ΑΠΟΦΑΣΗ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 31ης Μαρτίου 1992

στον τομέα της ασφάλειας των συστημάτων πληροφοριών

(92/242/ΕΟΚ)

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ,

Έχοντας υπόψη:

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Οικονομικής Κοινότητας, και ιδίως το άρθρο 235,

την πρόταση της Επιτροπής [1],

τη γνώμη του Ευρωπαϊκού Κοινοβουλίου [2],

τη γνώμη της Οικονομικής και Κοινωνικής Επιτροπής [3],

Εκτιμώντας:

ότι η Κοινότητα έχει ως αποστολή, με τη δημιουργία της κοινής αγοράς και την προοδευτική προσέγγιση της οικονομικής πολιτικής των κρατών μελών, να προάγει την αρμονική ανάπτυξη τών οικονομικών δραστηριοτήτων στο σύνολο της Κοινότητας, τη συνεχή και ισόρροπη επέκταση της οικονομίας, αυξημένη σταθερότητα, επιταχυνόμενη ανύψωση του βιοτικού επιπέδου, και σχέσεις περισσότερο στενές μεταξύ των κρατών που συνενώνει·

ότι η ηλεκτρονική φύλαξη, επεξεργασία και διαβίβαση των πληροφοριών διαδραματίζει όλο και σημαντικότερο ρόλο κατά τις οικονομικές και κοινωνικές δραστηριότητες·

ότι η καθιέρωση αποτελεσματικών καθολικών επικοινωνιών και η ευρεία χρήση της ηλεκτρονικής διαχείρισης των πληροφοριών δίδουν έμφαση στην ανάγκη επαρκούς προστασίας·

ότι το Ευρωπαϊκό Κοινοβούλιο, στις συζητήσεις και τα ψηφίσματα του, έχει τονίσει επανειλημμένα τη σημασία της ασφάλειας των συστημάτων πληροφοριών·

ότι η Οικονομική και Κοινωνική Επιτροπή έχει υπογραμμίσει την ανάγκη αντιμετώπισης των ζητημάτων που αφορούν την ασφάλεια των συστημάτων πληροφοριών, στα πλαίσια κοινοτικών δράσεων, κυρίως ενόψει της επικείμενης ολοκλήρωσης της εσωτερικής αγοράς·

ότι η ανάληψη δράσεων σε εθνικό, διεθνές και κοινοτικό επίπεδο αποτελούν την κατάλληλη βάση·

ότι υπάρχει στενή σχέση μεταξύ των τηλεπικοινωνιών, της τεχνολογίας των πληροφοριών, της τυποποίησης, της αγοράς του τομέα των πληροφοριών, των πολιτικών Έρευνας, Ανάπτυξης και Τεχνολογίας (ΕΑ&Τ), καθώς και των εργασιών που ήδη έχουν αναληφθεί σ' αυτούς τους τομείς από την Κοινότητα·

ότι είναι σκόπιμο να εξασφαλισθεί ο συντονισμός των προσπαθειών με βάση την υπάρχουσα εθνική και διεθνή εργασία και με την προαγωγή της συνεργασίας μεταξύ των σημαντικότερων ενδιαφερομένων μερών· ότι είναι, κατά συνέπεια, πρόσφορη η ένταξη των σχετικών ενεργειών στα πλαίσια ενός συγκροτημένου προγράμματος δράσης·

ότι η πολυπλοκότητα της ασφάλειας των συστημάτων πληροφοριών απαιτεί την ανάπτυξη στρατηγικών για τη διευκόλυνση της ελεύθερης κυκλοφορίας των πληροφοριών στην ενιαία αγορά με ταυτόχρονη εξασφάλιση της ασφάλειας της χρήσης των συστημάτων πληροφοριών σε ολόκληρη την Κοινότητα·

ότι κάθε κράτος μέλος είναι υποχρεωμένο να λάβει υπόψη του τους περιορισμούς που επιβάλλονται από την ασφάλεια και τη δημόσια τάξη·

ότι οι αρμοδιότητες των κρατών μελών στον τομέα αυτό συνεπάγονται συντονισμένη προσέγγιση βασισμένη σε στενή συνεργασία μεταξύ ανωτέρων υπαλλήλων των κρατών μελών·

ότι θα πρέπει να προβλεφθεί μια δράση που θα περιλαμβάνει σχέδιο δράσης για μια αρχική περίοδο εικοσιτεσσάρων μηνών και τη σύσταση επιτροπής ανωτέρων υπαλλήλων με μακροπρόθεσμη εντολή προκειμένου να συμβουλεύει την Επιτροπή σχετικά με δράσεις στον τομέα της ασφάλειας των συστημάτων πληροφοριών·

ότι ένα ποσό 12 εκατομμυρίων Ecu κρίνεται αναγκαίο για την εφαρμογή της δράσης για μια αρχική περίοδο εικοσιτεσσάρων μηνών· ότι, για το 1992, στα πλαίσια των υφισταμένων δημοσιονομικών προοπτικών, το ποσό που κρίνεται αναγκαίο είναι δύο εκατομμύρια Ecu·

ότι τα ποσά που θα διατεθούν για τη χρηματοδότηση του προγράμματος για την περίοδο μετά το οικονομικό έτος 1992 θα υπαχθούν στα ισχύοντα κοινοτικά δημοσιονομικά πλαίσια,

ΑΠΟΦΑΣΙΖΕΙ:

Άρθρο 1

Με την παρούσα απόφαση θεσπίζεται δράση στον τομέα της ασφάλειας των συστημάτων πληροφοριών η οποία περιλαμβάνει:

— την ανάπτυξη συνολικών στρατηγικών για την ασφάλεια των συστημάτων πληροφοριών (σχέδιο δράσης), για μια αρχική περίοδο εικοσιτεσσάρων μηνών και

— τη σύσταση ομάδας ανώτερων υπαλλήλων, με μακροπρόθεσμη εντολή, εφεξής καλούμενη «επιτροπή», για να συμβουλεύει την Επιτροπή για δράσεις στον τομέα της ασφάλειας των συστημάτων πληροφοριών.

---

(1) ΕΕ αριθ. C 277 της 5. 11. 1990, σ. 18.
(2) ΕΕ αριθ. C 94 της 13. 3. 1992.
(3) ΕΕ αριθ. C 159 της 17. 6. 1991, σ. 38.

