτρων που αφορούν την ασφάλεια, ενώ στο πεδίο των δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών οι υπεύθυνοι επεξεργασίας δεδομένων οφείλουν να κοινοποιούν τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα στις αρμόδιες εθνικές αρχές.

Παρά την επιτευχθείσα πρόοδο βάσει εθελοντικών δεσμεύσεων, υφίστανται ακόμη κενά ανά την ΕΕ, ιδίως όσον αφορά τις εθνικές ικανότητες, τον συντονισμό σε περιπτώσεις συμβάντων διασυνοριακής διάστασης και όσον αφορά την συμμετοχή και την ετοιμότητα ου ιδιωτικού τομέα. Η παρούσα στρατηγική συνοδεύεται από **νομοθετική** πρόταση με στόχο κυρίως:

- να καθιερώσει κοινές ελάχιστες απαιτήσεις για την ασφάλεια δικτύων και πληροφοριών (NIS-ΑΔΠ) σε εθνικό επίπεδο με βάση τις οποίες τα κράτη μέλη θα υποχρεωθούν: να ορίσουν αρμόδιες εθνικές αρχές για την ΑΔΠ, να συγκροτήσουν μια καλά λειτουργούσα ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) και να θεσπίσουν εθνική στρατηγική και ένα εθνικό σχέδιο συνεργασίας για την ΑΔΠ. Η ανάπτυξη ικανοτήτων και ο συντονισμός αφορούν επίσης και τα θεσμικά όργανα της ΕΕ: το 2012 συγκροτήθηκε μόνιμη ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική («CERT-EU») με αρμοδιότητα την ασφάλεια των συστημάτων πληροφορικής των θεσμικών οργάνων, των υπηρεσιών και των φορέων της ΕΕ.
- να δημιουργήσει μηχανισμούς συντονισμένης πρόληψης, ανίχνευσης, άμβλυνσης των επιπτώσεων και επέμβασης, που να επιτρέπουν την ανταλλαγή πληροφοριών και την αμοιβαία συνδρομή των εθνικών αρμόδιων αρχών ασφάλειας δικτύων και πληροφοριών. Θα ζητηθεί από τις εθνικές αρμόδιες αρχές ασφάλειας δικτύων και πληροφοριών να εξασφαλίσουν την κατάλληλη πανευρωπαϊκή συνεργασία, ιδίως με βάση ένα ενωσιακό

---

9 Το 2001, η Επιτροπή εξέδωσε ανακοίνωση σχετικά με την Ασφάλεια δικτύων και πληροφοριών: Πρόταση ευρωπαϊκής πολιτικής (COM(2001)298). Και το 2006 εξέδωσε Στρατηγική για ασφαλή κοινωνία της πληροφορίας (COM(2006)251). Από το 2009 και μετά, η Επιτροπή έχει επίσης εκδώσει ένα σχέδιο δράσης και μια Ανακοίνωση σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας (COM(2009)149, που εγκρίθηκε με το ψήφισμα του Συμβουλίου 2009/C 321/01 και COM(2011)163, που εγκρίθηκε με τα συμπεράσματα του Συμβουλίου 10299/11).

10 Κανονισμός (ΕΚ) αριθ. 460/2004

11 COM (2010) 521. Τα μέτρα που προτείνονται στην παρούσα στρατηγική δεν συνεπάγονται τροποποιήσεις της μελλοντικής αποστολής του ENISA.

12 Άρθρο 13α και β της οδηγίας 2002/21/ΕΚ

13 στ) το άρθρο 17 της οδηγίας 95/46/ΕΚ· Άρθρο 4 της οδηγίας 2002/58/ΕΚ

σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών, που θα έχει καταρτιστεί με στόχο την αντιμετώπιση περιστατικών ασφάλειας στον κυβερνοχώρο με διασυνοριακή διάσταση. Η εν λόγω συνεργασία θα αξιοποιήσει επίσης την επιτευχθείσα πρόοδο στο πλαίσιο του ευρωπαϊκού φόρουμ των κρατών μελών (EFMS)[14] , που οργάνωσε εποικοδομητικές συζητήσεις και ανταλλαγές σχετικά με τη δημόσια πολιτική ασφάλειας δικτύων και πληροφοριών και μπορεί να ενσωματωθεί στον μηχανισμό συνεργασίας μόλις αυτός δημιουργηθεί.

- να βελτιώσει την ετοιμότητα και την ανάληψη δέσμευσης από τον ιδιωτικό τομέα. Δεδομένου ότι την συντριπτική πλειοψηφία των δικτύων και συστημάτων πληροφοριών κατέχουν και λειτουργούν ιδιώτες, η βελτίωση της εμπλοκής του ιδιωτικού τομέα για την ενίσχυση της ασφάλειας του κυβερνοχώρου είναι ζωτικής σημασίας. Ο ιδιωτικός τομέας πρέπει να αναπτύξει σε τεχνικό επίπεδο τις δικές τους δυνατότητες ανθεκτικότητας όσον αφορά την ασφάλεια του κυβερνοχώρου και να ανταλλάξει βέλτιστες πρακτικές με άλλους τομείς. Από τα εργαλεία που έχει αναπτύξει ο κλάδος για την αντιμετώπιση συμβάντων, προσδιορισμό των αιτίων και διεξαγωγή εγκληματολογικών ερευνών πρέπει επίσης να επωφεληθεί και ο δημόσιος τομέας.

Ωστόσο, οι ιδιωτικοί φορείς δεν διαθέτουν ακόμη αποτελεσματικά κίνητρα ώστε να διαθέσουν αξιόπιστα στοιχεία σχετικά με την ύπαρξη ή τις επιπτώσεις συμβάντων ασφάλειας δικτύων και πληροφοριών, να υιοθετήσουν νοοτροπία διαχείρισης κινδύνων ή να επενδύσουν σε λύσεις στον τομέα της ασφάλειας. Κατά συνέπεια, η προτεινόμενη νομοθεσία έχει στόχο να εξασφαλίσει ότι οι παράγοντες σε αρκετούς τομείς ζωτικής σημασίας (συγκεκριμένα στην ενέργεια, τις μεταφορές, τις τράπεζες, τα χρηματιστήρια, καθώς και παράγοντες που συμβάλουν στην παροχή διαδικτυακών υπηρεσιών ζωτικής σημασίας και η δημόσια διοίκηση) θα εκτιμήσουν τους κινδύνους ηλεκτρονικής ασφάλειας που αντιμετωπίζουν, θα εξασφαλίσουν την αξιοπιστία και την ανθεκτικότητα δικτύων και πληροφοριακών συστημάτων μέσω κατάλληλης διαχείρισης κινδύνων και, τέλος, θα ανταλλάξουν τις εντοπισθείσες πληροφορίες με τις εθνικές αρμόδιες αρχές ασφάλειας δικτύων και πληροφοριών. Η υιοθέτηση μιας νοοτροπίας ασφάλειας του κυβερνοχώρου θα μπορούσε να ενισχύσει τις επιχειρηματικές ευκαιρίες και την ανταγωνιστικότητα στον ιδιωτικό τομέα, γεγονός που θα μπορούσε να μετατρέψει την ασφάλεια του κυβερνοχώρου σε εμπορικό πλεονέκτημα.

Οι εν λόγω φορείς θα πρέπει να αναφέρουν στις αρμόδιες εθνικές αρχές ασφάλειας δικτύων και πληροφοριών τα συμβάντα με σημαντικές επιπτώσεις στην αδιάλειπτη παροχή ζωτικών υπηρεσιών και την διάθεση εμπορευμάτων που εξαρτώνται από δίκτυα και πληροφοριακά συστήματα.

Οι αρμόδιες εθνικές αρχές ΑΔΠ πρέπει να συνεργάζονται και να ανταλλάσουν πληροφορίες με άλλους ρυθμιστικούς φορείς, ιδίως με τις αρχές προστασίας προσωπικών δεδομένων. Οι αρμόδιες εθνικές αρχές ΑΔΠ πρέπει με τη σειρά τους να αναφέρουν τα συμβάντα εικαζόμενης σοβαρής εγκληματικής φύσης στις αρχές επιβολής του νόμου. Οι αρμόδιες εθνικές αρχές πρέπει επίσης να δημοσιεύουν τακτικά σε ιδιαίτερο ιστότοπο μη διαβαθμισμένες πληροφορίες σχετικά με εν εξελίξει έγκαιρες προειδοποιήσεις για συμβάντα και κινδύνους και σχετικά με συντονισμένες επεμβάσεις. Οι νομικές υποχρεώσεις δεν πρέπει ούτε να υποκαταστήσουν ούτε να εμποδίσουν την ανάπτυξη ανεπίσημης και εθελοντικής συνεργασίας – συμπεριλαμβανομένης της συνεργασίας μεταξύ του δημόσιου και του

[14] Το ευρωπαϊκό φόρουμ των κρατών μελών δημιουργήθηκε βάσει του COM(2009) 149 ως βήμα ενίσχυσης των συζητήσεων μεταξύ των δημόσιων αρχών των κρατών μελών σχετικά με ορθή πρακτική πολιτικής στον τομέα της ασφάλειας και της ανθεκτικότητας των υποδομών πληροφοριών ζωτικής σημασίας.

ιδιωτικού τομέα – για την ενίσχυση των επιπέδων ασφάλειας και την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών. Συγκεκριμένα, η ευρωπαϊκή σύμπραξη δημόσιου-ιδιωτικού τομέα για την ανθεκτικότητα (EP3R)[15] αποτελεί στερεά και αξιόπιστη πλατφόρμα σε επίπεδο ΕΕ και πρέπει να αναπτυχθεί περαιτέρω.

Η Διευκόλυνση «Συνδέοντας την Ευρώπη» (CEF)[16] θα χορηγήσει οικονομική στήριξη για υποδομές ζωτικής σημασίας με τις οποίες θα συνδέονται οι ικανότητες ασφάλειας δικτύων και πληροφοριών των κρατών μελών, με αποτέλεσμα να διευκολυνθεί η συνεργασία ανά την ΕΕ.

Τέλος, οι ασκήσεις αντιμετώπισης συμβάντων ασφάλειας στην κυβερνοχώρο σε επίπεδο ΕΕ είναι ζωτικής σημασίας για την προσομοίωση της συνεργασίας μεταξύ των κρατών μελών και του ιδιωτικού τομέα. Η πρώτη άσκηση με τη συμμετοχή των κρατών μελών διεξήχθη το 2010 («Cyber Europe 2010») και μια δεύτερη άσκηση, επίσης με τη συμμετοχή του ιδιωτικού τομέα, διεξήχθη τον Οκτώβριο του 2012 («Cyber Europe 2012»). Μια άσκηση επί χάρτου μεταξύ ΕΕ-ΗΠΑ διεξήχθη το Νοέμβριο του 2011 («Cyber Atlantic 2011»). Στο μέλλον προγραμματίζεται η διεξαγωγή επιπλέον ασκήσεων, και με τη συμμετοχή διεθνών εταίρων.

