# ΚΕΦΑΛΑΙΟ 5

## ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ (ΕΣΑΔΠ)

Η ΑΔΑΕ έχει επανειλημμένα επισημάνει αρμοδίως ότι, παρ' όλο που στον Ν. 3431/ 2006 (άρθρο 4) αλλά και στους προγενέστερους από αυτόν νόμους προβλέπεται ο σχεδιασμός πολιτικής από το Υπουργείο Υποδομών, Μεταφορών και Δικτύων και τα συναρμόδια υπουργεία για το θέμα της ασφάλειας δικτύων και πληροφοριών, δεν έχει μέχρι σήμερα καταρτιστεί τέτοια πολιτική.

Η Αρχή, επειδή θεωρεί ότι η ασφάλεια των δικτύων και των πληροφοριών είναι μεγάλης σημασίας, δεδομένου ότι, ως γνωστόν, η πληροφορική πλέον υπεισέρχεται σε πλείστες όσες δραστηριότητες μιας σύγχρονης κοινωνίας, έχει προτείνει, ήδη από το 2004, να καταρτίσει η πολιτεία μια ολοκληρωμένη εθνική στρατηγική ασφάλειας δικτύων και πληροφοριών και έχει διαβιβάσει στα αρμόδια υπουργεία αρχές μιας τέτοιας στρατηγικής.

Πρέπει να σημειωθεί ότι στον Ν. 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ 136/Α΄/10.07.2008) έχουν υιοθετηθεί κάποια σημεία από την πρόταση της ΑΔΑΕ και έχει συμπεριληφθεί η εφαρμογή ενός εθνικού σχεδίου ασφάλειας επικοινωνιών (ΕΣΑΕ). Η ΑΔΑΕ επισήμανε τις επιφυλάξεις της σχετικά με τα προβλεπόμενα στο σχέδιο νόμου για την κατάρτιση του ΕΣΑΕ, τόσο στον τότε Πρόεδρο της νομοπαρασκευαστικής επιτροπής όσο και στον τότε Υπουργό Δικαιοσύνης. Συγκεκριμένα, κατά την άποψη της ΑΔΑΕ, η σύνθεση της επιτροπής, κυρίως από υπαλλήλους των γενικών γραμματειών των αρμόδιων υπουργείων, καθώς και από εκπροσώπους της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), της ΑΔΑΕ και της ΕΕΤΤ, δεν μπορεί να εξασφαλίσει ένα ΕΣΑΕ που θα αποτελεί «αποτελεσματική θωράκιση των υποδομών και των μέσων στον τομέα των ηλεκτρονικών επικοινωνιών», όπως αναφέρεται ότι είναι ο σκοπός κατάρτισής του. Και τούτο διότι το εν λόγω σχέδιο δεν θα μπορεί να ανταποκριθεί διαχρονικά σε όλες τις παραμέτρους που προβλέπεται να περιλαμβάνει, όπως, στα πρότυπα, τα όργανα και τα μέσα, τους κινδύνους, τα μέτρα οργανωτικού και εκπαιδευτικού χαρακτήρα για την αντιμετώπιση των κινδύνων, την ενημέρωση των χρηστών κ.ά.

Οι επιφυλάξεις της ΑΔΑΕ έγκεινται στο ότι οι εξελίξεις στον τομέα της ασφάλειας των ηλεκτρονικών επικοινωνιών είναι συνεχείς και ανατρέπονται διαρκώς και, βεβαίως, ανάλογα μεταβάλλονται και όλες οι παραπάνω παράμετροι που θα πρέπει να εξασφαλίσει το ΕΣΑΕ. Για παράδειγμα, οι κίνδυνοι στους οποίους αναφέρεται το προτεινόμενο σχέδιο μεταβάλλονται συνεχώς, πολλαπλασιάζονται, μπορούν να εξαπλώνονται ταχύτατα μέσω των δικτύων και καθίστανται πολυπλοκότεροι, καθώς η επιτηδειότητα των επιτιθέμενων βελτιώνεται συνεχώς. Ως εκ τούτου, η κατάρτιση ενός εθνικού σχεδίου ασφάλειας επικοινωνιών θα πρέπει να είναι μια δυναμική διαδικασία, που απαιτεί μια πολυπαραγοντική και πολυεπίπεδη προσέγγιση, καθώς και μια συνεχή μελέτη και ενημέρωση για τις εξελίξεις. Από τα παραπάνω καθίσταται φανερό ότι δεν επαρκεί μια ad hoc προσέγγιση από μια εννεαμελή επιτροπή, τα μέλη της οποίας –στελέχη διαφόρων υπουργείων και φορέων– δεν θα είναι –τουλάχιστον όλα– γνώστες των συγκεκριμένων θεμάτων στον απαιτούμενο βαθμό.