Άρθρο 2

1. Η Επιτροπή συμβουλεύεται συστηματικά την επιτροπή σχετικά με θέματα που αφορούν την ασφάλεια των συστημάτων πληροφοριών των διάφορων κοινοτικών δραστηριοτήτων, ειδικότερα δε σχετικά με τον καθορισμό των στρατηγικών και προγραμμάτων εργασίας.

2. Το σχέδιο δράσης, όπως εκτίθεται στο παράρτημα, περιλαμβάνει προπαρασκευαστικές εργασίες με τα εξής θέματα:

I. ανάπτυξη στρατηγικού πλαισίου για την ασφάλεια των συστημάτων πληροφοριών,

II. προσδιορισμός των αναγκών των χρήστων και των παρεχόντων υπηρεσίες σε θέματα ασφάλειας των συστημάτων πληροφοριών,

III. λύσεις για άμεσες και προσωρινές ανάγκες των χρήστων, των προμηθευτών και των παρεχόντων υπηρεσίες,

IV. κατάρτιση προδιαγραφών, προτύπων, αξιολόγιση και πιστοποίηση όσον αφορά την ασφάλεια των συστημάτων πληροφοριών,

V. τεχνολογικές και λειτουργικές εξελίξεις σε θέματα ασφάλειας των συστημάτων πληροφοριών,

VI. κατοχύρωση της ασφάλειας των συστημάτων πληροφοριών.

Άρθρο 3

1. Το ποσό των κοινοτικών χρηματοδοτικών μέσων που κρίνεται αναγκαίο για την εφαρμογή της δράσης, για την αρχική περίοδο, ανέρχεται σε 12 εκατομμύρια Ecu εκ των οποίων δύο εκατομμύρια Ecu προορίζονται για το 1992 στα πλαίσια των δημοσιονομικών προοπτικών για την περίοδο 1988-1992.

Για τη μεταγενέστερη περίοδο εφαρμογής του προγράμματος, το ποσό θα υπαχθεί στα ισχύοντα κοινοτικά δημοσιονομικά πλαίσια.

2. Η αρμόδια για τον προϋπολογισμό αρχή θα καθορίσει τις διαθέσιμες πιστώσεις για κάθε οικονομικό έτος, λαμβάνοντας υπόψη τις αρχές ορθής διαχείρισης που αναφέρονται στο άρθρο 2 του δημοσιονομικού κανονισμού που εφαρμόζεται στο γενικό προϋπολογισμό των Ευρωπαϊκών Κοινοτήτων.

Άρθρο 4

Ομάδα ανεξάρτητων εμπειρογνωμόνων θα πραγματοποιήσει, για λογαριασμό της Επιτροπής, αξιολόγηση της προόδου που θα έχει επιτευχθεί κατά την αρχική περίοδο. Η έκθεση της ομάδας αυτής, μαζί με τις τυχόν παρατηρήσεις της Επιτροπής, θα υποβληθεί στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

Άρθρο 5

1. Η Επιτροπή είναι υπεύθυνη για την εφαρμογή της δράσης. Επικουρείται από συμβουλευτική επιτροπή απαρτιζόμενη από αντιπροσώπους των κρατών μελών υπό την προεδρία του αντιπροσώπου της Επιτροπής.

2. Το σχέδιο δράσης εφαρμόζεται σύμφωνα με τους στόχους που ορίζονται στο άρθρο 2 και ενημερώνεται όποτε χρειάζεται. Στο εν λόγω σχέδιο εκτίθενται λεπτομερώς οι επιδιωκόμενοι στόχοι και οι αναληπτέες δράσεις, καθώς και οι δημοσιονομικές ρυθμίσεις που προβλέπονται σχετικά. Η Επιτροπή οργανώνει προσκλήσεις υποβολής προτάσεων βάσει του σχεδίου δράσης.

3. Το σχέδιο δράσης τίθεται σε εφαρμογή σε στενή συνεργασία με τους φορείς του κλάδου. Λαμβάνει υπόψη τις εν εξελίξει ευρωπαϊκές και διεθνείς δραστηριότητες τυποποίησης στον υπόψη τομέα, τις οποίες προωθεί και συμπληρώνει.

Άρθρο 6

1. Η διαδικασία που προβλέπεται στο άρθρο 7 εφαρμόζεται στα μέτρα κοινοτικής πολιτικής στον τομέα της ασφάλειας των συστημάτων πληροφοριών.

2. Η διαδικασία που καθορίζεται στο άρθρο 8 εφαρμόζεται:

— στην προετοιμασία και την ενημέρωση του σχεδίου δράσης που αναφέρεται στο άρθρο 5,

— στο περιεχόμενο των προσκλήσεων υποβολής προτάσεων, την αξιολόγηση των προτάσεων και την εκτίμηση του ποσού συμμετοχής της Κοινότητας στα μέτρα όταν το ποσό αυτό υπερβαίνει τα 200 000 Ecu,

— στη συνεργασία μη κοινοτικών οργανισμών σε κάθε δραστηριότητα που αναλαμβάνεται δυνάμει της παρούσας αποφάσεως,

— στις ρυθμίσεις για τη διάδοση, προστασία και εκμετάλλευση των αποτελεσμάτων των μέτρων,

— στα μέτρα που θα πρέπει να ληφθούν για την αξιολόγηση της δράσης.

3. Όταν το ποσό της κοινοτικής συνεισφοράς στα μέρα είναι ίσο ή μικρότερο από 200 000 Ecu, η Επιτροπή συμβουλεύεται την επιτροπή για τα μέτρα που πρέπει να ληφθούν και την ενημερώνει για το αποτέλεσμα των εκτιμήσεών της.

Άρθρο 7

Ο αντιπρόσωπος της Επιτροπής υποβάλλει στην επιτροπή σχέδιο των μέτρων που πρόκειται να ληφθούν. Η επιτροπή διατυπώνει τη γνώμη της για το σχέδιο αυτό μέσα σε προθεσμία που μπορεί να ορίσει ο πρόεδρος ανάλογα με τον επείγοντα χαρακτήρα του θέματος, και, αν χρειασθεί, προβαίνει σε ψηφοφορία.

