ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ

Βρυξέλλες, 31.5.2006
COM(2006) 251 τελικό

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

Στρατηγική για ασφαλή κοινωνία της πληροφορίας – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων»

{SEC(2006) 656}

ΠΕΡΙΕΧΟΜΕΝΑ

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

Στρατηγική για ασφαλή κοινωνία της πληροφορίας – «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων »

1. ΕΙΣΑΓΩΓΗ

Στην ανακοίνωση «Η στρατηγική i2010 – Ευρωπαϊκή κοινωνία της πληροφορίας για την ανάπτυξη και την απασχόληση»"[1], υπογραμμίστηκε η σημασία της ασφάλειας δικτύων και πληροφοριών για τη δημιουργία ενός ενιαίου ευρωπαϊκού χώρου πληροφοριών. Η δυνατότητα διάθεσης, η αξιοπιστία και η ασφάλεια των δικτύων και των συστημάτων πληροφοριών αποκτούν διαρκώς περισσότερο κεντρική σημασία για τις οικονομίες μας και για τον κοινωνικό ιστό.

Σκοπός της παρούσας ανακοίνωσης είναι η αναζωογόνηση της στρατηγικής που η Ευρωπαϊκή Επιτροπή παρουσίασε το 2001, με την ανακοίνωση "Ασφάλεια δικτύων και πληροφοριών: Πρόταση ευρωπαϊκής πολιτικής"[2]. Πραγματοποιείται επισκόπηση της τρέχουσας κατάστασης όσον αφορά τις επιβουλές εναντίον της ασφάλειας της κοινωνίας της πληροφορίας και προσδιορίζονται τα πρόσθετα βήματα που πρέπει να πραγματοποιηθούν για τη βελτίωση της ασφάλειας δικτύων και πληροφοριών (NIS).

Με έμπνευση από την εμπειρία των κρατών μαλών και της Ευρωπαϊκής Κοινότητας, επιδιώκεται η περαιτέρω εξέλιξη μιας δυναμικής, σφαιρικής στρατηγικής στην Ευρώπη, βασιζόμενης στην ανάπτυξη κλίματος ασφάλειας και στηριζόμενης **στο διάλογο, σε πνεύμα συνεργασίας και στην ενίσχυση των ικανοτήτων**.

Κατά την αντιμετώπιση των προκλήσεων που αφορούν την ασφάλεια της κοινωνίας της πληροφορίας, η Ευρωπαϊκή Κοινότητα έχει αναπτύξει μια τριμερή προσέγγιση που καλύπτει: ειδικά μέτρα ασφάλειας δικτύων και πληροφοριών, πλαίσιο κανονιστικών ρυθμίσεων για τις ηλεκτρονικές επικοινωνίες (το οποίο περιλαμβάνει θέματα προστασίας της ιδιωτικής ζωής και προστασίας των δεδομένων), καθώς και καταπολέμηση αξιόποινων πράξεων στον κυβερνοχώρο. Μολονότι οι τρεις αυτές πτυχές μπορούν, σε ορισμένο βαθμό, να αναπτυχθούν χωριστά, οι πολυάριθμες μεταξύ τους αλληλεξαρτήσεις επιβάλλουν την εκπόνηση συντονισμένης στρατηγικής. Στην παρούσα ανακοίνωση καθορίζεται η στρατηγική και παρέχεται το πλαίσιο για τη συνέχιση και λεπτομερέστερη επεξεργασία συνεκτικής μεθόδου για την ασφάλεια δικτύων και πληροφοριών.

Στην ανακοίνωση του 2001, η ασφάλεια δικτύων και πληροφοριών ορίζεται ως "*ικανότητα ενός δικτύου ή ενός συστήματος πληροφοριών να προβάλλει αντίσταση, σε δεδομένο επίπεδο εμπιστοσύνης, σε τυχαία συμβάντα ή σε κακόβουλη δράση. Παρόμοια συμβάντα ή δράσεις μπορούν να θέσουν σε κίνδυνο τη διάθεση, την αυθεντικότητα, την ακεραιότητα και την εμπιστευτικότητα (τήρηση του απορρήτου) αποθηκευμένων ή μεταδιδόμενων δεδομένων, καθώς επίσης και συναφών υπηρεσιών που παρέχονται μέσω των εν λόγω δικτύων και συστημάτων.*"

---

[1] COM(2005) 229 τελικό 05.

[2] COM(2001) 298 τελικό της 6.6.2001.

Κατά τα τελευταία έτη, η Ευρωπαϊκή Κοινότητα έχει προχωρήσει στην υλοποίηση σειράς δράσεων για τη βελτίωση της ασφάλειας δικτύων και πληροφοριών.

Το πλαίσιο κανονιστικών ρυθμίσεων για τις ηλεκτρονικές επικοινωνίες, η ανασκόπηση του οποίου βρίσκεται σε εξέλιξη, περιλαμβάνει διατάξεις που αφορούν την ασφάλεια. Συγκεκριμένα, στην οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)[3] περιλαμβάνεται η υποχρέωση, για τους παρόχους δημόσια διαθεσίμων υπηρεσιών ηλεκτρονικών επικοινωνιών, να διασφαλίζουν την ασφάλεια των υπηρεσιών τους. Προβλέπονται διατάξεις εναντίον των ανεπίκλητων μηνυμάτων[4] και του κατασκοπευτικού λογισμικού[5].

