ΚΕΦΑΛΑΙΟ 3ο

ΕΝΙΣΧΥΣΗ ΤΟΥ ΘΕΣΜΙΚΟΥ ΠΛΑΙΣΙΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΤΗΝ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1. Προστασία δικτύων και πληροφοριακών συστημάτων

Σύμφωνα με το υφιστάμενο θεσμικό πλαίσιο, η ΑΔΑΕ έχει την αρμοδιότητα ελέγχου της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημοσίου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την απόκριση ή επικοινωνία.

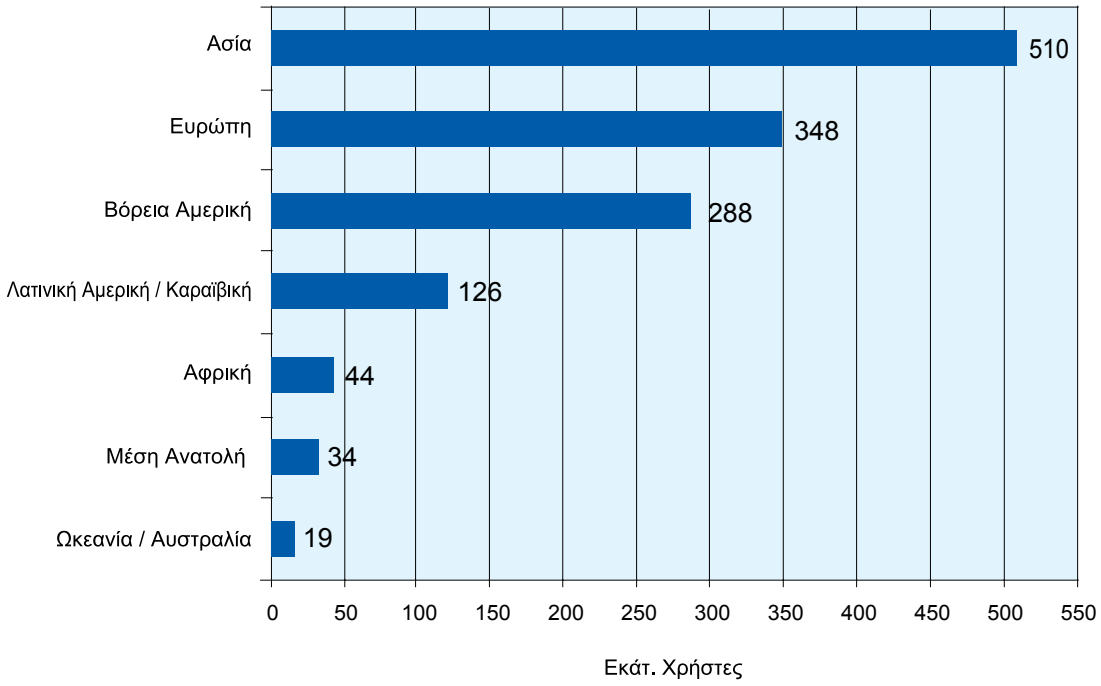
Η Αρχή, για την καλύτερη δυνατή άσκηση των αρμοδιοτήτων της, έχει εκπονήσει από την αρχή της σύστασής της Κανονισμούς που καλύπτουν όλα τα είδη και τις μορφές των σύγχρονων ηλεκτρονικών επικοινωνιών και των ταχυδρομικών υπηρεσιών. Στις αρχές του 2005, υπέβαλε στους παρόχους ηλεκτρονικών υπηρεσιών, μετά από διαβούλευση, πολιτικές ασφάλειας σύμφωνες με τους Κανονισμούς που είχαν ήδη καταρτιστεί και προχώρησε σε ελέγχους των παρόχων, μετά από καταγγελίες φυσικών προσώπων και εταιρειών για παραβίαση του απορρήτου τους.

Θα πρέπει, όμως, να τονιστεί ότι το θέμα της ασφάλειας των δικτύων είναι γενικότερο και αγγίζει όλα τα δίκτυα (δίκτυα οργανισμών που περιέχουν κρίσιμες υποδομές, δίκτυα υπουργείων, δίκτυα μεγάλων και μικρών επιχειρήσεων, δίκτυα απλών χρηστών), δεδομένου ότι σήμερα κάθε χρήστης δικτύου αποτελεί κρίκο του ευρύτερου φάσματος των επικοινωνιών με δυνατότητες πρόσβασης σε απόρρητες πληροφορίες.

Η ασφάλεια, επομένως, ηλεκτρονικών δικτύων και πληροφοριακών συστημάτων θα πρέπει να αντιμετωπιστεί σφαιρικά και, βεβαίως, να μην περιοριστεί μόνο σε παρόχους ηλεκτρονικών υπηρεσιών και δικτύων μέσω του ελέγχου τους από την ΑΔΑΕ, όπως συμβαίνει σήμερα.

Τα πληροφοριακά συστήματα και δίκτυα αποτελούν νευραλγικό τομέα της σύγχρονης κοινωνίας. Η πληροφορική έχει δημιουργήσει παγκόσμια διασυνδεσιμότητα, φέρνοντας σε επαφή εκατομμύρια δικτύων με εκατοντάδες εκατομμύρια μεμονωμένους προσωπικούς υπολογιστές, ο αριθμός των οποίων αυξάνεται συνεχώς. Παράλληλα, υποστηρίζει υποδομές μεγάλης σημασίας για μια χώρα, όπως εγκαταστάσεις ενέργειας, μεταφορών, καθώς και μεγάλα χρηματοπιστωτικά ιδρύματα, παίζει σημαντικό ρόλο στη διοίκηση του σύγχρονου κράτους, των μεγάλων και μικρών επιχειρήσεων και παρέχει υπηρεσίες στον πολίτη μέσω του κυβερνητικού μηχανισμού. Τα παραπάνω έχουν ως συνέπεια να έχει κυριολεκτικά εκτιναχθεί στα ύψη ο όγκος των πληροφοριών που διακινούνται στο διαδίκτυο, μέρος του οποίου είναι και πληροφορίες ιδιάζουσας σημασίας (βλ. Διάγραμμα 1 στη συνέχεια).

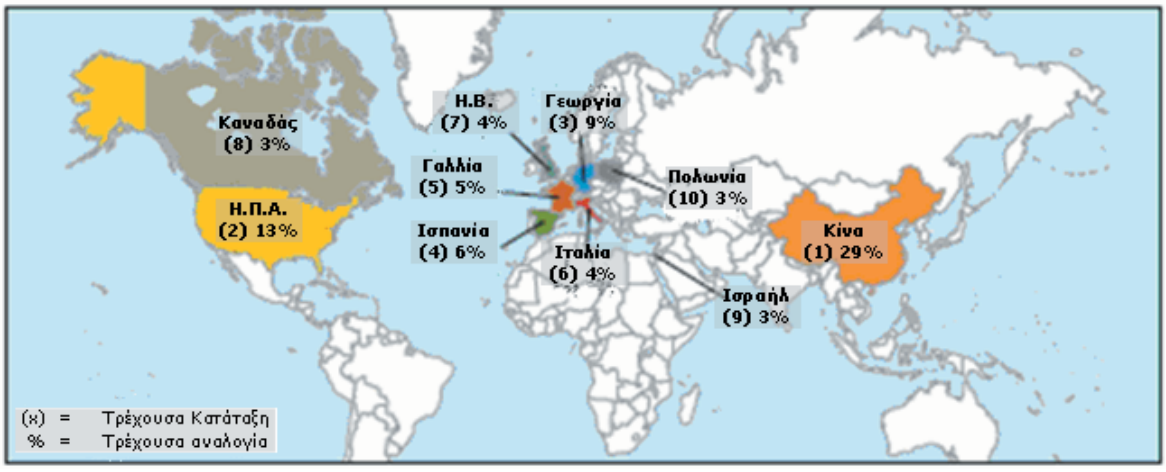
Διάγραμμα 1: **Χρήστες Διαδικτύου Παγκοσμίως έτος 2007 (σε εκ.)**