Η γνώμη καταχωρείται στα πρακτικά· επιπλέον, κάθε κράτος μέλος έχει το δικαίωμα να ζητήσει να καταχωρηθεί η θέση του στα πρακτικά.

Η Επιτροπή λαμβάνει ιδιαίτερα υπόψη τη γνώμη της επιτροπής και την ενημερώνει για τον τρόπο με τον οποίο έλαβε υπόψη τη γνώμη αυτή.

Άρθρο 8

Ο αντιπρόσωπος της Επιτροπής υποβάλλει στην εν λόγω επιτροπή σχέδιο των μέτρων που πρόκειται να ληφθούν. Η επιτροπή διατυπώνει τη γνώμη της για το σχέδιο αυτό μέσα σε προθεσμία που μπορεί να ορίσει ο πρόεδρος ανάλογα με τον επείγοντα χαρακτήρα του θέματος. Αποφασίζει με την

ειδική πλειοψηφία που προβλέπεται στο άρθρο 148 παράγραφος 2 της συνθήκης για την έκδοση των αποφάσεων που καλείται να λάβει το Συμβούλιο βάσει προτάσεως της Επιτροπής. Κατά την ψηφοφορία στην επιτροπή, οι ψήφοι των αντιπροσώπων των κρατών μελών σταθμίζονται σύμφωνα με το προαναφερόμενο άρθρο. Ο πρόεδρος δεν λαμβάνει μέρος στην ψηφοφορία.

Η Επιτροπή θεσπίζει τα σχεδιαζόμενα μέτρα όταν είναι σύμφωνα με τη γνώμη της Επιτροπής.

Όταν τα σχεδιαζόμενα μέτρα δεν είναι σύμφωνα με τη γνώμη της επιτροπής, ή ελλείψει γνώμης, η Επιτροπή υποβάλλει χωρίς καθυστέρηση στο Συμβούλιο πρόταση σχετικά με τα μέτρα που πρέπει να ληφθούν. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία.

Εάν το Συμβούλιο δεν αποφασίσει εντός τριών μηνών από την ημερομηνία υποβολής της πρότασης, τα προτεινόμενα μέτρα θεσπίζονται από την Επιτροπή, εκτός εάν το Συμβούλιο έχει αποφασίσει με απλή πλειοψηφία ότι αντιτίθεται προς τα εν λόγω μέτρα.

Βρυξέλλες, 31 Μαρτίου 1992.

Για το Συμβούλιο

Ο Πρόεδρος

Vitor MARTINS

ΠΑΡΑΡΤΗΜΑ

Περίληψη των κατευθύνσεων δράσης

ΠΡΟΣΑΝΑΤΟΛΙΣΜΟΙ ΓΙΑ ΣΧΕΔΙΟ ΔΡΑΣΗΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

ΕΙΣΑΓΩΓΗ

Το σχέδιο δράσης έχει ως στόχο την ανάπτυξη συνολικών στρατηγικών για την παροχή, στους χρήστες και παραγωγούς ηλεκτρονικά φυλασσόμενων, υφιστάμενων επεξεργασία ή μεταδιδομένων πληροφοριών, της ενδεδειγμένης προστασίας των συστημάτων πληροφοριών έναντι τυχαίων ή σκόπιμων απειλών.

Το σχέδιο δράσης λαμβάνει υπόψη και συμπληρώνει τις εν εξελίξει ευρωπαϊκές και παγκόσμιες δραστηριότητες τυποποίησης στον τομέα αυτόν.

Το σχέδιο περιλαμβάνει τις ακόλουθες κατευθύνσεις δράσης:

— ανάπτυξη στρατηγικού πλαισίου για την ασφάλεια των συστημάτων πληροφοριών,

— προσδιορισμός των αναγκών των χρήστων και των παρεχόντων υπηρεσίες σε θέματα ασφάλειας των συστημάτων πληροφοριών,

— λύσεις για άμεσες και προσωρινές ανάγκες των χρήστων, των προμηθευτών και των παρεχόντων υπηρεσίες,

— κατάρτιση προδιαγραφών, προτύπων, αξιολόγηση και πιστοποίηση σε θέματα ασφάλειας των συστημάτων πληροφοριών,

— τεχνολογικές και λειτουργικές εξελίξεις σε θέματα ασφάλειας των συστημάτων πληροφοριών,

— κατοχύρωση της ασφάλειας των συστημάτων πληροφοριών.

Το σχέδιο δράσης εφαρμόζεται από την Επιτροπή, σε στενό συσχετισμό με συναφείς δράσεις στα κράτη μέλη, και σε συνδυασμό με συναφείς κοινοτικές δράσεις έρευνας και ανάπτυξης.

1. Πρώτη κατεύθυνση δράσης — Ανάπτυξη ενός στρατηγικού πλαισίου για την ασφάλεια των συστημάτων πληροφοριών

1.1. *Ζητούμενο*

Η ασφάλεια των συστημάτων πληροφοριών αναγνωρίζεται σαν ένα ευρέως διαδεδομένο χαρακτηριστικό, αναγκαίο στη σύγχρονη κοινωνία. Οι ηλεκτρονικές υπηρεσίες πληροφοριών χρειάζονται ασφαλή τηλεπικοινωνιακή υποδομή, ασφαλή υλικό εξοπλισμό και λογισμικό καθώς και ασφαλή χρήση και διαχείριση. Είναι αναγκαίο να καθοριστεί μια συνολική στρατηγική που να λαμβάνει υπόψη όλες τις πτυχές της ασφάλειας των συστημάτων πληροφοριών και να αποφευχθούν έτσι οι αποσπασματικές προσεγγίσεις. Κάθε στρατηγική για την ασφάλεια των πληροφοριών που υφίστανται ηλεκτρονική επεξεργασία πρέπει να αντανακλά την επιθυμία κάθε κοινωνίας να λειτουργεί αποτελεσματικά, αλλά ταυτόχρονα να προστατεύεται, σε ένα κόσμο που αλλάζει με ταχύ ρυθμό.