Η εμπιστοσύνη και ασφάλεια αποτελούν επίσης σημαντικό σκέλος των προγραμμάτων της Ευρωπαϊκής Κοινότητας που αφορούν την έρευνα και την ανάπτυξη. Ευρύ φάσμα έργων του 6ου προγράμματος πλαισίου έρευνας πραγματεύεται τα εν λόγω θέματα. Η έρευνα που αφορά την ασφάλεια θα ενισχυθεί στο 7ο πρόγραμμα πλαίσιο, με την κατάρτιση ενός ευρωπαϊκού προγράμματος έρευνας στον τομέα της ασφάλειας (ESRP)[6]. Περαιτέρω, στο πρόγραμμα Safer Internet Plus, υποστηρίζεται η δικτύωση έργων και η ανταλλαγή βέλτιστης πρακτικής για την καταπολέμηση επιβλαβούς περιεχομένου που κυκλοφορεί σε δίκτυα πληροφοριών.

Ως μέρος της απόκρισης της σε επιβουλές εναντίον της ασφάλειας, η Ευρωπαϊκή Κοινότητα αποφάσισε το 2004 να δημιουργήσει τον ευρωπαϊκό οργανισμό ασφάλειας δικτύων και πληροφοριών (ENISA). Ο ENISA συμβάλλει στην ανάπτυξη και εμπέδωση ενός κλίματος ασφάλειας δικτύων και πληροφοριών προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των οργανισμών του δημόσιου τομέα, σε όλη την έκταση της Ευρωπαϊκής Ένωσης (ΕΕ).

Η ΕΕ έχει επίσης ενεργό ρόλο στα διεθνή fora που εξετάζουν τα θέματα αυτά, όπως ο ΟΟΣΑ, το Συμβούλιο της Ευρώπης ή τα Ηνωμένα Έθνη. Κατά την παγκόσμια διάσκεψη κορυφής για την κοινωνία της πληροφορίας, στην Τύνιδα, η ΕΕ υποστήριξε ένθερμα τις συζητήσεις γύρω από τη διάθεση, την αξιοπιστία και την ασφάλεια δικτύων και πληροφοριών. Το θεματολόγιο της Τύνιδας[7], που μαζί με τη δεσμευτική δήλωση της Τύνιδας καθορίζει τα περαιτέρω βήματα για τη συζήτηση των πολιτικών που αφορούν την παγκόσμια κοινωνία της πληροφορίας, όπως υιοθετήθηκαν από τους ηγέτες του κόσμου, υπογραμμίζει την ανάγκη να συνεχιστεί η καταπολέμηση των αξιόποινων πράξεων στον κυβερνοχώρο και των ανεπιθύμητων μηνυμάτων, με παράλληλη διασφάλιση της προστασίας της ιδιωτικής ζωής και της ελευθερίας της έκφρασης. Αναγνωρίζεται η ανάγκη συναντίληψης στα θέματα που αφορούν την ασφάλεια του Διαδικτύου, καθώς και περαιτέρω συνεργασίας για τη διευκόλυνση της συλλογής και διάδοσης πληροφοριών που αφορούν την ασφάλεια, και της ανταλλαγής ορθής πρακτικής μεταξύ όλων των ενδιαφερομένων σχετικά με μέτρα καταπολέμησης των επιβουλών εναντίον της ασφάλειας.

---

3 Οδηγία 2002/58/ΕΚ.

4 Ή ανεπίκλητα μηνύματα εμπορικού χαρακτήρα

5 Το κατασκοπευτικό λογισμικό είναι λογισμικό ιχνηλάτησης που εγκαθίσταται χωρίς σχετική υπόμνηση, συναίνεση ή έλεγχο του χρήστη.

6 Το ESPR καταρτίζεται κατά τη διάρκεια προκαταρκτικής δράσης έρευνας στον τομέα της ασφάλειας κατά τη χρονική περίοδο 2004-2006.

7 *Προς μια παγκόσμια εταιρική συνεργασία στην κοινωνία της πληροφορίας: Η συνέχεια στη δεύτερη φάση (Τύνιδα)της Παγκόσμιας Διάσκεψης Κορυφής για την Κοινωνία της Πληροφορίας (WSIS)*, COM(2006) 181 τελικό της 27.4.2006.

2. ΒΕΛΤΙΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ: ΟΙ ΒΑΣΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ

Παρά τις προσπάθειες που έχουν καταβληθεί σε διεθνές, ευρωπαϊκό και εθνικό επίπεδο, η ασφάλεια συνεχίζει να παρουσιάζει προβλήματα που ισοδυναμούν με αντίστοιχες προκλήσεις.

Κατά πρώτο, οι επιθέσεις εναντίον των συστημάτων πληροφορικής έχουν ως κίνητρο διαρκώς περισσότερο το κέρδος και όχι την πρόκληση διαταραχής και μόνο. Πραγματοποιείται παράνομη εξόρυξη δεδομένων, διαρκώς περισσότερο εν αγνοία του χρήστη, ενώ αυξάνεται με ταχείς ρυθμούς ο αριθμός των παραλλαγών (και ο ρυθμός εξέλιξης) του κακόβουλου λογισμικού[8]. Τα ανεπίκλητα μηνύματα αποτελούν χαρακτηριστικό παράδειγμα της εξέλιξης αυτής: καθίστανται το όχημα για επιθέσεις ιών και για δόλιες και αξιόποινες δραστηριότητες, όπως κατασκοπευτικό λογισμικό, ηλεκτρονικό 'ψάρεμα'[9] και άλλες μορφές κακόβουλου λογισμικού. Η ευρύτατη διάδοση των ανεπίκλητων μηνυμάτων βασίζεται διαρκώς περισσότερο σε δίκτυα ρομπότ (botnets)[10], δηλαδή σε εκτεθειμένους εξυπηρετητές και προσωπικούς υπολογιστές, οι οποίοι χρησιμοποιούνται ως αναμεταδότες εν αγνοία των ιδιοκτητών τους.