Η Επιτροπή πρόκειται:

- Να συνεχίσει τις δραστηριότητές της, μέσω του Κοινού Κέντρου Ερευνών, σε στενή συνεργασία με τις αρχές των κρατών μελών και με τους ιδιοκτήτες υποδομών ζωτικής σημασίας και τους οργανισμούς εκμετάλλευσης, για τον εντοπισμό των ευάλωτων σημείων της ΑΔΠ των ευρωπαϊκών υποδομών ζωτικής σημασίας και θα ενθαρρύνει την ανάπτυξη ανθεκτικών συστημάτων.
- Να δρομολογήσει στις αρχές του 2013 πιλοτικό έργο[17] με ενωσιακή χρηματοδότηση για την **καταπολέμηση δικτύων-ρομπότ (botnets) και κακόβουλου λογισμικού**, με στόχο να παρασχεθεί πλαίσιο για τον συντονισμό και τη συνεργασία μεταξύ των κρατών μελών της ΕΕ, οργανισμών του ιδιωτικού τομέα όπως οι πάροχοι υπηρεσιών διαδικτύου, και διεθνών εταίρων.

Η Επιτροπή καλεί τον ENISA:

- Να βοηθήσει τα κράτη μέλη να αναπτύξουν ισχυρές **εθνικές ικανότητες ανθεκτικότητας όσον αφορά την ασφάλεια του κυβερνοχώρου**, ιδίως με την ανάπτυξη εμπειρογνωμοσύνης στην ασφάλεια και την ανθεκτικότητα βιομηχανικών συστημάτων ελέγχου, και υποδομών μεταφορών και ενέργειας.
- Να εξετάσει το 2013 την σκοπιμότητα δημιουργίας ομάδας (ή ομάδων) αντιμετώπισης περιστατικών ασφάλειας πληροφορικής για τα βιομηχανικά συστήματα ελέγχου (ICS-CSIRTs) για την ΕΕ.

---

15 Η ευρωπαϊκή σύμπραξη δημόσιου-ιδιωτικού τομέα για την ανθεκτικότητα δρομολογήθηκε με το COM(2009) 149. Στο πλαίσιο της πλατφόρμας ξεκίνησαν εργασίες και ενισχύθηκε η συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα όσον αφορά τον εντοπισμό στοιχείων ενεργητικού, πόρων, λειτουργιών και βασικών απαιτήσεων ζωτικής σημασίας για την ανθεκτικότητα καθώς και όσον αφορά ανάγκες και μηχανισμούς συνεργασίας για την αντιμετώπιση διαταραχών μεγάλης κλίμακας που επηρεάζουν τις ηλεκτρονικές επικοινωνίες.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Γραμμή του προϋπολογισμού για την CEF – Δίκτυα τηλεπικοινωνιών (προώθηση της διασύνδεσης και της διαλειτουργικότητας των εθνικών διαδικτυακών δημόσιων υπηρεσιών καθώς και την πρόσβαση στα εν λόγω δίκτυα).

17 CIP-ICT PSP-2012-6, 325188. Συνολικός προϋπολογισμός 15 εκατομμύρια ευρώ με ενωσιακή χρηματοδότηση ανερχόμενη σε 7,7 εκατομμύρια ευρώ.

- Να συνεχίσει να υποστηρίζει τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ στην διεξαγωγή τακτικών **πανευρωπαϊκών ασκήσεων αντιμετώπισης συμβάντων ασφάλειας στην κυβερνοχώρο** που θα αποτελέσουν επίσης την επιχειρησιακή βάση για την συμμετοχή της ΕΕ σε διεθνείς ασκήσεις αντιμετώπισης συμβάντων ασφάλειας στην κυβερνοχώρο.

Η Επιτροπή καλεί το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο:

- Να εγκρίνουν χωρίς καθυστέρηση την πρόταση οδηγίας για **κοινό υψηλό επίπεδο ασφάλειας δικτύων και πληροφοριών (ΑΔΠ)** ανά την Ένωση, που καλύπτει τις εθνικές ικανότητες και ετοιμότητα, την συνεργασία σε ενωσιακό επίπεδο, την υιοθέτηση πρακτικών διαχείρισης κινδύνου και την ανταλλαγή πληροφοριών σχετικά με την ΑΔΠ.

Η Επιτροπή καλεί τον κλάδο:

- Να αναλάβει ηγετικό ρόλο στις **επενδύσεις** σε ασφάλεια κυβερνοχώρου υψηλής ποιότητας και να αναπτύξει βέλτιστες πρακτικές και ανταλλαγή πληροφοριών σε επίπεδο κλάδου και με τις δημόσιες αρχές με στόχο να εξασφαλιστεί ισχυρή και αποτελεσματική προστασία των στοιχείων ενεργητικού και των προσώπων, ιδίως μέσω συμπράξεων δημόσιου-ιδιωτικού τομέα όπως η EP3R και η σύμπραξη «Trust in Digital Life» (TDL)[18].

Ευαισθητοποίηση

Η ευθύνη για την ασφάλεια στον κυβερνοχώρο είναι κοινή. Οι τελικοί χρήστες διαδραματίζουν ρόλο ζωτικής σημασίας όσον αφορά την ασφάλεια δικτύων και πληροφορικών συστημάτων, πρέπει δε να αντιληφθούν τους κινδύνους που αντιμετωπίζουν στο διαδίκτυο και να αναλάβουν την ευθύνη λήψης απλών μέτρων για να αυτοπροστατευθούν.

Στο πρόσφατο παρελθόν έχουν αναπτυχθεί πολλές πρωτοβουλίες οι οποίες και πρέπει να συνεχιστούν. Συγκεκριμένα ο ENISA συμμετείχε στην ευαισθητοποίηση με δημόσιες εκθέσεις, διοργάνωση συναντήσεων εργασίας εμπειρογνωμόνων και με τη σύσταση συμπράξεων δημόσιου-ιδιωτικού τομέα. Στον τομέα της ευαισθητοποίησης δραστηριοποιούνται η Europol, η Eurojust και οι εθνικές αρχές προστασίας δεδομένων. Τον Οκτώβριο του 2012, ο ENISA και ορισμένα κράτη μέλη έθεσαν σε δοκιμαστική εφαρμογή την «Πανευρωπαϊκή Εβδομάδα Ασφάλειας στην Κυβερνοχώρο». Η ευαισθητοποίηση είναι ένας από τους τομείς που θα προωθήσει η ομάδα εργασίας ΕΕ-ΗΠΑ για την ασφάλεια στην κυβερνοχώρο και το ηλεκτρονικό έγκλημα[19] και είναι επίσης ζωτικής σημασίας στο πλαίσιο του προγράμματος για ασφαλέστερη χρήση του διαδικτύου[20] (που εστιάζεται στην ασφάλεια των παιδιών στο διαδίκτυο).

---

18 http://www.trustindigitallife.eu/

19 Στην εν λόγω ομάδα εργασίας που συνεστήθη στην διάσκεψη κορυφής ΕΕ-ΗΠΑ το Νοέμβριο του 2010 (MEMO/10/597) έχει ανατεθεί η ανάπτυξη συνεργατικών προσεγγίσεων σε ευρύ φάσμα ζητημάτων ασφάλειας στον κυβερνοχώρο και ηλεκτρονικού εγκλήματος.

20 Στο πλαίσιο του προγράμματος για ασφαλέστερη χρήση του διαδικτύου χρηματοδοτείται ένα δίκτυο ΜΚΟ που δραστηριοποιούνται στον τομέα της διαδικτυακής προστασίας των παιδιών, ένα δίκτυο φορέων επιβολής του νόμου που ανταλλάσουν πληροφορίες και βέλτιστες πρακτικές σχετικά με την εγκληματική αξιοποίηση του διαδικτύου για την διανομή υλικού παιδικής σεξουαλικής κακοποίησης

Η Επιτροπή καλεί τον ENISA:

- Να προτείνει το 2013 έναν χάρτη πορείας για ένα «πιστοποιητικό στον τομέα της ασφάλειας δικτύων και πληροφοριών» ως πρόγραμμα εθελοντικής πιστοποίησης για την προαγωγή ενισχυμένων δεξιοτήτων και εξειδίκευσης των επαγγελματιών της πληροφορικής (π.χ. των διαχειριστών ιστοτόπων).

Η Επιτροπή πρόκειται:

- Να οργανώσει, το 2014, με την υποστήριξη του ENISA, ένα **πρωτάθλημα** ασφάλειας στον κυβερνοχώρο στο οποίο θα διαγωνιστούν φοιτητές προτείνοντας λύσεις ΑΔΠ.

Η Επιτροπή καλεί τα κράτη μέλη[21] :

- Να διοργανώσουν από το 2013 και εφεξής σε ετήσια βάση ένα **μήνα ασφάλειας στον κυβερνοχώρο** με την υποστήριξη του ENISA και την συμμετοχή του ιδιωτικού τομέα με στόχο την ευαισθητοποίηση των τελικών χρηστών. Αρχής γενομένης από το 2014 θα οργανωθεί ένας συγχρονισμένος μήνας ασφάλειας στον κυβερνοχώρο μεταξύ ΕΕ-ΗΠΑ.
- **Να αναβαθμίσουν τις εθνικές προσπάθειες εκπαίδευσης και κατάρτισης στον τομέα της ΑΔΠ**, εισάγοντας: εκπαίδευση στην ΑΔΠ στα σχολεία μέχρι το 2014, εκπαίδευση για την ΑΔΠ, την ασφαλή ανάπτυξη λογισμικού και την προστασία προσωπικών δεδομένων για τους σπουδαστές πληροφορικής, και βασική εκπαίδευση ΑΔΠ για το προσωπικό που εργάζεται στις δημόσιες διοικήσεις.

Η Επιτροπή καλεί τον κλάδο:

- Να προωθήσει την **ευαισθητοποίηση** σχετικά με την ασφάλεια του κυβερνοχώρου **σε όλα τα επίπεδα**, τόσο στις επιχειρηματικές πρακτικές όσο και στις επαφές με τους πελάτες. Συγκεκριμένα, ο κλάδος πρέπει να αναζητήσει τρόπους ώστε διευθυντές και διοικητικά συμβούλια να καταστούν πιο υπεύθυνα με σκοπό την εξασφάλιση της ασφάλειας στον κυβερνοχώρο.