Δυστυχώς, οι επιφυλάξεις της ΑΔΑΕ δεν ελήφθησαν υπόψη και ψηφίστηκε το άρθρο 13 του Ν. 3674/2008 (ΦΕΚ 136/Α΄/10.7.2008) «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις», που προβλέπει την κατάρτιση του παραπάνω αναφερόμενου σχεδίου, αλλά μέχρι στιγμής, δεν έχει γίνει καμία ενέργεια προς την κατεύθυνση υλοποίησης του άρθρου αυτού.

Η άποψη της ΑΔΑΕ ήταν και παραμένει ότι, προκειμένου να υπάρξει μια σωστή πολιτική, η οποία θα φέρει τα επιδιωκόμενα αποτελέσματα, διαχρονικά, απαιτείται τα στελέχη που θα ασχοληθούν με την κατάρτιση της πολιτικής και τη συνεχή αναπροσαρμογή της να έχουν την απαραίτητη εξειδίκευση και να παρακολουθούν διαρκώς, σε διεθνές επίπεδο, όλους τους παράγοντες που επιδρούν στην ασφάλεια. Γι' αυτό η Αρχή θεωρεί απαραίτητη τη δημιουργία ενός

εξειδικευμένου φορέα για το θεσμικό πλαίσιο της ασφάλειας των δικτύων και των πληροφοριακών συστημάτων, ο οποίος, εκτός από την κατάρτιση της πολιτικής, μεταξύ άλλων, θα:

- συμβουλεύει την πολιτεία σε εξειδικευμένα θέματα ασφάλειας δικτύων και πληροφοριακών συστημάτων,
- μελετάει την εξέλιξη των κινδύνων διεθνώς,
- συμβάλλει με παρεμβάσεις κανονιστικού χαρακτήρα ή με συστάσεις στον τομέα της ασφάλειας και θα απευθύνεται προς όλους τους φορείς και χρήστες της χώρας, από τους πιο σημαντικούς (π.χ. φορείς που περιλαμβάνουν δίκτυα κρίσιμων υποδομών ή υπουργεία) μέχρι τους φορείς με απλά δίκτυα και ακόμη παραπέρα μέχρι τους απλούς χρήστες,
- μελετάει συνεχώς, σε συνεργασία με αντίστοιχους φορείς στο εξωτερικό, τις βέλτιστες πρακτικές για την αντιμετώπιση των κινδύνων στον τομέα της ασφάλειας δικτύων και πληροφοριών, και
- ενημερώνει διαρκώς τους φορείς και τους χρήστες για τους κινδύνους της ασφάλειας των δικτύων και των υπολογιστικών συστημάτων, καθώς και τους τρόπους αντιμετώπισής τους.

Βεβαίως, η πολιτική αυτή και η εκάστοτε αναθεώρησή της θα εγκρίνεται από το Υπουργείο Υποδομών, Μεταφορών και Δικτύων και από όλα τα συναρμόδια υπουργεία.

Στο πλαίσιο αυτό, η ΑΔΑΕ πιστεύει ότι είναι απαραίτητο, αντί του προβλεπόμενου στο άρθρο 13 του Ν. 3674/2008 σχεδίου, να εγκριθεί μια εθνική στρατηγική για την ασφάλεια δικτύων και πληροφοριών, οι αρχές και οι στόχοι της οποίας καταγράφονται παρακάτω.

## 1. Αρχές της εθνικής στρατηγικής για την ασφάλεια δικτύων και πληροφοριών

Η εθνική στρατηγική ασφάλειας δικτύων και πληροφοριών πρέπει να περικλείει τις παρακάτω κατευθυντήριες αρχές που έχουν δεχθεί τα κράτη-μέλη του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ).

### 1.1 Ενημέρωση

*Οι χρήστες πρέπει να είναι ενήμεροι για την ανάγκη ασφάλειας των πληροφοριακών συστημάτων και των δικτύων και για το τι πρέπει να κάνουν για την επαύξηση της ασφάλειας.*

Η ενημέρωση επί των κινδύνων και των διαθέσιμων μέτρων προστασίας είναι η πρώτη γραμμή άμυνας για την ασφάλεια των πληροφοριακών συστημάτων και των δικτύων, τα οποία μπορεί να επηρεαστούν από εσωτερικούς και εξωτερικούς κινδύνους. Οι χρήστες πρέπει να κατανοήσουν ότι λάθη και παραλείψεις τους στην ασφάλεια μπορεί να βλάψουν σοβαρά τα συστήματα και τα δίκτυα που χρησιμοποιούν. Πρέπει επίσης να είναι ενήμεροι ως προς τη δυνητική βλάβη που μπορεί να προξενήσουν σε άλλους χρήστες, η οποία ξεκινάει από τη δική τους διασύνδεση λόγω της αλληλεξάρτησης μεταξύ των δικτύων.

Τέλος, οι χρήστες πρέπει να είναι ενήμεροι για τις κατάλληλες πρακτικές που μπορούν να εφαρμόσουν στο σύστημά τους για την ενίσχυση της ασφάλειας.