Η αυξανόμενη ανάπτυξη και εγκατάσταση κινητών συσκευών (συμπεριλαμβανομένων των κινητών τηλεφώνων τρίτης γενιάς, των φορητών βιντεοπαιχνιδιών κλπ.), καθώς και των δικτυακών υπηρεσιών που βασίζονται σε κινητά, θα αποτελέσουν νέες προκλήσεις, δεδομένης της ταχείας ανάπτυξης των υπηρεσιών που βασίζονται στο πρωτόκολλο διαδικτύου (IP). Οι διατάξεις αυτές θα μπορούσαν τελικά να αποβούν η συνηθέστερη δίοδος για πραγματοποίηση επιθέσεων από ό,τι οι προσωπικοί υπολογιστές, δεδομένου ότι οι τελευταίοι παρουσιάζουν ήδη σημαντικό επίπεδο ασφάλειας. Πράγματι, κάθε νέα μορφή πλατφόρμας επικοινωνίας και συστήματος πληροφοριών παρέχει αναπόφευκτα νέες ευκαιρίες για δόλιες προσβολές.

Μια άλλη σημαντική εξέλιξη είναι η εμφάνιση της «περιβάλλουσας νοημοσύνης», όπου σημειώνεται γενικευμένη παρουσία ευφυών συσκευών, με την υποστήριξη της υπολογιστικής τεχνολογίας και της δικτύωσης (π.χ. μέσω RFID[11], IPv6 και δικτύων από αισθητήρες). Η ολικά διασυνδεδεμένη και δικτυωμένη καθημερινή ζωή επαγγέλλεται σημαντικές ευκαιρίες. Ωστόσο, θα προκύψουν επίσης πρόσθετοι κίνδυνοι όσον αφορά την ασφάλεια και την προστασία της ιδιωτικής ζωής. Ενώ οι κοινές πλατφόρμες και εφαρμογές έχουν θετική συμβολή στη διαλειτουργικότητα και την αφομοίωση τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ), μπορούν επίσης να αυξήσουν τους κινδύνους. Όσο μεγαλύτερη είναι, παραδείγματος χάρη, η χρήση ετοιμοπαράδοτου λογισμικού, τόσο μεγαλύτερος ο αντίκτυπος σε περίπτωση εκμετάλλευσης του εύτρωτου χαρακτήρα ή της εμφάνισης ανεπαρκειών/βλαβών. Η εμφάνιση ορισμένων περιπτώσεων «μονοκαλλιέργειας» σε πλατφόρμες και εφαρμογές λογισμικού μπορεί να διευκολύνει κατά πολύ την αύξηση και διάδοση επιβουλών κατά της ασφάλειας, όπως το κακόβουλο λογισμικό και οι ιοί. **Η**

---

8 «Malware»

9 Το ηλεκτρονικό 'ψάρεμα' («phishing») είναι μια μορφή απάτης στο Διαδίκτυο, που αποβλέπει στην κλοπή πολύτιμων πληροφοριών, όπως πιστωτικές κάρτες, αριθμοί τραπεζικών λογαριασμών, ταυτότητες χρηστών και κωδικοί πρόσβασης.

10 Τα botnet είναι δίκτυα προγραμμάτων ρομπότ, δηλαδή εφαρμογές που εκτελούν δράσεις για λογαριασμό χειριστή εξ αποστάσεως, οι οποίες εγκαθίστανται μυστικά στη μηχανή του θύματος.

11 Ραδιοσυχνοτική αναγνώριση (Radio Frequency Identification).

διαφοροποίηση, ο ανοιχτός χαρακτήρας και η διαλειτουργικότητα είναι αναπόσπαστες συνιστώσες της ασφάλειας και πρέπει να προωθούνται.

Η σημασία του τομέα των ΤΠΕ για την ευρωπαϊκή οικονομία και για την ευρωπαϊκή κοινωνία ως σύνολο είναι αναμφισβήτητη. Οι ΤΠΕ αποτελούν καθοριστικής σημασίας συνιστώσα καινοτομίας και σε αυτές οφείλεται ποσοστό περίπου 40% της αύξησης της παραγωγικότητας. Επιπλέον, ο ιδιαίτερα καινοτομικός αυτός τομέας συμβάλλει κατά περισσότερο από ένα τέταρτο στη συνολική ευρωπαϊκή προσπάθεια Ε&Α και διαδραματίζει καίριο ρόλο στη δημιουργία οικονομικής ανάπτυξης και απασχόλησης σε όλους τους κλάδους της οικονομίας. Διαρκώς περισσότεροι ευρωπαίοι ζουν σε μια γνήσια κοινωνία της πληροφορίας όπου η χρήση ΤΠΕ έχει αυξηθεί με ταχείς ρυθμούς, ως βασική λειτουργία στις κοινωνικές και οικονομικές επαφές των ανθρώπων. Σύμφωνα με την Eurostat, 89% των κοινοτικών επιχειρήσεων χρησιμοποιούσαν ενεργά το Διαδίκτυο κατά το 2004, ενώ περίπου 50% των καταναλωτών το είχαν πρόσφατα χρησιμοποιήσει[12].

