ΠΡΟΛΟΓΟΣ

ΕΚΘΕΣΗ ΠΕΠΡΑΓΜΕΝΩΝ
ΕΤΟΥΣ 2005

Βιώσαμε το τελευταίο διάστημα με την υπόθεση των υποκλοπών ένα από τα πιο κρίσιμα εθνικά προβλήματα της χώρας μας.

Η ΑΔΑΕ είχε επισημάνει, σχεδόν από την αρχή του μικρού σχετικά χρόνου λειτουργίας της, ότι παράλληλα με τα εξαιρετικά θετικά αποτελέσματα για τις σύγχρονες κοινωνίες από την εκρηκτική εξέλιξη των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών δημιουργούνται και σοβαροί κίνδυνοι από κακόβουλες προσβάσεις στα δίκτυα και τις πληροφορίες.

Στους κινδύνους αυτούς περιλαμβάνονται οι παραβιάσεις του προσωπικού απορρήτου, η βιομηχανική κατασκοπία, 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. Θα πρέπει να αναφέρουμε ότι από στοιχεία που υπάρχουν οι επιθέσεις π.χ. στο διαδίκτυο αυξάνονται κατά εκθετικό τρόπο στις προηγμένες χώρες.

Είναι νομίζουμε προφανείς οι επιπτώσεις από τους κινδύνους αυτούς τόσο από πλευράς συνεπειών στις προσωπικές ελευθερίες των ανθρώπων όσο και στην πολιτική και οικονομική ζωή μιας χώρας με ενδεχόμενη βλάβη ακόμα και αυτής της ομαλής δημοκρατικής πορείας της.

Πιστεύουμε ότι πλέον είναι απαραίτητη η συστηματική λήψη μέτρων για την κατοχύρωση της ασφάλειας δικτύων και πληροφοριών σε μία χώρα και μάλιστα σε όλα τα επίπεδα μιας δομημένης κοινωνίας.

Η προσπάθεια πρέπει να εξικνείται από τον απλό πολίτη μέχρι την εκτελεστική εξουσία, τις μεγάλης στρατηγικής σημασίας εταιρείες, όπως είναι οι τράπεζες, οι εταιρείες παροχής ηλεκτρικής ενέργειας, οι εταιρείες μαζικών μεταφορών κ.λπ. αλλά και τις μικρότερες.

Βεβαίως είναι προφανές ότι σημαντικό μέρος της προσπάθειας πέφτει στους παρόχους τηλεπικοινωνιακών υπηρεσιών και υπηρεσιών διαδικτύου.

Είναι θέμα χρόνου το πότε θα υπάρξει στη χώρα μας μία επίθεση από διαδικτυακούς τρομοκράτες ή δικτυακούς πειρατές.
Γι αυτό η προσπάθεια για άμυνα της κοινωνίας πρέπει να είναι άμεση και σε πανεθνική κλίμακα.

Η ΑΔΑΕ εδώ και δύο χρόνια έχει προτείνει την εκπόνηση μιας ολοκληρωμένης Εθνικής Στρατηγικής Ασφάλειας Δικτύων και Πληροφοριών.

Η Εθνική Στρατηγική Ασφάλειας Δικτύων και Πληροφοριών θα πρέπει να αποτελείται από προγράμματα, συντονισμένα μεταξύ τους, που κάθε ένα θα απευθύνεται σε διαφορετικό επίπεδο της κοινωνίας.
Θα πρέπει να μη ξεχνά κανείς ότι με τη σημερινή εξέλιξη της τεχνολογίας κάθε απλός χρήστης ενός ατομικού υπολογιστή είναι ένας σημαντικός παίκτης που σπάζοντας κωδικούς μπορεί να κάνει σημαντική ζημιά στην κοινωνία.

Η ΑΔΑΕ καταβάλλει σημαντικές προσπάθειες και έχει ήδη επιβάλλει σύγχρονες πολιτικές ασφάλειας στους παρόχους ηλεκτρονικών υπηρεσιών, στους οποίους αναφέρεται σήμερα η αρμοδιότητά της. Έχει όμως περιορισμένες δυνατότητες ελέγχου και επομένως δυνατότητες ουσιαστικής παρέμβασης για την γενικότερη θωράκιση της κοινωνίας μας, λόγω του ελάχιστου προσωπικού που διαθέτει, των λίγων οικονομικών πόρων της αλλά και του μη ευέλικτου νομικού πλαισίου που την διέπει.

