ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ

Βρυξέλλες, 30.3.2009
COM(2009) 149 τελικό

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας

«Προστασία της Ευρώπης από επιθέσεις στον κυβερνοχώρο και διαταραχές μεγάλης κλίμακας: αναβάθμιση της ετοιμότητας, της ασφάλειας και της ικανότητας αποκατάστασης»

{SEC(2009) 399}
{SEC(2009) 400}

(υποβληθείσα από την Επιτροπή)

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας

«Προστασία της Ευρώπης από προσβολές στον κυβερνοχώρο και διαταραχές μεγάλης κλίμακας: αναβάθμιση της ετοιμότητας, της ασφάλειας και της ικανότητας αποκατάστασης»

1. ΕΙΣΑΓΩΓΗ

Οι Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ) είναι όλο και πιο αλληλένδετες με τις καθημερινές μας δραστηριότητες. Ορισμένα από αυτά τα συστήματα, υπηρεσίες, δίκτυα και υποδομές ΤΠΕ (εν συντομία υποδομές ΤΠΕ) αποτελούν ζωτικό τμήμα της ευρωπαϊκής οικονομίας και της κοινωνίας, είτε παρέχοντας βασικά αγαθά και υπηρεσίες ή αποτελώντας την πλατφόρμα στήριξης άλλων κρίσιμων υποδομών. Κατά κανόνα θεωρούνται υποδομές πληροφοριών ζωτικής σημασίας (ΥΖΣ)[1] δεδομένου ότι διαταραχή ή καταστροφή τους θα είχε σοβαρές επιπτώσεις στις ζωτικής σημασίας κοινωνικές λειτουργίες. Στα πρόσφατα παραδείγματα περιλαμβάνονται μεγάλης κλίμακας προσβολές στον κυβερνοχώρο με στόχο την Εσθονία το 2007 και η αποκοπή διηπειρωτικών καλωδίων το 2008.

Το Παγκόσμιο Οικονομικό Φόρουμ, εκτίμησε το 2008 ότι υπάρχει πιθανότητα 10 έως 20% για μεγάλης κλίμακας κατάρρευση ΥΖΣ κατά την επόμενη 10ετία, με δυνητικό παγκόσμιο οικονομικό κόστος περίπου 250 δισ. δολαρίων[2].

Η παρούσα ανακοίνωση επικεντρώνεται στην πρόληψη, την ετοιμότητα και την ευαισθητοποίηση, και καθορίζει ένα πρόγραμμα άμεσων δράσεων για την ενίσχυση της ασφάλειας και της ικανότητας αποκατάστασης των ΥΖΣ. Η εστίαση αυτή είναι συνεπής με τη συζήτηση που δρομολογήθηκε έπειτα από αίτημα του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου για την αντιμετώπιση των προκλήσεων και των προτεραιοτήτων όσον αφορά την πολιτική ασφάλειας δικτύων και πληροφοριών (NIS) και τα πλέον κατάλληλα μέσα που απαιτούνται σε επίπεδο ΕΕ για την αντιμετώπισή τους. Οι προτεινόμενες δράσεις είναι επίσης συμπληρωματικές προς αυτές που αφορούν την πρόληψη, την καταπολέμηση και τη δίωξη των εγκληματικών δραστηριοτήτων που στοχεύουν ΥΖΣ και συνδρομές με τις τρέχουσες και τις μελλοντικές ερευνητικές προσπάθειες της ΕΕ στο πεδίο της ασφάλειας δικτύων και πληροφοριών, καθώς και με διεθνείς πρωτοβουλίες στο πεδίο αυτό.

2. ΠΛΑΙΣΙΟ ΠΟΛΙΤΙΚΗΣ

Στην παρούσα ανακοίνωση αναπτύσσεται η ευρωπαϊκή πολιτική για την ενίσχυση της ασφάλειας και της εμπιστοσύνης στην κοινωνία της πληροφορίας. Ήδη το 2005, η Επιτροπή[3]

---

1 Ορισμός των ΥΖΣ προτείνεται COM(2005) 576 τελικό.
2 Global Risks 2008
3 COM(2005) 229

τόνισε την επείγουσα ανάγκη συντονισμού των προσπαθειών για την οικοδόμηση εμπιστοσύνης των ενδιαφερόμενων στον τομέα των ηλεκτρονικών επικοινωνιών και υπηρεσιών. Για το σκοπό αυτό εκδόθηκε το 2006 μια στρατηγική για ασφαλή κοινωνία της πληροφορίας[4]. Τα κύρια στοιχεία της, καθώς και η ασφάλεια και ικανότητα αποκατάστασης των υποδομών ΤΠΕ, εγκρίθηκαν στο ψήφισμα 2007/068/01 του Συμβουλίου. Ωστόσο, το ιδιοκτησιακό καθεστώς και η εφαρμογή από τα ενδιαφερόμενα μέρη φαίνονται ανεπαρκή. Η στρατηγική αυτή ενισχύει επίσης το ρόλο, σε τακτικό και επιχειρησιακό επίπεδο, του ευρωπαϊκού οργανισμού ασφάλειας δικτύων και πληροφοριών (ENISA), που ιδρύθηκε το 2004 για να συμβάλει στην επίτευξη των στόχων εξασφάλισης υψηλού και ουσιαστικού επιπέδου των NIS εντός της Κοινότητας και ανάπτυξης νοοτροπίας NIS προς όφελος των πολιτών της ΕΕ, των καταναλωτών, των επιχειρήσεων και της δημόσιας διοίκησης.

Το 2008 η εντολή προς τον ENISA παρατάθηκε, με τους ίδιους ακριβώς όρους έως το Μάρτιο του 2012[5]. Ταυτόχρονα, το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο ζήτησαν *«περαιτέρω συζήτηση σχετικά με το μέλλον του ENISA, καθώς και σχετικά με τη γενική κατεύθυνση των ευρωπαϊκών προσπαθειών στην αύξηση της ασφάλειας δικτύων και πληροφοριών»*. Για να υποστηρίξει τη συζήτηση αυτή, η Επιτροπή ξεκίνησε τον περασμένο Νοέμβριο διαδικτυακή δημόσια διαβούλευση[6], η ανάλυση της οποίας θα είναι διαθέσιμη σύντομα.

