I

(Ψηφίσματα, συστάσεις, κατευθυντήριες γραμμές και γνωμοδοτήσεις)

ΨΗΦΙΣΜΑΤΑ

ΣΥΜΒΟΥΛΙΟ

ΨΗΦΙΣΜΑ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 22ης Μαρτίου 2007

σχετικά με τη στρατηγική για ασφαλή κοινωνία της πληροφορίας στην Ευρώπη

(2007/C 68/01)

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

ΕΚΔΙΔΕΙ ΤΟ ΠΑΡΟΝ ΨΗΦΙΣΜΑ ΚΑΙ

ΧΑΙΡΕΤΙΖΕΙ

την ανακοίνωση της Επιτροπής προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, της 31ης Μαΐου 2006 — Στρατηγική για ασφαλή κοινωνία της πληροφορίας — «διάλογος, πνεύμα συνεργασίας και ενίσχυση των ικανοτήτων» ·

ΣΗΜΕΙΩΝΕΙ

την ανακοίνωση της Επιτροπής προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, της 15ης Νοεμβρίου 2006, για την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων (spam), του κατασκοπευτικού λογισμικού και του κακόβουλου λογισμικού·

ΥΠΕΝΘΥΜΙΖΕΙ

1. Το ψήφισμα του Συμβουλίου της 28ης Ιανουαρίου 2002 σχετικά με κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας δικτύων και πληροφοριών [1]·

2. Το ψήφισμα του Συμβουλίου της 18ης Φεβρουαρίου 2003 σχετικά με την ευρωπαϊκή αντίληψη για την ασφάλεια των δικτύων και των πληροφοριών [2]·

3. Τα συμπεράσματα του Συμβουλίου της 8ης και 9ης Μαρτίου 2004 για τα ανεπίκλητα μηνύματα εμπορικού χαρακτήρα (spam) και της 9ης και 10ης Δεκεμβρίου 2004 για την καταπολέμηση των spam·

4. Τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου του Μαρτίου 2005 για την επανενεργοποίηση της στρατηγικής της Λισσαβώνας και τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου του Μαρτίου 2006 που καλούν την Επιτροπή και τα κράτη μέλη να εφαρμόσουν σθεναρά τη νέα στρατηγική i2010·

5. Το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες [3] και, ειδικότερα, τις διατάξεις που αφορούν την ασφάλεια των επικοινωνιών, την ιδιωτική ζωή και το απόρρητο, οι οποίες έχουν συμβάλει στην εξασφάλιση υψηλού επιπέδου προστασίας των δεδομένων προσωπικής φύσεως και της ιδιωτικής ζωής, επίσης δε στην ακεραιότητα και την ασφάλεια των δημοσίων δικτύων επικοινωνιών·

6. Τον κανονισμό (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) [4]·

7. Την Ατζέντα της Τύνιδας και τη Δέσμευση της Τύνιδας στην Παγκόσμια Διάσκεψη Κορυφής για την Κοινωνία της Πληροφορίας (WSIS), όπου τονίζεται η ανάγκη να συνεχιστεί η καταπολέμηση του εγκλήματος στον κυβερνοχώρο και των αυτόκλητων μηνυμάτων με παράλληλη προστασία της ιδιωτικής ζωής και της ελευθερίας του εκφράζεσθαι, επίσης δε να προωθηθεί, να καλλιεργηθεί και να πραγματωθεί, σε συνεργασία με όλους τους ενδιαφερόμενους, ένα παγκόσμιο κλίμα ασφάλειας του κυβερνοχώρου·

8. Τα συμπεράσματα της Προεδρίας της Ετήσιας Ευρωπαϊκής Διάσκεψης για την Κοινωνία της Πληροφορίας (27-28 Σεπτεμβρίου 2006) με τίτλο «i2010- Προς μια πανταχού παρούσα Ευρωπαϊκή Κοινωνία της Πληροφορίας» που πραγματοποιήθηκε στο Espoo της Φινλανδίας·