2.2. Δραστική μείωση του ηλεκτρονικού εγκλήματος

Όσο περισσότερο η ζωή μας εξελίσσεται στον ψηφιακό κόσμο, τόσο αυξάνονται οι ευκαιρίες που μπορούν να αξιοποιήσουν οι ηλεκτρονικοί εγκληματίες. Το ηλεκτρονικό έγκλημα είναι μια από τις ταχύτερα αναπτυσσόμενες μορφές εγκλήματος, με θύματα σε παγκόσμιο επίπεδο που ξεπερνούν το ένα εκατομμύριο άτομα ημερησίως. Οι ηλεκτρονικοί εγκληματίες και τα δίκτυα ηλεκτρονικού εγκλήματος γίνονται όλο και πιο πολύπλοκα και πρέπει να διαθέτουμε τα σωστά επιχειρησιακά εργαλεία και ικανότητες για να τα αντιμετωπίσουμε. Το ηλεκτρονικό έγκλημα αποφέρει υψηλά κέρδη με μικρό κίνδυνο και οι εγκληματίες συχνά εκμεταλλεύονται την ανωνυμία των διαδικτυακών χώρων. Το ηλεκτρονικό έγκλημα δεν γνωρίζει σύνορα – η παγκόσμια διάδοση του διαδικτύου σημαίνει ότι η επιβολή του νόμου

και ένα δίκτυο ερευνητών που συλλέγουν πληροφορίες σχετικά με τις χρήσεις, τους κινδύνους και τις συνέπειες των διαδικτυακών τεχνολογιών για τη ζωή των παιδιών.

[21] Και με την συμμετοχή των συναφών δημόσιων αρχών συμπεριλαμβανομένων και αρμόδιων αρχών για ΑΔΠ και αρχών προστασίας δεδομένων.

πρέπει να υιοθετήσει συντονισμένη και συνεργατική διασυνοριακή προσέγγιση για να αντιμετωπίσει αυτή την αυξανόμενη απειλή.

Ισχυρή και αποτελεσματική νομοθεσία

Για να αντιμετωπίσουν το ηλεκτρονικό έγκλημα, η ΕΕ και τα κράτη μέλη χρειάζονται ισχυρή και αποτελεσματική νομοθεσία. Η σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, γνωστή επίσης και ως Σύμβαση της Βουδαπέστης, είναι μια δεσμευτική διεθνής συνθήκη που παρέχει αποτελεσματικό πλαίσιο για την θέσπιση εθνικής νομοθεσίας.

Η ΕΕ έχει ήδη εκδώσει νομοθεσία σχετικά με το ηλεκτρονικό έγκλημα συμπεριλαμβανομένης μιας οδηγίας σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας[22]. Η ΕΕ πρόκειται σύντομα να συμφωνήσει επί οδηγίας για τις επιθέσεις κατά πληροφοριακών συστημάτων, ιδίως μέσω της χρήσης δικτύων-ρομπότ (botnets).

Η Επιτροπή πρόκειται:

- Να εξασφαλίσει την ταχεία ενσωμάτωση στο εθνικό δίκαιο και την εφαρμογή των οδηγιών που σχετίζονται με το ηλεκτρονικό έγκλημα.
- Να παροτρύνει τα κράτη μέλη που δεν έχουν ακόμη κυρώσει την **σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο**, να την κυρώσουν και να εφαρμόσουν τις διατάξεις της το ταχύτερο δυνατόν.

Ενισχυμένη επιχειρησιακή ικανότητα καταπολέμησης του ηλεκτρονικού εγκλήματος

Η εξέλιξη των τεχνικών του ηλεκτρονικού εγκλήματος έχει επιταχυνθεί με γοργό ρυθμό: οι υπηρεσίες επιβολής του νόμου δεν μπορούν να καταπολεμήσουν το ηλεκτρονικό έγκλημα με παρωχημένα επιχειρησιακά εργαλεία. Σήμερα, πολλά κράτη μέλη της ΕΕ δεν διαθέτουν την απαιτούμενη επιχειρησιακή ικανότητα για να αντιμετωπίσουν αποτελεσματικά το ηλεκτρονικό έγκλημα. Όλα τα κράτη μέλη χρειάζονται αποτελεσματικές εθνικές μονάδες αντιμετώπισης του ηλεκτρονικού εγκλήματος.

Η Επιτροπή πρόκειται:

- Να υποστηρίξει, μέσω των χρηματοδοτικών της προγραμμάτων[23], τα κράτη μέλη **να εντοπίσουν κενά και να ενισχύσουν τις ικανότητές τους** όσον αφορά την διερεύνηση και την καταπολέμηση του ηλεκτρονικού εγκλήματος. Η Επιτροπή θα υποστηρίξει περαιτέρω τους φορείς που συνδέουν την έρευνα/τα πανεπιστήμια, τους υπεύθυνους επιβολής του νόμου και τον ιδιωτικό τομέα, με τρόπο παρόμοιο με τις εν εξελίξει εργασίες στα χρηματοδοτούμενα από την Επιτροπή κέντρα αριστείας για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο που έχουν ήδη δημιουργηθεί σε ορισμένα κράτη μέλη.
- Σε συνεργασία με τα κράτη μέλη, και με την υποστήριξη του ΚΚΕρ, να συντονίσει τις προσπάθειες εντοπισμού βέλτιστων πρακτικών και βέλτιστων

[22] Οδηγία 2011/92/ΕΕ που αντικαθιστά την απόφαση-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου

[23] Για το 2013, βάσει του προγράμματος «Πρόληψη και καταπολέμηση της εγκληματικότητας» (ISEC). Μετά το 2013, στο πλαίσιο του ταμείου εσωτερικής ασφάλειας (νέο μέσο βάσει του ΠΔΠ).

διαθέσιμων τεχνικών για την καταπολέμηση του ηλεκτρονικού εγκλήματος (π.χ. όσον αφορά την ανάπτυξη εργαλείων για εγκληματολογικές έρευνες ή για την ανάλυση απειλών).

- Να συνεργαστεί στενά με το πρόσφατα ιδρυθέν **ευρωπαϊκό κέντρο για εγκλήματα στον κυβερνοχώρο (EC3) στο πλαίσιο της Europol και με την Eurojust** για να συντονίσει τις εν λόγω προσεγγίσεις πολιτικής με βέλτιστες πρακτικές από επιχειρησιακής πλευράς.

Βελτιωμένος συντονισμός σε επίπεδο ΕΕ

Η ΕΕ μπορεί να συμπληρώσει το έργο των κρατών μελών διευκολύνοντας μια συντονισμένη και συνεργατική προσέγγιση, συγκεντρώνοντας τις αστυνομικές και δικαστικές αρχές καθώς και τους ενδιαφερόμενους του δημόσιου και του ιδιωτικού τομέα από την ΕΕ και εκτός αυτής.

Η Επιτροπή πρόκειται:

- Να υποστηρίξει το πρόσφατα ιδρυθέν **ευρωπαϊκό κέντρο για εγκλήματα στον κυβερνοχώρο** (EC3) ως ευρωπαϊκό σημείο αναφοράς για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Το EC3 θα παράσχει ανάλυση και πληροφορίες, θα υποστηρίξει τις ανακρίσεις, θα παράσχει υψηλού επιπέδου εγκληματολογικές έρευνες, θα διευκολύνει τη συνεργασία, θα δημιουργήσει διαύλους για την ανταλλαγή πληροφοριών μεταξύ των αρμόδιων αρχών στα κράτη μέλη, τον ιδιωτικό τομέα και άλλους ενδιαφερόμενους, και θα χρησιμεύσει σταδιακά ως εκπρόσωπος της κοινότητας επιβολής του νόμου[24].
- Να υποστηρίξει τις προσπάθειες αναβάθμισης της λογοδοσίας των καταχωριστών ονομάτων χώρου και να εξασφαλίσει την ακρίβεια των πληροφοριών σχετικά με την ιδιοκτησία ιστοτόπων βάσει των συστάσεων περί επιβολής του νόμου του Οργανισμού του διαδικτύου για την εκχώρηση ονομάτων και αριθμών (ICANN), τηρουμένου του ενωσιακού δικαίου, συμπεριλαμβανομένων των κανόνων για την προστασία των δεδομένων.
- Να αξιοποιήσει την πρόσφατη νομοθεσία για περαιτέρω ενίσχυση των προσπαθειών της ΕΕ όσον αφορά την αντιμετώπιση της διαδικτυακής σεξουαλικής κακοποίησης παιδιών. Η Επιτροπή έχει εκδώσει ευρωπαϊκή στρατηγική για ένα διαδίκτυο καλύτερα προσαρμοσμένο στα παιδιά[25], και σε συνεργασία με χώρες εντός και εκτός της ΕΕ, έχει δρομολογήσει μια **Παγκόσμια συμμαχία κατά της σεξουαλικής εκμετάλλευσης παιδιών στο διαδίκτυο[26]**. Η Συμμαχία αποτελεί φορέα για περαιτέρω δράσεις από τα κράτη μέλη με την υποστήριξη της Επιτροπής και του EC3.

Η Επιτροπή καλεί την Europol (EC3):

- Να εστιάσει αρχικά την αναλυτική και επιχειρησιακή υποστήριξή της στις

[24] Στις 28 Μαρτίου 2012 η Ευρωπαϊκή εξέδωσε ανακοίνωση με τίτλο «Αντιμετώπιση του εγκλήματος στην ψηφιακή μας εποχή: ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο».

[25] COM(2012) 196 τελικό

[26] Συμπεράσματα του Συμβουλίου για μια παγκόσμια συμμαχία κατά της σεξουαλικής εκμετάλλευσης παιδιών στο διαδίκτυο (κοινή δήλωση ΕΕ-ΗΠΑ) της 7ης και 8ης Ιουνίου 2012 και δήλωση για την δρομολόγηση της παγκόσμιας συμμαχίας κατά της σεξουαλικής εκμετάλλευσης παιδιών στο διαδίκτυο (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

έρευνες των κρατών μελών στον τομέα του ηλεκτρονικού εγκλήματος, να συμβάλλει στην εξάρθρωση και αποσταθεροποίηση των δικτύων ηλεκτρονικού εγκλήματος κυρίως στους τομείς της σεξουαλικής κακοποίησης παιδιών, της απάτης στις πληρωμές, των δικτύων-ρομπότ και της παρείσδυσης.

- Να καταρτίζει σε τακτική βάση στρατηγικές και επιχειρησιακές εκθέσεις επί των τάσεων και των αναδυόμενων απειλών για τον προσδιορισμό προτεραιοτήτων και την επικέντρωση των διερευνητικών δράσεων των ομάδων καταπολέμησης του ηλεκτρονικού εγκλήματος στα κράτη μέλη.

Η Επιτροπή καλεί την Ευρωπαϊκή Αστυνομική Ακαδημία (CEPOL) σε συνεργασία με την Europol:

- Να συντονίσει τον σχεδιασμό και τον προγραμματισμό εκπαιδευτικών προγραμμάτων προκειμένου οι υπηρεσίες επιβολής του νόμου να αποκτήσουν τις γνώσεις και την εμπειρογνωμοσύνη για την αποτελεσματική αντιμετώπιση του ηλεκτρονικού εγκλήματος.