1.2. *Στόχος*

Πρέπει να θεσπιστεί πλαίσιο με στρατηγικό προσανατολισμό, που να συμβιβάζει τους κοινωνικούς, οικονομικούς και πολιτικούς στόχους με τις τεχνικές, λειτουργικές και νομικές επιλογές της Κοινότητας σε διεθνές πλαίσιο. Η λεπτή ισορροπία ανάμεσα σε διαφορετικά συμφέροντα, στόχους και περιορισμούς πρέπει να βρεθεί μέσω της συνεργασίας των φορέων των οικείων τομέων για την επεξεργασία πλαισίου κοινής αντίληψης και στρατηγικής. Αυτές είναι οι προϋποθέσεις για το συμβιβασμό συμφερόντων και αναγκών, τόσο στον τομέα της χάραξης της πολιτικής όσο και στον τομέα των βιομηχανικών εξελίξεων.

1.3. *Σημερινή κατάσταση και τάσεις*

Η κατάσταση χαρακτηρίζεται από την αυξανόμενη επίγνωση της ανάγκης για δράση. Ωστόσο, σε περίπτωση έλλειψης πρωτοβουλιών για συντονισμό των προσπαθειών, είναι πολύ πιθανή η ανάληψη αυτόνομων προσπαθειών σε διάφορους κλάδους και τομείς, οι οποίες εκ των πραγμάτων θα δημιουργήσουν μια αντιφατική κατάσταση, προξενώντας βαθμηδόν σοβαρότερα νομικά, κοινωνικά και οικονομικά προβλήματα.

1.4. *Ανάγκες, επιλογές και προτεραιότητες*

Ένα τέτοιο κοινά αποδεκτό πλαίσιο θα πρέπει να αντιμετωπίσει και να οριοθετήσει την ανάλυση και τη διαχείριση δυσμενών ενδεχομένων σχετικά με το ευπρόσβλητο των πληροφοριών καθώς και των σχετικών υπηρεσιών, την εναρμόνιση των νομοθετικών και κανονιστικών διατάξεων σχετικά με την κατάχρηση και την κακή χρήση των υπολογιστών και των τηλεπικοινωνιών, τη διοικητική υποδομή, συμπεριλαμβανομένων των πολιτικών ασφάλειας και του τρόπου που αυτές μπορούν αποτελεσματικά να τεθούν σε εφαρμογή από διάφορους βιομηχανικούς και επιστημονικούς κλάδους, τα μελήματα κοινωνικού χαρακτήρα και προστασίας της ιδιωτικής ζωής (π.χ. την εφαρμογή σχεδίων για προσδιορισμό ταυτότητας, απόδειξη γνησιότητας, αδυναμίας εκ των υστέρων άρνησης και, πιθανόν, χορήγησης αδειών σε ένα δημοκρατικό περιβάλλον).

Πρέπει να δοθούν σαφείς κατευθύνσεις για την ανάπτυξη υλικών και λογικών αρχιτεκτονικών για ασφαλείς υπηρεσίες κατανεμημένων πληροφοριών, την εκπόνηση προτύπων, κατευθυντήριων γραμμών και ορισμών για προϊόντα και υπηρεσίες εγγυημένης ασφάλειας, την υλοποίηση πειραματικών εφαρμογών και πρωτοτύπων που να καταδεικνύουν τη βιωσιμότητα διαφόρων διοικητικών δομών, αρχιτεκτονικών και προτύπων σχετικών με τις ανάγκες ειδικών τομέων.

Πρέπει να υπάρξει επίγνωση για τη σημασία της ασφάλειας, έτσι ώστε να επηρεαστεί θετικά η στάση των χρήστων ως προς την αυξανόμενη μέριμνα για ασφάλεια στις τεχνολογίες των πληροφοριών.

2. **Δεύτερη κατεύθυνση δράσης — Προσδιορισμός των αναγκών των χρήστων και των παρεχόντων υπηρεσίες σε θέματα ασφάλειας των συστημάτων πληροφοριών**

2.1. *Ζητούμενο*

Η ασφάλεια των συστημάτων πληροφοριών είναι εγγενής προϋπόθεση για την ακεραιότητα και αξιοπιστία των επιχειρηματικών εφαρμογών, της πνευματικής ιδιοκτησίας και του απορρήτου. Αυτό οδηγεί αναπόφευκτα σε μια λεπτή ισορροπία και μερικές φορές σε επιλογές ανάμεσα στη δέσμευση για ελεύθερο εμπόριο και τη δέσμευση για την προστασία της ιδιωτικής ζωής και της πνευματικής ιδιοκτησίας. Αυτές οι επιλογές και οι συμβιβαστικές λύσεις πρέπει να βασιστούν σε μια πλήρη εκτίμηση των αναγκών και στη δυνατότητα των διαφόρων εναλλακτικών επιλογών σχετικά με την ασφάλεια των συστημάτων πληροφοριών να ανταποκριθούν σ' αυτές τις ανάγκες.

Οι ανάγκες των χρήστων συνεπάγονται την αλληλεξάρτηση των λειτουργιών των σχετικών με την ασφάλεια των συστημάτων πληροφοριών με διάφορες πτυχές τεχνολογικού, λειτουργικού και κανονιστικού χαρακτήρα. Κατά συνέπεια, η συστηματική εξέταση των αναγκών για ασφάλεια των συστημάτων πληροφοριών αποτελεί ουσιαστικό μέρος της επεξεργασίας κατάλληλων και αποτελεσματικών μέτρων.

2.2. *Στόχος*

Ο καθορισμός της φύσης και των χαρακτηριστικών των αναγκών των χρήστων και των παρεχόντων υπηρεσίες και η σχέση τους με μέτρα για την ασφάλεια των συστημάτων πληροφοριών.

2.3. *Σημερινή κατάσταση και τάσεις*

Μέχρι τώρα δεν έχει αναληφθεί καμία συτονισμένη προσπάθεια με στόχο να προσδιορίσει τις ταχύτατα εξελισσόμενες και μεταβαλλόμενες ανάγκες των κυριοτέρων φορέων στον τομέα της ασφάλειας των συστημάτων πληροφοριών. Ορισμένα κράτη μέλη της Κοινότητας έχουν καθορίσει τις προϋποθέσεις για εναρμόνιση των εθνικών δραστηριοτήτων (ιδιαίτερα των «κριτηρίων αξιολόγησης της ασφάλειας των τεχνολογιών των πληροφοριών»). Ιδιαίτερη σημασία έχουν τα ενιαία κριτήρια αξιολόγησης και οι κανόνες για αμοιβαία αναγνώριση των πιστοποιητικών αξιολόγησης.