Οι δραστηριότητες που προβλέπονται στην παρούσα ανακοίνωση, διεξάγονται στο πλαίσιο και παράλληλα με το Ευρωπαϊκό πρόγραμμα προστασίας των υποδομών ζωτικής σημασίας (EPCIP)[7]. Βασικό στοιχείο του EPCIP είναι η οδηγία[8] για την ταυτοποίηση και τον χαρακτηρισμό των ευρωπαϊκών ΥΖΣ[9], η οποία προσδιορίζει τον τομέα των ΤΠΕ ως μελλοντικό τομέα προτεραιότητας. Ένα άλλο σημαντικό στοιχείο του EPCIP είναι το δίκτυο πληροφοριών προειδοποίησης υποδομών ζωτικής σημασίας (ΔΠΥΖΣ).[10]

Από κανονιστικής πλευράς, η πρόταση της Επιτροπής σχετικά με τη μεταρρύθμιση του κανονιστικού πλαισίου για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών[11] περιλαμβάνει νέες διατάξεις σχετικά με την ασφάλεια και την ακεραιότητα, ιδίως για την ενίσχυση των υποχρεώσεων των φορέων εκμετάλλευσης ώστε να υπάρξει εξασφάλιση ότι λαμβάνονται κατάλληλα μέτρα για την κάλυψη αναγνωρισμένων κινδύνων, να παρασχεθούν εγγυήσεις για τη συνέχεια της παροχής υπηρεσιών και να κοινοποιούνται οι παραβιάσεις της ασφάλειας[12]. Η προσέγγιση αυτή συμβάλει στο γενικό στόχο της βελτίωσης της ασφάλειας και της ικανότητας αποκατάστασης των ΥΖΣ. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο υποστηρίζουν ευρύτερα τις εν λόγω διατάξεις.

Οι δράσεις που προτείνονται στην παρούσα ανακοίνωση συμπληρώνουν τα υφιστάμενα και μελλοντικά μέτρα στο πεδίο της αστυνομικής και δικαστικής συνεργασίας για την πρόληψη, καταπολέμηση και δίωξη εγκληματικών και τρομοκρατικών δραστηριοτήτων με στόχο υποδομές ΤΠΕ, όπως προβλέπεται μεταξύ άλλων στην απόφαση-πλαίσιο του Συμβουλίου

---

4 COM(2006) 251
5 Κανονισμός (ΕΚ) αριθ. 1007/2008
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 τελικό
8 2008/114/ΕΚ
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
10 COM(2008) 676 τελικό
11 COM(2007) 697, COM(2007) 698, COM(2007) 699
12 Οδηγία πλαίσιο, άρθρο 13

σχετικά με τις επιθέσεις κατά των συστημάτων πληροφοριών[13] και την προγραμματισμένη επικαιροποίησή του[14].

Η πρωτοβουλία αυτή λαμβάνει υπόψη τις δραστηριότητες του ΝΑΤΟ για κοινή πολιτική στην άμυνα του κυβερνοχώρου, δηλαδή της διαχειριστικής αρχής για την άμυνα του κυβερνοχώρου και του συνεργατικού κέντρου αριστείας για την άμυνα του κυβερνοχώρου.

Τέλος, αποδίδεται δέουσα προσοχή στις διεθνείς πολιτικές εξελίξεις, ιδίως στις αρχές του G8 για προστασία ΥΖΣ[15]· στο ψήφισμα 58/199 της Γενικής Συνέλευσης του ΟΗΕ για *δημιουργία παγκόσμιας παιδείας ασφάλειας στον κυβερνοχώρο και προστασία των υποδομών πληροφοριών ζωτικής σημασίας* και στην πρόσφατη σύσταση του ΟΟΣΑ για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας.

3. ΤΙ ΔΙΑΚΥΒΕΥΕΤΑΙ

3.1. Οι υποδομές πληροφοριών ζωτικής σημασίας είναι καίριες για την οικονομία και την κοινωνική ανάπτυξη της ΕΕ

Ο οικονομικός και κοινωνικός ρόλος του τομέα των ΤΠΕ και των υποδομών ΤΠΕ τονίζεται σε πρόσφατες εκθέσεις για την καινοτομία και την οικονομική ανάπτυξη. Σε αυτές περιλαμβάνονται η ανακοίνωση για την ενδιάμεση επανεξέταση της πρωτοβουλίας i2010[16], η έκθεση της ομάδας Aho[17] και οι ετήσιες οικονομικές εκθέσεις της Ευρωπαϊκής Ένωσης[18]. Ο ΟΟΣΑ υπογραμμίζει τη σημασία των ΤΠΕ και του Διαδικτύου *«για την ενίσχυση των οικονομικών επιδόσεων και της κοινωνικής ευημερίας, για την ενδυνάμωση της ικανότητας των κοινωνιών για βελτίωση της ποιότητας ζωής των πολιτών σε όλο τον κόσμο»* [19]. Επίσης, συνιστά πολιτικές που ενισχύουν την εμπιστοσύνη στην υποδομή του Διαδικτύου.

Ο τομέας των ΤΠΕ είναι καίριος για όλα τα τμήματα της κοινωνίας. Οι εμπορικές συναλλαγές βασίζονται στον τομέα των ΤΠΕ, τόσο από άποψη απευθείας πωλήσεων όσο και ως προς την αποτελεσματικότητα των εσωτερικών διαδικασιών. Οι ΤΠΕ αποτελούν καθοριστικής σημασίας συνιστώσα καινοτομίας ενώ σε αυτές οφείλεται το 40% περίπου της αύξησης της παραγωγικότητας[20]. Η χρήση τους είναι επίσης διαδεδομένη στο έργο κυβερνήσεων και δημόσιων διοικήσεων: η αφομοίωση υπηρεσιών ηλε-διακυβέρνησης σε όλα τα επίπεδα, καθώς και νέες εφαρμογές, όπως καινοτόμες λύσεις που σχετίζονται με την υγεία, την ενέργεια και την πολιτική συμμετοχή, καθιστούν το δημόσιο τομέα εξαρτώμενο σε μεγάλο βαθμό από τις ΤΠΕ. Τέλος, αν μη τι άλλο, οι πολίτες στις καθημερινές τους δραστηριότητες προσφεύγουν σε διαρκώς μεγαλύτερο βαθμό στη χρήση ΤΠΕ: η ενίσχυση της ασφάλειας των ΥΖΣ θα αυξήσει την εμπιστοσύνη των πολιτών στις ΤΠΕ, τουλάχιστον λόγω καλύτερης προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής.