Πρόσφατα μετά την υπόθεση των υποκλοπών και μετά από πρωτοβουλία του Πρωθυπουργού της χώρας έχει ξεκινήσει σε Κυβερνητικό επίπεδο η προσπάθεια γενικότερης ενίσχυσης της ΑΔΑΕ, προκειμένου να είναι σε θέση να παίζει καλύτερα το ρόλο της.

Η ΑΔΑΕ έχει ήδη στείλει στον κ. Υπουργό Δικαιοσύνης πλήρεις προτάσεις ενίσχυσής της τόσο από πλευράς νομικού πλαισίου όσο και από πλευράς ανθρώπινου δυναμικού και υλικοτεχνικής υποδομής.

Θέλουμε όμως να επαναλάβουμε ότι είναι απαραίτητο να μελετηθεί άμεσα μία Εθνική Στρατηγική Ασφάλειας Δικτύων και Πληροφοριών και να ξεκινήσει το συντομότερο μία συντονισμένη προσπάθεια στη Χώρα μας για την κατά το δυνατόν πιο ουσιαστική αντιμετώπιση των υπαρκτών κινδύνων.

Αθήνα, 25 Σεπτεμβρίου 2006

Ο Πρόεδρος
Ανδρέας Λαμπρινόπουλος

ΣΥΝΘΕΣΗ Α.Δ.Α.Ε.

Πρόεδρος
Ανδρέας Λαμπρινόπουλος

Αντιπρόεδρος
Βασίλειος Κούτρης

Μέλη

1. Μιχαήλ Καρατζάς
Αναπληρωτής: Δημήτριος Δεδούσης

2. Χρήστος Καψάλης
Αναπληρωτής: Γεώργιος Στασινόπουλος

3. Ιάκωβος Βενιέρης
Αναπληρωτής: Χρήστος Δουληγέρης

4. Σταύρος Σκοπετέας
Αναπληρωτής: Αικατερίνη Καραμάνου

5. Κωνσταντίνος Μαραβέλας
Αναπληρωτής: Κωνσταντίνος Βρεττός

ΚΕΦΑΛΑΙΟ Ι.
ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

ΚΕΦΑΛΑΙΟ Ι.

ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

Α. ΘΕΣΜΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

1. Σύσταση Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών

Η ΑΔΑΕ συστάθηκε με το Ν. 3115/2003, κατ΄επιταγή της παραγράφου 2 του άρθρου 19 του Συντάγματος. Σύμφωνα με το άρθρο ι του ιδρυτικού της νόμου, σκοπός της είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

Η Α.Δ.Α.Ε. είναι ανεξάρτητη αρχή, η οποία απολαμβάνει διοικητικής αυτοτέλειας. Έδρα της Α.Δ.Α.Ε. είναι η Αθήνα, μπορεί όμως με απόφασή της να εγκαθιστά και να θέτει σε λειτουργία γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της Α.Δ.Α.Ε. κοινοποιούνται με μέριμνά της στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους υποβάλλεται έκθεση των πεπραγμένων της στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο.

Η Α.Δ.Α.Ε. υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον Κανονισμό της Βουλής.

2. Υποχρεώσεις των μελών

Τα μέλη της Α.Δ.Α.Ε. κατά την άσκηση των καθηκόντων τους δεσμεύονται από το νόμο και υπόκεινται στο καθήκον εχεμύθειας, το οποίο υφίσταται και μετά την με οποιονδήποτε τρόπο αποχώρησή τους.

Τα μέλη της Α.Δ.Α.Ε. υποβάλλουν κατ' έτος στην Εισαγγελία του Αρείου Πάγου την προβλεπόμενη από το Ν. 2429/1996 (ΦΕΚ 155 Α'), όπως εκάστοτε ισχύει, δήλωση περιουσιακής κατάστασης.

3. Κωλύματα και ασυμβίβαστα μελών

Σύμφωνα με το άρθρο 4 του Ν. 3115/03 τα μέλη της ΑΔΑΕ υπόκεινται στους ακόλουθους περιορισμούς:

1. α) Δεν δύναται να διοριστεί μέλος της Αρχής όποιος έχει καταδικαστεί με τελεσίδικη δικαστική απόφαση για αδίκημα που συνεπάγεται κώλυμα διορισμού ή έκπτωση

δημοσίου υπαλλήλου σύμφωνα με τις διατάξεις του Υπαλληλικού Κώδικα.