### 1.2 Υπευθυνότητα

*Όλοι οι χρήστες πρέπει να κατανοήσουν ότι είναι υπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων και των δικτύων τα οποία χρησιμοποιούν.*

Οι χρήστες βασίζονται σε αλληλοσυνδεόμενα τοπικά και διεθνή πληροφοριακά συστήματα και δίκτυα και θα πρέπει να είναι υπόλογοι κατά τρόπο που προσιδιάζει στον ατομικό τους ρόλο σε αυτά. Επιβάλλεται να αναθεωρούν περιοδικά τις πρακτικές τους, τις διαδικασίες και τα μέτρα ασφάλειας που εφαρμόζουν και να αξιολογούν εάν αυτά είναι τα καλύτερα στο περιβάλλον τους.

### 1.3 Αντιμετώπιση ζητημάτων ασφάλειας

*Οι χρήστες πρέπει να ενεργούν με κατάλληλο τρόπο για την αποφυγή κινδύνων, την ανίχνευσή τους και την ανταπόκριση σε ζητήματα ασφάλειας.*

Με δεδομένη τη διασυνδεσιμότητα και την αλληλεπίδραση των πληροφοριακών συστημάτων και των δικτύων και την πιθανότητα να εξαπλωθεί ραγδαία και σε ευρεία κλίμακα μια ζημία, οι χρήστες πρέπει να δρουν έγκαιρα και να συνεργάζονται με τους αρμόδιους φορείς για να αντιμετωπίζουν ζητήματα ασφάλειας.

Πρέπει ακόμα να ανταλλάσσουν μεταξύ τους πληροφορίες για πιθανούς κινδύνους και να εφαρμόζουν διαδικασίες για γρήγορη και αποτελεσματική συνεργασία προκειμένου να προλαμβάνουν, να ανιχνεύουν περιστατικά ασφάλειας και να ανταποκρίνονται σε αυτά.

### 1.4 Δεοντολογία

*Οι χρήστες πρέπει να σέβονται τα νόμιμα συμφέροντα των άλλων.*

Λαμβανομένων υπόψη της μεγάλης διάδοσης και της αλληλεπίδρασης των πληροφοριακών συστημάτων και των δικτύων στις σύγχρονες κοινωνίες, οι χρήστες πρέπει να κατανοούν ότι οι ενέργειές τους ή οι παραλείψεις τους μπορεί να βλάπτουν άλλους. Η συμπεριφορά των χρηστών σύμφωνα με έναν κώδικα δεοντολογίας είναι θέμα κρισιμότατο.

### 1.5 Δημοκρατία

*Η ασφάλεια των πληροφοριακών συστημάτων και των δικτύων πρέπει να συμβιβάζεται με τις βασικές αρχές μιας δημοκρατικής κοινωνίας.*

Η ασφάλεια πρέπει να εφαρμόζεται με τρόπο που να μην αφίσταται των αξιών που έχουν καθιερωθεί σε μια δημοκρατική κοινωνία, όπως είναι η ελευθερία ανταλλαγής σκέψεων και ιδεών, η ελευθερία ροής πληροφοριών, το απόρρητο της επικοινωνίας, η προστασία των προσωπικών δεδομένων και η διαφάνεια.

### 1.6 Εκτίμηση κινδύνων

*Οι χρήστες πρέπει να αξιολογούν τους κινδύνους.*

Η αξιολόγηση του κινδύνου αποβλέπει στην αναγνώρισή του και των ευάλωτων σε επιθέσεις σημείων εκ μέρους των χρηστών και πρέπει να είναι αρκετά ευρεία ώστε να περιλαμβάνει εσωτερικούς και εξωτερικούς παράγοντες/κλειδιά, όπως την τεχνολογία, τον ανθρώπινο παράγοντα, τις εφαρμοζόμενες πολιτικές και τις υπηρεσίες από τρίτους που ενέχουν θέματα ασφάλειας.

Η εκτίμηση του κινδύνου θα επιτρέπει να καθοριστεί ένα αποδεκτό επίπεδό του και θα βοηθάει στην επιλογή του κατάλληλου τρόπου για τη διαχείριση του κινδύνου από δυνητική βλάβη των πληροφοριακών συστημάτων και των δικτύων με κριτήριο τη φύση και τη σπουδαιότητα της πληροφορίας που πρέπει να προστατευτεί.

### 1.7 Σχεδιασμός της ασφάλειας και του τρόπου εφαρμογής της

*Ενσωμάτωση της ασφάλειας ως σημαντικού στοιχείου των πληροφοριακών συστημάτων και των δικτύων.*

Συστήματα, δίκτυα και πολιτικές πρέπει να σχεδιάζονται, να εφαρμόζονται και να συντονίζονται κατάλληλα ώστε να μεγιστοποιείται η ασφάλεια.

Ένας σημαντικός αλλά όχι και αποκλειστικός στόχος αυτής της προσπάθειας είναι ο σχεδιασμός και η υιοθέτηση κατάλληλων λύσεων προς αποφυγή ή περιορισμό εξακριβωμένων κινδύνων.