Η Επιτροπή καλεί την Eurojust:

- Να εντοπίσει τα κύρια εμπόδια που παρεμβάλλονται στην δικαστική συνεργασία στον τομέα των διερευνήσεων ηλεκτρονικών εγκλημάτων και στον συντονισμό μεταξύ κρατών μελών και τρίτων χωρών και να υποστηρίξει την διερεύνηση και την δίωξη του ηλεκτρονικού εγκλήματος σε επιχειρησιακό και στρατηγικό επίπεδο καθώς και τις εκπαιδευτικές δραστηριότητες στον τομέα.

Η Επιτροπή καλεί την Eurojust και την Europol (EC3):

- Να συνεργαστούν στενά, μεταξύ άλλων μέσω ανταλλαγής πληροφοριών, προκειμένου να ενισχύσουν την αποτελεσματικότητά τους στην καταπολέμηση του ηλεκτρονικού εγκλήματος, με βάση τις αντίστοιχες εντολές και τις αρμοδιότητές τους.
-

2.3. Επεξεργασία πολιτικής και ανάπτυξη ικανοτήτων για την άμυνα στον κυβερνοχώρο σε σχέση με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ)

Οι προσπάθειες της ΕΕ για ενίσχυση της ασφάλειας στον κυβερνοχώρο περιλαμβάνουν επίσης και τη διάσταση της άμυνας. Για να ενισχυθεί η ανθεκτικότητα των συστημάτων επικοινωνιών και πληροφοριών που υποστηρίζουν τα αμυντικά και εθνικά συμφέροντα των κρατών μελών, η ανάπτυξη της ικανότητας άμυνας στον κυβερνοχώρο πρέπει να επικεντρωθεί στον εντοπισμό, την αντιμετώπιση και την αποκατάσταση από πολύπλοκες απειλές στον κυβερνοχώρο.

Επειδή οι απειλές είναι πολυσχιδείς, πρέπει να ενισχυθούν οι συνέργειες μεταξύ των στρατιωτικών και των μη στρατιωτικών προσεγγίσεων για την προστασία πόρων ζωτικής σημασίας του κυβερνοχώρου. Οι εν λόγω προσπάθειες πρέπει να υποστηριχτούν από έρευνα και ανάπτυξη και από στενότερη συνεργασία μεταξύ κυβερνήσεων, του ιδιωτικού τομέα και των πανεπιστημίων στην ΕΕ. Για να αποφευχθούν οι επικαλύψεις, η ΕΕ θα διερευνήσει τις δυνατότητες αλληλοσυμπλήρωσης των προσπαθειών της ΕΕ και του ΝΑΤΟ όσον αφορά την

ενίσχυση της ανθεκτικότητας κυβερνητικών, αμυντικών και άλλων πληροφοριακών υποδομών ζωτικής σημασίας από τις οποίες εξαρτώνται τα μέλη αμφοτέρων των οργανισμών.

Η Ύπατη Εκπρόσωπος θα επικεντρωθεί στις ακόλουθες δραστηριότητες ζωτικής σημασίας και καλεί τα κράτη μέλη και τον Ευρωπαϊκό Οργανισμό Άμυνας να συνεργαστούν στα ακόλουθα:

- Εκτίμηση των επιχειρησιακών απαιτήσεων της ΕΕ για άμυνα στον κυβερνοχώρο και προώθηση της ανάπτυξης ενωσιακών ικανοτήτων και τεχνολογιών άμυνας στον κυβερνοχώρο για την αντιμετώπιση όλων των πτυχών της ανάπτυξης ικανοτήτων – συμπεριλαμβανομένων του δόγματος, της ηγεσίας, της οργάνωσης, του προσωπικού, της εκπαίδευσης, της τεχνολογίας, της υποδομής, της εφοδιαστικής και της διαλειτουργικότητας.

- Διαμόρφωση του ενωσιακού πλαισίου πολιτικής της άμυνας στον κυβερνοχώρο για την προστασία δικτύων στο πλαίσιο των αποστολών της ΚΠΑΑ, συμπεριλαμβανόμενης της δυναμικής διαχείρισης κινδύνων, της βελτιωμένης ανάλυσης απειλών και της ανταλλαγής πληροφοριών. Βελτίωση των ευκαιριών για εκπαίδευση και ασκήσεις άμυνας στον κυβερνοχώρο για τους στρατιωτικούς σε ευρωπαϊκό και πολυεθνικό πλαίσιο, συμπεριλαμβανομένης της ενσωμάτωσης στοιχείων άμυνας στον κυβερνοχώρο σε υφιστάμενους καταλόγους ασκήσεων.

- Προώθηση του διαλόγου και του συντονισμού μεταξύ πολιτικών και στρατιωτικών φορέων στην ΕΕ – με ιδιαίτερη έμφαση στα εξής: ανταλλαγή καλών πρακτικών, πληροφοριών και έγκαιρης προειδοποίησης, αντιμετώπιση συμβάντων, εκτίμηση κινδύνου, ευαισθητοποίηση και απόδοση προτεραιότητας στην ασφάλεια στον κυβερνοχώρο.

- Διάλογος με διεθνείς εταίρους, συμπεριλαμβανομένου του ΝΑΤΟ, άλλους διεθνείς οργανισμούς και διεθνή κέντρα αριστείας για να εξασφαλιστούν αποτελεσματικές αμυντικές δυνατότητες, να προσδιοριστούν τομείς συνεργασίας και να αποφευχθεί αλληλοεπικάλυψη προσπαθειών.

2.4. Ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο

Η Ευρώπη διαθέτει άριστες ικανότητες έρευνας και ανάπτυξης πολλές όμως από τις επιχειρήσεις που καταλαμβάνουν ηγετικές θέσεις παγκοσμίως και που διαθέτουν καινοτόμα προϊόντα και υπηρεσίες ΤΠΕ βρίσκονται εκτός ΕΕ. Υπάρχει κίνδυνος η Ευρώπη να καταστεί υπερβολικά εξαρτημένη από ΤΠΕ που παράγονται αλλού, αλλά και από λύσεις ασφάλειας που αναπτύσσονται εκτός ευρωπαϊκών συνόρων. Είναι ιδιαίτερης σημασίας να εξασφαλιστεί η αξιοπιστία, η ασφάλεια και η εγγυημένη προστασία των προσωπικών δεδομένων των στοιχείων υλισμικού και λογισμικού που παράγονται στην ΕΕ και σε τρίτες χώρες, τα οποία χρησιμοποιούνται σε υπηρεσίες και υποδομές ζωτικής σημασίας, ολοένα δε και περισσότερο σε κινητές διατάξεις.

Προώθηση της ενιαίας αγοράς για προϊόντα ασφάλειας στον κυβερνοχώρο

Είναι δυνατό να εξασφαλιστεί υψηλό επίπεδο ασφάλειας μόνο εάν όλοι όσοι συμμετέχουν στην αξιακή αλυσίδα (π.χ. κατασκευαστές εξοπλισμού, φορείς ανάπτυξης λογισμικού, πάροχοι υπηρεσιών της κοινωνίας των πληροφοριών) θεωρήσουν την ασφάλεια ως ζήτημα

προτεραιότητας. Φαίνεται[27] ωστόσο, ότι πολλοί φορείς εξακολουθούν να θεωρούν την ασφάλεια σχεδόν σαν μια πρόσθετη επιβάρυνση και η ζήτηση για λύσεις ασφάλειας είναι περιορισμένη. Σε ολόκληρη την αξιακή αλυσίδα για τα προϊόντα ΤΠΕ που χρησιμοποιούνται στην Ευρώπη επιβάλλεται να ισχύσουν κατάλληλες απαιτήσεις ως προς τις επιδόσεις στην ασφάλεια του κυβερνοχώρου . Ο ιδιωτικός τομέας χρειάζεται κίνητρα για να εξασφαλίσει υψηλό επίπεδο ασφάλειας στον κυβερνοχώρο· για παράδειγμα, οι ετικέτες που θα αναφέρουν ικανοποιητικές επιδόσεις ασφάλειας στον κυβερνοχώρο θα επιτρέψουν στις επιχειρήσεις με καλές επιδόσεις και ιστορικό στον τομέα της ασφάλειας κυβερνοχώρου να τις χρησιμοποιήσουν ως εμπορικό και ανταγωνιστικό πλεονέκτημα. Παράλληλα, οι υποχρεώσεις που θεσπίζονται με την προτεινόμενη οδηγία ΑΔΠ θα συμβάλλουν σημαντικά στην ενίσχυση της ανταγωνιστικότητας των επιχειρήσεων στους καλυπτόμενους κλάδους.

Πρέπει επίσης να τονωθεί η πανευρωπαϊκή ζήτηση της αγοράς για εξαιρετικά ασφαλή προϊόντα. Πρώτον, η παρούσα στρατηγική έχει ως στόχο την αύξηση της συνεργασίας και της διαφάνειας όσον αφορά την ασφάλεια των προϊόντων ΤΠΕ. Απαιτεί τη δημιουργία μιας πλατφόρμας, που θα συγκεντρώνει τους ευρωπαίους ενδιαφερόμενους από τον δημόσιο και τον ιδιωτικό τομέα, για τον προσδιορισμό καλών πρακτικών στον τομέα της ασφάλειας του κυβερνοχώρου σε ολόκληρη την αξιακή αλυσίδα και τη δημιουργία ευνοϊκών συνθηκών στην αγορά για την ανάπτυξη και υιοθέτηση ασφαλών λύσεων ΤΠΕ. Η προσοχή πρέπει να εστιαστεί κυρίως στη δημιουργία κινήτρων για την κατάλληλη διαχείριση του κινδύνου και την θέσπιση προτύπων και λύσεων ασφάλειας, καθώς και για την ενδεχόμενη δημιουργία εθελοντικών πανενωσιακών προγραμμάτων πιστοποίησης που θα αξιοποιούν υφιστάμενα προγράμματα στην ΕΕ και διεθνώς. Η Επιτροπή θα προωθήσει την θέσπιση συνεκτικών προσεγγίσεων μεταξύ των κρατών μελών ώστε να αποφευχθούν τυχόν ανισότητες που θα κατέληγαν σε μειονεκτήματα ως προς τη θέση εγκατάστασης των επιχειρήσεων.