β) Μέλος της ΑΔΑΕ δεν δύναται να είναι εταίρος, μέτοχος, μέλος διοικητικού συμβουλίου, διαχειριστής, υπάλληλος, σύμβουλος, μελετητής, ατομικής ή άλλης επιχείρησης, η οποία δραστηριοποιείται στους τομείς των ταχυδρομικών υπηρεσιών, των τηλεπικοινωνιών, της πληροφορικής ή της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

2. Εκπίπτει από την ιδιότητα του μέλους της αρχής όποιος μετά το διορισμό του:

α) Καταδικαστεί με τελεσίδικη δικαστική απόφαση για αδίκημα που συνεπάγεται κώλυμα διορισμού ή έκπτωση δημοσίου υπαλλήλου σύμφωνα με τις διατάξεις του Υπαλληλικού Κώδικα.

β) Καταστεί εταίρος, μέτοχος, μέλος διοικητικού συμβουλίου, διαχειριστής, υπάλληλος, σύμβουλος, μελετητής ατομικής ή άλλης επιχείρησης, η οποία δραστηριοποιείται στους τομείς των ταχυδρομικών υπηρεσιών, των τηλεπικοινωνιών, της πληροφορικής ή της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Αν τα μέλη κατέχουν εταιρικά μερίδια ή μετοχές των ανωτέρω επιχειρήσεων, τις οποίες απέκτησαν κατά τη διάρκεια της θητείας τους από κληρονομική διαδοχή, υποχρεούνται να απέχουν από την ενάσκηση των δικαιωμάτων συμμετοχής και ψήφου στα όργανα διοίκησης, διαχείρισης και ελέγχου των εν λόγω επιχειρήσεων, μέχρι το χρόνο λήξης της θητείας τους.

γ) Προβαίνει σε πράξεις, αναλαμβάνει εργασία ή έργο ή αποκτά άλλη ιδιότητα που, κατά την κρίση της Αρχής, δεν συμβιβάζεται με τα καθήκοντά του ως μέλους της Αρχής.

3. Τα μέλη της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) τελούν, κατά τη διάρκεια της θητείας τους, σε αναστολή άσκησης οποιουδήποτε δημόσιου λειτουργήματος ή επαγγέλματος και δεν επιτρέπεται να αναλαμβάνουν άλλα καθήκοντα, αμειβόμενα ή μη στον δημόσιο ή τον ιδιωτικό τομέα. Στα μέλη της Α.Δ.Α.Ε., εκτός του Προέδρου που είναι πλήρους και αποκλειστικής απασχόλησης, επιτρέπεται η άσκηση διδακτικών καθηκόντων μέλους διδακτικού προσωπικού πανεπιστημίων υπό καθεστώς πλήρους ή μερικής απασχόλησης.

4. Η έκπτωση των μελών της Α.Δ.Α.Ε. συνεπεία τελεσίδικης καταδικαστικής απόφασης, σύμφωνα με το εδάφιο α' της παρ. 2 του παρόντος άρθρου, καθώς και η αποδοχή της παραίτησής τους γίνεται με απόφαση του Υπουργού Δικαιοσύνης εντός προθεσμίας δεκαπέντε (15) ημερών από την κοινοποίηση σε αυτόν της απόφασης της Διάσκεψης των Προέδρων της Βουλής. Στη διαπίστωση των υπολοίπων κωλυμάτων και ασυμβιβάστων του παρόντος άρθρου προβαίνει η Α.Δ.Α.Ε., χωρίς συμμετοχή του μέλους της, στο πρόσωπο του οποίου ενδέχεται να συντρέχει το ασυμβίβαστο. Η Α.Δ.Α.Ε. αποφασίζει ύστερα από ακρόαση του εν λόγω μέλους. Τη διαδικασία κινεί ο Πρόεδρος της Α.Δ.Α.Ε. ή ο Υπουργός Δικαιοσύνης. Την απόφαση της Α.Δ.Α.Ε. μπορεί να προσβάλει ενώπιον του πειθαρχικού συμβουλίου το μέλος της Α.Δ.Α.Ε., για το οποίο εκδόθηκε η απόφαση, ο Υπουργός Δικαιοσύνης και ο Πρόεδρος της Α.Δ.Α.Ε.