---

13 2005/222/JHA

14 COM(2008) 712

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_YZΣP_Principles.pdf

16 COM(2008) 199 τελικό

17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm

18 Ανασκόπηση 2007 της οικονομίας της ΕΕ
http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

19 http://www.oecd.org/dataoecd/1/29/40821707.pdf

20 http://epp.eurostat.ec.europa.eu/ - Επιστήμη και τεχνολογία/Κοινωνία της πληροφορίας

3.2. Οι κίνδυνοι που απειλούν τις υποδομές πληροφοριών ζωτικής σημασίας

Οι κίνδυνοι που οφείλονται σε ανθρωπογενείς επιθέσεις, φυσικές καταστροφές ή τεχνικές αστοχίες συχνά δεν είναι πλήρως κατανοητοί ή/και επαρκώς αναλυμένοι. Κατά συνέπεια, το επίπεδο συνειδητοποίησης μεταξύ των ενδιαφερόμενων είναι ανεπαρκές για την εκπόνηση και εφαρμογή αποτελεσματικών διασφαλίσεων και αντιμέτρων.

Οι επιθέσεις στον κυβερνοχώρο έχουν αυξηθεί σε άνευ προηγουμένου επίπεδο τεχνολογικής επιτήδευσης. Απλά πειράματα έχουν πλέον μετατραπεί σε πολύπλοκες δραστηριότητες που πραγματοποιούνται με σκοπό το κέρδος ή πολιτικούς λόγους. Η πρόσφατες μεγάλης κλίμακας επιθέσεις στον κυβερνοχώρο εναντίον της Εσθονίας, της Λιθουανίας και της Γεωργίας είναι τα ευρύτερα γνωστά παραδείγματα μιας γενικής τάσης. Ο τεράστιος αριθμός ιών, 'σκουληκιών' και άλλες μορφές κακόβουλου λογισμικού, η επέκταση των δικτύων προγραμμάτων ρομπότ (botnets) και η συνεχής αύξηση των ανεπίκλητων οχληρών μηνυμάτων (spam) επιβεβαιώνουν τη σοβαρότητα του προβλήματος [21].

Η υψηλή εξάρτηση από τις ΥΖΣ, οι διασυνοριακές τους διασυνδέσεις και αλληλεξαρτήσεις με άλλες υποδομές, καθώς και τα ευάλωτα σημεία και οι επιβουλές που αντιμετωπίζουν ορίζουν την ανάγκη αντιμετώπισης της ασφάλειας και της ικανότητα αποκατάστασής τους σε μια συστημική προοπτική, ως πρώτη γραμμή άμυνας εναντίων αστοχιών και επιθέσεων.

3.3. Ασφάλεια και ικανότητα αποκατάστασης των υποδομών πληροφοριών ζωτικής σημασίας με στόχο την τόνωση της εμπιστοσύνης στην κοινωνία της πληροφορίας

Για να εξασφαλιστεί ότι οι υποδομές ΤΠΕ χρησιμοποιούνται στο μέγιστο βαθμό, αξιοποιώντας έτσι πλήρως τις οικονομικές και κοινωνικές ευκαιρίες της κοινωνίας της πληροφορίας, πρέπει όλοι οι ενδιαφερόμενοι να έχουν υψηλό επίπεδο αξιοπιστίας και εμπιστοσύνης σε αυτές. Τούτο εξαρτάται από διάφορα στοιχεία, το σημαντικότερο από τα οποία είναι η εγγύηση υψηλού επιπέδου ασφάλειας και ικανότητας αποκατάστασης. Η ποικιλομορφία, ο ανοιχτός χαρακτήρας, η διαλειτουργικότητα, η χρηστικότητα, η διαφάνεια, η λογοδοσία, η ελεγξιμότητα των διαφόρων στοιχείων και ο ανταγωνισμός αποτελούν τις βασικές κινητήριες δυνάμεις για την ανάπτυξη ασφάλειας και την τόνωση της εξάπλωσης προϊόντων, διεργασιών και υπηρεσιών βελτιωμένης ασφάλειας. Όπως έχει ήδη υπογραμμίσει η Επιτροπή[22], πρόκειται για ζήτημα που μας αφορά: κανένας μεμονωμένος ενδιαφερόμενος δεν διαθέτει τα μέσα για να εγγυηθεί την ασφάλεια και την ικανότητα αποκατάστασης του συνόλου των υποδομών ΤΠΕ και για να αναλάβει όλες τις σχετικές ευθύνες.

Για την ανάληψη των ευθυνών αυτών απαιτείται προσέγγιση και παιδεία διαχείρισης του κινδύνου που θα είναι σε θέση να ανταποκριθεί σε γνωστές απειλές και να προλάβει άγνωστες μελλοντικές, χωρίς υπεραντίδραση και χωρίς να καταπνίξει την εμφάνιση καινοτόμων υπηρεσιών και εφαρμογών.

3.4. Οι προκλήσεις που αντιμετωπίζει η Ευρώπη

Επιπλέον και συμπληρωματικά προς το σύνολο των δραστηριοτήτων που σχετίζονται με την εφαρμογή της οδηγίας για τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών ΥΖΣ, ιδίως τον προσδιορισμό των τομεακών κριτηρίων για ΤΠΕ, πρέπει να αντιμετωπιστούν

---

[21] COM(2006) 688 τελικό

[22] COM(2006) 251 τελικό

ορισμένα ευρύτερα προβλήματα ώστε να ενισχυθεί η ασφάλεια και η ικανότητα αποκατάστασης των ΥΖΣ.

3.4.1. Άνισες και ασυντόνιστες εθνικές προσεγγίσεις

Παρόλο που υπάρχουν κοινά σημεία στα προβλήματα που έχουν να αντιμετωπίσουν, διαφέρουν μεταξύ των κρατών μελών τα μέτρα και τα καθεστώτα για την εγγύηση της ασφάλειας και της ικανότητας αποκατάστασης των ΥΖΣ, καθώς και το επίπεδο της εμπειρογνωμοσύνης και της ετοιμότητας.