([1]) ΕΕ C 43 της 16.2.2002, σ. 2.
([2]) ΕΕ C 48 της 28.2.2003, σ. 1.
([3]) Οδηγίες 2002/58/ΕΚ (Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), 2002/20/ΕΚ (Οδηγία για την αδειοδότηση), 2002/22/ΕΚ (Οδηγία καθολικής υπηρεσίας) (ΕΕ L 201, 31.7.2002, σ. 37, ΕΕ L 108 της 24.4.2002, σ. 21 και ΕΕ L 108 της 24.4.2002, σ. 51, αντιστοίχως).
([4]) ΕΕ L 77 της 13.3.2004, σ. 1.

ΤΟΝΙΖΕΙ ΩΣ ΕΚ ΤΟΥΤΟΥ ΟΤΙ:

1. Οι κοινωνίες μας κινούνται γοργά προς μια νέα φάση ανάπτυξης, προς μια πανταχού παρούσα κοινωνία της πληροφορίας, στην οποία όλο και περισσότερες καθημερινές δραστηριότητες των πολιτών βασίζονται στη χρήση Τεχνολογιών των Πληροφοριών και των Επικοινωνιών (ΤΠΕ), επίσης δε στη χρήση ηλεκτρονικών δικτύων επικοινωνιών· η ασφάλεια δικτύων και πληροφοριών θα πρέπει να θεωρείται αποφασιστικός παράγοντας για αυτή την εξέλιξη και για την επιτυχία της·

2. Η εμπιστοσύνη αποτελεί βασική παράμετρο για την επιτυχία της νέας κοινωνίας της πληροφορίας· η εμπιστοσύνη σχετίζεται επίσης με τις εμπειρίες των τελικών χρηστών και με την ανάγκη σεβασμού της ιδιωτικής τους ζωής· συνεπώς, η ασφάλεια δικτύων και πληροφοριών δεν θα πρέπει να θεωρείται απλώς ένα τεχνικής φύσεως ζήτημα·

3. Η ασφάλεια δικτύων και πληροφοριών αποτελεί ουσιώδες στοιχείο της δημιουργίας ενός Ευρωπαϊκού Χώρου Πληροφοριών ως μέρους της πρωτοβουλίας i2010, ούτως ώστε να συμβάλει στην επιτυχία της επανενεργοποιημένης στρατηγικής της Λισσαβώνας· οι δε ΤΠΕ αποτελούν επίσης ζωτική συνιστώσα καινοτομίας, οικονομικής μεγέθυνσης και θέσεων απασχόλησης σε ολόκληρο το φάσμα της οικονομίας·

4. Ήδη αναπτύσσονται νέες τεχνολογίες που θα μας οδηγήσουν στην πανταχού παρούσα κοινωνία της πληροφορίας· η εμφάνιση πρωτοποριακών τεχνολογιών (όπως τα ασύρματα δίκτυα υψηλών ταχυτήτων, οι διατάξεις ραδιοσυχνικής αναγνώρισης (RFID), τα δίκτυα αισθητήρων) και καινοτόμων υπηρεσιών πλουσίου περιεχομένου (όπως η τηλεόραση μέσω διαδικτυακού πρωτοκόλλου (IPTV), η φωνητική τηλεφωνία μέσω διαδικτυακού πρωτοκόλλου (VoIP), η τηλεόραση κινητής επικοινωνίας και οι λοιπές κινητές τηλεοπτικές υπηρεσίες) απαιτούν τα προσήκοντα επίπεδα ασφάλειας δικτύων και επικοινωνιών ευθύς από την έναρξη της φάσης ανάπτυξης, ούτως ώστε να επιτυγχάνεται πραγματική εμπορική αξία· η έγκαιρη υιοθέτηση των νέων και πολλά υποσχόμενων καινοτομιών έχει μεγάλη σημασία για την ανάπτυξη της κοινωνίας της πληροφορίας και την ανταγωνιστικότητα της Ευρώπης· οι κυβερνητικοί οργανισμοί και οι επιχειρήσεις θα πρέπει να υιοθετήσουν μόλις καταστεί εφικτό ασφαλείς πρωτοεμφανιζόμενες τεχνολογίες και υπηρεσίες προκειμένου να επιταχυνθεί η εκτεταμένη αποδοχή τους·