Μια παραβίαση της ασφάλειας δικτύων και πληροφοριών (NIS) μπορεί να προκαλέσει επιπτώσεις που υπερβαίνουν την οικονομική διάσταση. Πράγματι, υπάρχει γενικότερη ανησυχία ότι τα προβλήματα ασφάλειας μπορούν να αποθαρρύνουν και να περιορίσουν την αφομοίωση των ΤΠΕ, ενώ η διάθεση, η αξιοπιστία και η ασφάλεια αποτελούν προϋποθέσεις για την εγγύηση των θεμελιωδών δικαιωμάτων στις επιγραμμικές επικοινωνίες.

Εξάλλου, εξαιτίας της αυξημένης συνδετικότητας μεταξύ δικτύων, και άλλες υποδομές καθοριστικής σημασίας (όπως οι μεταφορές, η ενέργεια κλπ.) καθίστανται επίσης διαρκώς περισσότερο εξαρτημένες από την ακεραιότητα των αντίστοιχων συστημάτων πληροφοριών τους.

Τόσο οι επιχειρήσεις όσο και οι πολίτες στην Ευρώπη συνεχίζουν να υποτιμούν τους κινδύνους. Τούτο οφείλεται σε διάφορους λόγους, ο σημαντικότερος όμως, στην περίπτωση των επιχειρήσεων, είναι μάλλον ότι δεν προκύπτει σαφώς η απόδοση των επενδύσεων στον τομέα της ασφάλειας, ενώ στην περίπτωση των πολιτών το γεγονός ότι δεν είναι ενήμεροι για το μερίδιο ευθύνης που τους αντιστοιχεί στην παγκόσμια αλυσίδα της ασφάλειας.

Πράγματι, δεδομένης της γενικευμένης παρουσίας των ΤΠΕ και των συστημάτων πληροφοριών, η ασφάλεια δικτύων και πληροφοριών συνιστά πρόκληση για όλους ανεξαιρέτως:

- **Οι δημόσιες διοικήσεις** πρέπει να αντιμετωπίσουν το ζήτημα της ασφάλειας των συστημάτων τους, όχι απλώς για την προστασία των πληροφοριών του δημόσιου τομέα, αλλά και για να αποτελέσουν υπόδειγμα βέλτιστης πρακτικής για άλλους παράγοντες·

- **Οι επιχειρήσεις** πρέπει να αντιμετωπίσουν την ασφάλεια δικτύων και πληροφοριών (NIS) μάλλον ως μέρος του ενεργητικού τους και στοιχείο ανταγωνιστικού πλεονεκτήματος, παρά ως «αρνητικό κόστος»·

- **Οι μεμονωμένοι χρήστες** πρέπει να αντιληφθούν ότι τα οικιακά συστήματά τους είναι καθοριστικής σημασίας για το σύνολο της «αλυσίδας της ασφάλειας».

---

12 Eurostat, *Internet activities in the European Union*, 40/2005.

Για την επιτυχή αντιμετώπιση των προβλημάτων που περιγράφονται παραπάνω, πρέπει όλοι οι ενδιαφερόμενοι να διαθέτουν αξιόπιστα δεδομένα αναφορικά με συμβάντα και τάσεις στον τομέα της ασφάλειας. Ωστόσο, είναι δύσκολη η συγκέντρωση αξιόπιστων και σφαιρικών δεδομένων για συμβάντα αυτού του είδους, και τούτο για πολλούς λόγους, από την ταχύτητα με την οποία μπορούν να εμφανιστούν συμβάντα ασφαλείας, έως την έλλειψη προθυμίας ορισμένων οργανισμών όσον αφορά την αποκάλυψη και δημοσίευση παραβιάσεων που αφορούν την ασφάλεια. Ωστόσο, ένας από τους ακρογωνιαίους λίθους για την ανάπτυξη της κλίματος ασφάλειας είναι η **βελτίωση των γνώσεών μας σχετικά με το πρόβλημα**.

Προγράμματα ευαισθητοποίησης, που προορίζονται να υπογραμμίσουν τις επιβουλές σε βάρος της ασφάλειας, είναι σημαντικό να μην υποσκάπτουν την εμπιστοσύνη των καταναλωτών και των χρηστών εστιαζόμενα αποκλειστικά στις αρνητικές πτυχές της ασφάλειας. Θα πρέπει κατά συνέπεια, οπότε δίδεται η ευκαιρία, **η ασφάλεια δικτύων και πληροφοριών να παρουσιάζεται ως αξία και ως ευκαιρία**, και όχι ως βάρος και ως κόστος. Πρέπει να θεωρείται ως ένα προσόν για την οικοδόμηση της εμπιστοσύνης των καταναλωτών, ως ανταγωνιστικό πλεονέκτημα για τις επιχειρήσεις που λειτουργούν συστήματα πληροφοριών, καθώς και ως θέμα που αφορά την ποιότητα των προσφερόμενων υπηρεσιών για παρόχους του δημόσιου και του ιδιωτικού τομέα.