2.4. *Ανάγκες, επιλογές και προτεραιότητες*

Θεωρείται αναγκαία η επεξεργασία μιας κοινά αποδεκτής κατάταξης των αναγκών των χρήστων καθώς και η σχέση της με τα μέτρα που αφορούν την ασφάλεια των συστημάτων πληροφοριών σαν βάση για μια συγκροτημένη και διαφανή αντιμετώπιση των αιτιολογημένων αναγκών των φορέων των διαφόρων τομέων.

Επίσης θεωρείται σημαντικός ο προσδιορισμός των αναγκών για νομοθεσία, ρυθμίσεις και κώδικες καλής πρακτικής υπό το φως της αξιολόγησης των τάσεων σχετικά με τα χαρακτηριστικά των υπηρεσιών και της τεχνολογίας, ο καθορισμός εναλλακτικών στρατηγικών για επίτευξη των στόχων μέσω διοικητικών διατάξεων ή μέτρων που αφορούν το λειτουργικό ή τον τεχνικό τομέα ή τον τομέα των υπηρεσιών, και η αξιολόγηση της αποτελεσματικότητας, της ευκολίας στη χρήση και του κόστους εναλλακτικών επιλογών σχετικά με την ασφάλεια καθώς και των στρατηγικών των συστημάτων πληροφοριών για τους χρήστες, τους φορείς παροχής υπηρεσιών και τους φορείς εκμετάλλευσης.

3. **Τρίτη κατεύθυνση δράσης — Εξεύρεση λύσεων για άμεσες και προσωρινές ανάγκες των χρήστων, των προμηθευτών και των παρεχόντων υπηρεσίες**

3.1. *Ζητούμενο*

Προς το παρόν, είναι δυνατή η επαρκής προστασία των ηλεκτρονικών υπολογιστών από πρόσβαση χωρίς άδεια από τον έξω κόσμο με «απομόνωση», δηλαδή με εφαρμογή συμβατικών οργανωτικών και υλικών μέτρων. Αυτό, επίσης, ισχύει και στις ηλεκτρονικές επικοινωνίες μιας κλειστής ομάδας χρήστων που λειτουργεί με βάση ένα ειδικό δίκτυο. Η κατάσταση είναι πολύ διαφορετική σε περίπτωση που οι πληροφορίες μοιράζονται ανάμεσα σε διάφορες ομάδες χρήστων ή ανταλλάσσονται μέσω ενός δικτύου που είναι είτε δημόσιο είτε γενικώς προσιτό. Ούτε η τεχνολογία, οι τερματικοί σταθμοί και οι υπηρεσίες ούτε και τα σχετικά πρότυπα και διαδικασίες είναι γενικά σε θέση να προσφέρουν ανάλογη ασφάλεια των συστημάτων πληροφοριών σ' αυτές τις περιπτώσεις.

3.2. *Στόχος*

Ο στόχος πρέπει να είναι η εξεύρεση, εντός βραχείας προθεσμίας, λύσεων που να μπορούν να ανταποκριθούν στις πιο επείγουσες ανάγκες των χρήστων, των παρεχόντων υπηρεσίες και των κατασκευαστών, πράγμα που συμπεριλαμβάνει και τη χρησιμοποίηση κοινών κριτηρίων αξιολόγησης της ασφάλειας στις τεχνολογίες πληροφοριών. Ο σχεδιασμός τους θα πρέπει να λαμβάνει υπόψη μέλλουσες απαιτήσεις και λύσεις.

3.3. *Σημερινή κατάσταση και τάσεις*

Μερικές ομάδες χρήστων έχουν αναπτύξει τεχνικές και διαδικασίες, για δική τους αποκλειστική χρήση, που ανταποκρίνονται ιδιαίτερα στην ανάγκη για απόδειξη γνησιότητας της ταυτότητας, αρτιότητας και αδυναμίας εκ των υστέρων άρνησης. Γενικά, γίνεται χρήση μαγνητικών καρτών ή καρτών με μνήμη. Μερικές ομάδες χρησιμοποιούν κρυπτογραφικές τεχνικές περισσότερο ή λιγότερο πολύπλοκες. Αυτό συχνά συνεπάγεται τον καθορισμό «εξουσιοδοτημένων ατόμων» ειδικών για κάθε ομάδα χρήστων. Ωστόσο, η γενίκευση αυτών των τεχνικών και μεθόδων για την ικανοποίηση των αναγκών ενός ανοικτού περιβάλλοντος είναι δύσκολη.

Ο ISO εργάζεται για την ασφάλεια των πληροφοριών στο πλαίσιο του μοντέλου ISO (ISO DIS 7498-2) και η CCITT στο πλαίσιο του X400. Είναι επίσης δυνατή η παρεμβολή τμημάτων ασφάλειας στα μηνύματα. Τα ζητήματα της απόδειξης γνησιότητας της ταυτότητας, της αρτιότητας και της αδυναμίας εκ των υστέρων άρνησης αντιμετωπίζονται ως μέρος των μηνυμάτων (EDIFACT) καθώς και ως μέρος του X400 MHS.

Προς το παρόν, το νομικό πλαίσιο της ηλεκτρονικής ανταλλαγής δεδομένων (EDI) βρίσκεται ακόμη στο στάδιο του σχεδιασμού. Το Διεθνές Εμπορικό Επιμελητήριο έχει δημοσιεύσει ενιαίους κανόνες συμπεριφοράς που αφορούν την ανταλλαγή εμπορικών στοιχείων διαμέσου δικτύου τηλεπικοινωνιών.

Μερικές χώρες (π.χ. Γερμανία, Γαλλία, Ηνωμένο Βασίλειο και Ηνωμένες Πολιτείες) έχουν αναπτύξει ή αναπτύσσουν κριτήρια για την αξιολόγηση της αξιοπιστίας των συστημάτων και προϊόντων τεχνολογιών των πληροφοριών και τηλεπικοινωνιών καθώς επίσης και αντίστοιχες διαδικασίες για τη διενέργεια των αξιολογήσεων. Ο καθορισμός των κριτηρίων έχει γίνει σε συνεργασία με εθνικούς κατασκευαστές και θα οδηγήσει, αρχίζοντας από απλά προϊόντα, σε ένα αυξανόμενο αριθμό αξιόπιστων προϊόντων και συστημάτων. Η δημιουργία εθνικών οργανώσεων οι οποίες θα διενεργούν τις αξιολογήσεις και θα χορηγούν πιστοποιητικά θα στηρίξει αυτή την τάση.