Πηγή: Internet World Statistics, 2007

Ωστόσο, λόγω της έκρηξης στην ανταλλαγή πληροφοριών μέσω δικτύων, τα πληροφοριακά συστήματα και τα δίκτυα είναι εκτεθειμένα σε ένα ευρύτατο πλήθος κινδύνων, στους οποίους περιλαμβάνονται οι παραβιάσεις του προσωπικού απορρήτου, η βιομηχανική κατασκοπεία, η κακόβουλη πρόσβαση στα αρχεία των υπολογιστών, η εισαγωγή ιών στους υπολογιστές, η δικτυακή τρομοκρατία, ο ηλεκτρονικός πόλεμος κ.λπ. Οι κίνδυνοι αυτοί μπορούν σήμερα να εξαπλώνονται, μέσα σε ελάχιστο χρόνο, σε όλο τον κόσμο, μέσω των δικτύων πληροφοριών (βλ. Πίνακα 1).

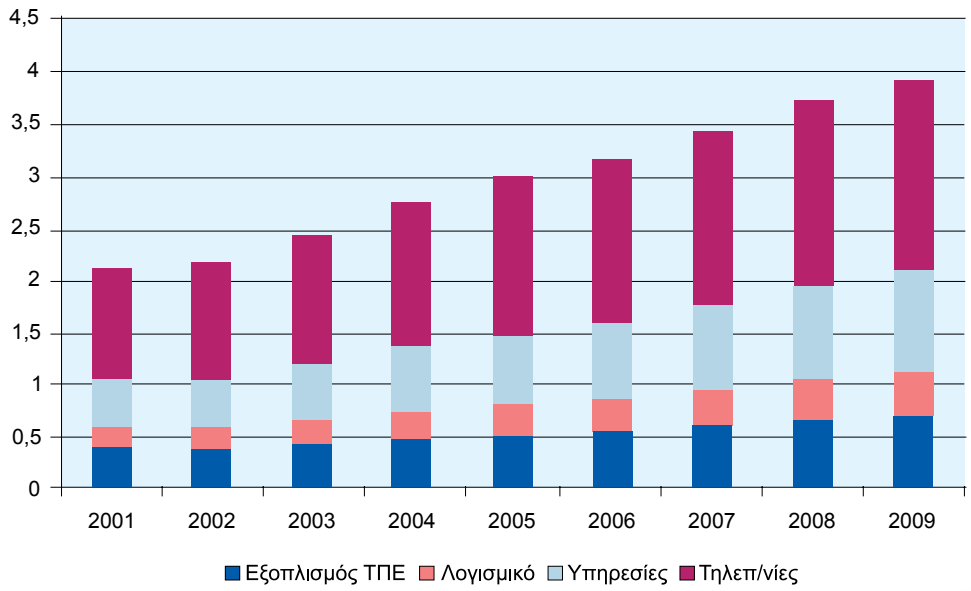
Πίνακας 1: **Κακόβουλα περιστατικά στο διαδίκτυο**



Πηγή: Symantec Internet Security Threat Report, 2007

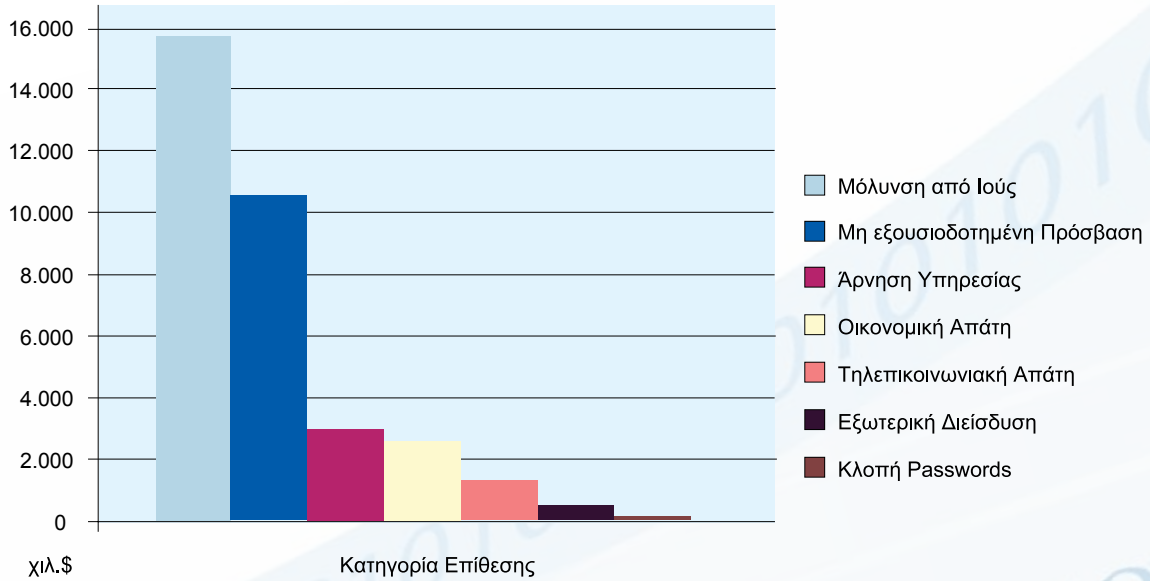
Οι εξωτερικές επιβουλές μπορούν πλέον με μικρότερο κόστος να αποκτήσουν πρόσβαση σε πολύτιμες πληροφορίες. Είναι προφανές ότι κακόβουλες προσβάσεις στα αρχεία υπολογιστών είναι δυνατόν να δημιουργήσουν τεράστια προβλήματα στην εθνική ασφάλεια, κυκλοφοριακό χάος στην εναέρια ή επίγεια κυκλοφορία, σοβαρές διακοπές στη διανομή ηλεκτρικής ενέργειας αλλά και οικονομικό χάος, ανάλογα με τα δίκτυα, στα οποία θα υπάρξει η κακόβουλη πρόσβαση (βλ. Διαγράμματα 2 και 3).

Διάγραμμα 2: **Δαπάνες σε ΤΠΕ παγκοσμίως, 2001-2009 (σε τρισεκατ. $)**



Πηγή: WITSA, 2006

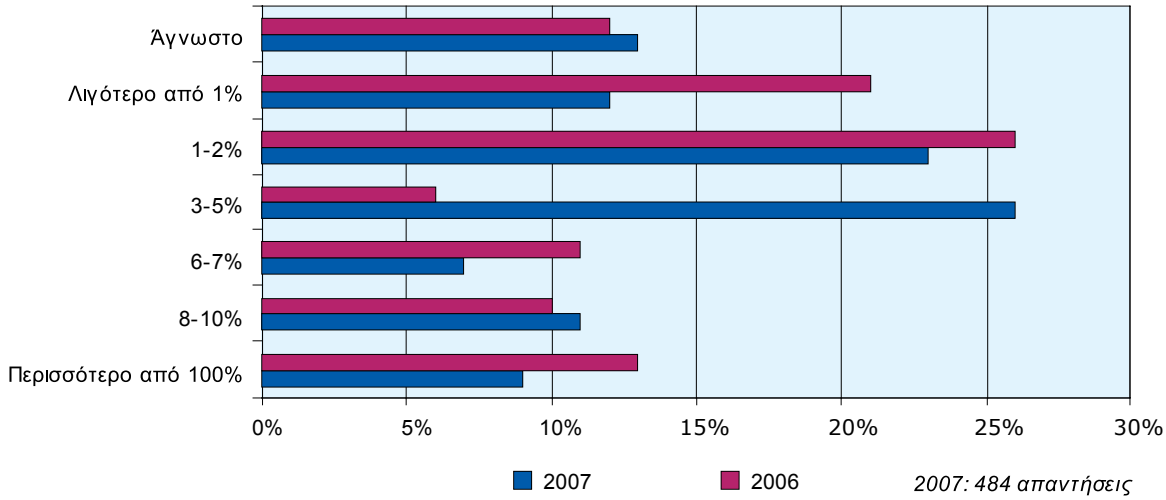
Διάγραμμα 3: **Οικονομικές Απώλειες ανά Κατηγορία Επίθεσης**