Η βασική πρόκληση την οποία αντιμετωπίζουν οι ιθύνοντες χάραξης πολιτικής είναι η επίτευξη μιας ολιστικής προσέγγισης. Στην προσέγγιση αυτή θα πρέπει να αναγνωρίζονται οι αντίστοιχοι ρόλοι των διαφόρων ενδιαφερομένων. Πρέπει να εξασφαλίζεται κατάλληλος συντονισμός των διαφόρων διατάξεων που αφορούν τη δημόσια πολιτική και τις κανονιστικές ρυθμίσεις και που έχουν άμεσο ή έμμεσο αντίκτυπο στην NIS. Από τις διαδικασίες ελευθέρωσης, κατάργησης των κανονιστικών ρυθμίσεων και σύγκλισης προέκυψε πλήθος πρωταγωνιστών μεταξύ των διάφορων ομάδων εμπλεκόμενων παραγόντων, γεγονός που δυσχεραίνει περαιτέρω το εν λόγω έργο. Η συμβολή του ENISA στην επίτευξη αυτού του στόχου μπορεί να είναι σημαντική. Ο οργανισμός θα μπορούσε να λειτουργήσει ως κέντρο ανταλλαγής πληροφοριών, συνεργασίας μεταξύ όλων των εμπλεκόμενων παραγόντων, καθώς και ανταλλαγής συνιστώμενης πρακτικής, τόσο μέσα στην Ευρώπη όσο και με τον υπόλοιπο κόσμο, ώστε να συμβάλει στην ανταγωνιστικότητα του ευρωπαϊκού κλάδου ΤΠΕ και στην εύρυθμη λειτουργία της εσωτερικής αγοράς.

3. ΠΡΟΣ ΜΙΑ ΔΥΝΑΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΗΣ ΚΟΙΝΩΝΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΜΕ ΑΣΦΑΛΕΙΑ

Η κοινωνία της πληροφορίας με ασφάλεια πρέπει να βασίζεται σε **βελτιωμένη ασφάλεια δικτύων και πληροφοριών** και σε ευρύτατα διαδεδομένο **κλίμα ασφάλειας**. Για το σκοπό αυτό, η Ευρωπαϊκή Επιτροπή προτείνει μια **δυναμική και ολοκληρωμένη προσέγγιση** που περιλαμβάνει όλους τους εμπλεκόμενους παράγοντες και βασίζεται **στο διάλογο, σε πνεύμα συνεργασίας και στην ενίσχυση των ικανοτήτων**. Με δεδομένους τους συμπληρωματικούς ρόλους του δημόσιου και του ιδιωτικού τομέα για τη δημιουργία ενός κλίματος ασφάλειας, οι πρωτοβουλίες πολιτικής στο εν λόγω πεδίο πρέπει να βασίζονται σε **ανοιχτό και περιεκτικό πολυμερή διάλογο**.

Η εν λόγω προσέγγιση και οι συνδεδεμένες με αυτήν δράσεις θα συμπληρώσουν και θα εμπλουτίσουν το σχέδιο της Επιτροπής για τη συνέχιση της ανάπτυξης ενός περιεκτικού και δυναμικού πλαισίου πολιτικής μέσα από σειρά πρωτοβουλιών κατά το 2006:

(1) Ενασχόληση με τις εξελίξεις στα ανεπίκλητα μηνύματα και τις επιβουλές, όπως το κατασκοπευτικό λογισμικό και άλλες μορφές κακόβουλου λογισμικού, σε ανακοίνωση που θα αφορά τα συγκεκριμένα αυτά θέματα.

(2) Υποβολή προτάσεων για τη βελτίωση της συνεργασίας μεταξύ των αρχών επιβολής του νόμου και αντιμετώπιση νέων μορφών αξιόποινων δράσεων που εκμεταλλεύονται το Διαδίκτυο και υποσκάπτουν τη λειτουργία νευραλγικών υποδομών. Τούτο θα αποτελέσει αντικείμενο ειδικής ανακοίνωσης σχετικά με τις αξιόποινες πράξεις στον κυβερνοχώρο.

Οι εν λόγω πρωτοβουλίες πολιτικής συμπληρώνουν επίσης την προγραμματιζόμενη δραστηριότητα για την επίτευξη των στόχων της πράσινης βίβλου της Επιτροπής για το Ευρωπαϊκό Πρόγραμμα Προστασίας των Υποδομών Ζωτικής Σημασίας (EPCIP)[13], που εκπονήθηκε σε ανταπόκριση αιτήματος του Συμβουλίου του Δεκεμβρίου 2004. Η διαδικασία της πράσινης βίβλου αναμένεται ότι θα καταλήξει σε σχέδιο δράσης που θα συνδυάζει συνολική προσέγγιση πλαισίου αναφορικά με την προστασία νευραλγικών υποδομών με τις απαραίτητες κλαδικές πολιτικές, συμπεριλαμβανομένης και μιας για τον κλάδο των ΤΠΕ. Στην κλαδική πολιτική για τις ΤΠΕ θα εξεταστούν, μέσω **πολυμερούς διαλόγου**, οι σχετικές οικονομικές, επιχειρηματικές και κοινωνικές κινητήριες δυνάμεις αποβλέποντας στη βελτίωση της ασφάλειας και την ανθεκτικότητα των δικτύων και των συστημάτων πληροφοριών.

Επίσης, στην ανασκόπηση του 2006 του πλαισίου των κανονιστικών ρυθμίσεων για τις ηλεκτρονικές επικοινωνίες, θα εξεταστούν και στοιχεία βελτίωσης των NIS, όπως μέτρα τεχνικού και οργανωτικού χαρακτήρα που πρέπει να ληφθούν από παρόχους υπηρεσιών, διατάξεις που αφορούν την κοινοποίηση παραβιάσεων ασφαλείας, καθώς και συγκεκριμένα επανορθωτικά μέτρα και κυρώσεις αναφορικά με παραβάσεις υποχρεώσεων.