Η αμιγώς εθνική προσέγγιση ενέχει τον κίνδυνο κατακερματισμού και αναποτελεσματικότητας σε ευρωπαϊκή κλίμακα. Οι διαφορές των εθνικών προσεγγίσεων και η έλλειψη συστηματικής διασυνοριακής συνεργασίας περιορίζουν σημαντικά την αποτελεσματικότητα των εγχώριων αντιμέτρων, μεταξύ άλλων, διότι, λόγω της διασύνδεσης των ΥΖΣ, η ύπαρξη χαμηλού επιπέδου ασφάλειας και ικανότητας αποκατάστασης των ΥΖΣ σε μια χώρα συνεπάγεται το ενδεχόμενο να αυξηθούν τα ευπαθή σημεία και οι κίνδυνοι σε άλλες.

Για να εξουδετερωθεί αυτή η κατάσταση απαιτείται ευρωπαϊκή προσπάθεια ώστε να επιτευχθεί προστιθέμενη αξία στις εθνικές πολιτικές και προγράμματα με την υποστήριξη της ευαισθητοποίησης και συναντίληψης των προκλήσεων· την τόνωση της υιοθέτησης κοινών πολιτικών στόχων και προτεραιοτήτων· την ενίσχυση της συνεργασίας μεταξύ κρατών μελών και τη μεγαλύτερη ενσωμάτωση των εθνικών πολιτικών σε ευρωπαϊκή και παγκόσμια διάσταση.

3.4.2. Η ανάγκη για ένα νέο ευρωπαϊκό μοντέλο διακυβέρνησης για τις ΥΖΣ

Η ενίσχυση της ασφάλειας και η ικανότητα αποκατάστασης των ΥΖΣ θέτει ιδιαίτερα προβλήματα διακυβέρνησης. Ενώ τα κράτη μέλη εξακολουθούν να φέρουν την τελική ευθύνη για τον καθορισμό των πολιτικών όσον αφορά τις ΥΖΣ, η εφαρμογή τους εξαρτάται από τη συμμετοχή του ιδιωτικού τομέα, ο οποίος κατέχει ή ελέγχει μεγάλο αριθμό ΥΖΣ. Από την άλλη πλευρά, οι αγορές δεν παρέχουν πάντοτε επαρκή κίνητρα ώστε ο ιδιωτικός τομέας να επενδύσει στην προστασία των ΥΖΣ στο επιθυμητό και αναμενόμενο από τις κυβερνήσεις επίπεδο.

Για την αντιμετώπιση αυτού του προβλήματος διακυβέρνησης έχουν εμφανιστεί συμπράξεις δημόσιου-ιδιωτικού τομέα (ΣΔΙΤ) σε εθνικό επίπεδο, όπως το υπόδειγμα αναφοράς. Ωστόσο, παρά τη συναίνεση ότι οι ΣΔΙΤ είναι επίσης σκόπιμες σε ευρωπαϊκό επίπεδο, οι ευρωπαϊκές ΣΔΙΤ δεν έχουν μέχρι σήμερα υλοποιηθεί. Ένα πανευρωπαϊκό πολυμερές πλαίσιο διακυβέρνησης, που μπορεί να περιλαμβάνει ενισχυμένο ρόλο για τον ENISA, θα μπορούσε να προωθήσει τη συμμετοχή του ιδιωτικού τομέα κατά τον καθορισμό των στρατηγικών στόχων δημόσιας πολιτικής, καθώς και τις επιχειρησιακές προτεραιότητες και τα μέτρα. Το πλαίσιο αυτό θα μπορούσε να γεφυρώσει το χάσμα μεταξύ εθνικής πολιτικής και της εκάστοτε επιχειρησιακής πραγματικότητας.

3.4.3. Περιορισμένη ευρωπαϊκή ικανότητα έγκαιρης προειδοποίησης και ανταπόκρισης σε συμβάντα

Οι μηχανισμοί διακυβέρνησης θα είναι πραγματικά αποτελεσματικοί μόνο αν όλοι οι συμμετέχοντες διαθέτουν αξιόπιστα στοιχεία προτού αναλάβουν δράση. Τούτο είναι

ιδιαίτερα σημαντικό για τις κυβερνήσεις που έχουν την τελική ευθύνη για τη εγγύηση της ασφάλειας και της ευημερίας των πολιτών.

Ωστόσο, οι διαδικασίες και οι πρακτικές για την παρακολούθηση και την υποβολή εκθέσεων σχετικά με συμβάντα που αφορούν την ασφάλεια του δικτύου διαφέρουν σημαντικά μεταξύ των κρατών μελών. Ορισμένα δεν διαθέτουν οργανισμό αναφοράς ως σημείο παρακολούθησης και ελέγχου. Ακόμη πιο σημαντικό, η συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των κρατών μελών για αξιόπιστα και αξιοποιήσιμα δεδομένα σχετικά με συμβάντα ασφάλειας δεν φαίνεται επαρκώς αναπτυγμένη, παραμένοντας άτυπη ή περιορισμένη σε διμερείς ή πολυμερείς ανταλλαγές μικρής έκτασης. Επιπλέον, η προσομοίωση συμβάντων και η εκτέλεση ασκήσεων για τον έλεγχο της ικανότητας αντίδρασης είναι στρατηγικής σημασίας για την ενίσχυση της ασφάλειας και της ικανότητας αποκατάστασης των ΥΖΣ, αποδίδοντας ιδιαίτερη προσοχή σε ευέλικτες στρατηγικές και διαδικασίες για την αντιμετώπιση της αδυναμίας πρόβλεψης ενδεχόμενων κρίσεων. Στην ΕΕ, οι ασκήσεις ασφάλειας στον κυβερνοχώρο παραμένουν ακόμα σε εμβρυακό στάδιο. Οι υπερεθνικές ασκήσεις είναι πολύ περιορισμένες. Όπως προέκυψε από πρόσφατα γεγονότα[23], η αλληλοβοήθεια αποτελεί ουσιώδες στοιχείο μιας ενδεδειγμένης απάντησης σε επιβουλές και προσβολές μεγάλης κλίμακας εναντίον ΥΖΣ.