Πηγή: CSI/FBI Computer Crime and Security Survey "Computer Security Institute", 2006

Η κατοχύρωση της ασφάλειας δικτύων και πληροφοριών αυξάνει την αίσθηση ελεύθερης δράσης των πολιτών, δημιουργεί νέες επιχειρηματικές ευκαιρίες και μειώνει το κόστος λειτουργίας μιας επιχείρησης, η δραστηριότητα της οποίας συνεπάγεται πολλαπλές διασυνδέσεις με τα δίκτυα επικοινωνιών. Αυτός είναι και ο λόγος, για τον οποίο οι εταιρείες, και περισσότερο οι μεγάλες, επενδύουν συνεχώς και μεγαλύτερα ποσά στην ενίσχυση της ασφάλειας των δικτύων τους (βλ. Διάγραμμα 4).

Διάγραμμα 4: **Ποσοστό Προϋπολογισμού Πληροφορικής Εταιρειών (Δαπάνες για την Ασφάλεια)**



Πηγή: CSI/FBI Computer Crime and Security Survey "Computer Security Institute", 2007

Σε συνθήκες ασφάλειας αυξάνεται η αξιοποίηση του διαδικτύου με επακόλουθο τη μείωση του κόστους των προϊόντων και της διάθεσής τους, δεδομένου ότι βελτιώνεται η παραγωγικότητα και ο ανταγωνισμός, μηδενίζονται οι αποστάσεις και δημιουργούνται νέες αγορές και επιχειρηματικές ευκαιρίες. Από πλευράς δημόσιας διοίκησης, εξάλλου, παρέχεται η δυνατότητα βελτίωσης των υπηρεσιών προς τον πολίτη και την επιχείρηση, με καλύτερη χρησιμοποίηση των ανθρώπινων πόρων.

Η ασφάλεια δικτύων και πληροφοριακών συστημάτων αναφέρεται, αφενός, στην προστασία ηλεκτρονικών υπηρεσιών και συστημάτων οποιασδήποτε μορφής, απαιτεί όμως κατάλληλο τεχνικό εξοπλισμό και λογισμικό. Αφετέρου, αναφέρεται στη διαφοροποίηση της συμπεριφοράς των απλών χρηστών, οι οποίοι, έχοντας συνειδητοποιήσει τους κινδύνους, λαμβάνουν απαραίτητα μέτρα για την προστασία του δικού τους υπολογιστή.

Γενικότερα, η ασφάλεια των δικτύων ηλεκτρονικών επικοινωνιών περιλαμβάνει τις παραμέτρους α) ιδιωτικότητα (η επικοινωνία δεν υποκλέπτεται), β) ακεραιότητα (τα στοιχεία της επικοινωνίας φθάνουν στους αποδέκτες χωρίς αλλοίωση), γ) αυθεντικότητα (τα πρόσωπα που συνδιαλέγονται είναι τα πραγματικά), και δ) διαθεσιμότητα (τα δίκτυα μπορούν να αντιμετωπίσουν και καταστάσεις κρίσεως). Όπως προκύπτει από αυτές

τις παραμέτρους, το απόρρητο των επικοινωνιών και η ασφάλεια, με εξαίρεση την παράμετρο της διαθεσιμότητας, είναι παράλληλες έννοιες. Για το λόγο αυτό, η αρμοδιότητα της ασφάλειας πρέπει να περιέλθει στην ΑΔΑΕ, η οποία έχει εκδώσει ήδη σχετικούς Κανονισμούς (η ΕΕΤΤ διατηρεί την αρμοδιότητα της διαθεσιμότητας των δικτύων).

2. Αναγκαιότητα και σκοπιμότητα χάραξης Εθνικής Στρατηγικής Ασφάλειας Δικτύων και Πληροφοριών (ΕΣΑΔΠ)

Ο τομέας των ηλεκτρονικών επικοινωνιών και εφαρμογών παρουσιάζεται σήμερα εξαιρετικά δυναμικός, στο βαθμό που οι τεχνολογικές εξελίξεις είναι συνεχείς και ανατρεπτικές. Κατά συνέπεια, επιβάλλεται διαρκής παρακολούθηση των συντελούμενων μεταβολών και άμεση λήψη μέτρων για την αποτροπή νέων κινδύνων που απειλούν την ασφάλεια δικτύων και υπηρεσιών.

Ακριβώς γι' αυτό, αλλά και λόγω της μεγάλης διάχυσης, διασυνδεσιμότητας και αλληλεπίδρασης των περιφερειακών συστημάτων και δικτύων, καθώς και της σημασίας που έχουν σε μια σύγχρονη κοινωνία τα δίκτυα και οι πληροφορίες, η ΑΔΑΕ θεωρεί επιτακτική ανάγκη, και προτείνει συνέχεια από το 2004, την εκπόνηση ολοκληρωμένης Εθνικής Στρατηγικής Ασφάλειας Δικτύων και Πληροφοριών (ΕΣΑΔΠ), όπως άλλωστε έχει υιοθετηθεί και από τα περισσότερα προηγμένα κράτη. Στο πλαίσιο της ΕΕ, το Συμβούλιο Υπουργών, σε ψήφισμά του την 24η Μαρτίου 2007 σχετικά με τη «Στρατηγική για Ασφαλή Κοινωνία της Πληροφορίας στην Ευρώπη»[30], επιδοκιμάζει την πρόθεση της Ευρωπαϊκής Επιτροπής[31] και ζητά μεταξύ άλλων:

α) να συνεχίσει την ανάπτυξη συνολικής και δυναμικής πανευρωπαϊκής στρατηγικής για την ασφάλεια δικτύων και συστημάτων πληροφοριών,

β) να αντιμετωπίσει την ασφάλεια των δικτύων και πληροφοριών ως έναν από τους στόχους της επανεξέτασης του κανονιστικού πλαισίου της Ευρωπαϊκής Ένωσης για τις ηλεκτρονικές επικοινωνίες,

γ) να ενθαρρύνει τα κράτη-μέλη να εξετάσουν την ανάπτυξη πολιτικής για την προστασία κρίσιμων υποδομών.

Η Εθνική Στρατηγική Ασφάλειας που προτείνει η ΑΔΑΕ μπορεί να συμβάλει στην αντιμετώπιση των προαναφερθέντων κινδύνων από κακόβουλες προσβάσεις στα αρχεία υπολογιστικών συστημάτων φορέων στρατηγικής σημασίας για τη χώρα (π.χ. ΔΕΗ, αερομεταφορές, τραπεζικά συστήματα κ.λπ.).

Βασικός στόχος της Εθνικής Στρατηγικής Ασφάλειας θα πρέπει να είναι η προώθηση της διαπίστωσης και προληπτικής διαχείρισης των κινδύνων, στο επίπεδο του ατόμου, της επιχείρησης, του κράτους και της κοινωνίας γενικά. Η κατάλληλη πρόληψη προσφέρει τη μεγαλύτερη δυνατή ασφάλεια με ελαχιστοποίηση του κόστους.

[30] ΕΕ C 68/1 της 24.3.2007.

[31] COM (2006) 251 τελικό της 31.5.2006.