Μέτρα σχετικά με τον εμπιστευτικό χαρακτήρα των στοιχείων θεωρούνται λιγότερο επείγοντα από τους περισσότερους χρήστες. Ωστόσο, είναι πιθανόν να αλλάξει αργότερα αυτή η κατάσταση, καθώς εξελιγμένες υπηρεσίες επικοινωνιών, και ιδιαίτερα κινητές υπηρεσίες, θα έχουν διαδοθεί ευρέως.

3.4. *Ανάγκες, επιλογές και προτεραιότητες*

Η ανάπτυξη, όσο το δυνατόν γρηγορότερα, διαδικασιών, προτύπων, προϊόντων και μέσων ικανών να εξασφαλίσουν την ασφάλεια τόσο των συστημάτων πληροφοριών αυτών καθεαυτών (υπολογιστές, περιφερειακά), όσο και των δημόσιων δικτύων επικοινωνιών, είναι θέμα ζωτικής σημασίας. Μεγάλη προτεραιότητα θα πρέπει να δοθεί στα ζητήματα της απόδειξης της γνησιότητας της ταυτότητας, της αρτιότητας και της αδυναμίας εκ των υστέρων άρνησης. Θα πρέπει να πραγματοποιηθούν δοκιμαστικές εφαρμογές σε μικρή κλίμακα έτσι ώστε να εδραιωθεί η εγκυρότητα των προτεινόμενων λύσεων. Οι λύσεις σε ανάγκες που έχουν προτεραιότητα στον τομέα της EDI εξετάζονται από το πρόγραμμα TEDIS, στα πλαίσια του γενικότερου περιεχομένου του παρόντος σχεδίου δράσης.

4. Τέταρτη κατεύθυνση δράσης — Εκπόνηση προδιαγραφών, προτύπων, αξιολόγηση και πιστοποίηση σε θέματα ασφάλειας των συστημάτων πληροφοριών

4.1. *Ζητούμενο*

Οι ανάγκες για την ασφάλεια των συστημάτων πληροφοριών είναι ευρέως διαδεδομένες, και γι' αυτό το λόγο η ύπαρξη κοινών προδιαγραφών και προτύπων είναι αποφασιστικής σημασίας. Η έλλειψη συμφωνημένων προδιαγραφών και προτύπων για την ασφάλεια των τεχνολογιών των πληροφοριών μπορεί να αποτελέσει ουσιαστικό εμπόδιο στην ανάπτυξη υπηρεσιών και διαδικασιών που θα έχουν βάση τις πληροφορίες στην οικονομία και στην κοινωνία. Απαιτούνται επίσης δράσεις για την επιτάχυνση της ανάπτυξης και χρήσης τεχνολογιών και προτύπων σε τομείς σχετικούς με τις επικοινωνίες και τα δίκτυα υπολογιστών που έχουν εξαιρετική σημασία για τους χρήστες, τη βιομηχανία και τη διοίκηση.

4.2. *Στόχος*

Απαιτούνται προσπάθειες για την παροχή μέσων για τη στήριξη και την εκτέλεση ειδικών λειτουργιών ασφαλείας στους γενικούς τομείς του OSI, ONP, ISDN/IBC και τη διαχείριση των δικτύων. Εγγενώς συνδεδεμένες με την τυποποίηση και τις προδιαγραφές είναι οι τεχνικές και οι προσεγγίσεις που απαιτούνται για την επαλήθευση, συμπεριλαμβανομένης και της πιστοποίησης η οποία οδηγεί στην αμοιβαία αναγνώριση. Όπου είναι δυνατόν πρέπει να υποστηρίζονται λύσεις που έχουν συμφωνηθεί διεθνώς. Θα πρέπει επίσης να ενθαρρυνθεί η ανάπτυξη και χρήση συστημάτων υπολογιστών με λειτουργίες ασφαλείας.

4.3. *Σημερινή κατάσταση και τάσεις*

Οι Ηνωμένες Πολιτείες έχουν, κατ' εξοχήν, αναλάβει σημαντικές πρωτοβουλίες για να αντιμετωπίσουν το ζήτημα της ασφάλειας των συστημάτων πληροφοριών. Στην Ευρώπη το θέμα αντιμετωπίζεται στα πλαίσια της τεχνολογίας των πληροφοριών και της τυποποίησης των τηλεπικοινωνιών στα πλαίσια του ETSI και της CEN/CENELEC, κατά την προετοιμασία της σχετικής εργασίας της CCITT και της ISO.

Λόγω του αυξανόμενου ενδιαφέροντος, οι εργασίες στις Ηνωμένες Πολιτείες εντείνονται με ταχύ ρυθμό, και όχι μόνο οι κατασκευαστές αλλά και οι φορείς παροχής υπηρεσιών αυξάνουν τις προσπάθειές τους στον τομέα αυτό. Στην Ευρώπη, η Γαλλία, η Γερμανία και το Ηνωμένο Βασίλειο έχουν αναλάβει μεμονωμένα παρόμοιες δραστηριότητες, αλλά μια κοινή προσπάθεια, αντίστοιχη με αυτή των Ηνωμένων Πολιτειών, εξελίσσεται αλλά αργά.

4.4. *Ανάγκες, επιλογές και προτεραιότητες*

Στον τομέα της ασφάλειας των συστημάτωνν πληροφοριών υπάρχει έμφυτη μια πολύ στενή σχέση στα θέματα ρυθμιστικού, λειτουργικού, διοικητικού και τεχνικού χαρακτήρα. Οι κανονιστικές ρυθμίσεις πρέπει να αντανακλώνται σε πρότυπα, και τα μέτρα για την ασφάλεια των συστημάτων πληροφοριών πρέπει να είναι σύμφωνα προς τα πρότυπα και τις κανονιστικές ρυθμίσεις με τρόπο που να επιδέχεται επαλήθευση. Σε ορισμένα θέματα, οι κανονιστικές ρυθμίσεις απαιτούν προδιαγραφές πέραν του συμβατικού πεδίου της τυποποίησης, δηλαδή περιλαμβάνουν κώδικες ορθής πρακτικής. Οι ανάγκες για πρότυπα και κώδικες ορθής πρακτικής υπάρχουν σε όλους τους τομείς της ασφάλειας των συστημάτων πληροφοριών, ενώ πρέπει να γίνει μια διάκριση ανάμεσα στις ανάγκες για προστασία που αντιστοιχούν στους στόχους για ασφάλεια και μερικές από τις τεχνικής φύσεως ανάγκες, οι οποίες μπορούν να ανατεθούν στους αρμόδιους ευρωπαϊκούς οργανισμούς τυποποίησης (CEN/CENELEC/ETSI).