Η παροχή λύσεων, υπηρεσιών και προϊόντων ασφαλείας στους τελικούς χρήστες είναι σε μεγάλο βαθμό έργο του ιδιωτικού τομέα. Έχει επομένως στρατηγική σημασία να είναι η **ευρωπαϊκή βιομηχανία απαιτητικός χρήστης** προϊόντων και υπηρεσιών ασφαλείας, **καθώς και ανταγωνιστικός προμηθευτής** προϊόντων και υπηρεσιών NIS.

Οι εθνικές κυβερνήσεις πρέπει να είναι σε θέση να προσδιορίζουν και να υλοποιούν βέλτιστη πρακτική κατά τη χάραξη πολιτικών, καθώς επίσης να επιδεικνύουν τη δέσμευσή τους στους εν λόγω στόχους πολιτικής μέσω της ασφαλούς διαχείρισης των δικών τους συστημάτων πληροφοριών. Οι δημόσιες αρχές, στα κράτη μέλη και σε κοινοτικό επίπεδο, θα έχουν καίριο ρόλο στην ορθή ενημέρωση των χρηστών ώστε να τους δοθεί η δυνατότητα να συμβάλουν στη δική τους ασφάλεια. Η αύξηση της ευαισθητοποίησης σε θέματα NIS και η παροχή κατάλληλης και έγκαιρης πληροφόρησης μέσα από αποκλειστικές δικτυακές πύλες ηλεκτρονικής ασφάλειας για θέματα επιβουλών, κινδύνων και προειδοποιήσεων, καθώς και σχετικά με περιπτώσεις βέλτιστης πρακτικής θα πρέπει να αντιμετωπιστούν κατά προτεραιότητα. Για το σκοπό αυτό, μείζων στόχος για τον ENISA θα μπορούσε να είναι η εξέταση της σκοπιμότητας **δημιουργίας ευρωπαϊκού πολυγλωσσικού συστήματος ανταλλαγής πληροφοριών και έγκαιρης προειδοποίησης**, το οποίο θα βασίζεται και θα συνδέει υφιστάμενες ή προγραμματιζόμενες εθνικές, δημόσιες και ιδιωτικές πρωτοβουλίες.

---

[13] COM(2005) 576 τελικό της 17.11.2005.

Η παγκόσμια διάσταση των προκλήσεων όσον αφορά την ασφάλεια δικτύων και πληροφοριών συνιστά πρόκληση για την Επιτροπή, τόσο σε διεθνές επίπεδο όσο και σε συνεργασία με τα κράτη μέλη, να αυξήσει της προσπάθειες που καταβάλλει για την **προώθηση της παγκόσμιας συνεργασίας στην ασφάλεια δικτύων και πληροφοριών**, ιδίως εφαρμόζοντας το θεματολόγιο που εγκρίθηκε κατά την παγκόσμια διάσκεψη κορυφής για την κοινωνία της πληροφορίας, το Νοέμβριο του 2005.

Τέλος, η έρευνα και ανάπτυξη, ιδίως σε κοινοτικό επίπεδο, θα συμβάλουν στην εξέλιξη νέων και καινοτόμων εταιρικών σχέσεων για την προώθηση της ανάπτυξης του ευρωπαϊκού κλάδου ΤΠΕ γενικότερα, και του ευρωπαϊκού κλάδου ΤΠΕ εν προκειμένω. Προς τούτο, η Επιτροπή θα επιδιώξει να εξασφαλίσει κατάλληλους οικονομικούς πόρους για έρευνα σε θέματα NIS και τεχνολογιών αξιοπιστίας στο 7ο κοινοτικό πρόγραμμα πλαίσιο.

3.1. Διάλογος

*3.1.1. Ως πρώτο βήμα για τη βελτίωση του διαλόγου μεταξύ των δημόσιων αρχών, η Επιτροπή προτείνει τη δρομολόγηση **συγκριτικής αξιολόγησης εθνικών πολιτικών που αφορούν NIS**, συμπεριλαμβανομένων ειδικών πολιτικών ασφάλειας για το δημόσιο τομέα. Τούτο θα συμβάλει στον προσδιορισμό των πλέον αποτελεσματικών πρακτικών, ώστε να μπορούν στη συνέχεια να αναπτύσσονται, όπου αυτό είναι δυνατό, σε ευρύτερη βάση και σε κοινοτική κλίμακα, συμβάλλοντας ώστε η δημόσια διοίκηση της να καταστεί κινητήρια δύναμη όσον αφορά βέλτιστη πρακτική σε θέματα ασφάλειας. Σημαντικό ρόλο από την άποψη αυτή μπορεί, π.χ., να έχουν οι εργασίες για την ηλεκτρονική ταυτοποίηση, ως μέρος του πρόσφατου σχεδίου δράσης ηλε-κυβέρνηση (eGovernment).*

Με την κατάλληλη διάρθρωση, στα αποτελέσματα της εν λόγω συγκριτικής αξιολόγησης θα προσδιοριστούν **περιπτώσεις βέλτιστης πρακτικής για τη βελτίωση της ευαισθητοποίησης μεταξύ ΜΜΕ και πολιτών** όσον αφορά τις ανάγκες τους να αντιμετωπίσουν τις εκάστοτε συγκεκριμένες προκλήσεις και απαιτήσεις σε NIS , καθώς και τις σχετικές δυνατότητές τους. Θα πρέπει να κληθεί ο ENISA να αναλάβει ενεργό ρόλο στο διάλογο αυτό, καθώς και στην παγίωση και ανταλλαγή βέλτιστης πρακτικής.