2.1. Αρχές της Εθνικής Στρατηγικής Ασφάλειας Δικτύων και Πληροφοριών

Με την προτεινόμενη Εθνική Στρατηγική Ασφάλειας συνδέονται οι εξής αρχές:

2.1.1 Ενημέρωση

Όλοι οι χρήστες πρέπει να ενημερώνονται για την ανάγκη ασφάλειας των πληροφοριακών συστημάτων και των δικτύων τους και να ενθαρρύνονται για την ενίσχυση της ασφάλειάς τους. Οφείλουν να κατανοούν ότι ενδεχόμενα λάθη και παραλήψεις στην ασφάλεια μπορεί να βλάψουν σοβαρά τα συστήματα και τα δίκτυα που χρησιμοποιούν, αλλά και να προκαλέσουν βλάβη και σε άλλους, με τους οποίους διασυνδέονται.

2.1. 2 Υπευθυνότητα

Οι χρήστες οφείλουν να συνειδητοποιήσουν ότι είναι υπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και ότι είναι υπόλογοι κατά τρόπο που προσιδιάζει στον ατομικό τους ρόλο στο διαδίκτυο. Παράλληλα, επιβάλλεται να αναθεωρούν περιοδικά τις πρακτικές τους και τα μέτρα ασφάλειας που εφαρμόζουν.

2.1.3 Αντιμετώπιση ζητημάτων ασφάλειας

Με δεδομένη τη διασυνδεσιμότητα και την αλληλεπίδραση των πληροφοριακών συστημάτων και δικτύων, οι χρήστες πρέπει να δρουν έγκαιρα και με συνεργάσιμο τρόπο για την αντιμετώπιση κινδύνων, ανταλλάσσοντας μεταξύ τους πληροφορίες για πιθανούς κινδύνους και εφαρμόζοντας διαδικασίες για γρήγορη και αποτελεσματική αντίδραση, προκειμένου να ανιχνεύσουν και να εμποδίσουν κινδύνους που διακυβεύουν την ασφάλειά τους.

2.1.4 Δεοντολογία

Η δεοντολογική συμπεριφορά των χρηστών είναι πολύ σημαντική. Λαμβανομένης υπόψη της μεγάλης διάδοσης και αλληλεπίδρασης των πληροφοριακών συστημάτων και δικτύων στις σύγχρονες κοινωνίες, οι χρήστες οφείλουν να κατανοήσουν ότι θα πρέπει να αποφεύγουν ενέργειες που μπορεί να βλάπτουν τους άλλους.

2.1. 5 Δημοκρατία

Η ασφάλεια των πληροφοριακών συστημάτων και δικτύων και ο τρόπος εφαρμογής της πρέπει να συμβιβάζεται με τις βασικές αρχές μιας δημοκρατικής κοινωνίας, όπως η ελευθερία ανταλλαγής σκέψεων και ιδεών, η ελευθερία ροής πληροφοριών, η εμπιστευτικότητα των πληροφοριών και της επικοινωνίας, η κατάλληλη προστασία των προσωπικών πληροφοριών και η διαφάνεια.

2.1. 6 Εκτίμηση κινδύνων

Οι χρήστες οφείλουν να εκτιμούν ορθά τις καταστάσεις, να αναγνωρίζουν τους κινδύνους και τα ευαίσθητα σημεία που θίγονται, καθώς και το εύρος των συνεπειών. Η αξιολόγηση και η αντιμετώπιση των κινδύνων, στους οποίους είναι εκτεθειμένες πληροφορίες και δίκτυα, αποτελεί μια διαδικασία που είναι αποτέλεσμα σύνθεσης της τεχνολογίας με τον ανθρώπινα παράγοντα, τις εφαρμοζόμενες πολιτικές ασφάλειας και τις υπηρεσίες από τρίτους.

2.1. 7 Σχεδίαση και εφαρμογή της ασφάλειας στα πληροφοριακά συστήματα και τα δίκτυα

Ο σχεδιασμός και η εφαρμογή της πολιτικής ασφάλειας διασφαλίζει την απρόσκοπτη λειτουργία συστημάτων και δικτύων. Οι τεχνικές παρέμβασης που απαιτούνται για το σκοπό αυτό εξαρτώνται από την επιλογή των προϊόντων, των υπηρεσιών και των διαδικασιών για κάθε σύστημα και είναι ανάλογες με τη σημασία των πληροφοριών που διακινούνται.

2.1. 8 Περιεκτική προσέγγιση στη διαχείριση ασφάλειας

Οι απαιτήσεις διαχείρισης της ασφάλειας βασίζονται σε ένα σύνολο στοιχείων που αφορούν στους κινδύνους (με τις ανάλογες εκτιμήσεις), στους χρήστες και την ποιότητα των συστημάτων και δικτύων που διαθέτουν, στις πολιτικές και τις διαδικασίες που εφαρμόζουν, καθώς και στα μέτρα που παίρνουν. Όλα αυτά χρειάζονται ειδικό συντονισμό.

2.1. 9 Επαναξιολόγηση

Λόγω των συνεχών αλλαγών των τεχνολογικών μέσων, αλλά και των νέων κινδύνων που ανακύπτουν απαιτείται συνεχής επαναξιολόγηση της ασφάλειας των πληροφοριακών συστημάτων και δικτύων. Οι χρήστες οφείλουν να προσαρμόζονται ανάλογα, να ελέγχουν τα ληφθέντα μέτρα και να προβαίνουν στις κατάλληλες τροποποιήσεις της Πολιτικής Ασφάλειάς τους.

2.2. Βασικοί στόχοι της Εθνικής Στρατηγικής Ασφάλειας των Δικτύων και Πληροφοριών

Οι κύριοι στόχοι της Εθνικής Στρατηγικής Ασφάλειας των Δικτύων και Πληροφοριών μπορούν να συνοψιστούν στα παρακάτω σημεία:

2.2.1 Εθνική και διεθνής συνεργασία για την Ασφάλεια Δικτύων και Πληροφοριών (ΑΔΠ)

Στόχος της ΕΣΑΔΠ είναι να ενισχύσει σε εθνικό επίπεδο τη συνεργασία για την προώθηση της ΑΔΠ και να καταστήσει σαφή την κατανομή των ευθυνών μεταξύ των ενδιαφερομένων.

Προς την κατεύθυνση αυτή, προτείνονται ως μέτρα η ενεργός συμμετοχή στην προετοιμασία νομοθεσίας στο πλαίσιο της ΕΕ και των άλλων διεθνών οργανισμών, η υλοποίηση ερευνητικών προγραμμάτων για τη σπουδαιότητα της ΑΔΠ στη νέα οικονομία και η ανάπτυξη πρωτοβουλιών για προώθηση της ΑΔΠ σε συλλογική βάση, ώστε να δημιουργηθεί ένα ενιαίο συνεκτικό πλέγμα.

2.2.2 Ενίσχυση της εθνικής ανταγωνιστικότητας

Η διασφάλιση της ανοικτής διαθεσιμότητας και της ασφαλούς χρήσης των πληροφοριών δημιουργεί νέες ευκαιρίες για τις επιχειρήσεις και σταθερό επιχειρησιακό περιβάλλον που βελτιώνει την ανταγωνιστικότητα της εθνικής οικονομίας και δημιουργεί πόρους για περαιτέρω ανάπτυξη. Στο πλαίσιο αυτό, προτείνονται:

- καινοτομίες που σχετίζονται με την ΑΔΠ και τη συνεργασία μεταξύ φορέων του δημοσίου και ιδιωτικού τομέα,
- ενθάρρυνση των εταιρειών και των ερευνητικών ιδρυμάτων για ανάπτυξη νέων προϊόντων ασφάλειας των πληροφοριών,
- ενθάρρυνση της συνεργασίας μεταξύ δημοσίου και ιδιωτικού τομέα για βελτίωση της συμβατότητας των διαδικασιών της ΑΔΠ,
- προώθηση των διαδικασιών αξιολόγησης σχετικά με την επίδραση της νομοθεσίας και των διεθνών συμφωνιών στην ασφαλή ψηφιακή χρήση των πληροφοριών.