Δεύτερον, η Επιτροπή θα υποστηρίξει την ανάπτυξη προτύπων ασφάλειας και θα στηρίξει τα πανενωσιακά προγράμματα εθελοντικής πιστοποίησης στον τομέα του υπολογιστικού νέφους, συνεκτιμώντας ταυτόχρονα την ανάγκη εξασφάλισης της προστασίας των δεδομένων. Οι εργασίες πρέπει να εστιαστούν στην ασφάλεια της εφοδιαστικής αλυσίδας, ιδίως σε οικονομικούς κλάδους ζωτικής σημασίας (βιομηχανικά συστήματα ελέγχου, υποδομές ενέργειας και μεταφορών). Οι εν λόγω εργασίες πρέπει να αξιοποιήσουν τις εν εξελίξει εργασίες τυποποίησης των ευρωπαϊκών οργανισμών τυποποίησης (CEN, CENELEC και ETSI)[28], της Ομάδας συντονισμού για την ασφάλεια του κυβερνοχώρου (CSCG), καθώς και της εμπειρογνωμοσύνης του ENISA, της Επιτροπής και άλλων συναφών φορέων.

Η Επιτροπή πρόκειται:

- Να εγκαινιάσει το 2013 μια **πλατφόρμα σχετικά με λύσεις ΑΔΠ** δημόσιου-ιδιωτικού τομέα που θα αναπτύξει κίνητρα για την θέσπιση ασφαλών λύσεων ΤΠΕ και την αφομοίωση καλών επιδόσεων ασφάλειας κυβερνοχώρου που θα εφαρμοστεί σε προϊόντα ΤΠΕ που χρησιμοποιούνται στην Ευρώπη.
- Να προτείνει το 2014 συστάσεις για την ασφάλεια στον κυβερνοχώρο ολόκληρης της αξιακής αλυσίδας των ΤΠΕ, αξιοποιώντας τις εργασίες της εν λόγω πλατφόρμας.

[27] Βλέπε το έγγραφο εργασίας των υπηρεσιών της Επιτροπής με την εκτίμηση επιπτώσεων που συνοδεύει την πρόταση της Επιτροπής για οδηγία σχετικά με την ασφάλεια δικτύων και πληροφοριών, τμήμα 4.1.5.2.

[28] Ιδιαίτερα στο πλαίσιο του προτύπου M/490 για τα ευφυή δίκτυα όσον αφορά το πρώτο σύνολο προτύπων για ευφυές δίκτυο και αρχιτεκτονική αναφοράς.

- Να εξετάσει τρόπους με τους οποίους οι μεγάλοι πάροχοι υλισμικού και λογισμικού ΤΠΕ θα ήταν δυνατόν να ενημερώνουν τις αρμόδιες εθνικές αρχές περί των ευάλωτων σημείων που εντοπίζουν και τα οποία θα μπορούσαν να έχουν σημαντικές επιπτώσεις ασφάλειας.

Η Επιτροπή καλεί τον ENISA:

- Να αναπτύξει, σε συνεργασία με τις συναφείς αρμόδιες εθνικές αρχές, τους ενδιαφερόμενους φορείς, τους διεθνείς και ευρωπαϊκούς οργανισμούς τυποποίησης και το Κοινό Κέντρο Ερευνών της Ευρωπαϊκής Επιτροπής, **τεχνικές κατευθυντήριες γραμμές και συστάσεις για την θέσπιση προτύπων ΑΔΠ και καλών πρακτικών** στον δημόσιο και τον ιδιωτικό τομέα.

Η Επιτροπή καλεί τους ενδιαφερόμενους από τον δημόσιο και τον ιδιωτικό τομέα:

- Να προωθήσουν την ανάπτυξη και θέσπιση, υπό την καθοδήγηση της βιομηχανίας, προτύπων ασφάλειας, τεχνικών προτύπων και αρχές για την ασφάλεια βάσει σχεδιασμού και την ιδιωτικότητα βάσει σχεδιασμού, από τους κατασκευαστές προϊόντων ΤΠΕ και τους παρόχους υπηρεσιών, συμπεριλαμβανομένων και των παρόχων υπηρεσιών υπολογιστικού νέφους· οι νέες γενιές λογισμικού και υλισμικού πρέπει να είναι εξοπλισμένες με **ισχυρότερα, ενσωματωμένα και εύχρηστα χαρακτηριστικά ασφάλειας**.
- Να αναπτύξουν, υπό την καθοδήγηση της βιομηχανίας, πρότυπα για τις επιδόσεις των επιχειρήσεων στον τομέα της ασφάλειας του κυβερνοχώρου και να βελτιώσουν τις διαθέσιμες στο κοινό πληροφορίες αναπτύσσοντας **σήματα ασφάλειας** ή επίσημα σήματα που θα υποβοηθούν τους καταναλωτές στη διερεύνηση της αγοράς.

Ενίσχυση των επενδύσεων Ε&Α και της καινοτομίας

Η Ε&Α είναι σε θέση να υποστηρίξει μια ισχυρή βιομηχανική πολιτική, να προωθήσει μια αξιόπιστη ευρωπαϊκή βιομηχανία ΤΠΕ, να απογειώσει την εσωτερική αγορά και να μειώσει την ευρωπαϊκή εξάρτηση από αλλοδαπές τεχνολογίες. Η Ε&Α πρέπει να καλύψει τα τεχνολογικά κενά στον τομέα της ασφάλειας ΤΠΕ, να συμβάλλει στην προετοιμασία αντιμετώπισης της επόμενης γενιάς προκλήσεων ασφάλειας, να συνεκτιμήσει την διαρκή εξέλιξη των αναγκών των χρηστών και να αποκομίσει τα οφέλη από τις τεχνολογίες διπλής χρήσεως. Πρέπει επίσης να συνεχίσει να υποστηρίζει την ανάπτυξη της κρυπτογραφίας. Τα παραπάνω πρέπει να συμπληρωθούν με προσπάθειες τα αποτελέσματα της Ε&Α να μετατραπούν σε εμπορικές λύσεις με την παροχή των αναγκαίων κινήτρων και με την δημιουργία των κατάλληλων προϋποθέσεων από πλευράς πολιτικής.

Η ΕΕ πρέπει να αξιοποιήσει με τον καλύτερο τρόπο το πρόγραμμα πλαίσιο «Ορίζοντας 2020»[29] για την έρευνα και την καινοτομία, που θα ξεκινήσει το 2014. Η πρόταση της Επιτροπής περιέχει συγκεκριμένους στόχους για αξιόπιστες ΤΠΕ καθώς και για την πάταξη του ηλεκτρονικού εγκλήματος, που συμβαδίζουν με την παρούσα στρατηγική. Το πρόγραμμα Ορίζοντας 2020 θα υποστηρίξει έρευνα ασφάλειας που σχετίζεται με αναδυόμενες

[29] Το πρόγραμμα «Ορίζοντας 2020» είναι το χρηματοδοτικό μέσο υλοποίησης της εμβληματικής πρωτοβουλίας «Ένωση καινοτομίας» της στρατηγικής «Ευρώπη 2020» που αποσκοπεί στη διασφάλιση της ανταγωνιστικότητας της Ευρώπης σε παγκόσμια κλίμακα. Το νέο πρόγραμμα πλαίσιο έρευνας και καινοτομίας της ΕΕ θα υλοποιηθεί από το 2014 έως το 2020 ως μέρος της ώθησης για την δημιουργία νέας οικονομικής μεγέθυνσης και θέσεων απασχόλησης στην Ευρώπη.

τεχνολογίες ΤΠΕ, θα εξασφαλίσει λύσεις για ασφαλή διατερματικά συστήματα, υπηρεσίες και εφαρμογές ΤΠΕ, θα δώσει κίνητρα για την εφαρμογή και υιοθέτηση υφιστάμενων λύσεων, και θα αντιμετωπίσει την διαλειτουργικότητα μεταξύ δικτύων και συστημάτων πληροφοριών. Ιδιαίτερη προσοχή θα καταβληθεί σε επίπεδο ΕΕ για την βελτιστοποίηση και τον καλύτερο συντονισμό διαφόρων προγραμμάτων χρηματοδότησης (Ορίζοντας 2020, ταμείο εσωτερικής ασφάλειας, έρευνες του Ευρωπαϊκού Οργανισμού Άμυνας συμπεριλαμβανομένου του ευρωπαϊκού πλαισίου συνεργασίας).

Η Επιτροπή πρόκειται:

- Να χρησιμοποιήσει το πρόγραμμα Ορίζοντας 2020 για την αντιμετώπιση σειράς τομέων ιδιωτικότητας και ασφάλειας ΤΠΕ από την Ε&Α μέχρι την καινοτομία και την εγκατάσταση. Με το πρόγραμμα Ορίζοντας 2020 θα αναπτυχθούν επίσης εργαλεία και μέσα καταπολέμησης των εγκληματικών και τρομοκρατικών δραστηριοτήτων με στόχο τον κυβερνοχώρο.
- Να δημιουργήσει μηχανισμούς για τον καλύτερο συντονισμό των ερευνητικών θεματολογίων των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης και των κρατών μελών και να θεσπίσει κίνητρα προκειμένου τα κράτη μέλη να επενδύσουν περισσότερο στην Ε&Α.

Η Επιτροπή καλεί τα κράτη μέλη:

- Να αναπτύξουν, μέχρι το τέλος τους 2013, καλές πρακτικές προκειμένου να χρησιμοποιήσουν την **αγοραστική δύναμη της δημόσιας διοίκησης** (πχ. μέσω των δημόσιων συμβάσεων) για να τονώσουν την ανάπτυξη και την εγκατάσταση χαρακτηριστικών ασφάλειας σε προϊόντα και υπηρεσίες ΤΠΕ.
- Να προωθήσουν την έγκαιρη εμπλοκή της βιομηχανίας και της πανεπιστημιακής κοινότητας στην ανάπτυξη και τον συντονισμό λύσεων. Αυτό θα επιτευχθεί μέσω της πλήρους αξιοποίησης της ευρωπαϊκής βιομηχανικής βάσης και των συναφών τεχνολογικών καινοτομιών Ε&Α και θα αποτελέσει αντικείμενο συντονισμού των ερευνητικών θεματολογίων πολιτικών και στρατιωτικών οργανισμών.

Η Επιτροπή καλεί την Europol και τον ENISA:

- Να προσδιορίσουν τις αναδυόμενες τάσεις και ανάγκες με βάση τα εξελισσόμενα χαρακτηριστικά του ηλεκτρονικού εγκλήματος και της ασφάλειας στον κυβερνοχώρο, έτσι ώστε να αναπτυχθούν επαρκή ψηφιακά εργαλεία και τεχνολογίες για εγκληματολογικές έρευνες.

Η Επιτροπή καλεί τους ενδιαφερόμενους από τον δημόσιο και τον ιδιωτικό τομέα:

- Να αναπτύξουν, σε συνεργασία με τον κλάδο των ασφαλειών, **εναρμονισμένα συστήματα μέτρησης για τον υπολογισμό των ασφαλίστρων κινδύνου**, που θα επιτρέψουν στις εταιρείες οι οποίες έχουν κάνει επενδύσεις στον τομέα της ασφάλειας να επωφεληθούν από χαμηλότερα ασφάλιστρα κινδύνου.