Επίσης απαιτούνται τεχνικές και άλλες λύσεις οι οποίες πρέπει να είναι ανάλογες με τη σημασία των πληροφοριών που διακινούνται στα πληροφοριακά συστήματα και τα δίκτυα.

Η ασφάλεια πρέπει να αποτελεί ουσιαστικό στοιχείο όλων των προϊόντων, των υπηρεσιών, των συστημάτων και των δικτύων και έναν σημαντικό παράγοντα της αρχιτεκτονικής του κάθε συστήματος.

Για τους χρήστες, καθοριστικό κριτήριο στην επιλογή προϊόντων και την εφαρμογή διαδικασιών για το σύστημά τους πρέπει να αποτελεί ο σχεδιασμός τους που έχει γίνει με γνώμονα την ασφάλεια.

### 1.8 Διαχείριση ασφάλειας

*Οι χρήστες πρέπει να υιοθετήσουν μια περιεκτική προσέγγιση στη διαχείριση της ασφάλειας.*

Η διαχείριση της ασφάλειας πρέπει να βασίζεται στην εκτίμηση των κινδύνων και να είναι μια δυναμική που καλύπτει όλα τα επίπεδα των δραστηριοτήτων των χρηστών και όλες τις λειτουργίες των συστημάτων που χρησιμοποιούν αυτοί.

Πληροφοριακά συστήματα, πολιτικές, πρακτικές, μέτρα και διαδικασίες πρέπει να συντονίζονται για να δημιουργούν ένα συνεκτικό σύστημα ασφάλειας.

Οι απαιτήσεις διαχείρισης για την ασφάλεια εξαρτώνται και από τον ρόλο των χρηστών, τον βαθμό εμπλοκής τους στο σύστημα, τον πιθανό κίνδυνο και τις απαιτήσεις του συστήματος.

### 1.9 Επαναξιολόγηση

*Οι χρήστες πρέπει να διενεργούν αξιολογήσεις των κινδύνων.*

Οι χρήστες πρέπει σε τακτά χρονικά διαστήματα, αλλά και όταν προκύπτει μια έκτακτη ανάγκη, να επαναξιολογούν την ασφάλεια των πληροφοριακών τους συστημάτων και των δικτύων, να προβαίνουν στις κατάλληλες τροποποιήσεις της πολιτικής ασφάλειας, των πρακτικών και των διαδικασιών που εφαρμόζουν και να λαμβάνουν τα κατάλληλα μέτρα.

Η επαναξιολόγηση είναι απαραίτητη, δεδομένου ότι ανακύπτουν συνεχώς νέοι κίνδυνοι και ευάλωτα σημεία των συστημάτων πληροφορικής και των δικτύων.

## 2. Στόχοι της εθνικής στρατηγικής για την ασφάλεια δικτύων και πληροφοριών και μέτρα για την επίτευξή τους [1]

### 1ος στόχος: Προώθηση της συνεργασίας σε εθνικό και διεθνές επίπεδο για την ασφάλεια δικτύων και πληροφοριών (ΑΔΠ)

Η παραγωγή και η χρήση πληροφοριών μέσα από τις νέες τεχνολογίες πληροφορικής και επικοινωνιών, χωρίς γεωγραφικούς περιορισμούς, αποτελεί την κινητήρια δύναμη της παγκοσμιοποίησης. Οι παράμετροι ασφάλειας των νέων αυτών ευκαιριών συνιστούν σε διεθνές επίπεδο μεγάλη πρόκληση για δημόσιες αρχές, επιχειρήσεις και πολίτες. Ένας από τους στόχους της ΕΣΑΔΠ είναι να συμβάλει στη δημιουργία, σε εθνικό επίπεδο, προτύπων, θέσεων πολιτικής και συνεργασίας φορέων για την προώθηση της ΑΔΠ και να διασφαλίζει τη σαφή κατανομή ευθυνών μεταξύ των εμπλεκομένων φορέων στον τομέα αυτόν.

Για την υλοποίηση του στόχου αυτού προτείνονται τα ακόλουθα μέτρα:

**α)** Ενεργός συμμετοχή των εμπλεκόμενων κρατικών φορέων στην προετοιμασία νομοθεσίας, προτύπων και άλλων μέτρων συνεργασίας για την ΑΔΠ στην Ευρωπαϊκή Ένωση, καθώς και σε άλλους διεθνείς οργανισμούς και fora που αφορούν το εμπόριο και τη βιομηχανία (Υπουργεία Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας, Οικονομικών, Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, Υποδομών, Μεταφορών και Δικτύων, Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και Προστασίας του Πολίτη).

**β)** Υλοποίηση ερευνητικού προγράμματος για τη σπουδαιότητα της ΑΔΠ και το αίσθημα εμπιστοσύνης που απορρέει από αυτή στον τομέα της οικονομίας. Χρησιμοποίηση π.χ. του ελληνικού τραπεζικού τομέα ως πεδίου μελέτης του θέματος των επενδύσεων στην ΑΔΠ και των πλεονεκτημάτων από τις επενδύσεις αυτές.