2.2.3 Προληπτική διαχείριση και αντιμετώπιση των κινδύνων για την ασφάλεια δικτύων και πληροφοριών

Βασικός στόχος της Εθνικής Στρατηγικής Ασφάλειας είναι η προώθηση της προληπτικής διαπίστωσης και διαχείρισης των κινδύνων σε επίπεδο ατόμου, επιχείρησης, κράτους και κοινωνίας γενικά. Προς αυτή την κατεύθυνση προτείνονται:

- δημιουργία συστήματος παρακολούθησης σε εθνική κλίμακα της κατάστασης αναφορικά με τους κινδύνους της ΑΔΠ,
- περιοδικές αξιολογήσεις των νέων κινδύνων που απειλούν την ΑΔΠ και παροχή πληροφοριών για τους κινδύνους αυτούς,
- επισήμανση των ευάλωτων σημείων της ασφάλειας δικτύων και πληροφοριών και ενημέρωση όλων των φορέων για τις βέλτιστες πρακτικές στην αντιμετώπισή τους.

2.2.4 Διασφάλιση των θεμελιωδών δικαιωμάτων και προστασία του εθνικού κεφαλαίου γνώσης

Η προστασία των προσωπικών δεδομένων αποτελεί βασική προϋπόθεση στην εδραίωση της Κοινωνίας της Πληροφορίας. Η απρόσκοπτη πρόσβαση στις πληροφορίες δε

θα πρέπει να γίνεται σε βάρος των θεμελιωδών δικαιωμάτων. Προς το σκοπό αυτό προτείνεται:

- στις νέες ρυθμίσεις για την ασφάλεια δικτύων και πληροφοριών να λαμβάνονται υπόψη τα θεμελιώδη δικαιώματα,
- να αναθεωρηθεί η παραδοσιακή νομοθεσία που δεν είναι συμβατή με τις νέες απαιτήσεις για προστασία των θεμελιωδών δικαιωμάτων.

2.2.5 Βελτίωση της ενημέρωσης και των επαγγελματικών δεξιοτήτων των φορέων της ΑΔΠ

Η ενημέρωση όλων των εμπλεκόμενων φορέων σχετικά με τους κινδύνους που απειλούν την ΑΔΠ εξελίσσεται σε βασική προϋπόθεση για τη λειτουργία μιας ασφαλούς ΚτΠ. Η εξειδίκευση των επαγγελματιών της ΑΔΠ καθίσταται πλέον αναγκαία. Στο νόημα αυτό προτείνεται η:

- προώθηση βελτιωμένων προγραμμάτων επαγγελματικής επάρκειας στην ΑΔΠ,
- ένταξη των προγραμμάτων εκπαίδευσης της ΑΔΠ σε όλα τα επίπεδα εκπαίδευσης,
- βελτίωση της ενημέρωσης σε εταιρείες, φορείς τοπικής αυτοδιοίκησης και οργανισμών και ακόμα μεμονωμένων ομάδων ατόμων σε θέματα της ΑΔΠ,
- συμβολή στην ανάπτυξη και χρήση πιστοποιητικών ποιότητας σχετικά με την ΑΔΠ.

Η ΕΣΑΔΠ θα πρέπει να εγκρίνεται από τους αρμόδιους Υπουργούς. Σχετική πρόταση έχει υποβληθεί στα συναρμόδια υπουργεία. Θα πρέπει, επίσης, να δημιουργηθεί αποτελεσματικό σύστημα παρακολούθησης, σε εθνική κλίμακα, των κινδύνων που διατρέχει η ασφάλεια δικτύων και πληροφοριών. Η διαχείριση αυτού του συστήματος θα ανατεθεί σε κάποιο φορέα, ο οποίος θα ενημερώνεται συνεχώς ως προς τους κινδύνους διεθνώς για τα διάφορα είδη επικοινωνιών και θα παρέχει πληροφορίες, ανά πάσα στιγμή, προς όλους, όσοι σχετίζονται με την ασφάλεια δικτύων και υπηρεσιών, τόσο για τους κινδύνους όσο και για τα μέτρα που πρέπει να ληφθούν για την αντιμετώπισή τους. Επίσης, θα αναπτύξει μεθόδους ανάλυσης των ευάλωτων σημείων της ασφάλειας δικτύων και πληροφοριών και θα μελετήσει τις βέλτιστες πρακτικές που επιβάλλονται για τα σημεία αυτά προς χρήση τους από όλους τους φορείς. Τέλος, θα υποβάλει στην κυβέρνηση σχέδιο της ΕΣΑΔΠ που θα εναρμονίζει όλα τα αναγκαία μέτρα υλοποίησης της στρατηγικής και θα περιλαμβάνει προτάσεις για επικαιροποίηση της ΕΣΑΔΠ προς τα αρμόδια υπουργεία, τα οποία και θα προχωρήσουν σε έγκριση τόσο της συγκεκριμένης στρατηγικής όσο και της ενδεχόμενης επικαιροποίησής της.

Η ΑΔΑΕ προτείνει να αναλάβει η ίδια το ρόλο αυτό ως η πλέον αρμόδια αρχή σε παρόμοια θέματα.

3. Ειδικότερες Νομοθετικές Προτάσεις της ΑΔΑΕ

Το Φεβρουάριο του 2006, με πρωτοβουλία του Πρωθυπουργού, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) εκλήθησαν να εκθέσουν τις απόψεις τους σχετικά με την ενίσχυση του θεσμικού πλαισίου για την προστασία του απορρήτου των επικοινωνιών και γενικά την ενίσχυση των Αρχών αυτών, ώστε να μπορούν να ανταποκριθούν σωστά στο ρόλο τους.

Η ΑΔΑΕ ανταποκρίθηκε άμεσα στην πρόσκληση, υποβάλλοντας αναλυτικό υπόμνημα με τις θέσεις της. Η Επιτροπή Εμπειρογνωμόνων, η οποία συγκροτήθηκε με απόφαση του Πρωθυπουργού, για να εξετάσει τα υπομνήματα που υποβλήθηκαν από τις παραπάνω Αρχές, δεν κατέληξε σε σχέδιο νόμου, αλλά παρέδωσε σχετική γνωμάτευση, στην οποία υιοθετούνται σε μεγάλο βαθμό οι απόψεις της ΑΔΑΕ ως προς τις προτεινόμενες νομοθετικές παρεμβάσεις που κρίνονται αναγκαίες για την προστασία της ασφάλειας και του απορρήτου των επικοινωνιών.

Οι νομοθετικές προτάσεις αφορούσαν τόσο σε θέματα θεσμικού πλαισίου, όσο και σε θέματα ενίσχυσης της υλικοτεχνικής υποδομής και της στελέχωσης της ΑΔΑΕ, καθώς και της οικονομικής και διοικητικής της ευελιξίας.

Σε συνέχεια των ανωτέρω, το Υπουργείο Δικαιοσύνης συνέστησε Ειδική Νομοπαρασκευαστική Επιτροπή που είχε σκοπό την κατάρτιση Σχεδίου Νόμου για την «Ενίσχυση του νομοθετικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας».

Οι νομοθετικές προτάσεις, τις οποίες έχει υποβάλει η ΑΔΑΕ, παρατίθενται εν συντομία στη συνέχεια.