2.5. Θέσπιση συνεκτικής διεθνούς πολιτικής κυβερνοχώρου για την Ευρωπαϊκή Ένωση και προώθηση των βασικών αξιών της ΕΕ

Η διατήρηση ανοικτού, ελεύθερου και ασφαλούς κυβερνοχώρου αποτελεί διεθνή πρόκληση, την οποία πρέπει να αντιμετωπίσει η ΕΕ με τους συναφείς διεθνείς εταίρους και οργανισμούς, τον ιδιωτικό τομέα και την κοινωνία των πολιτών.

Στο πλαίσιο της διεθνούς της πολιτικής για τον κυβερνοχώρο, η ΕΕ θα επιδιώξει να προωθήσει την διαφάνεια και την ελευθερία του διαδικτύου, να ενθαρρύνει τις προσπάθειες ανάπτυξης προτύπων συμπεριφοράς και την εφαρμογή του υφιστάμενου διεθνούς δικαίου στον κυβερνοχώρο. Η ΕΕ θα εργαστεί επίσης προς την κατεύθυνση κάλυψης του ψηφιακού χάσματος και θα συμμετάσχει ενεργά στις διεθνείς προσπάθειες δημιουργίας ικανότητας ασφάλειας στον κυβερνοχώρο. Η διεθνής δέσμευση της ΕΕ σε θέματα κυβερνοχώρου θα στηρίζονται στις θεμελιώδεις αξίες της ΕΕ για ανθρώπινη αξιοπρέπεια, ελευθερία, δημοκρατία, ισότητα, κράτος δικαίου και σεβασμό των θεμελιωδών δικαιωμάτων.

Ενσωμάτωση των ζητημάτων που αφορούν τον κυβερνοχώρο στις εξωτερικές σχέσεις της ΕΕ και στην κοινή εξωτερική πολιτική και την πολιτική ασφάλειας

Η Επιτροπή, η Ύπατη Εκπρόσωπος και τα κράτη μέλη πρέπει να διαμορφώσουν μια συνεκτική διεθνή πολιτική της ΕΕ για τον κυβερνοχώρο, με στόχο αυξημένη εμπλοκή και ισχυρότερες σχέσεις με διεθνείς εταίρους και οργανισμούς ζωτικής σημασίας, καθώς και με την κοινωνία των πολιτών και τον ιδιωτικό τομέα. Οι διαβουλεύσεις της ΕΕ με διεθνείς εταίρους σε ζητήματα κυβερνοχώρου πρέπει να σχεδιάζονται, να συντονίζονται και να υλοποιούνται με στόχο προστιθέμενη αξία σε υφιστάμενες διμερείς διαπραγματεύσεις μεταξύ των κρατών μελών της ΕΕ και τρίτων χωρών. Η ΕΕ θα ανανεώσει την έμφαση που αποδίδει στον διάλογο με τρίτες χώρες, εστιάζοντας ιδιαίτερα σε εταίρους με ανάλογες θέσεις και κοινές με την ΕΕ αξίες. Θα προωθήσει την επίτευξη υψηλού επιπέδου προστασίας των δεδομένων, συμπεριλαμβανομένης της διαβίβασης προσωπικών δεδομένων σε τρίτες χώρες Για την αντιμετώπιση των παγκόσμιων προκλήσεων στον κυβερνοχώρο, η ΕΕ θα επιδιώξει στενότερη συνεργασία με οργανισμούς που δραστηριοποιούνται στον εν λόγω τομέα όπως το Συμβούλιο της Ευρώπης, ο ΟΟΣΑ, τα Ηνωμένα Έθνη, ο ΟΑΣΕ, το ΝΑΤΟ, η Αφρικανική Ένωση, η Ένωση κρατών της νοτιοανατολικής Ασίας (ASEAN) και ο Οργανισμός Αμερικανικών Κρατών (OAS). Σε διμερές επίπεδο, η συνεργασία με τις Ηνωμένες Πολιτείες έχει ιδιαίτερη σημασία και θα αναπτυχθεί περαιτέρω, ιδίως στο πλαίσιο της ομάδας εργασίας ΕΕ-ΗΠΑ για την ασφάλεια στην κυβερνοχώρο και το ηλεκτρονικό έγκλημα.

Ένα από τα σημαντικά στοιχεία της διεθνούς πολιτικής της ΕΕ στον κυβερνοχώρο θα είναι η προβολή του κυβερνοχώρου ως περιοχής ελευθερίας και θεμελιωδών δικαιωμάτων. Η επέκταση της πρόσβασης στο διαδίκτυο αναμένεται να προωθήσει τις δημοκρατικές μεταρρυθμίσεις και την προαγωγή τους παγκοσμίως. Η αυξημένη παγκόσμια συνδεσιμότητα δεν πρέπει να συνοδευτεί από λογοκρισία ή μαζική επιτήρηση. Η ΕΕ πρέπει να προωθήσει την εταιρική κοινωνική ευθύνη[30] και να δρομολογήσει διεθνείς πρωτοβουλίες για την βελτίωση του παγκόσμιου συντονισμού στο εν λόγω πεδίο.

Η ευθύνη για ασφαλέστερο κυβερνοχώρο ανήκει σε όλους τους φορείς της παγκόσμιας κοινωνίας της πληροφορίας, από τους πολίτες μέχρι τις κυβερνήσεις. Η ΕΕ υποστηρίζει τις προσπάθειες καθορισμού προτύπων συμπεριφοράς στον κυβερνοχώρο τους οποίους πρέπει να υιοθετήσουν όλοι οι ενδιαφερόμενοι. Όπως η ΕΕ αναμένει από τους πολίτες να σέβονται τις υποχρεώσεις τους ως πολίτες, την κοινωνική ευθύνη και τους νόμους όταν βρίσκονται στο διαδίκτυο, έτσι και τα κράτη πρέπει να εφαρμόζουν τα πρότυπα και την κείμενη νομοθεσία. Σε ζητήματα διεθνούς ασφάλειας, η ΕΕ ενθαρρύνει την ανάπτυξη μέτρων οικοδόμησης εμπιστοσύνης στον τομέα της ασφάλειας του κυβερνοχώρου για την αύξηση της διαφάνειας και περιορισμό του κινδύνου παρανοήσεων στην συμπεριφορά των κρατών.

[30] Μια ανανεωμένη στρατηγική ΕΕ 2011-14 για την εταιρική κοινωνική ευθύνη, COM(2011) 681 τελικό

Η ΕΕ δεν ζητά να δημιουργηθούν νέα διεθνή νομικά μέσα για τα ζητήματα που αφορούν τον κυβερνοχώρο.

Πρέπει επίσης να γίνονται σεβαστές στο διαδίκτυο, οι νομικές υποχρεώσεις που περιλαμβάνονται στο Διεθνές Σύμφωνο των Ηνωμένων Εθνών για τα ατομικά και πολιτικά δικαιώματα, την Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων και στον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Η ΕΕ θα επικεντρωθεί επίσης στον τρόπο εξασφάλισης της εφαρμογής των εν λόγω μέτρων και στον κυβερνοχώρο.

Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, η σύμβαση της Βουδαπέστης αποτελεί μέσο που είναι ανοικτό για κύρωση από τρίτες χώρες. Παρέχει υπόδειγμα κατάρτισης εθνικής νομοθεσίας για την αντιμετώπιση του ηλεκτρονικού εγκλήματος και βάση για διεθνή συνεργασία στον εν λόγω τομέα.

Σε περίπτωση επέκτασης ένοπλων συγκρούσεων στον κυβερνοχώρο, εφαρμόζονται το διεθνές ανθρωπιστικό δίκαιο, και κατά περίπτωση, τα νομικά μέσα του δικαίου των ανθρωπίνων δικαιωμάτων. **Η ανάπτυξη ικανοτήτων στους τομείς της ασφάλειας του κυβερνοχώρου και των ανθεκτικών υποδομών πληροφοριών σε τρίτες χώρες**

Η ομαλή λειτουργία των βασικών υποδομών για την παροχή και διευκόλυνση υπηρεσιών επικοινωνιών θα επωφεληθεί από την αύξηση της διεθνούς συνεργασίας. Αυτή περιλαμβάνει ανταλλαγή βέλτιστων πρακτικών, ανταλλαγή πληροφοριών, κοινές ασκήσεις διαχείρισης κοινών συμβάντων έγκαιρης προειδοποίησης, κλπ.. Η ΕΕ θα συμβάλλει στην επίτευξη του στόχου αυτού εντείνοντας τις σε εξέλιξη διεθνείς προσπάθειες ενίσχυσης των δικτύων συνεργασίας για την προστασία υποδομών πληροφοριών ζωτικής σημασίας, με τη συμμετοχή κυβερνήσεων και του ιδιωτικού τομέα.

Από τις θετικές επιπτώσεις του διαδικτύου δεν επωφελούνται όλα τα μέρη του κόσμου, λόγω της έλλειψης ανοικτής, ασφαλούς, διαλειτουργικής και αξιόπιστης πρόσβασης. Κατά συνέπεια, η Ευρωπαϊκή Ένωση θα συνεχίσει να υποστηρίζει τις προσπάθειες των χωρών που επιδιώκουν να επεκτείνουν την πρόσβαση και τη χρήση του διαδικτύου για τους πολίτες τους, προκειμένου να εξασφαλιστεί η ακεραιότητα και η ασφάλειά του και να καταπολεμηθεί αποτελεσματικά το ηλεκτρονικό έγκλημα.

Σε συνεργασία με τα κράτη μέλη, η Επιτροπή και η Ύπατη Εκπρόσωπος πρόκειται:

- Να εργαστούν προς την κατεύθυνση κατάρτισης συνεκτικής διεθνούς πολιτικής της ΕΕ για τον κυβερνοχώρο ώστε να ενισχυθεί η συνεργασία με διεθνείς εταίρους και οργανισμούς ζωτικής σημασίας, να ενσωματωθούν τα ζητήματα που αφορούν τον κυβερνοχώρο στην ΚΕΠΠΑ και να βελτιωθεί ο συντονισμός όσον αφορά τα ζητήματα που αφορούν τον κυβερνοχώρο σε παγκόσμιο επίπεδο.
- Να υποστηρίξουν την ανάπτυξη προτύπων συμπεριφοράς και μέτρων οικοδόμησης εμπιστοσύνης στον τομέα της ασφάλειας του κυβερνοχώρου. Να διευκολύνουν το διάλογο σχετικά με τον τρόπο εφαρμογής του ισχύοντος διεθνούς δικαίου στον κυβερνοχώρο και θα προωθήσουν την σύμβαση της Βουδαπέστης για την αντιμετώπιση του ηλεκτρονικού εγκλήματος.
- Να υποστηρίξουν την προώθηση και την προστασία των θεμελιωδών δικαιωμάτων, συμπεριλαμβανομένων της πρόσβασης στις πληροφορίες και

της ελευθερίας της έκφρασης, εστιάζοντας στα ακόλουθα: α) ανάπτυξη νέων δημόσιων κατευθυντηρίων γραμμών σχετικά με την ελευθερία της έκφρασης ηλεκτρονικά, είτε σε διαδικτυακή σύνδεση είτε εκτός, β) παρακολούθηση της εξαγωγής προϊόντων ή υπηρεσιών που ενδέχεται να χρησιμοποιηθούν για διαδικτυακή λογοκρισία ή μαζική επιτήρηση, γ) ανάπτυξη μέτρων και εργαλείων για την επέκταση της πρόσβασης στο διαδίκτυο, του ανοικτού χαρακτήρα του και της ανθεκτικότητας για την αντιμετώπιση λογοκρισίας ή μαζικής επιτήρησης από τεχνολογίες επικοινωνιών, δ) ενίσχυση των ενδιαφερόμενων για να χρησιμοποιούν τεχνολογίες επικοινωνιών προκειμένου να προωθήσουν τα θεμελιώδη δικαιώματα.