**γ)** Περαιτέρω ανάπτυξη του δυναμικού των κρατικών φορέων για την προώθηση της ΑΔΠ και υποβολή προτάσεων στον εξειδικευμένο φορέα που έχει προταθεί (βλ. 3ο στόχο) για τη βελτίωση του δυναμικού αυτού και την επέκταση της συνεργασίας. Για την επίτευξη αυτού του στόχου σημαντική θα είναι η συμμετοχή των εμπλεκομένων φορέων για την ΑΔΠ.

### 2ος στόχος: Προώθηση της ανταγωνιστικότητας και της διαμόρφωσης κατάλληλου λειτουργικού περιβάλλοντος για τις ελληνικές επιχειρήσεις πληροφορικής και επικοινωνιών

Η πληροφορική γίνεται μια διαρκώς αυξανόμενη πολύτιμη μορφή κεφαλαίου λόγω της παγκόσμιας αγοράς που συνδέεται με αυτή. Στόχος της ΕΣΑΔΠ είναι να διασφαλίσει τη διαθεσιμότητα και την ασφαλή χρήση των πληροφοριών και έτσι να συμβάλει θετικά στις νέες επιχειρηματικές ευκαιρίες και στη δημιουργία σταθερού επιχειρηματικού περιβάλλοντος για εταιρείες που παράγουν, διακινούν, χρησιμοποιούν και προστατεύουν τις πληροφορίες. Με αυτή την πρακτική θα βελτιωθεί η ανταγωνιστικότητα της εθνικής οικονομίας και θα δημιουργηθούν πόροι που μπορούν να χρησιμοποιηθούν για περαιτέρω ανάπτυξη.

Για την υλοποίηση του στόχου αυτού προτείνονται μεταξύ άλλων και τα ακόλουθα μέτρα:

**α)** Αξιοποίηση της πολιτικής της ΑΔΠ και της πολιτικής ανάπτυξης της τεχνολογίας από το Υπουργείο Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας προκειμένου να υποστηριχθούν

[1] Με βάση το ψήφισμα του Υπουργείου Μεταφορών και Επικοινωνιών της Φινλανδίας.

καινοτόμες μορφές ανάπτυξης που σχετίζονται με την ΑΔΠ και να διαμορφωθούν δίκτυα εξειδίκευσης μεταξύ εταιρειών και οργανισμών και προγράμματα συνεργασίας μεταξύ φορέων του δημόσιου και του ιδιωτικού τομέα.

**β)** Ενθάρρυνση από το Υπουργείο Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας εταιρειών και ερευνητικών ιδρυμάτων ώστε να εισαγάγουν στην αγορά νέα προϊόντα ασφάλειας πληροφοριών, να αναπτύξουν μεθόδους διάγνωσης και προστασίας από κινδύνους συμβατές με άλλα προϊόντα και εύκολες στη χρήση και να προωθήσουν πρόσφορες πρακτικές προς χρήση.

**γ)** Καθοδήγηση από τον εξειδικευμένο φορέα (βλ. 3ο στόχο) όλων των φορέων του δημόσιου τομέα ώστε να βελτιωθεί η συμβατότητα των διαδικασιών της ΑΔΠ τόσο στον δημόσιο τομέα όσο και μεταξύ του δημόσιου και του ιδιωτικού τομέα.

**δ)** Πραγματοποίηση, μέσω του forum των εμπλεκομένων φορέων, σε κανονικά χρονικά διαστήματα αξιολογήσεων για το πώς επιδρά η εθνική νομοθεσία και οι διεθνείς συμβάσεις, που αναφέρονται στην ασφάλεια των πληροφοριών και στην κοινωνία της πληροφορίας, στις υπηρεσίες επικοινωνιών, στις τραπεζικές υπηρεσίες on-line, στις υπηρεσίες ηλεκτρονικής ταυτοποίησης, ηλεκτρονικού εμπορίου και ηλεκτρονικών συναλλαγών και υποβολή προτάσεων για τις απαιτούμενες δράσεις.

### 3ος στόχος: Βελτίωση της διαχείρισης των κινδύνων που αφορούν την ασφάλεια δικτύων και πληροφοριών και της αποτελεσματικότητας των μέτρων αντιμετώπισής τους

Η ασφαλής χρήση των πληροφοριών αποτελεί μια διαρκώς αυξανόμενη πρόκληση για όλους τους παράγοντες, διότι οι γνωστοί κίνδυνοι μεταβάλλονται και νέες απειλές ανακύπτουν συνεχώς. Στόχος της ΕΣΑΔΠ είναι να προωθήσει την πρόληψη σε όσο το δυνατόν μεγαλύτερο βαθμό και τη διαχείριση των κινδύνων στο επίπεδο του ατόμου, της επιχείρησης, του κράτους και της κοινωνίας γενικά. Η πρόληψη μπορεί να συμβάλλει στη μεγαλύτερη δυνατή ασφάλεια και ελαχιστοποιεί το κόστος που απαιτεί η επίτευξή της.