3.1. Αρμοδιότητα επί εσωτερικών δικτύων και επί προμηθευτών εξοπλισμού ηλεκτρονικών επικοινωνιών

Οι απειλές για την ασφάλεια των επικοινωνιών δεν περιορίζονται μόνο σε οργανισμούς και επιχειρήσεις που ασχολούνται με τις επικοινωνίες. Συνεπώς, προτείνεται να υπάρξει ρητή πρόβλεψη, σύμφωνα με την οποία η ΑΔΑΕ θα δύναται να προβαίνει σε ελέγχους και των νομικών ή φυσικών προσώπων που διαθέτουν εσωτερικά δίκτυα (intranet) ή ιδιωτικά τηλεφωνικά κέντρα (π.χ. ξενοδοχεία, επιχειρήσεις κ.λπ.), πέραν εκείνων που ασχολούνται με τηλεπικοινωνιακές, ταχυδρομικές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία, καθώς και των φυσικών ή νομικών προσώπων που προμηθεύουν εξοπλισμό ηλεκτρονικών επικοινωνιών ή παρέχουν υπηρεσίες σχετικές με δραστηριότητες ηλεκτρονικών επικοινωνιών σε οργανισμούς και επιχειρήσεις, οι οποίες υπάγονται ήδη, σύμφωνα με την ισχύουσα νομοθεσία, στην ελεγκτική αρμοδιότητα της ΑΔΑΕ.

3.2. Έλεγχος ΕΥΠ και άλλων Αρχών που έχουν τη δυνατότητα να ζητούν άρση του απορρήτου

Οι Αρχές αυτές θα πρέπει να οριοθετήσουν τους τομείς δράσης τους σε σχέση με τον τομέα των επικοινωνιών και να διευκολύνουν τον έλεγχο του ελεγκτικού φορέα, στον οποίον υπάγονται.

3.3. Πιστοποίηση ασφάλειας του εξοπλισμού των παρόχων ηλεκτρονικών επικοινωνιών

Η ΑΔΑΕ θα πρέπει να πιστοποιεί την ύπαρξη μέτρων ασφάλειας του εξοπλισμού και του λογισμικού που χρησιμοποιείται ή μπορεί να χρησιμοποιηθεί από τις υπαγόμενες στον έλεγχό της υπηρεσίες, τους οργανισμούς και τις επιχειρήσεις, σε σχέση με τις κανονιστικές πράξεις για τη διασφάλιση του απορρήτου των επικοινωνιών, τις οποίες εκδίδει. Η διάθεση και χρήση του εξοπλισμού αυτού χωρίς την εν λόγω πιστοποίηση θα καθίστανται παράνομες.

3.4. Ενημέρωση ΑΔΑΕ κατά την προμήθεια εξοπλισμού

Οι προμηθευτές εξοπλισμού παραβίασης του απορρήτου θα πρέπει να ενημερώνουν την ΑΔΑΕ για οποιοδήποτε αίτημα αγοράς σχετικού εξοπλισμού ή και ανταλλακτικών του. Σχετική εξουσιοδότηση για την έκδοση ΚΥΑ, με την οποία θα ρυθμίζεται το όλο θέμα, έχει περιληφθεί στο Ν. 3431/2006.

3.5. Έλεγχος καταγγελιών για παραβίαση του απορρήτου των επικοινωνιών

Με βάση το ισχύον θεσμικό πλαίσιο, η ΑΔΑΕ εξετάζει καταγγελίες σχετικά με τον τρόπο και τη διαδικασία άρσης του απορρήτου. Ο έλεγχος αυτός θα πρέπει να επεκταθεί και στις καταγγελίες πολιτών για κάθε παραβίαση του απορρήτου των επικοινωνιών τους.

3.6. Δυνατότητα της ΑΔΑΕ να ζητεί την άσκηση ένδικων μέσων κατά βουλευμάτων για την άρση απορρήτου

Με το Ν. 2225/94 προβλέπονται οι όροι και η διαδικασία άρσης του απορρήτου. Προς τούτο απαιτείται βούλευμα του Συμβουλίου Εφετών ή του Συμβουλίου Πλημμελειοδικών, ανάλογα με τη βαρύτητα του υπό διερεύνηση αδικήματος, ή εισαγγελική διάταξη που επικυρώνεται με αντίστοιχο βούλευμα. Σε θέματα εθνικής ασφάλειας απαιτείται απλώς διάταξη του Εισαγγελέα Εφετών. Προβλέπεται, επίσης, να ενημερώνεται η ΑΔΑΕ σε κάθε περίπτωση, ανεξαρτήτως της Αρχής που υποβάλλει το σχετικό αίτημα άρσης του

απορρήτου. Στο πλαίσιο αυτό, η ΑΔΑΕ, όπως προαναφέρθηκε, ελέγχει τους όρους και τη διαδικασία άρσης του απορρήτου, χωρίς να εξετάζει την κρίση των αρμοδίων δικαστικών αρχών. Η διάταξη όμως αυτή, ελλείψει πρόβλεψης εννόμων συνεπειών σε περίπτωση που διαπιστωθεί παραβίαση των όρων και της διαδικασίας άρσης του απορρήτου, παραμένει ατελής. Για το λόγο αυτό, στις συγκεκριμένες περιπτώσεις θα πρέπει να προβλεφθεί η δυνατότητα να ζητά η ΑΔΑΕ από τον καθ΄ ύλην αρμόδιο Εισαγγελέα (Εφετών ή Αρείου Πάγου) την άσκηση ένδικων μέσων (έφεση, αναίρεση) κατά βουλευμάτων για την άρση απορρήτου. Σε περίπτωση εισαγγελικής διάταξης για λόγους εθνικής ασφάλειας, θα πρέπει να επιλαμβάνεται ο Εισαγγελέας του Αρείου Πάγου, κατόπιν αιτήματος της ΑΔΑΕ.

3.7. Ενημέρωση της ΑΔΑΕ για αξιόποινες πράξεις παραβίασης της κείμενης νομοθεσίας σχετικά με την προστασία του απορρήτου των επικοινωνιών

Προτείνεται να προβλεφθεί ρητά η υποχρέωση κάθε αρχής, συμπεριλαμβανομένης και της δικαστικής αρχής, να ενημερώνει την ΑΔΑΕ για αξιόποινες πράξεις παραβίασης της κείμενης νομοθεσίας σχετικά με την προστασία του απορρήτου των επικοινωνιών. Επιπλέον, εφόσον κρίνεται σκόπιμο από τη δικαστική αρχή, η ΑΔΑΕ θα καλείται να λάβει γνώση της σχετικής δικογραφίας και εντός τριάντα ημερών το αργότερο, από την επίδοση της κλήσης, να υποβάλει, εφόσον επιθυμεί, έκθεση με τις απόψεις της για όλες τις καταγγελλόμενες πράξεις που βρίσκονται υπό διερεύνηση.

3.8. Αποφασιστική αρμοδιότητα της ΑΔΑΕ κατά την εφαρμογή του ΠΔ 47/2005

Θα πρέπει να προβλεφθεί ρητά στο εν λόγω ΠΔ ότι η ΑΔΑΕ ελέγχει την ορθή εφαρμογή του Προεδρικού Διατάγματος, επιλύει τις αναφυόμενες κατά τη διαδικασία άρσης του απορρήτου διαφορές μεταξύ των παρόχων υπηρεσιών επικοινωνίας και των αρμοδίων αρχών και αποφασίζει, στο πλαίσιο εκτέλεσης αυτού του Προεδρικού Διατάγματος, για κάθε θέμα σχετικό με τη διαδικασία άρσης του απορρήτου των επικοινωνιών.