5. Για την ΕΕ έχει στρατηγική σημασία το γεγονός ότι η ευρωπαϊκή βιομηχανία είναι απαιτητικός χρήστης αλλά και ανταγωνιστικός προμηθευτής δικτύων και ασφαλών προϊόντων και υπηρεσιών· η ποικιλία, η διαφάνεια και η διαλειτουργικότητα συνιστούν αναπόσπαστες παραμέτρους ασφαλείας και θα πρέπει να προωθηθούν·

6. Οι γνώσεις και οι δεξιότητες στον τομέα των δικτύων και πληροφοριών θα πρέπει και αυτές να καταστούν αναπόσπαστο μέρος της καθημερινής ζωής κάθε ατόμου και κάθε κοινωνικού συντελεστή· έχουν ήδη διεξαχθεί κάποιες εκστρατείες ευαισθητοποίησης σε εθνικό επίπεδο και επίπεδο ΕΕ, μπορούν όμως ακόμα να γίνουν πολλά στον τομέα αυτόν, ιδίως όσον αφορά τους τελικούς χρήστες και τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) · θα πρέπει να δοθεί ιδιαίτερη προσοχή στους χρήστες με ειδικές ανάγκες ή με μικρή γνώση στα θέματα της ασφάλειας δικτύων και πληροφοριών· όλοι οι φορείς θα πρέπει να συνειδητοποιήσουν ότι αποτελούν μέρος της παγκόσμιας αλυσίδας ασφάλειας, θα πρέπει δε να τους δοθεί η δυνατότητα να ενεργούν υπό την ιδιότητά τους αυτή· τα θέματα της ασφάλειας δικτύων και πληροφοριών θα πρέπει να ενσωματώνονται σε όλους τους τομείς της εκπαίδευσης και της κατάρτισης που σχετίζονται με τις ΤΠΕ·

7. Η σύσταση του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) υπήρξε σημαντικό βήμα για την ασφάλεια δικτύων και πληροφοριών· η εμβέλεια, οι στόχοι, τα καθήκοντα και η διάρκεια του Οργανισμού ορίζονται στον κανονισμό (ΕΚ) αριθ. 460/2004·

8. Οι πόροι που προορίζονται για την έρευνα και την ανάπτυξη (Ε&Α) και την καινοτομία, τόσο σε επίπεδο εθνικό όσο και σε επίπεδο ΕΕ, συνιστούν ένα από τα βασικά στοιχεία για την ενίσχυση του επιπέδου ασφάλειας των δικτύων και πληροφοριών στα νέα συστήματα, συσκευές και υπηρεσίες· θα πρέπει να ενταθούν οι προσπάθειες της ΕΕ στους τομείς της έρευνας και της καινοτομίας σε θέματα ασφάλειας, ιδίως μέσω του Εβδόμου Προγράμματος Πλαισίου για την Ανταγωνιστικότητα και την Καινοτομία (ΠΑΚ)· οι προσπάθειες θα πρέπει να στρέφονται προς μέτρα για τη διάδοση και την προώθηση της εμπορικής εκμετάλλευσης των ερευνητικών αποτελεσμάτων, μεταξύ των οποίων η αξιολόγηση της χρησιμότητάς τους για την ευρύτερη κοινωνία· αυτό θα καταστήσει τους Ευρωπαίους προμηθευτές ικανότερους στο να παρέχουν λύσεις ασφαλείας που θα πληρούν τις ανάγκες της ευρωπαϊκής αγοράς·