*3.1.2. Απαιτείται **διαρθρωμένη πολυμερής συζήτηση** με καλύτερο τρόπο αξιοποίησης των υφιστάμενων εργαλείων και ρυθμίσεων για την επίτευξη της ενδεδειγμένης κοινωνικής ισορροπίας μεταξύ ασφάλειας και προστασίας των θεμελιωδών δικαιωμάτων, συμπεριλαμβανομένης της προστασίας της ιδιωτικής ζωής. Ως συμβολή στη συζήτηση αυτή θεωρείται η προγραμματισμένη διάσκεψη "i2010 – Towards a Ubiquitous European Information Society" (γενικευμένη παρουσία της κοινωνίας της πληροφορίας) που διοργανώνεται από την προσεχή φινλανδική προεδρία, καθώς και η διαβούλευση για τον αντίκτυπο της RFID στην ασφάλεια και την προστασία της ιδιωτικής ζωής, η οποία αποτελεί μέρος της ευρύτερης διαβούλευσης που δρομολογήθηκε πρόσφατα από την Επιτροπή. Εξάλλου, η Επιτροπή θα διοργανώσει:*

- Επιχειρηματική εκδήλωση για την ενθάρρυνση της συμμετοχής του κλάδου στην υιοθέτηση αποτελεσματικών μεθόδων για την υλοποίηση παιδείας ασφάλειας **στον κλάδο**.

- Σεμινάριο προβληματισμού σχετικά με τρόπους αύξησης της ευαισθητοποίησης σε θέματα ασφάλειας και ενίσχυσης της εμπιστοσύνης των **τελικών χρηστών** στη χρήση ηλεκτρονικών δικτύων και συστημάτων πληροφοριών.

3.2. Εταιρική σχέση

*3.2.1. Για την αποτελεσματική χάραξη πολιτικής απαιτείται σαφής αντίληψη του χαρακτήρα και της έκτασης των προκλήσεων. Προς τούτο δεν αρκούν μόνο αξιόπιστα και επικαιροποιημένα στατιστικά και οικονομικά δεδομένα σχετικά με συμβάντα στην ασφάλεια πληροφοριών και με το επίπεδο της εμπιστοσύνης καταναλωτών και χρηστών, αλλά επίσης και επικαιροποιημένα δεδομένα αναφορικά με το μέγεθος και τις τάσεις του κλάδου ασφαλείας ΤΠΕ στην Ευρώπη. Η Επιτροπή προτίθεται να ζητήσει από τον ENISA να αναπτύξει **εταιρική σχέση εμπιστοσύνης με τα κράτη μέλη και με τους ενδιαφερόμενους** για την εκπόνηση **ενδεδειγμένου πλαισίου συλλογής δεδομένων**, συμπεριλαμβανομένων των διαδικασιών και των μηχανισμών συλλογής και ανάλυσης δεδομένων σε ευρωπαϊκή κλίμακα αναφορικά με συμβάντα σχετικά με την ασφάλεια και την εμπιστοσύνη των καταναλωτών.*

Παράλληλα, λόγω της ιδιαίτερα κατακερματισμένης αγοράς στην ΕΕ και του μάλλον ειδικού χαρακτήρα της, η Επιτροπή θα καλέσει τα κράτη μέλη, τον ιδιωτικό τομέα και την ερευνητική κοινότητα **να συμπήξουν στρατηγική εταιρική σχέση** για την εξασφάλιση της διάθεσης δεδομένων σχετικά με τον κλάδο ασφαλείας ΤΠΕ και με τις εξελισσόμενες τάσεις της αγοράς για προϊόντα και υπηρεσίες στην ΕΕ.

*3.2.2. Αποβλέποντας στην βελτίωση των ευρωπαϊκών δυνατοτήτων απόκρισης σε επιβουλές κατά της ασφάλειας, η Επιτροπή θα ζητήσει από τον ENISA να εξετάσει τη **σκοπιμότητα ενός ευρωπαϊκού συστήματος ανταλλαγής πληροφοριών και έγκαιρης προειδοποίησης** με σκοπό τη διευκόλυνση αποτελεσματικής απόκρισης σε υφιστάμενες και μελλοντικές επιβουλές εναντίον ηλεκτρονικών δικτύων. Μια από τις απαιτήσεις ενός τέτοιου συστήματος θα είναι μια **πολυγλωσσική κοινοτική δικτυακή πύλη** που θα παρέχει προσαρμοσμένες στη ζήτηση πληροφορίες αναφορικά με επιβουλές, κινδύνους και προειδοποιήσεις.*

3.3. Ενίσχυση των ικανοτήτων

Η ενίσχυση των ικανοτήτων κάθε ομάδας ενδιαφερομένων αποτελεί προϋπόθεση για την καλύτερη επίδοση των αναγκών ασφάλειας και των κινδύνων με σκοπό την προώθηση της ασφάλειας δικτύων και πληροφοριών.