Οι προδιαγραφές και τα πρότυπα πρέπει να καλύπτουν τα θέματα των υπηρεσιών ασφάλειας των συστημάτων πληροφοριών (απόδειξη γνησιότητας της ταυτότητας των προσώπων και των επιχειρήσεων, πρωτόκολλα μη εκ των υστέρων άρνησης, ηλεκτρονικά αποδεικτικά μέσα αποδεκτά από το νόμο, έλεγχος της χορήγησης αδειών), των υπηρεσιών των επικοινωνιών τους (μυστικότητα της επικοινωνίας μέσω εικόνας, των κινητών επικοινωνιών μέσω ήχου και των στοιχείων, προστασία των στοιχείων και των βάσεων οπτικών στοιχείων, ασφάλεια των συνδυασμένων υπηρεσιών), της διαχείρισης των επικοινωνιών και του χειρισμού ζητημάτων ασφαλείας τους (δημόσια/ιδιωτικα συστήματα κλείδας για λειτουργία ανοικτών δικτύων, προστασία της διαχείρισης των δικτύων, προστασία των φορέων παροχής υπηρεσιών) και της πιστοποίησής τους (κριτήρια και επίπεδα εγγυήσεων, διαδικασίες εγγυήσεων σχετικών με την ασφάλεια για ασφαλή συστήματα πληροφοριών).

5. Πέμπτη κατεύθυνση δράσης — Τεχνολογικές και επιχειρησιακές εξελίξεις σε θέματα ασφάλειας των συστημάτων πληροφοριών

5.1. *Ζητούμενο*

Η συστηματική εξέταση και ανάπτυξη της τεχνολογίας που θα επιτρέψει οικονομικά βιώσιμες και λειτουργικά ικανοποιητικές λύσεις σε μια σειρά σημερινών και μελλοντικών αναγκών για την ασφάλεια των συστημάτων πληροφοριών αποτελεί προϋπόθεση για την ανάπτυξη της αγοράς των υπηρεσιών και την ανταγωνιστικότητα της ευρωπαϊκής οικονομίας στο σύνολό της.

Κάθε τεχνολογική εξέλιξη στον τομέα της ασφάλειας συστημάτων πληροφοριών θα πρέπει να λάβει υπόψη όχι μόνο ζητήματα ασφάλειας των υπολογιστών, αλλά και ασφάλειας των επικοινωνιών, καθώς τα περισσότερα σημερινά συστήματα είναι κατανεμημένα συστήματα, και η πρόσβαση σε τέτοια συστήματα γίνεται μέσω υπηρεσιών επικοινωνιών.

5.2. *Στόχος*

Συστηματική εξέταση και ανάπτυξη της τεχνολογίας που θα επιτρέψει οικονομικά βιώσιμες και λειτουργικά ικανοποιητικές λύσεις σε μια σειρά σημερινών και μελλοντικών αναγκών ασφάλειας των πληροφοριών.

5.3. *Ανάγκες, επιλογές και προτεραιότητες*

Οι εργασίες στον τομέα της ασφάλειας των συστημάτων πληροφοριών θα πρέπει να αφορούν τις στρατηγικές για την ανάπτυξη και την εφαρμογή, τις τεχνολογίες καθώς και το συνδυασμό σε ενιαίο σύνολο και την επαλήθευση.

Η εργασία ΕΑ§Τ στρατηγικού χαρακτήρα θα πρέπει να περιλάβει θεωρητικά μοντέλα για ασφαλή συστήματα (ασφαλή σε ό,τι αφορά φθορά των στοιχείων, τροποποιήσεις χωρίς τη σχετική άδεια και άρνηση υπηρεσίας), μοντέλα λειτουργικών απαιτήσεων, μοντέλα ανάλυσης δυσμενών ενδεχομένων και αρχιτεκτονικές για ασφάλεια.

Η εργασία ΕΑ§Τ με τεχνολογικό προσανατολισμό θα πρέπει να συμπεριλάβει την απόδειξη γνησιότητας της ταυτότητας του χρήστη και του μηνύματος (για παράδειγμα με ανάλυση φωνής και ηλεκτρονικών υπογραφών), τεχνικά συστήματα διασύνδεσης και πρωτόκολλα για κρυπτογράφηση, μηχανισμούς ελέγχου της πρόσβασης και μεθόδους για ασφαλή συστήματα που επιδέχονται απόδειξη.

Η επαλήθευση και η επικύρωση της ασφάλειας τεχνικού συστήματος και το εφαρμόσιμόν του θα πρέπει να ερευνηθούν μέσω σχεδίων ολοκλήρωσης και επαλήθευσης.

Εκτός από την εδραίωση και ανάπτυξη της τεχνολογίας για ασφάλεια, απαιτείται μια σειρά συνοδευτικών μέτρων που αφορά τη δημιουργία, διατήρηση και συγκροτημένη εφαρμογή των προτύπων, καθώς και την κύρωση και την πιστοποίηση των τεχνολογιών των πληροφοριών και των προϊόντων στον τομέα των τηλεπικοινωνιών σ' ό,τι αφορά την παρεχόμενη ασφάλεια, συμπεριλαμβανομένης της κύρωσης και της πιστοποίησης των μεθόδων για σχεδιασμό και εγκατάσταση συστημάτων.

Το τρίτο κοινοτικό πρόγραμμα-πλαίσιο για την Έρευνα, την Ανάπτυξη και την Τεχνολογία θα μπορούσε να χρησιμοποιηθεί για να ενισχύσει σχέδια συνεργασίας σε στάδια που προηγούνται του ανταγωνισμού και της τυποποίησης.