9. Ενώ χορηγεί μεγάλα οφέλη, η πανταχού παρούσα κοινωνία της πληροφορίας γεννά επίσης και σημαντικές προκλήσεις, δημιουργώντας έτσι ένα νέο τοπίο ενδεχομένων κινδύνων· οι απειλές κατά της ασφάλειας και της ιδιωτικής ζωής, συν τοις άλλοις από την παράνομη συλλογή και εκμετάλλευση δεδομένων, γίνονται ολοένα σοβαρότερες, ευστοχότερες και κερδοσκοπικότερες, θα πρέπει δε να επινοηθούν νέοι τρόποι αντίδρασης για τους αναφαινόμενους και τους ήδη υπάρχοντες κινδύνους με καινοτόμο πνεύμα, οι οποίοι να καλύπτουν επίσης προβλήματα οφειλόμενα στο περίπλοκο των συστημάτων, στα λάθη, στα ατυχήματα ή στην ασάφεια των οδηγιών· θα πρέπει να ενθαρρυνθεί και να προωθηθεί περισσότερο η δημιουργία και η ανάπτυξη εθνικών οργάνων αντίδρασης σε έκτακτες περιστάσεις ηλεκτρονικής φύσεως, με στροφή προς διάφορους φορείς και η συνεργασία μεταξύ αυτών των οργάνων καθώς και με άλλους αρμόδιους φορείς·

10. Η τυποποίηση και η πιστοποίηση των προϊόντων, των υπηρεσιών και των συστημάτων διαχείρισης, την οποία παρέχουν ιδίως υπάρχοντες οργανισμοί, χρήζουν ιδιαίτερης προσοχής στα πλαίσια της πολιτικής δικτύων και πληροφοριών της ΕΕ ως μέσο για τη διάδοση ορθών πρακτικών και επαγγελματικού πνεύματος στον τομέα της ασφάλειας δικτύων και πληροφοριών· ειδικότερα οι πρωτοεμφανιζόμενες τεχνολογίες όπως η ραδιοσυχνική αναγνώριση (RFID) και οι κινητές τηλεοπτικές υπηρεσίες θα πρέπει να ωφεληθούν από την έγκαιρη θέσπιση τυχόν νεότευκτων προτύπων, διαφανών και διαλειτουργικών·θα πρέπει να ενισχυθεί η λειτουργία των ευρωπαϊκών οργανισμών τυποποίησης σε αυτόν τον τομέα·

11. Καθώς τα ηλεκτρονικά δίκτυα και τα συστήματα πληροφοριών παίζουν ολοένα πιο κεντρικό ρόλο στην όλη λειτουργία των νευραλγικών υποδομών, η διαθεσιμότητα και η ακεραιότητά τους καθίσταται απαραίτητη για τις διοικήσεις, τις επιχειρήσεις, την ασφάλεια και ποιότητα ζωής των πολιτών καθώς και για την εν γένει λειτουργία των κοινωνιών·

12. Η συνεργασία και οι πρακτικές μεθοδεύσεις είναι πιο απαραίτητες από ποτέ· οι διάφοροι φορείς θα πρέπει να προσδιορίσουν και να αναγνωρίσουν τους οικείους ρόλους, ευθύνες και δικαιώματα.

ΚΑΙ ΣΥΝΕΠΩΣ ΚΑΛΕΙ ΤΑ ΚΡΑΤΗ ΜΕΛΗ:

1. Να παράσχουν στήριξη σε προγράμματα κατάρτισης και να προβούν σε γενική ευαισθητοποίηση για θέματα ασφάλειας των δικτύων και των πληροφοριών, εγκαινιάζοντας επί παραδείγματι ενημερωτικές εκστρατείες με αντικείμενο την ασφάλεια των δικτύων και των πληροφοριών, με αποδέκτη όλους τους πολίτες/χρήστες και τομείς της οικονομίας, προ πάντων δε τις ΜΜΕ και τους τελικούς χρήστες με ειδικές ανάγκες ή με περιορισμένη γνώση· θα πρέπει έως το 2008 να επιλεγεί μια κοινή ημερομηνία ως πανευρωπαϊκή ημέρα ευαισθητοποίησης (π.χ. «Ημέρα Ασφάλειας Δικτύων και Πληροφοριών») η οποία να λαμβάνει χώραν σε ετήσια και εθελοντική βάση σε κάθε κράτος μέλος·