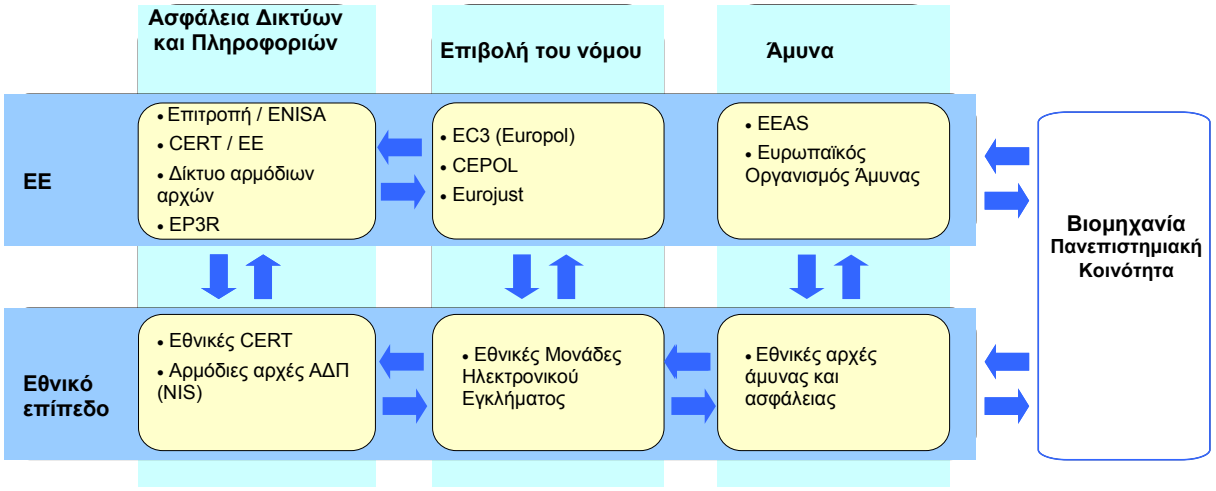
- Να συνεργαστούν με διεθνείς εταίρους και οργανισμούς, τον ιδιωτικό τομέα και την κοινωνία των πολιτών για την υποστήριξη της γενικής οικοδόμησης ικανοτήτων σε τρίτες χώρες αποβλέποντας στη βελτίωση της πρόσβασης στις πληροφορίες και στο ανοικτό διαδίκτυο, την πρόληψη και την αντιμετώπιση απειλών στον κυβερνοχώρο, συμπεριλαμβανομένων τυχαίων συμβάντων, του ηλεκτρονικού εγκλήματος και της τρομοκρατίας στον κυβερνοχώρο, καθώς και για την ανάπτυξη συντονισμού μεταξύ των δωρητών με στόχο την καθοδήγηση των προσπαθειών οικοδόμησης ικανοτήτων.
- Να χρησιμοποιήσουν διάφορα ενωσιακά μέτρα παροχής βοήθειας για την οικοδόμηση ικανοτήτων στον τομέα της ασφάλειας του κυβερνοχώρου. Συμπεριλαμβάνονται η στήριξη της κατάρτισης του προσωπικού των υπηρεσιών εφαρμογής του νόμου, δικαστικού και τεχνικού προσωπικού για την αντιμετώπιση απειλών στον κυβερνοχώρο, καθώς και η υποστήριξη της κατάρτισης συναφών εθνικών πολιτικών, στρατηγικών και θεσμικών οργάνων σε τρίτες χώρες.
- Να ενισχύσουν τον συντονισμό σε θέματα πολιτικής και ανταλλαγής πληροφοριών μέσω των διεθνών δικτύων προστασίας υποδομών πληροφοριών ζωτικής σημασίας όπως το δίκτυο Meridian, η συνεργασία μεταξύ των αρμόδιων αρχών ΑΔΠ και άλλων φορέων.

3. ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

Στην διασυνδεδεμένη ψηφιακή οικονομία και κοινωνία, τα συμβάντα στον κυβερνοχώρο δεν σταματούν στα σύνορα. Όλοι οι φορείς, από τις αρμόδιες αρχές ΑΔΠ, τις ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) και τις υπηρεσίες εφαρμογής του νόμου μέχρι και την βιομηχανία, πρέπει να αναλάβουν τις ευθύνες τους – τόσο εθνικά όσο και σε επίπεδο ΕΕ – και να συνεργαστούν για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Επειδή ίσως να εμπλέκονται διαφορετικά νομικά πλαίσια και δικαιοδοσίες, η κύρια πρόκληση για την ΕΕ είναι να αποσαφηνίσει τους ρόλους και τις αρμοδιότητες των πολυάριθμων εμπλεκόμενων φορέων.

Με δεομένη την πολυπλοκότητα του ζητήματος και την πολυμορφία των εμπλεκόμενων φορέων η απάντηση δεν είναι η κεντρική επιτήρηση σε ευρωπαϊκό επίπεδο. Οι εθνικές κυβερνήσεις βρίσκονται στην καλύτερη θέση για να οργανώσουν την πρόληψη και την επέμβαση σε περιπτώσεις συμβάντων και επιθέσεων στον κυβερνοχώρο και να αποκαταστήσουν επαφές και δίκτυα με τον ιδιωτικό τομέα και το κοινό στο πλαίσιο των υφιστάμενων πολιτικών και των δικαιακών συστημάτων. Ταυτόχρονα, λόγω του δυνητικού ή συγκεκριμένου διασυνοριακού χαρακτήρα των κινδύνων, η αποτελεσματική εθνική επέμβαση θα απαιτήσει συχνά την εμπλοκή και σε επίπεδο ΕΕ. Για την αντιμετώπιση της ασφάλειας

στον κυβερνοχώρο κατά ενδελεχή τρόπο, οι δραστηριότητες πρέπει να καλύπτουν τρεις πυλώνες ζωτικής σημασίας – ΑΔΠ, επιβολή του νόμου και άμυνα – που θα αναπτύσσονται μέσα σε διαφορετικά νομικά πλαίσια:



3.1. Συντονισμός μεταξύ αρμόδιων αρχών ΑΔΠ/CERT, υπηρεσιών επιβολής του νόμου και φορέων άμυνας

Εθνικό επίπεδο

Τα κράτη μέλη πρέπει να διαθέτουν, είτε ήδη σήμερα, είτε ως αποτέλεσμα της παρούσας στρατηγικής, δομές για ζητήματα ανθεκτικότητας στον κυβερνοχώρο, ηλεκτρονικού εγκλήματος και άμυνας, πρέπει δε να έχουν το απαιτούμενο επίπεδο ικανοτήτων για την αντιμετώπιση συμβάντων στον κυβερνοχώρο. Ωστόσο, λόγω του αριθμού των φορέων που ενδέχεται να έχουν αρμοδιότητες για διαφορετικές πτυχές της ασφάλειας στον κυβερνοχώρο και με δεδομένη τη σημασία της εμπλοκής του ιδιωτικού τομέα, ο συντονισμός σε εθνικό επίπεδο πρέπει να βελτιστοποιηθεί μεταξύ υπουργείων. Τα κράτη μέλη πρέπει να θεσπίσουν τις δικές τους εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο, καθώς και τους ρόλους και τις αρμοδιότητες των διάφορων εθνικών τους φορέων.

Πρέπει να υποστηριχτεί η ανταλλαγή πληροφοριών μεταξύ εθνικών φορέων και με τον ιδιωτικό τομέα ώστε τα κράτη μέλη και ο ιδιωτικός τομέας να μπορέσουν να διατηρήσουν σφαιρική αντίληψη των διαφόρων απειλών και να κατανοήσουν καλύτερα τις νέες τάσεις και τεχνικές που χρησιμοποιούνται, τόσο για να πραγματοποιηθούν επιθέσεις στον κυβερνοχώρο, όσο και για την ταχεία αντιμετώπισή τους. Καταρτίζοντας εθνικά σχέδια συνεργασίας ΑΔΠ που θα ενεργοποιηθούν σε περιπτώσεις συμβάντων στον κυβερνοχώρο, τα κράτη μέλη θα έχουν την δυνατότητα να κατανείμουν με σαφή τρόπο ρόλους και αρμοδιότητες και να βελτιστοποιήσουν μέτρα και ενέργειες επέμβασης.

Επίπεδο ΕΕ

Στο επίπεδο της ΕΕ όπως και στο εθνικό επίπεδο υπάρχουν αρκετοί φορείς που εμπλέκονται με την ασφάλεια στον κυβερνοχώρο. Συγκεκριμένα, ο ENISA, η Europol/EC3 και ο ΕΟΑ είναι τρεις υπηρεσίες που δραστηριοποιούνται στους τομείς της ΑΔΠ, της επιβολής του νόμου και της άμυνας αντίστοιχα. Οι εν λόγω υπηρεσίες έχουν διοικητικά συμβούλια στα οποία εκπροσωπούνται τα κράτη μέλη και αποτελούν πλατφόρμες για συντονισμό σε επίπεδο ΕΕ.

Θα ενθαρρυνθεί ο συντονισμός και η συνεργασία μεταξύ του ENISA, της Europol/EC3 και του ΕΟΑ σε σειρά τομέων στους οποίους εμπλέκονται από κοινού, ιδίως όσον αφορά την ανάλυση τάσεων, την εκτίμηση του κινδύνου, την εκπαίδευση και την ανταλλαγή βέλτιστων πρακτικών. Πρέπει να συνεργαστούν διατηρώντας τις ιδιαιτερότητές τους. Οι εν λόγω υπηρεσίες μαζί με την CERT της ΕΕ, την Επιτροπή και τα κράτη μέλη πρέπει να στηρίξουν την συγκρότηση μιας αξιόπιστης κοινότητας τεχνικών και πολιτικών εμπειρογνωμόνων στον υπόψη τομέα.