Για την υλοποίηση του στόχου αυτού προτείνονται μεταξύ άλλων και τα ακόλουθα μέτρα:

**α)** Ανάθεση σε φορέα της διαχείρισης ενός αποτελεσματικού συστήματος παρακολούθησης σε εθνική κλίμακα της κατάστασης αναφορικά με τους κινδύνους της ΑΔΠ (η ΑΔΑΕ, ως αρμόδια Αρχή για τη διασφάλιση του απορρήτου των επικοινωνιών –σημαντικού παράγοντα της ασφάλειας των δικτύων–, εύλογο είναι ότι θα μπορούσε να αποτελέσει τον φορέα αυτόν). Ο αρμόδιος αυτός φορέας θα ενημερώνεται διαρκώς ώστε να παρέχει πληροφορίες ανά πάσα στιγμή για την κατάσταση στα υπουργεία και σε όλους τους μείζονες φορείς που σχετίζονται με την ΑΔΠ.

**β)** Διενέργεια από τον εν λόγω φορέα περιοδικών αξιολογήσεων των νέων κινδύνων που απειλούν την ΑΔΠ και παροχή πληροφοριών προς όλους τους φορείς για τους κινδύνους αυτούς καθώς και για τα απαιτούμενα αντίμετρα (Υπουργείο Υποδομών, Μεταφορών και Δικτύων, Υπουργείο Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας, Υπουργείο Οικονομικών, Υπουργείο Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, Υπουργείο Προστασίας του Πολίτη, Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων).

**γ)** Ανάπτυξη από τον εν λόγω φορέα μεθόδων ανάλυσης των ευάλωτων σημείων της ασφάλειας δικτύων και πληροφοριών και διάδοση των βέλτιστων πρακτικών που επιβάλλονται γι' αυτά ώστε να χρησιμοποιούνται από όλους τους φορείς και ενημέρωση προς τα υπουργεία και τους μείζονες φορείς για την ΑΔΠ.

### 4ος στόχος: Περιφρούρηση θεμελιωδών δικαιωμάτων και προστασία του εθνικού κεφαλαίου γνώσης

Η οικοδόμηση της κοινωνίας της πληροφορίας με ΑΔΠ δεν μπορεί να γίνει εις βάρος των θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων. Σε μια ασφαλή κοινωνία της πληροφορίας όλοι πρέπει να έχουν εμπιστοσύνη ότι οι πληροφορίες και τα μηνύματά τους μεταφέρονται, επεξεργάζονται και αποθηκεύονται με εχεμύθεια και ότι δεν θα είναι προσιτά σε άλλους παρά μόνον στους παραλήπτες που αυτοί επιλέγουν. Επιπλέον, όλοι θα πρέπει να έχουν ευχερή πρόσβαση στις πληροφορίες για τις οποίες έχουν εξουσιοδότηση. Για τις επιχειρήσεις, το πληροφοριακό κεφάλαιο, που θα πρέπει να προστατεύεται, περιλαμβάνει τα πιο σημαντικά επιχειρηματικά μυστικά, τα στοιχεία των πελατών και τα δεδομένα ανάπτυξης των προϊόντων ή των υπηρεσιών τους.

Για την υλοποίηση του στόχου αυτού προτείνονται μεταξύ άλλων και τα ακόλουθα μέτρα:

**α)** Να διασφαλίζεται με μέριμνα του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων ότι η ελευθερία του λόγου, το απόρρητο των επικοινωνιών, η προστασία της ιδιωτικής ζωής και άλλα θεμελιώδη δικαιώματα θα λαμβάνονται υπόψη στη νομοθεσία, στις επίσημες οδηγίες και τα πρότυπα που σχετίζονται με τις υπηρεσίες της κοινωνίας της πληροφορίας, τις ηλεκτρονικές επικοινωνίες και την ΑΔΠ, καθώς και στις υπηρεσίες ηλεκτρονικών συναλλαγών.

**β)** Να εκτιμάται από το αρμόδιο Υπουργείο Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας κατά πόσον η νομοθεσία, που αφορά την προστασία των επιχειρηματικών μυστικών, των δεδομένων των πελατών, των δεδομένων ανάπτυξης προϊόντων, των μη υλικών δικαιωμάτων και άλλων πληροφοριών που είναι ουσιώδεις για τη δραστηριότητα της επιχείρησης, θα πρέπει να αναθεωρηθεί. Επίσης το ίδιο υπουργείο να αναλαμβάνει τις απαραίτητες πρωτοβουλίες για τα παραπάνω θέματα.