2. Να ενισχύσουν τη συμβολή στην Ε&Α που σχετίζεται με την ασφάλεια και να βελτιώσουν τη δυνατότητα αξιοποίησης και διάδοσης των ερευνητικών αποτελεσμάτων· να ενθαρρύνουν την ανάπτυξη καινοτόμων εταιρικών σχέσεων για μεγαλύτερη ανάπτυξη της ευρωπαϊκής βιομηχανίας ασφαλών ΤΠΕ και να αυξήσουν την άμεση χρησιμοποίηση νέων τεχνολογιών ασφάλειας των δικτύων και των πληροφοριών ούτως ώστε να τους δώσουν εμπορική ώθηση·

3. Να δώσουν τη δέουσα προσοχή στην ανάγκη πρόληψης των νέων και καταπολέμησης των υφισταμένων απειλών κατά της ασφάλειας στα δίκτυα ηλεκτρονικών επικοινωνιών, πράγμα που περιλαμβάνει ωσαύτως την παράνομη συλλογή και εκμετάλλευση δεδομένων, να αναγνωρίσουν και να αντιμετωπίσουν τους συναφείς κινδύνους και να ενθαρρύνουν, ενδεχομένως σε συνεργασία με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), την ουσιαστική ανταλλαγή πληροφοριών και συνεργασία μεταξύ αρμόδιων οργανισμών και υπηρεσιών σε εθνικό επίπεδο· να δεσμευθούν να καταπολεμήσουν τα αυτόκλητα μηνύματα, το κατασκοπευτικό και το κακόβουλο λογισμικό, ιδίως μέσω της βελτιωμένης συνεργασίας μεταξύ αρμόδιων αρχών σε εθνικό και παγκόσμιο επίπεδο·

4. Να εντείνουν την αμοιβαία τους συνεργασία εντός του πλαισίου i2010, ούτως ώστε να εντοπίσουν νέες και καινοτόμες πρακτικές για την βελτίωση της ασφάλειας των δικτύων και των πληροφοριών και να διαδώσουν τη γνώση των πρακτικών αυτών σε επίπεδο ΕΕ και σε προαιρετική βάση·

5. Να ενθαρρύνουν τη συνεχή βελτίωση των εθνικών οργάνων αντίδρασης σε έκτακτες περιστάσεις ηλεκτρονικής φύσεως·

6. Να καλλιεργήσουν περιβάλλον εντός του οποίου οι πάροχοι υπηρεσιών και οι χειριστές δικτύων θα παρακινούνται να παρέχουν στους πελάτες τους υπηρεσίες αντοχής και να εξασφαλίζουν στις υπηρεσίες και λύσεις ασφαλείας τους προσαρμοστικότητα και δυνατότητα των καταναλωτών να επιλέγουν· να προτρέπουν ή ενδεχομένως να απαιτούν από τους χειριστές δικτύων και παρόχους υπηρεσιών να εξασφαλίζουν ικανοποιητικό επίπεδο ασφάλειας δικτύων και πληροφοριών για τους πελάτες τους·

7. Να εξακολουθήσουν τη συζήτηση στρατηγικής στους κόλπους της Ομάδας Υψηλού Επιπέδου «i2010», λαμβάνοντας ταυτόχρονα υπ' όψη τις τρέχουσες εξελίξεις στην Κοινωνία της Πληροφορίας, να μεριμνήσουν δε για συγκροτημένη προσέγγιση των παραμέτρων της κανονιστικής ρύθμισης, της συρρύθμισης, της Ε&Α και της ηλεκτρονικής διακυβέρνησης σε συνδυασμό με τις επικοινωνίες και την εκπαίδευση·

8. Σε ευθυγράμμιση με το σχέδιο δράσης για την ηλεκτρονική διακυβέρνηση στο πλαίσιο της πρωτοβουλίας i2010, να προωθήσουν λύσεις για τη διαλειτουργική διαχείριση ταυτότητας και να προβούν σε όλες τις δέουσες οργανωτικές αλλαγές στον δημόσιο τομέα· οι κρατικές και δημόσιες διοικήσεις θα πρέπει να χρησιμεύουν ως υπόδειγμα ορθής πρακτικής με την προώθηση ασφαλών υπηρεσιών ηλεκτρονικής διακυβέρνησης για όλους τους πολίτες.