Μια ισχυρή ευρωπαϊκή ικανότητα έγκαιρης προειδοποίησης και αντίδρασης σε συμβάντα πρέπει να βασίζεται στη καλή λειτουργία εθνικών/κυβερνητικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT), δηλαδή, διαθέτοντας κοινή γραμμή βάσης από άποψη ικανοτήτων. Οι φορείς αυτοί πρέπει να δρουν σε εθνικό επίπεδο ως καταλύτες των συμφερόντων των ενδιαφερόμενων φορέων και των δυνατοτήτων για δραστηριότητες δημόσιας πολιτικής (συμπεριλαμβανομένων εκείνων που σχετίζονται με την ανταλλαγή πληροφοριών και με συστήματα συναγερμού που προορίζονται για τους πολίτες και τις ΜΜΕ) και να συμμετέχουν σε αποτελεσματική διασυνοριακή συνεργασία και ανταλλαγή πληροφοριών, ενδεχομένως με την εμπλοκή υφισταμένων οργανισμών όπως η ευρωπαϊκή ομάδα κυβερνητικών CERT (EGC).[24]

3.4.4. Διεθνής συνεργασία

Η ανάπτυξη του Διαδικτύου ως βασικής ΥΖΣ απαιτεί ιδιαίτερη προσοχή όσον αφορά την οικεία ικανότητα αποκατάστασης και τη σταθερότητα. Το Διαδίκτυο, χάρη στον κατανεμημένο, πλεονάζοντα σχεδιασμό του έχει αποδειχθεί πολύ ισχυρή υποδομή. Ωστόσο, η εκπληκτική του ανάπτυξη είχε ως αποτέλεσμα την αύξηση της φυσικής και λογικής πολυπλοκότητας και την εμφάνιση νέων υπηρεσιών και χρήσεων: είναι θεμιτό να αμφισβητείται η ικανότητα του Διαδικτύου να αντισταθεί στον αυξανόμενο αριθμό διαταραχών και προσβολών στον κυβερνοχώρο.

Η απόκλιση των απόψεων σχετικά με την κρισιμότητα των στοιχείων που συνθέτουν το Διαδίκτυο, εξηγεί εν μέρει την ποικιλία των κυβερνητικών θέσεων που διατυπώνονται σε διεθνή φόρουμ και τις συχνά αντιφατικές αντιλήψεις της σημασίας του θέματος. Το γεγονός αυτό θα μπορούσε να παρεμποδίσει κατάλληλη πρόληψη, ετοιμότητα και ικανότητά ανάκτησης από επιβουλές που αφορούν το Διαδίκτυο. Για παράδειγμα, οι συνέπειες της μετάβασης από το IPv4 στο IPv6 πρέπει επίσης να αξιολογηθούν από την άποψη ασφάλειας των ΥΖΣ.

---

23 http://ec.europa.eu/information_society/policy/nis/strategy/activities/YZΣp/large_scale/

24 http://www.egc-group.org/

Το Διαδίκτυο είναι ένα παγκόσμιο και σε μεγάλο βαθμό κατανεμημένο δίκτυο δικτύων, όπου τα κέντρα ελέγχου δεν συμπίπτουν απαραίτητα με τα εθνικά σύνορα. Προς τούτο απαιτείται ειδική, στοχοθετημένη προσέγγιση, προκειμένου να εξασφαλιστεί ικανότητα αποκατάστασης και σταθερότητα, με βάση δύο συγκλίνουσες δράσεις. Πρώτον, επίτευξη συναίνεσης ως προς τις ευρωπαϊκές προτεραιότητες για την ικανότητα αποκατάστασης της σταθερότητας του Διαδικτύου, από άποψη δημόσιας τάξης και επιχειρησιακής εξάπλωσης. Δεύτερον, παρότρυνση της παγκόσμιας κοινότητας στην ανάπτυξη ενός συνόλου αρχών που να αντανακλά τις βασικές αξίες της Ευρώπης, όσον αφορά την ικανότητα αποκατάστασης και τη σταθερότητα του Διαδικτύου, στο πλαίσιο τού στρατηγικού μας διαλόγου και συνεργασίας με τρίτες χώρες και διεθνείς οργανισμούς. Οι δραστηριότητες αυτές θα βασίζονται στην αναγνώριση, εκ μέρους της Παγκόσμιας Διάσκεψης Κορυφής για την Κοινωνία της Πληροφορίας[25], της καίριας σημασίας που έχει η σταθερότητα για το Διαδίκτυο.

4. Η ΜΕΛΛΟΝΤΙΚΗ ΠΟΡΕΙΑ: ΠΡΟΣ ΠΕΡΙΣΣΟΤΕΡΟ ΣΥΝΤΟΝΙΣΜΟ ΚΑΙ ΣΥΝΕΡΓΑΣΙΑ ΣΕ ΚΛΙΜΑΚΑ ΕΕ

Λόγω της κοινοτικής και της διεθνούς διάστασης του προβλήματος, μια ολοκληρωμένη κοινοτική προσέγγιση για την ενίσχυση της ασφάλειας και της ικανότητας αποκατάστασης των ΥΖΣ θα συμπλήρωνε και θα προσέθετε αξία στα εθνικά προγράμματα, καθώς και στα υφιστάμενα διμερή και πολυμερή προγράμματα συνεργασίας μεταξύ των κρατών μελών.

Συζητήσεις περί δημόσιας πολιτικής ύστερα από τα γεγονότα στην Εσθονία υποδηλώνουν ότι οι επιπτώσεις παρόμοιων επιθέσεων μπορούν να περιοριστούν με τη λήψη μέτρων αποτροπής και με συντονισμένη δράση κατά τη διάρκεια της κρίσης. Περισσότερο δομημένη ανταλλαγή πληροφοριών και ορθής πρακτικής σε κλίμακα ΕΕ θα μπορούσε να διευκολύνει σημαντικά την καταπολέμηση διασυνοριακών απειλών.

Είναι απαραίτητο να ενισχυθούν τα υφιστάμενα μέσα συνεργασίας, συμπεριλαμβανομένου του ENISA, και, αν απαιτηθεί, να δημιουργηθούν νέα εργαλεία. Απαιτείται πολυμερής, πολυεπίπεδη προσέγγιση σε ευρωπαϊκό επίπεδο, με πλήρη σεβασμό και σε συμπλήρωση των εθνικών αρμοδιοτήτων.