3.9. Διατύπωση γνώμης της ΑΔΑΕ για την έκδοση του Κανονισμού Γενικών Αδειών της ΕΕΤΤ

Ο προβλεπόμενος στο άρθρο 21 παρ.5 του Ν. 3431/2006 Κανονισμός Γενικών Αδειών θα πρέπει να εκδίδεται από την ΕΕΤΤ μετά από γνώμη της ΑΔΑΕ ως προς τους όρους που αφορούν στην: α) προστασία του απορρήτου στον τομέα των ηλεκτρονικών επικοινωνιών, β) ασφάλεια δημόσιων δικτύων ηλεκτρονικών επικοινωνιών έναντι μη επιτρεπόμενης πρόσβασης, γ) συμμόρφωση προς τα ισχύοντα πρότυπα και/ή τις προδιαγραφές του τομέα ηλεκτρονικών επικοινωνιών.

3.10. Διατύπωση γνώμης της ΑΔΑΕ για την έκδοση της ΚΥΑ του άρθρου 24 παρ.19 του Ν. 3431/2006

Προτείνεται να διατυπώνεται η γνώμη της ΑΔΑΕ για την έκδοση της προαναφερόμενης ΚΥΑ σχετικά με τις προϋποθέσεις και τη διαδικασία χορήγησης άδειας διάθεσης, κατοχής και χρήσης εξοπλισμού με δυνατότητα αποκρυπτογράφησης απορρήτων ή κρυπτογραφημένων μηνυμάτων ή λήψης εκπομπών που γίνονται από εξοπλισμούς κρατικών υπηρεσιών για την εφαρμογή των κανόνων οδικής κυκλοφορίας ή σάρωσης του φάσματος ραδιοσυχνοτήτων και συγχρόνως παρακολούθησης και αποκωδικοποίησης εκπομπών που δεν προορίζονται για λήψη από το ευρύ κοινό. Προτείνεται, επίσης, να ανατεθεί στην ΑΔΑΕ η αρμοδιότητα να διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, ελέγχους σχετικούς με τη διάθεση, κατοχή και χρήση του εν λόγω εξοπλισμού, ενημερώνοντας σχετικά την ΕΕΤΤ.

3.11. Δυνατότητα άρσης του απορρήτου για το αδίκημα της πορνογραφίας ανηλίκων

Στα αδικήματα, για τα οποία προβλέπεται άρση απορρήτου, δεν περιλαμβάνεται το αδίκημα της πορνογραφίας ανηλίκων μέσω του διαδικτύου, σύμφωνα με το άρθρο 348Α ΠΚ όπως τροποποιήθηκε με το Ν. 3625/2007 (ΦΕΚ Α' 290/24.12.2007). Ως εκ τούτου, προτείνεται, το ως άνω αδίκημα, καθώς επίσης τα αδικήματα των άρθρων 370, 370 Α, Β, Γ του Ποινικού Κώδικα, να προστεθούν στην πρώτη παράγραφο του άρθρου 4 του Ν. 2225/94, όπως αυτό ισχύει.

3.12. Άσκηση ελέγχου από το προσωπικό της ΑΔΑΕ

Λόγω του όγκου των ελέγχων που καλείται να διενεργήσει η ΑΔΑΕ, θα πρέπει να προβλεφθεί η δυνατότητα άσκησης ελέγχου όχι μόνο από μέλη της Ολομέλειας της ΑΔΑΕ, αλλά και από μέλη του προσωπικού της, κατόπιν σχετικής απόφασης της Ολομέλειας.

3.13. Υποκείμενα ακρόασης από την ΑΔΑΕ

Θα πρέπει να διευρυνθεί ο κύκλος των προσώπων, τα οποία είναι δυνατόν να κληθούν σε ακρόαση από την ΑΔΑΕ, εφόσον αυτά συμβάλλουν στην εκπλήρωση της αποστολής της.

3.14. Αυστηρότερες διοικητικές κυρώσεις

Οι διοικητικές κυρώσεις που μπορεί να επιβάλει η ΑΔΑΕ εξαντλούνται στην επιβολή σύστασης ή χρηματικού προστίμου ύψους από 15.000 μέχρι 1.500.000 ευρώ. Υπό τις συνθήκες αυτές, οι εν λόγω κυρώσεις, ενόψει ιδίως του κύκλου εργασιών των επιχειρήσεων, δεν μπορούν να έχουν αποτρεπτικό χαρακτήρα, παρόλο που η ίδρυση ανεξάρτητων διοικητικών αρχών επιβάλλεται κυρίως λόγω του προληπτικού χαρακτήρα του ελέγχου τους. Υπό την έννοια αυτή, χωρίς την πρόβλεψη αυστηρότερων διοικητικών κυρώσεων υποβαθμίζεται

ο ρόλος των ανεξάρτητων διοικητικών αρχών.

Ως εκ τούτου, προτείνεται η επιβολή διοικητικών κυρώσεων σε κυμαινόμενο ποσοστό, αναλόγως του κύκλου εργασιών των ελεγχόμενων επιχειρήσεων και της βαρύτητας της παράβασης, καθώς επίσης αυξημένες διοικητικές κυρώσεις σε περίπτωση διάπραξης αδικήματος εις βάρος της εθνικής ασφάλειας της χώρας.

Οι κυρώσεις θα πρέπει να συνδέονται με το σύνολο των αρμοδιοτήτων της ΑΔΑΕ και να μη σχετίζονται μόνο με το απόρρητο των επικοινωνιών και τους όρους και τη διαδικασία άρσης του.

3.15. Ελεγκτικός ρόλος της ΑΔΑΕ ως προς την Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία, σε συνάρτηση με την παροχή στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ

Όπως προβλέπεται από την Οδηγία, η διατήρηση δεδομένων επικοινωνίας για μακρά χρονική περίοδο καθιστά αναγκαία, κατά τη διαδικασία ενσωμάτωσής της στην εθνική έννομη τάξη, την πρόβλεψη ελέγχου από την ΑΔΑΕ και τη θέσπιση μέτρων για την προστασία των διατηρούμενων δεδομένων τόσο από τους παρόχους όσο και από τις αρμόδιες δημόσιες αρχές που ζητούν τα στοιχεία αυτά κατά τη διαδικασία άρσης του απορρήτου.

3.16. Ενίσχυση των μέσων για την υλοποίηση του θεσμικού ρόλου της ΑΔΑΕ

α. Προϋπολογισμός της ΑΔΑΕ

Το έτος 2007, ο προϋπολογισμός της ΑΔΑΕ ανήλθε στο ποσό των 2.145.000,00 €. Στον Πίνακα που ακολουθεί εμφανίζονται αναλυτικά τα εγκεκριμένα ποσά του προϋπολογισμού της Αρχής και τα αντίστοιχα ποσοστά αύξησης ανά έτος με αφετηρία το 2005, όταν ξεκίνησε ουσιαστικά το ελεγκτικό έργο της Αρχής:

ΕΤΟΣ	ΕΓΚΕΚΡΙΜΕΝΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ ΣΕ ΕΥΡΩ	ΕΤΗΣΙΟ ΠΟΣΟΣΤΟ ΑΥΞΗΣΗΣ
2005	2.000.000,00	-----
2006	2.100.000,00	5%
2007	2.145.000,00	2%

Σύμφωνα με τα παραπάνω στοιχεία, τα ποσοστά αύξησης του προϋπολογισμού της ΑΔΑΕ είναι σχετικά χαμηλά. Δεδομένου ότι για την αποτελεσματικότερη εκπλήρωση των καθηκόντων της απαιτείται εξοπλισμός με κατάλληλα τεχνικά μέσα και στελέχωση με ειδικευμένο προσωπικό, η άμεση αύξηση του προϋπολογισμού θεωρείται απολύτως αναγκαία.