4. Πειθαρχική διαδικασία για τα μέλη της ΑΔΑΕ

Σύμφωνα με το άρθρο 5 του Ν. 3115/03, για τα μέλη της ΑΔΑΕ προβλέπεται η ακόλουθη πειθαρχική διαδικασία:

ι. Για κάθε παράβαση των υποχρεώσεών τους που απορρέουν από τον παρόντα νόμο, τα μέλη της Α.Δ.Α.Ε. υπέχουν πειθαρχική ευθύνη. Την πειθαρχική διαδικασία ενώπιον του πειθαρχικού συμβουλίου κινεί ο Υπουργός Δικαιοσύνης για τον Πρόεδρο, τον Αντιπρόεδρο και τα μέλη της Α.Δ.Α.Ε. και ο Πρόεδρος για τον Αντιπρόεδρο και τα μέλη της. Το πειθαρχικό συμβούλιο αποφασίζει σε πρώτο και τελευταίο βαθμό την απαλλαγή ή την παύση του μέλους.

2. Το πειθαρχικό συμβούλιο αποτελείται από ένα Αντιπρόεδρο του Συμβουλίου της Επικρατείας, ως πρόεδρο, έναν Αρεοπαγίτη και τρεις Καθηγητές Α.Ε.Ι. με γνωστικό αντικείμενο του δικαίου. Χρέη γραμματέα του συμβουλίου εκτελεί υπάλληλος της Αρχής. Ο πρόεδρος, τα μέλη και ο γραμματέας του συμβουλίου ορίζονται με ισάριθμους αναπληρωτές. Για τα μέλη του συμβουλίου που είναι δικαστικοί λειτουργοί απαιτείται απόφαση του οικείου ανωτάτου δικαστικού συμβουλίου. Το συμβούλιο συγκροτείται με απόφαση του Υπουργού Δικαιοσύνης με τριετή θητεία. Η αμοιβή του προέδρου, των μελών και του γραμματέα καθορίζεται με κοινή απόφαση των Υπουργών Οικονομίας και Οικονομικών και Δικαιοσύνης.

3. Κάθε λεπτομέρεια σχετικά με την πειθαρχική ευθύνη των μελών της Α.Δ.Α.Ε. και την πειθαρχική διαδικασία ρυθμίζεται στον Κανονισμό Εσωτερικής Λειτουργίας της Α.Δ.Α.Ε.

5. Αρμοδιότητες

Σύμφωνα με το άρθρο 6 του Ν. 3115/03, η Α.Δ.Α.Ε., για την εκπλήρωση της αποστολής της, έχει τις ακόλουθες αρμοδιότητες :

α) Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, τακτικούς και έκτακτους ελέγχους, σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), άλλων δημοσίων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία. Τον έλεγχο διενεργεί μέλος ή μέλη της Α.Δ.Α.Ε., συμμετέχει δε και υπάλληλός της, ειδικά προς τούτο εντεταλμένος από τον Πρόεδρό της για γραμματειακή υποστήριξη της διαδικασίας του ελέγχου. Κατά τον έλεγχο αρχείων που τηρούνται για λόγους εθνικής ασφάλειας παρίσταται αυτοπροσώπως ο Πρόεδρος της Α.Δ.Α.Ε.

β) Λαμβάνει πληροφορίες σχετικές με την αποστολή της από τις υπό το στοιχείο α' υπηρεσίες, οργανισμούς και επιχειρήσεις, καθώς και από τους εποπτεύοντες Υπουργούς.

γ) Καλεί σε ακρόαση, από τις υπηρεσίες, οργανισμούς, νομικά πρόσωπα και επιχειρήσεις που αναφέρονται στο ως άνω στοιχείο α', τις διοικήσεις, τους νόμιμους εκπροσώπους, τους υπαλλήλους και κάθε άλλο πρόσωπο, το οποίο κρίνει ότι μπορεί να συμβάλλει στην εκπλήρωση της αποστολής της.

δ) Προβαίνει στην κατάσχεση μέσων παραβίασης του απορρήτου, που υποπίπτουν στην αντίληψή της κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

ε) Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.

στ) Στις περιπτώσεις των άρθρων 3,4 και 5 του Ν. 2225/ 1994, η Α.Δ.Α.Ε. υπεισέρχεται μόνο στον έλεγχο της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, χωρίς να εξετάζει την κρίση των αρμόδιων δικαστικών αρχών.