Είναι απαραίτητη η λεπτομερής κατανόηση του περιβάλλοντος και των σχετικών περιορισμών. Για παράδειγμα, ένα σοβαρό ζήτημα τίθεται από τον κατανεμημένο χαρακτήρα του Διαδικτύου, όπου ακραίοι κόμβοι μπορούν να χρησιμοποιηθούν ως όχημα προσβολής, όπως π.χ. είναι τα botnets, δίκτυα προγραμμάτων ρομπότ. Ωστόσο, ο εν λόγω κατανεμημένος χαρακτήρας είναι βασικό συστατικό στοιχείο της σταθερότητας και της ικανότητας αποκατάστασης, μπορεί δε να συμβάλει σε ταχύτερη ανάκαμψη από ό,τι θα συνέβαινε κανονικά στην περίπτωση υπερβολικά τυποποιημένων διαδικασιών από πάνω προς τα κάτω. Προς τούτο απαιτείται προσεκτική κατά περίπτωση ανάλυση των δημόσιων πολιτικών και των επιχειρησιακών διαδικασιών που θα τεθούν σε εφαρμογή.

Ο χρονικός ορίζοντας είναι επίσης σημαντικό θέμα. Υπάρχει σαφής ανάγκη για ανάληψη δράσης τώρα θέτοντας ταχέως σε εφαρμογή τα αναγκαία στοιχεία για την οικοδόμηση ενός πλαισίου που θα μας επιτρέψει να ανταποκριθούμε στις τρέχουσες προκλήσεις και που θα τροφοδοτήσει τη μελλοντική στρατηγική για την ασφάλεια δικτύων και πληροφοριών.

---

[25] Θεματολόγιο της Τύνιδας για την Κοινωνία της πληροφορίας, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

Για την αντιμετώπιση των προκλήσεων αυτών προτείνονται πέντε άξονες:

(1) Ετοιμότητα και πρόληψη: εξασφάλιση ετοιμότητας σε όλα τα επίπεδα·

(2) Ανίχνευση και απόκριση: πρόβλεψη επαρκών μηχανισμών έγκαιρης προειδοποίησης·

(3) Άμβλυνση των επιπτώσεων και ανάκτηση: ενίσχυση κοινοτικών μηχανισμών για ΥΖΣ·

(4) Διεθνής συνεργασία: προώθηση των προτεραιοτήτων της ΕΕ διεθνώς·

(5) Κριτήρια για τον τομέα των ΤΠΕ: υποστήριξη της εφαρμογής της οδηγίας για τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας [26].

5. ΤΟ ΣΧΕΔΙΟ ΔΡΑΣΗΣ

5.1. Ετοιμότητα και πρόληψη

Αφετηρία ικανοτήτων και υπηρεσιών για πανευρωπαϊκή συνεργασία. Η Επιτροπή καλεί τα κράτη μέλη και στους ενδιαφερόμενους φορείς

- να καθορίζουν, με την υποστήριξη του ENISA, ελάχιστο επίπεδο ικανοτήτων και υπηρεσιών για τις εθνικές/κυβερνητικές ομάδες CERT και για ενέργειες αντίδρασης σε συμβάντα, σε στήριξη της πανευρωπαϊκής συνεργασίας.
- να βεβαιωθούν ότι οι εθνικές/κυβερνητικές ομάδες CERT λειτουργούν ως η βασική συνιστώσα των εθνικών δυνατοτήτων ετοιμότητας, ανταλλαγής πληροφοριών, συντονισμού και ανταπόκρισης.

Στόχος: τέλος του 2010 για επίτευξη συμφωνίας επί ελάχιστων προτύπων· τέλος του 2011 για καθιέρωση εύρυθμων εθνικών/κυβερνητικών ομάδων CERT σε όλα τα κράτη μέλη.

Ευρωπαϊκή εταιρική συνεργασία δημόσιου-ιδιωτικού τομέα για την ικανότητα αποκατάστασης (EP3R). Η Επιτροπή

- θα ενισχύσει τη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα σε στόχους ασφάλειας και ικανότητας αποκατάστασης, βασικές απαιτήσεις, ορθή πρακτική μέτρων και πολιτικής. Το κύριο βάρος της EP3R θα αφορά την ευρωπαϊκή διάσταση προοπτικών στρατηγικού (π.χ. ορθές πρακτικές πολιτικής) και τακτικού/επιχειρησιακού χαρακτήρα (π.χ. βιομηχανική ανάπτυξη). Η EP3R πρέπει να στηρίζεται και να συμπληρώνει τις υπάρχουσες εθνικές πρωτοβουλίες και τις επιχειρησιακές δραστηριότητες του ENISA.

Στόχος: τέλος του 2009 για χάρτη πορείας για την EP3R· μέσα του 2010 για την καθιέρωση της EP3R· τέλος του 2010 ώστε η EP3R να παραγάγει τα πρώτα αποτελέσματά της.

[26] Οδηγία 2008/114/ΕΚ του Συμβουλίου

Ευρωπαϊκό φόρουμ για την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών. Η Επιτροπή

- θα συγκροτήσει ευρωπαϊκό φόρουμ ώστε τα κράτη μέλη να ανταλλάσσουν πληροφορίες και ορθή πολιτική πρακτική για την ασφάλεια και την ικανότητα αποκατάστασης των ΥΖΣ. Το φόρουμ θα επωφεληθεί από τα αποτελέσματα των δραστηριοτήτων άλλων οργανισμών, ιδίως του ENISA.

Στόχος: τέλος του 2009 για έναρξη λειτουργίας του φόρουμ· τέλος του 2010 για τα πρώτα αποτελέσματα.