### 5ος στόχος: Βελτίωση της ενημέρωσης και των επαγγελματικών δεξιοτήτων των φορέων της ΑΔΠ

Η εξειδίκευση στον τομέα της ΑΔΠ αποτελεί μια νέα και σημαντικά αναπτυσσόμενη επαγγελματική κατεύθυνση. Για μια ασφαλή κοινωνία της πληροφορίας, όλοι οι εμπλεκόμενοι πρέπει να είναι ενήμεροι για τους κινδύνους που απειλούν την ΑΔΠ, όπως και για τον ρόλο τους στην αποτροπή αυτών των κινδύνων. Η ΕΣΔΑΠ έχει στόχο να αυξήσει το επίπεδο των γνώσεων και των δεξιοτήτων των επαγγελματιών της ΑΔΠ επενδύοντας στην εξειδίκευσή του αφενός καθώς και στη γενική ενημέρωση όλων των εμπλεκομένων στην ασφάλεια αφετέρου.

Για την υλοποίηση του στόχου αυτού προτείνονται μεταξύ άλλων και τα ακόλουθα μέτρα:

**α)** Καταγραφή από το Υπουργείο Παιδείας, διά Βίου Μάθησης και Θρησκευμάτων της παρούσας κατάστασης στον τομέα της ενημέρωσης και της επαγγελματικής επάρκειας σε θέματα της ΑΔΠ όσο το δυνατόν ευρύτερα, καθορισμός του στόχου της επαγγελματικής επάρκειας και έναρξη εφαρμογής των αναγκαίων προγραμμάτων βελτίωσης της γενικής επάρκειας στην ΑΔΠ και της εκπαίδευσης για επαγγελματίες της ΑΔΠ.

**β)** Ενσωμάτωση από το Υπουργείο Παιδείας, διά Βίου Μάθησης και Θρησκευμάτων της εκπαίδευσης σε θέματα ΑΔΠ σε όλα τα επίπεδα εκπαίδευσης. Αποστολή πρακτικών οδηγιών για αναβάθμιση των υπαρχόντων προγραμμάτων και τη δημιουργία νέων, εξειδικευμένων προγραμμάτων, που να καλύπτουν τις σύγχρονες ανάγκες σε δεξιότητες και γνώσεις.

**γ)** Συνεχής ενημέρωση, με μέριμνα του προαναφερόμενου αρμόδιου φορέα (βλ. 3ο στόχο), των χρηστών αναφορικά με θέματα της ΑΔΠ με την αποστολή γραπτών πληροφοριών, την παραγωγή ενημερωτικών μηνυμάτων, διαφημιστικού υλικού κ.λπ.

**δ)** Αποτελεσματική προώθηση, από τα αρμόδια υπουργεία, της ενημέρωσης σχετικά με θέματα της ΑΔΠ σε εταιρείες, στους οργανισμούς της τοπικής αυτοδιοίκησης και σε άλλους οργανισμούς.

**ε)** Συμβολή στην ανάπτυξη και τη χρήση πιστοποιητικών ποιότητας σχετικών με την ΑΔΠ και συνεχής ενημέρωση των χρηστών για τη σπουδαιότητα των πιστοποιητικών στην αγορά προϊόντων και υπηρεσιών, με τη φροντίδα του προαναφερόμενου φορέα (βλ. 3ο στόχο).

## 3. Διαδικασία υλοποίησης των μέτρων για την επίτευξη των στόχων της εθνικής στρατηγικής

Σε μια κοινωνία της πληροφορίας, οι νέες πληροφορίες, η εξειδίκευση, η τεχνολογία και οι πρακτικές εκτείνονται σε όλους τους τομείς της ζωής. Η ΑΔΠ ως ουσιώδες συστατικό της κοινωνίας αυτής πρέπει ανάλογα να καλύπτει όλες τις πλευρές της ζωής. Αυτό σημαίνει πως χρειάζεται στενότερη συνεργασία ανάμεσα σε όλους τους εμπλεκόμενους φορείς. Η ΕΣΑΔΠ θέτει τη βάση για τέτοιου είδους συνεργασία ώστε η ΑΔΠ να κατευθύνεται προς συγκεκριμένους στόχους και να προωθούνται συνδυασμένα ο σχεδιασμός και η υλοποίηση προγραμμάτων καθώς και η ανταλλαγή πληροφοριών.

Για την υλοποίηση των μέτρων της εθνικής στρατηγικής πρέπει να γίνουν οι ακόλουθες ενέργειες:

- Να δημιουργηθεί, σε κάθε υπουργείο, υπηρεσία αρμόδια για την Ασφάλεια Δικτύων και Πληροφοριών.
- Ο προαναφερόμενος φορέας (παράγρ. α, 3ου στόχου) να υποβάλλει στην κυβέρνηση σχέδιο της ΕΣΑΔΠ που θα περιλαμβάνει όλα τα αναγκαία μέτρα υλοποίησής της. Επίσης θα υποβάλλει, όταν απαιτείται, προτάσεις για επικαιροποίηση της ΕΣΑΔΠ προς τα Υπουργεία Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας, Οικονομικών, Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, Υποδομών, Μεταφορών και Δικτύων, Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και Προστασίας του Πολίτη. Τα υπουργεία αυτά, με επισπεύδον το Υπουργείο Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, θα εγκρίνουν την ΕΣΑΔΠ όπως και την τυχόν επικαιροποίησή της.
- Να προωθηθούν από τον προαναφερόμενο φορέα (παράγρ. α, 3ου στόχου) οι διαθέσιμες κατάλληλες πληροφορίες αναφορικά με την ΑΔΠ στα υπουργεία και σε εταιρείες και οργανισμούς του ευρύτερου δημόσιου τομέα.
- Κάθε υπουργείο να εξετάζει τις εντός των υπηρεσιών του εφαρμοζόμενες πρακτικές καθώς και αυτές των οργανισμών και των εταιρειών που εποπτεύει και να υιοθετεί όποια μέτρα κρίνονται αναγκαία στο πλαίσιο της ΕΣΑΔΠ, ώστε να αναπτυχθεί η πλέον κατάλληλη ΑΔΠ για το υπουργείο και τους οργανισμούς και τις εταιρείες που εποπτεύει.
- Να αναπτυχθεί η ΑΔΠ στο πλαίσιο της ΕΣΑΔΠ για τα δίκτυα που συνδέουν όλη τη δημόσια διοίκηση με ευθύνη του Υπουργείου Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας, του Υπουργείου Οικονομικών και του Υπουργείου Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης.

- Να εκδοθούν από το Υπουργείο Οικονομικών και το Υπουργείο Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας, στο πλαίσιο της ΕΣΑΔΠ, ακριβείς οδηγίες για την ανάπτυξη της ΑΔΠ στις επίσημες ηλεκτρονικές συναλλαγές.
- Το Υπουργείο Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης να έχει στην αρμοδιότητά του την ανάπτυξη της ΑΔΠ στο πλαίσιο της ΕΣΑΔΠ κατά τη διαχείριση των ηλεκτρονικών συναλλαγών και πληροφοριών μεταξύ της κυβέρνησης και των οργανισμών της τοπικής αυτοδιοίκησης.
- Τον γενικό έλεγχο ως προς την εφαρμογή της ΕΣΑΔΠ από τους διάφορους φορείς θα έχει σε εθνικό επίπεδο ο προαναφερόμενος φορέας (παράγρ. α, 3ου στόχου).

Όλοι οι σχετιζόμενοι με την ΑΔΠ φορείς έχουν υποχρέωση να παρακολουθούν την εφαρμογή των διατάξεων του νόμου για την προστασία των προσωπικών δεδομένων (έλεγχος από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).

Ακόμη, ζωτικό θέμα για την υλοποίηση της ΑΔΠ είναι και τα διάφορα μέτρα για την ΑΔΠ που υλοποιούνται από εταιρείες, των οποίων την εφαρμογή θα προωθεί και θα ενθαρρύνει ο προαναφερόμενος φορέας (παράγρ. α, 3ου στόχου).

Ο ίδιος φορέας θα οργανώσει ένα μόνιμο forum με σκοπό την ανταλλαγή απόψεων και την ανάπτυξη κοινών, συντονισμένων προγραμμάτων διαχείρισης πληροφοριών της κυβέρνησης, των οργανισμών τοπικής αυτοδιοίκησης, των μεγάλων επιχειρήσεων και οργανισμών, των μικρών εταιρειών και των απλών χρηστών.

Τα προγράμματα αυτά θα λαμβάνονται υπόψη από τον εν λόγω φορέα κατά τη διαμόρφωση πολιτικών επί της ΕΣΑΔΠ τις οποίες θα εισηγείται στην κυβέρνηση (Υπουργεία Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας, Οικονομικών, Εσωτερικών Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, Υποδομών, Μεταφορών και Δικτύων, Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και Προστασίας του Πολίτη).

Στο πλαίσιο του forum θα λειτουργούν ομάδες εργασίας για την εκπόνηση των παραπάνω εξειδικευμένων συντονιστικών προγραμμάτων.

## 4. Προοπτικές από την εφαρμογή της εθνικής στρατηγικής

Η εφαρμογή της εθνικής στρατηγικής δημιουργεί προστιθέμενη αξία. Αναπτύσσει τη συνεργασία αναφορικά με την ΑΔΠ μεταξύ διαφόρων φορέων και αποτρέπει την επικάλυψη των μέτρων που υιοθετούνται, καθιστώντας έτσι τη χρήση των δημόσιων πόρων περισσότερο αποτελεσματική.

Η ΕΣΑΔΠ θα συμβάλει, επίσης, στη διαμόρφωση καλύτερου επιχειρηματικού περιβάλλοντος και στην ανάπτυξη νέων εύχρηστων προϊόντων και υπηρεσιών, αναβαθμίζοντας με τον τρόπο αυτόν την ανταγωνιστικότητα των ελληνικών εταιρειών. Ακόμη, η ΕΣΑΔΠ θα συνεισφέρει στην ενημέρωση όλων των χρηστών για την ΑΔΠ, θα βελτιώσει την εξειδίκευση των επαγγελματιών του τομέα αυτού και θα προσφέρει έτσι την ευκαιρία σε όλους τους φορείς για πλήρη χρήση του δυναμικού της κοινωνίας της πληροφορίας.