ΕΠΙΔΟΚΙΜΑΖΕΙ ΤΗΝ ΠΡΟΘΕΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ:

1. Να συνεχίσει την ανάπτυξη συνολικής και δυναμικής πανευρωπαϊκής στρατηγικής για την ασφάλεια των δικτύων και πληροφοριών· η ολιστική προσέγγιση που προτείνει η Επιτροπή έχει ιδιαίτερη σημασία·

2. Να αντιμετωπίσει την ασφάλεια των δικτύων και πληροφοριών ως έναν από τους στόχους της επανεξέτασης του κανονιστικού πλαισίου της ΕΕ για τις ηλεκτρονικές επικοινωνίες·

3. Να συνεχίσει να παίζει τον ρόλο της ούτως ώστε να συνειδητοποιηθεί περισσότερο η ανάγκη γενικής πολιτικής δέσμευσης για την καταπολέμηση των αυτόκλητων μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού, ιδίως μέσω συμφωνιών με τρίτες χώρες στις οποίες θα συμπεριλαμβάνεται το θέμα της καταπολέμησης των αυτόκλητων μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού·

4. Να ενισχύσει τη συμμετοχή του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) στην υποστήριξη της στρατηγικής για μια ασφαλή κοινωνία της πληροφορίας στην Ευρώπη σύμφωνα με το παρόν ψήφισμα, σε ευθυγράμμιση με τους στόχους και τα καθήκοντα που ορίζει ο κανονισμός (ΕΚ) αριθ. 460/2004,καθώς και σε εγγύτερη συνεργασία και στενότερη εργασιακή σχέση με τα κράτη μέλη και τους αρμόδιους φορείς·

5. Να αναπτύξει σε συσχετισμό με το πλαίσιο i2010, σε συνεργασία με τα κράτη μέλη και όλους τους αρμόδιους φορείς και ιδίως με τους εμπειρογνώμονες του τομέα της στατιστικής και της ασφάλειας της πληροφορίας στα κράτη μέλη, τους κατάλληλους δείκτες για τις μελέτες της Κοινότητας για πτυχές που άπτονται της ασφάλειας και της εμπιστοσύνης·

6. Να ενθαρρύνει τα κράτη μέλη να εξετάσουν μέσω διαλόγου με πολλούς φορείς τις οικονομικές, επιχειρηματικές και κοινωνικές κινητήριες δυνάμεις με σκοπό την ανάπτυξη πολιτικής ιδιαίτερα προσαρμοσμένης στον τομέα ΤΠΕ για την ενίσχυση και την αντοχή των συστημάτων δικτύων και πληροφοριών, ως πιθανή συμβολή στο σχεδιαζόμενο ευρωπαϊκό πρόγραμμα για την προστασία των νευραλγικών υποδομών·

7. Να συνεχίσει τις προσπάθειές της, σε συνεννόηση με τα κράτη μέλη, για την προώθηση του διαλόγου με αρμόδιους διεθνείς εταίρους και οργανώσεις προκειμένου να καλλιεργηθεί μια παγκόσμια συνεργασία για την ασφάλεια δικτύων και πληροφοριών, και δη με την εφαρμογή των κατευθυντηρίων γραμμών της Παγκόσμιας Διάσκεψης Κορυφής για την Κοινωνία της Πληροφορίας (WSIS) και την υποβολή τακτικών εκθέσεων προς το Συμβούλιο.