5.2. Ανίχνευση και απόκριση

Ευρωπαϊκό σύστημα συναγερμού και ανταλλαγής πληροφοριών (EISAS). Η Επιτροπή υποστηρίζει

την ανάπτυξη και εγκατάσταση του EISAS που προορίζεται για τους πολίτες και τις ΜΜΕ και βασίζεται σε εθνικά και ιδιωτικά συστήματα ανταλλαγής πληροφοριών και συναγερμού[27]. Η Επιτροπή στηρίζει οικονομικά δύο συμπληρωματικά έργα κατασκευής πρωτοτύπων. Ο ENISA καλείται να προβεί σε απολογισμό των αποτελεσμάτων των εν λόγω έργων και άλλων εθνικών πρωτοβουλιών και να καταρτίσει ένα χάρτη πορείας για την περαιτέρω ανάπτυξη και εξάπλωση του EISAS

Στόχος: τέλος του 2010 για ολοκλήρωση των έργων πρωτοτύπων· τέλος του *2010 για το χάρτη πορείας προς το ευρωπαϊκό σύστημα.*

5.3. Άμβλυνση των επιπτώσεων και αποκατάσταση

Σχεδιασμός αντιμετώπισης απρόοπτων καταστάσεων και ασκήσεις σε εθνική κλίμακα. Η Επιτροπή καλεί τα κράτη μέλη

- να καταρτίσουν εθνικά σχέδια έκτακτης ανάγκης και να διοργανώνουν τακτικά ασκήσεις για μεγάλης κλίμακας ανταπόκριση και αποκατάσταση καταστροφών σε περιπτώσεις συμβάντων σε δίκτυα ασφάλειας, ως βήμα προς στενότερο πανευρωπαϊκό συντονισμό. Σε εθνικές/κυβερνητικές ομάδες CERT/CSIRT μπορεί να ανατεθεί η διοργάνωση ασκήσεων και δοκιμών σχεδιασμού αντιμετώπισης απρόοπτων καταστάσεων σε εθνική κλίμακα, με συμμετοχή ενδιαφερόμενων από τον ιδιωτικό και το δημόσιο τομέα. Επιδιώκεται συμμετοχή του ENISA προς υποστήριξη της ανταλλαγής ορθής πρακτικής μεταξύ των κρατών μελών.

Στόχος: τέλος του 2010 για τη διεξαγωγή τουλάχιστο μιας άσκησης εθνικής κλίμακας σε κάθε κράτος μέλος.

---

[27] Στο πλαίσιο του κοινοτικού προγράμματος "*Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks*"
http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

Πανευρωπαϊκές ασκήσεις για περιπτώσεις συμβάντων ασφάλειας μεγάλης κλίμακας. Η Επιτροπή

- θα υποστηρίξει οικονομικά την ανάπτυξη πανευρωπαϊκών ασκήσεων σχετικά με συμβάντα ασφάλειας στο Διαδίκτυο[28], που μπορεί επίσης να αποτελέσουν την επιχειρησιακή πλατφόρμα για πανευρωπαϊκή συμμετοχή σε διεθνείς ασκήσεις για συμβάντα ασφάλειας μεγάλης κλίμακας, όπως η US Cyber Storm.

Στόχος: τέλος του 2010 για το σχεδιασμό και τη διοργάνωση της πρώτης πανευρωπαϊκής άσκησης· τέλος του 2010 για πανευρωπαϊκή συμμετοχή σε διεθνείς ασκήσεις.

Ενισχυμένη συνεργασία μεταξύ εθνικών/κυβερνητικών ομάδων CERT. Η Επιτροπή καλεί τα κράτη μέλη

- να ενισχύσουν τη συνεργασία μεταξύ εθνικών/κυβερνητικών ομάδων CERT, ενδεχομένως με συμβολή και επέκταση υφιστάμενων μηχανισμών συνεργασίας, όπως η EGC[29]. Καλείται ο ENISA να αναλάβει ενεργό ρόλο για την ενθάρρυνση και υποστήριξη της πανευρωπαϊκής συνεργασίας μεταξύ εθνικών/κυβερνητικών ομάδων CERT που αναμένεται να οδηγήσει σε αυξημένη ετοιμότητα· ενισχυμένη ευρωπαϊκή ικανότητα αντίδρασης και αντιμετώπισης περιστατικών· ασκήσεις σε πανευρωπαϊκή (ή/και περιφερειακή) κλίμακα.

Στόχος: τέλος του 2010 για διπλασιασμό του αριθμού των εθνικών φορέων που συμμετέχουν στην ECG· τέλος του 2010 για την εκπόνηση από τον ENISA υλικών αναφοράς προς υποστήριξη συνεργασίας σε πανευρωπαϊκή κλίμακα.

5.4. Διεθνής συνεργασία

Ικανότητα αποκατάστασης και σταθερότητα του Διαδικτύου. Προβλέπονται τρεις συμπληρωματικές ενέργειες

- Ευρωπαϊκές προτεραιότητες για την ικανότητα αποκατάστασης και τη σταθερότητα του διαδικτύου. Η Επιτροπή θα μεθοδεύσει πανευρωπαϊκή συζήτηση, με συμμετοχή όλων των σχετικών δημόσιων και ιδιωτικών ενδιαφερόμενων, ώστε να καθοριστούν οι προτεραιότητες της ΕΕ για μακροπρόθεσμη ικανότητα αποκατάστασης και σταθερότητας του διαδικτύου.

Στόχος: τέλος του 2010 για κοινοτικές προτεραιότητες για ζωτικής σημασίας συνιστώσες και θέματα του Διαδικτύου.

- Αρχές και κατευθύνσεις για ικανότητα αποκατάστασης και σταθερότητας του Διαδικτύου (σε ευρωπαϊκό επίπεδο). Η Επιτροπή θα συνεργαστεί με τα κράτη μέλη στον καθορισμό κατευθύνσεων για την ικανότητα αποκατάστασης και τη σταθερότητας του Διαδικτύου, εστιάζοντας μεταξύ άλλων σε περιφερειακές διορθωτικές δράσεις, συμφωνίες αμοιβαίας συνδρομής, συντονισμένες στρατηγικές αποκατάστασης και συνέχειας, γεωγραφική κατανομή ζωτικών πόρων του Διαδικτύου, τεχνολογικές διασφαλίσεις στην αρχιτεκτονική και τα πρωτόκολλα του Διαδικτύου, επανάληψη και διαφοροποίηση υπηρεσιών και

[28] *Βλ. παραπάνω, υπ.* 27
[29] *Βλ. παραπάνω, υπ* 24

δεδομένων. Η Επιτροπή χρηματοδοτεί ήδη μια ομάδα έργου για την ικανότητα ανάκτησης DNS η οποία, μαζί με άλλα σχετικά έργα, θα συμβάλει στην οικοδόμηση συναίνεσης[30].