ζ) Τηρεί αρχείο απόρρητης αλληλογραφίας, σύμφωνα με το στοιχείο Β' της παρ. 2 του άρθρου 12 του παρόντος νόμου.

η) Συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών, με ευρωπαϊκούς και διεθνείς οργανισμούς, για θέματα της αρμοδιότητάς της.

θ) Συντάσσει κάθε χρόνο την προβλεπόμενη στην παράγραφο 2 του άρθρου 1 του παρόντος νόμου έκθεση πεπραγμένων, στην οποία περιγράφει το έργο της, διατυπώνει παρατηρήσεις, επισημαίνει παραλείψεις και προτείνει τυχόν ενδεικνυόμενες νομοθετικές μεταβολές στον τομέα διασφάλισης του απορρήτου των επικοινωνιών.

ι) Γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

ια) Εκδίδει τον κανονισμό εσωτερικής λειτουργίας της, ο οποίος δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως. Ο κανονισμός εσωτερικής λειτουργίας πρέπει να είναι σύμφωνος με τις διατάξεις του Κώδικα Διοικητικής Διαδικασίας.

ιβ) Εκδίδει κανονιστικές πράξεις, δημοσιευόμενες στην Εφημερίδα της Κυβερνήσεως, δια των οποίων ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις ανωτέρω αρμοδιότητές της, καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών.

ιγ) Καταρτίζει τον κανονισμό οικονομικής διαχείρισης, ο οποίος υποβάλλεται και εγκρίνεται από τον Υπουργό Οικονομίας και Οικονομικών.

Τα μέλη και το προσωπικό της Α.Δ.Α.Ε., πλην του βοηθητικού προσωπικού, έχουν προς διαπίστωση των παραβάσεων της νομοθεσίας περί προστασίας του απορρήτου, τις εξουσίες και τα δικαιώματα που προβλέπονται στο Ν. 703/1977, όπως ισχύει. Τα πρόσωπα αυτά έχουν προς τούτο δικαίωμα να ελέγχουν τα προβλεπόμενα από το Π.Δ. 186/1992 (Κ.Β.Σ.) βιβλία και στοιχεία των ελεγχόμενων επιχειρήσεων και οργανισμών, αποκλειομένης της κατάσχεσης ή της παραλαβής τους, καθώς και πάσης φύσεως αρχεία, βιβλία, στοιχεία και λοιπά έγγραφα των προσώπων που ελέγχουν, να ενεργούν έρευνες στα γραφεία και λοιπές εγκαταστάσεις τους, να λαμβάνουν ένορκες και ανωμοτί κατά την κρίση τους καταθέσεις, με την επιφύλαξη του άρθρου 212 του Κώδικα Ποινικής Δικονομίας. Οι σχετικές διατάξεις, απαγορεύσεις, ποινές και κυρώσεις του Ν. 703/1977, ως ισχύει, εφαρμόζονται αναλόγως σε περίπτωση αρνήσεως παροχής στοιχείων, παρεμπόδισης ή δυσχέρανσης του έργου της Α.Δ.Α.Ε., επιφυλασσομένης της εφαρμογής των προβλεπόμενων από τον παρόντα νόμο κυρώσεων.

Η Α.Δ.Α.Ε. μπορεί με απόφασή της να συγκροτεί μόνιμες και έκτακτες επιτροπές και

ομάδες εργασίας για την εξέταση και έρευνα επί θεμάτων ειδικού ενδιαφέροντος που σχετίζονται με θέματα των αρμοδιοτήτων της. Στις επιτροπές και ομάδες εργασίας μπορούν να συμμετέχουν και πρόσωπα που δεν αποτελούν μέλη ή προσωπικό της Α.Δ.Α.Ε. Το έργο των επιτροπών ή των ομάδων εργασίας κατευθύνεται από μέλη της Α.Δ.Α.Ε. Οι εισηγήσεις και οι γνωμοδοτήσεις των επιτροπών και ομάδων εργασίας υποβάλλονται στα αρμόδια όργανα της Α.Δ.Α.Ε., που αποφασίζουν για την τυχόν δημοσιοποίηση των πορισμάτων.