ΚΑΙ ΚΑΛΕΙ:

1. Τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) να εξακολουθήσει να εργάζεται σε στενή σύμπραξη με τα κράτη μέλη, την Επιτροπή και άλλους αρμόδιους φορείς, προκειμένου να φέρει εις πέρας τα καθήκοντα και τους στόχους που προσδιορίζονται στον κανονισμό (ΕΚ) αριθ. 460/2004 και να συνδράμει την Επιτροπή και τα κράτη μέλη στην προσπάθειά τους να συμμορφωθούν προς τις προδιαγραφές της ασφάλειας δικτύων και πληροφοριών, συμβάλλοντας έτσι στην υλοποίηση και περαιτέρω ανάπτυξη της στρατηγικής για μια ασφαλή κοινωνία της πληροφορίας στην Ευρώπη, σύμφωνα με το παρόν ψήφισμα·

2. Όλους τους φορείς να βελτιώσουν την ασφάλεια του λογισμικού καθώς και την ασφάλεια και αντοχή των συστημάτων δικτύων και πληροφοριών σε ευθυγράμμιση με τη στρατηγική για μια ασφαλή κοινωνία της πληροφορίας στην Ευρώπη σύμφωνα με το παρόν ψήφισμα, να επιδοθούν δε σε συγκροτημένη συζήτηση με πολλούς φορείς για τον καλύτερο τρόπο αξιοποίησης των υπαρχόντων εργαλείων και κανονιστικών πράξεων·

3. Τις επιχειρήσεις να τηρήσουν θετική στάση έναντι της ασφάλειας δικτύων και πληροφοριών, ούτως ώστε να δημιουργηθούν πιο προηγμένα και ασφαλή προϊόντα και υπηρεσίες, θεωρώντας τη δυνατότητα επενδύσεων σε τέτοια προϊόντα και υπηρεσίες ως ανταγωνιστικό πλεονέκτημα·

4. Τους κατασκευαστές και παρόχους υπηρεσιών να ενσωματώσουν, όπου δει, προδιαγραφές ασφάλειας, ιδιωτικής ζωής και απορρήτου στον σχεδιασμό των προϊόντων και υπηρεσιών τους και στην εγκατάσταση της υποδομής δικτύων, στις συσκευές και στο λογισμικό, να εφαρμόσουν και να παρακολουθήσουν λύσεις ασφαλείας·

5. Τους φορείς να συνεργαστούν και να δημιουργήσουν πειραματικά περιβάλλοντα για την δοκιμή και την πειραματική λειτουργία τεχνολογιών και υπηρεσιών με ασφαλή τρόπο· τους φορείς να υιοθετούν έγκαιρα τις νέες ασφαλείς τεχνολογίες και υπηρεσίες όταν αυτές πρωτοβγαίνουν στην αγορά·

6. Όλους τους φορείς να εντείνουν τις προσπάθειές τους για την καταπολέμηση των αυτόκλητων μηνυμάτων και άλλων παράνομων ηλεκτρονικών πρακτικών και να συνεργαστούν ενεργά με τις αρμόδιες αρχές σε εθνικό και διεθνές επίπεδο·

7. Τους παρέχοντες υπηρεσίες και τη βιομηχανία ΤΠΕ να εστιάσουν την προσοχή τους στην ενίσχυση των παραμέτρων ασφαλείας, ιδιωτικής ζωής και δυνατής χρήσης προϊόντων, επεξεργασιών και υπηρεσιών ούτως ώστε να υπάρχει αξιοπιστία, να προλαμβάνεται και να καταστέλλεται η κλοπή ταυτότητας και άλλων προσβολών κατά της ιδιωτικής ζωής·

8. Τους χειριστές δικτύων, τους παρέχοντες υπηρεσίες και τον ιδιωτικό τομέα να μοιράζονται και να εφαρμόζουν ορθές πρακτικές ασφαλείας και να καλλιεργούν νοοτροπία ανάλυσης και διαχείρισης κινδύνων στις οργανώσεις και τις επιχειρήσεις, παρέχοντας στήριξη σε κατάλληλα προγράμματα κατάρτισης και τελειοποιώντας τον σχεδιασμό αντιμετώπισης απροόπτων, καθιστώντας δε επίσης διαθέσιμες για τους πελάτες τους τις λύσεις ασφαλείας ως μέρος των παρεχομένων υπηρεσιών.