Στόχος: τέλος του 2009 για ευρωπαϊκό χάρτη πορείας όσον αφορά αρχές και κατευθύνσεις για την ικανότητα αποκατάστασης και τη σταθερότητα του Διαδικτύου· τέλος του 2010 για τη συμφωνία επί του πρώτου σχεδίου αρχών και κατευθύνσεων.

- Αρχές και κατευθύνσεις για την ικανότητα αποκατάστασης και τη σταθερότητας του Διαδικτύου (σε παγκόσμιο επίπεδο). Η Επιτροπή θα συνεργαστεί με τα κράτη μέλη σχετικά με χάρτη πορείας για την προώθηση αρχών και κατευθύνσεων, σε παγκόσμια κλίμακα. Θα αναπτυχθεί στρατηγική συνεργασία με τρίτες χώρες, ιδίως στο πλαίσιο διαλόγων για την κοινωνία της πληροφορίας, ως μέσο για την οικοδόμηση παγκόσμιας συναίνεσης[31].

Στόχος: αρχές του 2010 για χάρτη πορείας όσον αφορά τη διεθνή συνεργασία σχετικά με αρχές και κατευθύνσεις για την ασφάλεια και την ικανότητα αποκατάστασης· τέλος του 2010 για το πρώτο σχέδιο διεθνώς αναγνωρισμένων αρχών και κατευθύνσεων που πρέπει να συζητηθούν με τρίτες χώρες και στα σχετικά φόρουμ, συμπεριλαμβανομένου του φόρουμ διαχείρισης του Διαδικτύου.

Ασκήσεις σε παγκόσμια διάσταση σχετικά με την αποκατάσταση και την άμβλυνση των επιπτώσεων συμβάντων μεγάλης κλίμακας στο Διαδίκτυο. Η Επιτροπή καλεί τους ευρωπαϊκούς ενδιαφερόμενους φορείς σε

- μελέτη πρακτικών τρόπων επέκτασης σε παγκόσμιο επίπεδο των ασκήσεων που διεξάγονται στο πλαίσιο του άξονα άμβλυνσης των επιπτώσεων και αποκατάστασης, με βάση περιφερειακά σχέδια και ικανότητες αντιμετώπισης απρόοπτων καταστάσεων.

Στόχος: τέλος του 2010 ώστε η Επιτροπή να προτείνει ένα πλαίσιο και έναν οδικό χάρτη για την υποστήριξη της ευρωπαϊκής συμμετοχής σε διεθνείς ασκήσεις σχετικά με την αποκατάσταση και την άμβλυνση των επιπτώσεων συμβάντων μεγάλης κλίμακας στο Διαδίκτυο.

5.5. Κριτήρια για ευρωπαϊκές υποδομές ζωτικής σημασίας στον τομέα των ΤΠΕ

Κλαδικά κριτήρια για ΤΠΕ. Βασιζόμενη στις αρχικές δραστηριότητες που διεξήχθησαν το 2008, η Επιτροπή

- θα συνεχίσει να αναπτύσσει, σε συνεργασία με τα κράτη μέλη και όλα τα ενδιαφερόμενα μέρη, τα κριτήρια για τον καθορισμό ευρωπαϊκών υποδομών ζωτικής σημασίας για τον τομέα των ΤΠΕ. Για το σκοπό αυτό, θα αντληθούν σχετικές πληροφορίες από ειδική μελέτη που έχει δρομολογηθεί[32].

Στόχος: πρώτο εξάμηνο του 2010 ώστε η Επιτροπή να καθορίσει τα κριτήρια για ευρωπαϊκές υποδομές ζωτικής σημασίας στον τομέα των ΤΠΕ.

30 *Βλ. παραπάνω, υπ* 27
31 COM(2008)588 τελικό
32 *Βλ. παραπάνω, υπ* 27

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ασφάλεια και η ικανότητα αποκατάστασης των ΥΖΣ είναι η πρώτη γραμμή άμυνας κατά των επιθέσεων και των αστοχιών. Η αναβάθμισή τους σε όλη την ΕΕ είναι απαραίτητη ώστε να αξιοποιηθούν πλήρως τα οφέλη της κοινωνίας της πληροφορίας. Για την επίτευξη του φιλόδοξου αυτού στόχου προτείνεται ένα σχέδιο δράσης για την ενίσχυση της τακτικής και επιχειρησιακής συνεργασίας σε ευρωπαϊκό επίπεδο. Η επιτυχία αυτών των δράσεων εξαρτάται από την αποτελεσματικότητά τους να βασιστούν και να επωφεληθούν από τις δραστηριότητες του δημόσιο και του ιδιωτικού τομέα, από τη δέσμευση και την πλήρη συμμετοχή των κρατών μελών, των ευρωπαϊκών θεσμικών οργάνων και των ενδιαφερόμενων φορέων.

Για το σκοπό αυτό, στις 27-28 Απριλίου 2009 θα διεξαχθεί υπουργική διάσκεψη ώστε να συζητηθούν με τα κράτη μέλη οι προτεινόμενες πρωτοβουλίες και να επισημοποιηθεί η δέσμευσή τους να συμμετάσχουν στο διάλογο σχετικά με μια εκσυγχρονισμένη και ενισχυμένη πολιτική NIS στην Ευρώπη.

Τέλος, η ενίσχυση της ασφάλειας και της ικανότητας αποκατάστασης των ΥΖΣ είναι μακροπρόθεσμος στόχος, του οποίου η στρατηγική και τα μέτρα έχουν ανάγκη από τακτικές αξιολογήσεις. Επομένως, δεδομένου ότι αυτός ο στόχος συμβαδίζει με την ευρύτερη συζήτηση για το μέλλον της πολιτικής ασφάλειας δικτύων και πληροφοριών στην ΕΕ μετά το 2012, προς το τέλος του 2010 η Επιτροπή θα δρομολογήσει μια απογραφή, με σκοπό, ανάλογα με την περίπτωση, την αξιολόγηση της πρώτης φάσης των δράσεων, τον προσδιορισμό και την διατύπωση πρότασης για τη λήψη περαιτέρω μέτρων.