β. Στελέχωση της ΑΔΑΕ

i) Το προσωπικό της Αρχής άρχισε να προσλαμβάνεται από το Νοέμβριο του 2004. Μέχρι τότε, η ΑΔΑΕ λειτουργούσε με την Ολομέλειά της. Το προβλεφθέν στο Νόμο 3115/2003 προσωπικό της ΑΔΑΕ (40 οργανικές θέσεις) είναι εντελώς ανεπαρκές, ώστε να μπορέσει η Αρχή να ανταποκριθεί ουσιαστικά στο ρόλο της. Με βάση τις σημερινές ανάγκες, αλλά και τις νέες απαιτήσεις, εκτιμάται ότι για τη στελέχωση της ΑΔΑΕ απαιτούνται συνολικά εκατό (100) θέσεις, από τις οποίες πενήντα επτά (57) θέσεις ειδικού επιστημονικού προσωπικού, τριάντα οκτώ (38) θέσεις τακτικού προσωπικού, τέσσερις (4) θέσεις δικηγόρων παρ' εφέταις με έμμισθη εντολή και μία (1) θέση νομικού συμβούλου.

ii) Το προσωπικό της ΑΔΑΕ πρέπει να αμείβεται αναλόγως των προσόντων του, λαμβανομένης υπόψη και της ανάγκης στελέχωσης της Αρχής με επιστήμονες υψηλής στάθμης και εξαιρετικής εξειδίκευσης. Για το λόγο αυτό, προτείνεται οι αποδοχές του προσωπικού της ΑΔΑΕ, το είδος των πρόσθετων απολαβών και το ύψος τους να καθορίζονται με κοινή απόφαση των Υπουργών Οικονομίας και Οικονομικών και Δικαιοσύνης, κατά παρέκκλιση από τις κείμενες διατάξεις.

iii) Με την υπάρχουσα στελέχωση της ΑΔΑΕ διαπιστώνεται αδυναμία νόμιμης συγκρότησης Υπηρεσιακού Συμβουλίου και Δευτεροβάθμιου Πειθαρχικού Συμβουλίου της Αρχής, λόγω της μη συγκέντρωσης από κάποιο υπάλληλο των απαιτούμενων από το νόμο προϋποθέσεων, ώστε να του ανατεθούν καθήκοντα προϊσταμένου των διοικητικών υπηρεσιών. Για το λόγο αυτό, είναι επιτακτική νομοθετική ρύθμιση, σύμφωνα με την οποία η Ολομέλεια της ΑΔΑΕ, κατά την πρώτη συγκρότηση του Υπηρεσιακού Συμβουλίου και του Δευτεροβάθμιου Πειθαρχικού Συμβουλίου, θα μπορεί με απόφασή της να αναθέτει σε άτομα του προσωπικού της καθήκοντα προϊσταμένου των διοικητικών υπηρεσιών της.

γ. Τεχνολογικός εξοπλισμός

Η διαρκής εξέλιξη της τεχνολογίας επιβάλλει τον εξοπλισμό της ΑΔΑΕ με σύγχρονα μέσα, ο οποίος αναφέρεται, ενδεικτικά, σε μηχανήματα:

- ανίχνευσης συσκευών παρακολούθησης τηλεφωνικών συνδιαλέξεων,
- ελέγχου του ασύρματου καναλιού στα δίκτυα κινητής τηλεφωνίας 2ης και 3ης γενιάς,
- ανάλυσης και διερεύνησης περιστατικών ασφάλειας των τηλεπικοινωνιακών συστημάτων των παρόχων,

• ελέγχου ασφάλειας δικτύων (vulnerability scanners, penetration testing κ.λπ.).

Η ΑΔΑΕ στερείται τεχνολογικού εξοπλισμού λόγω του μικρού προϋπολογισμού που της εγκρίνεται.

δ. Υποδομές

Για να ανταποκριθεί στο θεσμικό της ρόλο, η ΑΔΑΕ χρειάζεται κτηριακή και υλικοτεχνική υποδομή (π.χ. εξοπλισμό ανίχνευσης παραβίασης του απορρήτου, πληροφορικά συστήματα, οχήματα για μετάβαση στις περιοχές ελέγχου κ.λπ.).

ε. Οικονομική ευελιξία

Για τη διευκόλυνση του έργου της, η ΑΔΑΕ θα πρέπει να μπορεί να συνάπτει συμβάσεις παροχής υπηρεσιών, μελετών και προμηθειών για θέματα που άπτονται των σκοπών και της λειτουργίας της. Η σύναψη και η υλοποίηση αυτών των συμβάσεων θα γίνονται σύμφωνα με τους σχετικούς κανονισμούς της ΑΔΑΕ, οι οποίοι θα εκδίδονται κατά παρέκκλιση της κείμενης νομοθεσίας, πλην των διατάξεων του Δικαίου της Ευρωπαϊκής Ένωσης, και θα εγκρίνονται με απόφαση του Υπουργού Δικαιοσύνης.

Επίσης, προτείνεται να συσταθεί στην ΑΔΑΕ ειδικός λογαριασμός, στον οποίο θα αποδίδονται και θα περιέρχονται έσοδα και κάθε άλλο ποσό που εισπράττεται από οποιαδήποτε διοικητική ή δικαστική αρχή ή άλλον τίτλο ως χρηματική ποινή, δικαστικό πρόστιμο ή προϊόν δήμευσης σε σχέση με τις αρμοδιότητες της ΑΔΑΕ, όπως αυτές ορίζονται από το Νόμο.

Ο Ειδικός Λογαριασμός της ΑΔΑΕ θα υπόκειται στον έλεγχο ορκωτών ελεγκτών. Ο τρόπος της οικονομικής του διαχείρισης θα καθορίζεται με κοινή απόφαση των συναρμοδίων Υπουργών, μετά από εισήγηση της ΑΔΑΕ.

Σε κάθε περίπτωση, θα πρέπει να υπάρξει σχετική πρόβλεψη, ώστε η Ολομέλεια της ΑΔΑΕ να μπορεί να καθορίζει με αποφάσεις της τη σύσταση και τις αμοιβές ομάδων εργασίας, καθώς και την αποζημίωση για τη διενέργεια ελέγχων. Ως γνωστόν, οι έλεγχοι είναι χρονοβόροι και απαιτούν διαρκή ετοιμότητα και συχνή μετακίνηση των ελεγκτών.

στ. Ίδια έσοδα

Η ανεξαρτησία της ΑΔΑΕ πρέπει να συνοδεύεται από τη δυνατότητά της να διαθέτει ίδια έσοδα. Με τον τρόπο αυτό, άλλωστε, θα μειωθεί σταδιακά η επιβάρυνση του κρατικού προϋπολογισμού. Τα ίδια έσοδα της Αρχής θα είναι ανάλογα με εκείνα που προβλέπονται για την ΕΕΤΤ, θα περιέρχονται στον Ειδικό Λογαριασμό της και θα εισπράττονται σύμφωνα με τις διατάξεις του ΚΕΔΕ. Οι πόροι αυτού του Λογαριασμού θα προέρχονται από τα έσοδα από τις διοικητικές κυρώσεις (πρόστιμα) που επιβάλλονται από την Αρχή, τις αμοιβές από τις εργασίες πιστοποιήσεων, τα διοικητικά τέλη στο πλαίσιο ελέγχου της εφαρμογής της διαδικασίας άρσης του απορρήτου σύμφωνα με το ΠΔ 47/2005 κ.ά.

Η έγκαιρη, ορθή και συνολική ικανοποίηση των προτάσεων που προηγήθηκαν αποτελούν την αναγκαία προϋπόθεση, για να μπορέσει να ανταποκριθεί η ΑΔΑΕ με επιτυχία στις απαιτήσεις, τις οποίες θέτει το σύγχρονο περιβάλλον της απελευθερωμένης αγοράς στο θέμα της ασφάλειας των δικτύων τηλεπικοινωνιών και πληροφορικής και της διασφάλισης του απορρήτου.