Οι ανεπίσημοι δίαυλοι συντονισμού και συνεργασίας θα συμπληρωθούν με πιο δομημένες σχέσεις. Το στρατιωτικό προσωπικό της ΕΕ και η ομάδα έργου του ΕΟΑ για την άμυνα στον κυβερνοχώρο είναι δυνατόν να χρησιμοποιηθούν ως φορείς συντονισμού στην άμυνα. Στην επιτροπή προγραμματισμού της Europol/EC3 θα συμμετέχουν μεταξύ άλλων η EUROJUST, η CEPOL, τα κράτη μέλη[31], ο ENISA και η Επιτροπή και θα έχουν την ευκαιρία να ανταλλάξουν την εξειδικευμένη τους τεχνογνωσία και να εξασφαλίσουν ότι οι δράσεις της EC3 υλοποιούνται στο πλαίσιο εταιρικών σχέσεων με αναγνώριση της προστιθέμενης εμπειρογνωμοσύνης και σεβασμό των αντίστοιχων εντολών όλων των ενδιαφερόμενων. Η νέα αποστολή του ENISA πρέπει να καταστήσει δυνατή την ενίσχυση των σχέσεων με την Europol και με τους ενδιαφερόμενους της βιομηχανίας. Το σημαντικότερο είναι ότι με τη νομοθετική πρόταση της Επιτροπής σχετικά με την ΑΔΠ θα θεσπιστεί πλαίσιο συνεργασίας μέσω ενός δικτύου αρμόδιων εθνικών αρχών ΑΔΠ και θα αντιμετωπιστεί η ανταλλαγή πληροφοριών μεταξύ των αρχών ΑΔΠ και των αρχών επιβολής του νόμου.

Διεθνές επίπεδο

Η Επιτροπή και η Ύπατη Εκπρόσωπος εξασφαλίζουν, σε συνδυασμό με τα κράτη μέλη, συντονισμένη διεθνή δράση στον τομέα της ασφάλειας του κυβερνοχώρου. Σε αυτό το πλαίσιο η Επιτροπή και η Ύπατη Εκπρόσωπος θα προβάλλουν τις βασικές αξίες της ΕΕ και θα προωθήσουν την ειρηνική, ανοικτή και διαφανή χρήση των τεχνολογιών του κυβερνοχώρου. Η Επιτροπή, η Ύπατη Εκπρόσωπος και τα κράτη μέλη συμμετέχουν σε πολιτικό διάλογο με διεθνείς εταίρους και με διεθνείς οργανισμούς, όπως το Συμβούλιο της Ευρώπης, ο ΟΟΣΑ, ΟΑΣΕ, το ΝΑΤΟ και τα Ηνωμένα Έθνη.

3.2. Υποστήριξη της ΕΕ σε περίπτωση μείζονος συμβάντος ή επίθεσης στον κυβερνοχώρο

Τα μείζονα συμβάντα ή επιθέσεις στον κυβερνοχώρο είναι πιθανόν να επηρεάσουν κυβερνήσεις, επιχειρήσεις και άτομα στην ΕΕ. Ως αποτέλεσμα της παρούσας στρατηγικής, και ιδίως της προτεινόμενης οδηγίας περί ΑΔΠ, πρέπει να βελτιωθούν η πρόληψη, ο εντοπισμός και η επέμβαση σε περιπτώσεις συμβάντων στον κυβερνοχώρο ενώ τα κράτη μέλη και η Επιτροπή πρέπει να τηρούν αλλήλους επαρκώς ενήμερους σχετικά με τέτοιες περιπτώσεις συμβάντων ή επιθέσεων. Ωστόσο, οι μηχανισμοί επέμβασης θα διαφέρουν ανάλογα με τη φύση, το μέγεθος και τις διασυνοριακές επιπτώσεις του συμβάντος.

Εάν το συμβάν έχει σοβαρές επιπτώσεις στην συνέχεια της επιχειρηματικής δραστηριότητας, η οδηγία περί ΑΔΠ προτείνει την ενεργοποίηση των εθνικών ή των ενωσιακών σχεδίων συνεργασίας ΑΔΠ, ανάλογα με την διασυνοριακή φύση του συμβάντος. Το δίκτυο των αρμόδιων αρχών ΑΔΠ θα χρησιμοποιηθεί στο πλαίσιο αυτό για την ανταλλαγή πληροφοριών και υποστήριξης. Αυτό θα επιτρέψει την διατήρηση ή/και την αποκατάσταση των πληγέντων δικτύων και υπηρεσιών.

[31] μέσω εκπροσώπησης στο πλαίσιο της ειδικής ομάδας δίωξης ηλεκτρονικού εγκλήματος της ΕΕ, την οποία αποτελούν οι επικεφαλής των μονάδων δίωξης ηλεκτρονικού εγκλήματος των κρατών μελών

Εάν το συμβάν φαίνεται ότι συνδέεται με εγκληματική ενέργεια, πρέπει να ενημερωθεί η Europol/EC3 έτσι ώστε – σε συνεργασία να τις αρχές επιβολής του νόμου από τις πληγείσες χώρες – να διαταχθεί έρευνα, να φυλαχθούν τα αποδεικτικά στοιχεία, να εντοπιστούν οι δράστες και, εν τέλει, να προσαχθούν στη δικαιοσύνη.

Εάν το συμβάν φαίνεται ότι συνδέεται με ηλεκτρονική κατασκοπία ή κρατικά υποστηριζόμενη επίθεση, ή ότι έχει επιπτώσεις στην εθνική ασφάλεια, οι εθνικές αρχές ασφάλειας και άμυνας θα κινητοποιήσουν τους εκάστοτε ομολόγους τους, έτσι ώστε να ενημερωθούν πως υφίστανται επίθεση και αν είναι σε θέση να αμυνθούν. Στη συνέχεια θα ενεργοποιηθούν οι μηχανισμοί έγκαιρης προειδοποίησης και, εφόσον απαιτηθεί, οι διαδικασίες διαχείρισης κρίσεων ή και άλλες διαδικασίες. Ένα αρκετά σοβαρό περιστατικό ή μια επίθεση στον κυβερνοχώρο θα μπορούσε να αποτελέσει επαρκή αιτία προκειμένου ένα κράτος μέλος να επικαλεστεί την ενωσιακή ρήτρα αλληλεγγύης (άρθρο 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης).

Εάν το συμβάν φαίνεται ότι έχει προσβάλει προσωπικά δεδομένα, πρέπει να εμπλακούν οι εθνικές αρχές προστασίας προσωπικών δεδομένων ή η εθνική ρυθμιστική αρχή σύμφωνα με την οδηγία 2002/58/ΕΚ.

Τέλος, για την αντιμετώπιση συμβάντων και επιθέσεων στον κυβερνοχώρο χρήσιμα μπορεί θα αποβούν τα δίκτυα επαφών και η υποστήριξη από τους διεθνείς εταίρους. Η εν λόγω υποστήριξη μπορεί να λάβει τη μορφή τεχνικής άμβλυνσης των επιπτώσεων, εγκληματολογικής έρευνας ή ενεργοποίησης των μηχανισμών επέμβασης στο πλαίσιο της διαχείρισης κρίσεων.

4. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΣΥΝΕΧΕΙΑ ΠΟΥ ΘΑ ΔΟΘΕΙ

Η παρούσα πρόταση για μια στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο που υποβάλλει η Επιτροπή και η Ύπατη Εκπρόσωπος της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας, περιγράφει το όραμα της ΕΕ στον υπόψη τομέα και τις απαιτούμενες δράσεις με βάση την ισχυρή προστασία και προώθηση των δικαιωμάτων των πολιτών, έτσι ώστε το διαδικτυακό περιβάλλον της ΕΕ να καταστεί το ασφαλέστερο παγκοσμίως[32].

Το όραμα αυτό μπορεί να υλοποιηθεί μόνο μέσω μιας γνήσιας εταιρικής σχέσης μεταξύ πολλών φορέων με σκοπό να αναλάβουν ευθύνες και να αντιμετωπίσουν τις επερχόμενες προκλήσεις.

Συνεπώς, η Επιτροπή και η Ύπατη Εκπρόσωπος καλούν το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο να εγκρίνουν την στρατηγική και να συμβάλουν στην υλοποίηση των δράσεων

[32] Η χρηματοδότηση της στρατηγικής θα πραγματοποιηθεί στο πλαίσιο των προβλεπόμενων κονδυλίων για κάθε σχετικό τομέα πολιτικής (ΔΣΕ, Ορίζοντας 2020, ταμείο εσωτερικής ασφάλειας, ΚΕΠΠΑ και εξωτερική συνεργασία, ιδίως τον μηχανισμό σταθερότητας) όπως προβλέπεται στην πρόταση της Επιτροπής για το πολυετές δημοσιονομικό πλαίσιο 2014-2020 (υπό την αίρεση της έγκρισης από την αρμόδια για τον προϋπολογισμό αρχή και τα τελικά ποσά του εγκεκριμένου ΠΔΠ για την περίοδο 2014-2020). Όσον αφορά την ανάγκη εξασφάλισης της συνολικής συμβατότητας με τον αριθμό των θέσεων που διατίθενται στις αποκεντρωμένες υπηρεσίες και το επιμέρους ανώτατο όριο για τις αποκεντρωμένες υπηρεσίες σε κάθε κεφάλαιο δαπανών στο επόμενο ΠΔΠ, οι υπηρεσίες (CEPOL, EOA, ENISA, EUROJUST και EUROPOL/EC3) από τις οποίες η παρούσα ανακοίνωση ζητά να αναλάβουν νέα καθήκοντα θα λάβουν προς τούτο στήριξη εφόσον έχει αποδειχτεί η πραγματική ικανότητα της υπηρεσίας για απορρόφηση πρόσθετων πόρων και έχουν εντοπιστεί όλες οι δυνατότητες αναδιάταξης πόρων.

που περιγράφονται. Απαιτείται επίσης ισχυρή υποστήριξη και δέσμευση από τον ιδιωτικό τομέα και την κοινωνία των πολιτών, που είναι φορείς ζωτικής σημασίας για την ενίσχυση του επιπέδου της ασφάλειάς μας και της διαφύλαξης των δικαιωμάτων των πολιτών.

Η ώρα της δράσης έφτασε. Η Επιτροπή και η Ύπατη Εκπρόσωπος είναι αποφασισμένοι να συνεργαστούν με όλους τους φορείς για να εξασφαλίσουν την απαιτούμενη ασφάλεια για την Ευρώπη. Για να εξασφαλίσουν την έγκαιρη εφαρμογή της στρατηγικής και την αξιολόγησή της ενόψει των πιθανών εξελίξεων, θα συγκαλέσει όλα τα ενδιαφερόμενα μέρη σε συνέδριο υψηλού επιπέδου και θα αξιολογήσουν την πρόοδο σε 12 μήνες.