*3.3.1. Από την άποψη αυτή, η Επιτροπή καλεί τα **κράτη μέλη** :*

- να έχουν ενεργό συμμετοχή στην προτεινόμενη συγκριτική αξιολόγηση εθνικών πολιτικών NIS·

- να προωθήσουν, σε στενή συνεργασία με τον ENISA, εκστρατείες ευαισθητοποίησης σχετικά με τα πλεονεκτήματα, τα οφέλη και την ανταμοιβή από την υιοθέτηση αποτελεσματικών τεχνολογιών, πρακτικών και συμπεριφοράς ασφάλειας·

- να υποβοηθήσουν την εγκατάσταση υπηρεσιών ηλεκτρονικής διακυβέρνησης για την προβολή και προώθηση ορθής πρακτικής αναφορικά με την ασφάλεια, που θα μπορούσε στη συνέχεια να επεκταθεί και σε άλλους τομείς·

- να ενθαρρύνουν την ανάπτυξη προγραμμάτων ασφάλειας δικτύων και πληροφοριών ως τμήμα της διδακτέας ύλης στην ανώτερη εκπαίδευση.

3.3.2. *Η Επιτροπή καλεί επίσης τους εμπλεκόμενους παράγοντες του* ***ιδιωτικού τομέα*** *να αναλάβουν πρωτοβουλίες:*

- να εκπονήσουν κατάλληλο ορισμό των αρμοδιοτήτων και της ευθύνης παραγωγών λογισμικού και παρόχων υπηρεσιών Διαδικτύου σε σχέση με την παροχή επαρκών και ελέγξιμων επιπέδων ασφάλειας. Εν προκειμένω, απαιτείται υποστήριξη τυποποιημένων διαδικασιών που θα ανταποκρίνονται σε κοινά συμφωνημένα πρότυπα ασφάλειας και σε κανόνες βέλτιστης πρακτικής·

- να προωθήσουν την ποικιλομορφία, τον ανοιχτό χαρακτήρα, τη διαλειτουργικότητα, τη χρηστικότητα και τον ανταγωνισμό ως καίριες κινητήριες δυνάμεις για την ασφάλεια, καθώς επίσης να ενθαρρύνουν την ανάπτυξη και εγκατάσταση προϊόντων, διαδικασιών και υπηρεσιών βελτιωμένης ασφαλείας για την αποτροπή και καταπολέμηση της κλοπής ταυτότητας και άλλων επιθέσεων κατά της ιδιωτικής ζωής·

- να διαδώσουν ορθή πρακτική ασφαλείας για φορείς εκμετάλλευσης δικτύου, παρόχους υπηρεσιών και ΜΜΕ, υπό μορφή βασικού επιπέδου όσον αφορά την ασφάλεια και τη συνέχεια της επιχειρηματικής δραστηριότητας·

- να προωθήσουν προγράμματα κατάρτισης στον επιχειρηματικό τομέα, ιδίως για τις ΜΜΕ, ώστε οι απασχολούμενοι να αποκτήσουν τις απαραίτητες γνώσεις και δεξιότητες για την αποτελεσματική εφαρμογή πρακτικών σχετικών με την ασφάλεια·

- να εργαστούν για την εκπόνηση οικονομικά προσιτών προγραμμάτων πιστοποίησης της ασφάλειας για προϊόντα, διεργασίες και υπηρεσίες που θα αναφέρονται σε ιδιαίτερες κοινοτικές ανάγκες (ιδίως όσον αφορά την προστασία της ιδιωτικής ζωής)·

- να συμπεριλάβουν τον ασφαλιστικό τομέα στην κατάρτιση των κατάλληλων εργαλείων για τη διαχείριση των κινδύνων και για τις μεθόδους αντιμετώπισης των κινδύνων σχετικά με ΤΠΕ και να καλλιεργήσουν παιδεία διαχείρισης κινδύνων σε οργανισμούς και επιχειρήσεις (ιδιαιτέρως στις ΜΜΕ).

4. ΣΥΜΠΕΡΑΣΜΑΤΑ

Για τον προσδιορισμό και την αντιμετώπιση των σχετικών με την ασφάλεια προκλήσεων όσον αφορά συστήματα και δίκτυα πληροφοριών στην ΕΕ απαιτείται πλήρης συστράτευση όλων των εμπλεκόμενων παραγόντων. Η μεθοδολογική προσέγγιση πολιτικής που σκιαγραφείται στην παρούσα ανακοίνωση αποβλέπει στην επίτευξη του στόχου αυτού, με την ενίσχυση μιας **πολυμερούς προσέγγισης**, η οποία θα βασίζεται σε κοινά συμφέροντα, στον

προσδιορισμό των αντίστοιχων ρόλων και στην εκπόνηση ενός πλαισίου για την προώθηση αποτελεσματικής χάραξης δημόσιας πολιτικής και πρωτοβουλιών του ιδιωτικού τομέα.

Στα μέσα του 2007, η Επιτροπή θα υποβάλει στο Συμβούλιο και το Κοινοβούλιο έκθεση σχετικά με τις πρωτοβουλίες που θα έχει δρομολογήσει, με τα αρχικά πορίσματα και με την επισκόπηση της εξέλιξης κάθε πρωτοβουλίας, συμπεριλαμβανομένων αυτών του ENISA και όσων θα έχουν αναληφθεί σε επίπεδο κράτους μέλους ή από τον ιδιωτικό τομέα. Εφόσον κρίνει ενδεδειγμένο, η Επιτροπή θα υποβάλει σύσταση σχετικά με την ασφάλεια δικτύων και πληροφοριών (NIS).