6. Έκτη κατεύθυνση δράσης — Κατωχύρωση της ασφάλειας των συστημάτων πληροφοριών

6.1. *Ζητούμενο*

Ανάλογα με την ακριβή φύση των απαιτούμενων τεχνικών χαρακτηριστικών για την ασφάλεια των συστημάτων πληροφοριών, θα χρειαστεί να ενσωματωθούν διάφορες λειτουργίες σε διαφορετικά τμήματα των συστημάτων πληροφοριών, συμπεριλαμβανομένων όχι μόνο των τερματικών/υπολογιστών, των υπηρεσιών, της διαχείρισης δικτύων αλλά και των κρυπτογραφικών εξαρτημάτων, καρτών με μνήμη, δημόσιων και ιδιωτικών κλειδών κ.λπ. Αναμένεται ότι μερικές από αυτές θα ενσωματωθούν στον υλικό εξοπλισμό και στο λογισμικό από τους κατασκευαστές ενώ άλλες μπορεί είτε να αποτελέσουν τμήμα κατανεμημένων συστημάτων (π.χ. διαχείριση δικτύων), είτε να είναι ιδιοκτησία συγκεκριμένων χρηστών (π.χ. κάρτες με μνήνη), είτε να παρέχονται από έναν εξειδικευμένο οργανισμό (π.χ. δημόσιες/ιδιωτικές κλείδες).

Αναμένεται ότι η μεγάλη πλειοψηφία των προϊόντων και υπηρεσιών ασφαλείας θα παρέχεται από τους κατασκευαστές, τους φορείς παροχής υπηρεσιών ή τους φορείς εκμετάλλευσης. Για εξειδικευμένες λειτουργίες, όπως π.χ. την παροχή δημόσιων/ιδιωτικών κλειδών και την άδεια ελέγχου, μπορεί να χρειαστεί ο προσδιορισμός και η εξουσιοδότηση κατάλληλων οργανισμών.

Το ίδιο ισχύει για την πιστοποίηση, την αξιολόγηση και τον έλεγχο της ποιότητας των υπηρεσιών, οι οποίες είναι λειτουργίες που πρέπει να ανατεθούν σε οργανισμούς ανεξάρτητους από τους κατασκευαστές, τους φορείς παροχής υπηρεσιών ή τους φορείς εκμετάλλευσης. Οι οργανισμοί αυτοί θα μπορούσαν να είναι ιδιωτικοί, κυβερνητικοί, ή εξουσιοδοτημένοι από την κυβέρνηση για την εκτέλεση συγκεκριμένων λειτουργιών.

6.2. *Στόχος*

Είναι αναγκαία η ανάπτυξη μιας συγκροτημένης προσέγγισης σ' ό,τι αφορά την παροχή ασφάλειας των συστημάτων πληροφοριών, προκειμένου να διευκολυνθεί η αρμονική ανάπτυξη της ασφάλειας των συστημάτων πληροφοριών μέσα στην Κοινότητα, έτσι ώστε να προστατευθούν τα συμφέροντα του δημοσίου και του ιδιωτικού τομέα. Εκεί που θα χρειασθεί να εξουσιοδοτηθούν ανεξάρτητοι οργανισμοί, η αποστολή τους και οι όροι που τη διέπουν θα πρέπει να καθοριστούν, να συμφωνηθούν, και, όπου είναι αναγκαίο, να ενσωματωθούν σε ρυθμίσεις. Στόχος θα πρέπει να είναι η επίτευξη ενός σαφούς και κοινά αποδεκτού καταμερισμού ευθυνών μεταξύ των διαφόρων φορέων στην Κοινότητα, ως προϋπόθεση για την αμοιβαία αναγνώριση.

6.3. *Σημερινή κατάσταση και τάσεις*

Προς το παρόν, η καταχώρηση της ασφάλειας των συστημάτων πληροφοριών είναι καλά οργανωμένη μόνο σε εξειδικευμένους τομείς και περιορίζεται στην αντιμετώπιση των ειδικών αναγκών τους. Η οργάνωση σε ευρωπαϊκό επίπεδο γίνεται κατά κύριο λόγο άτυπα και δεν έχει ακόμη θεσπιστεί, εκτός κλειστών ομάδων, η αμοιβαία αναγνώριση των διαδικασιών επαλήθευσης και πιστοποίησης. Με την αυξανόμενη σημασία της ασφάλειας των συστημάτων πληροφοριών, γίνεται επείγουσα η ανάγκη για καθορισμό μιας συνεπούς προσέγγισης σχετικά με την καταχύρωση της ασφάλειας των συστημάτων πληροφοριών στην Ευρώπη και διεθνώς.

6.4. *Ανάγκες, επιλογές και προτεραιόττηες*

Λόγω του αριθμού των διαφόρων ενδιαφερομένων φορέων και της στενής σχέσης με ζητήματα κανονιστικών ρυθμίσεων και νόμων, η εκ των προτέρων συμφωνία σχετικά με τις αρχές που θα πρέπει να καθορίζουν την κατοχύρωση της ασφάλειας των συστημάτων πληροφοριών είναι ιδιαίτερα σημαντική.

Στην επεξεργασία μιας συνεπούς προσέγγισης του ζητήματος, θα χρειαστεί η αντιμετώπιση ζητημάτων όπως ο προσδιορισμός και η εξειδίκευση λειτουργιών που απαιτούν, από την ίδια τους τη φύση, την ύπαρξη ανεξάρτητων οργανώσεων (ή συνεργαζομένων οργανώσεων). Αυτό θα μπορούσε να συμπεριλάβει λειτουργίες όπως η διαχείριση ενός συστήματος δημόσιας/ιδιωτικής κλείδας.

Επιπλέον, απαιτείται ο προσδιορισμός και η εξειδίκευση, σε ένα αρχικό στάδιο, λειτουργιών οι οποίες για λόγους δημοσίου συμφέροντος θα πρέπει να ανατεθούν σε ανεξάρτητες οργανώσεις (ή σε συνεργαζόμενες οργανώσεις). Αυτές οι λειτουργίες θα μπορούσαν π.χ. να περιλάβουν τον έλεγχο, την εξασφάλιση της ποιότητας, την επαλήθευση, την πιστοποίηση και παρόμοιες λειτουργίες.