Κατά των εκτελεστών αποφάσεων της Α.Δ.Α.Ε. μπορεί να ασκηθεί αίτηση ακυρώσεως ενώπιον του Συμβουλίου της Επικρατείας, καθώς και οι προβλεπόμενες από το Σύνταγμα και τη νομοθεσία διοικητικές προσφυγές. Ένδικα βοηθήματα κατά των αποφάσεων της Α.Δ.Α.Ε. μπορεί να ασκεί και ο Υπουργός Δικαιοσύνης.

Η Α.Δ.Α.Ε. παρίσταται αυτοτελώς σε κάθε είδους δίκες που έχουν ως αντικείμενο πράξεις ή παραλείψεις της. Εκπροσωπείται δικαστικώς από μέλη του Νομικού Συμβουλίου του Κράτους ή από μέλη της Νομικής της Υπηρεσίας.

Βασικές Αρμοδιότητες της Α.Δ.Α.Ε

Τακτικοί και έκτακτοι έλεγχοι αυτεπαγγέλτως ή κατόπιν καταγγελίας	Ακροάσεις
Κατάσχεση μέσων παραβίασης του απορρήτου	Εξέταση Καταγγελιών
Τήρηση αρχείου απόρρητης αλληλογραφίας	Συνεργασία με άλλες αρχές, με ευρωπαϊκούς και διεθνής οργανισμούς
Έκθεση Πεπραγμένων	Γνωμοδοτήσεις, συστάσεις και υποδείξεις
Έκδοση κανονισμού εσωτερικής λειτουργίας	Έκδοση κανονιστικών πράξεων

Η Α.Δ.Α.Ε. μπορεί να συνάπτει συμβάσεις παροχής υπηρεσιών, μελετών και προμηθειών, για θέματα που άπτονται των σκοπών της και της λειτουργίας της. Η σύναψη και η υλοποίηση των συμβάσεων αυτών διέπονται από τις εκάστοτε ισχύουσες διατάξεις του Δικαίου της Ευρωπαϊκής Ενωσης, τις διατάξεις περί προμηθειών του Δημοσίου και από τους σχετικούς Κανονισμούς της Α.Δ.Α.Ε., οι οποίοι εγκρίνονται και τροποποιούνται με κοινή απόφαση των Υπουργών Οικονομίας και Οικονομικών και Δικαιοσύνης.

6. Λειτουργία της ΑΔΑΕ

Η δράση της Α.Δ.Α.Ε. διέπεται από τις αρχές της διαφάνειας, της αντικειμενικότητας και της αμεροληψίας.

Η Α.Δ.Α.Ε. συνέρχεται στην έδρα της ή και εκτός αυτής αν τούτο έχει οριστεί προηγουμένως, τακτικά τουλάχιστον μία φορά το μήνα και εκτάκτως όταν ζητηθεί από τον Πρόεδρο ή από δύο (2) από τα μέλη της. Η Α.Δ.Α.Ε. συνεδριάζει νομίμως εφόσον μετέχουν στη συνεδρίαση τουλάχιστον τρία (3) μέλη, αποφασίζει δε με απόλυτη πλειοψηφία των παρόντων μελών. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του Προέδρου ή, σε περίπτωση απουσίας αυτού, του Αντιπροέδρου. Η αδικαιολόγητη απουσία μέλους από τρεις (3) διαδοχικές συνεδριάσεις της Α.Δ.Α.Ε. συνεπάγεται την έκπτωσή του, σύμφωνα με την παράγραφο 4του άρθρου 4 του παρόντος νόμου.

Τα θέματα της ημερήσιας διάταξης καθορίζει ο Πρόεδρος, η δε εισήγηση επ' αυτών γίνεται από τον Πρόεδρο ή από άλλο μέλος, που το ορίζει ο Πρόεδρος. Οι αποφάσεις

της Α.Δ.Α.Ε. είναι αιτιολογημένες, καταχωρούνται σε ειδικό βιβλίο και μπορούν να ανακοινώνονται δημοσίως, εκτός αν αφορούν την εθνική άμυνα ή τη δημόσια ασφάλεια. Τα τηρούμενα κατά τις συνεδριάσεις πρακτικά, καθώς και οι φάκελοι των υποθέσεων που διεκπεραιώθηκαν από την Α.Δ.Α.Ε., είναι προσιτά στους άμεσα ενδιαφερόμενους, εκτός αν αφορούν την εθνική άμυνα ή τη δημόσια ασφάλεια. Σε κάθε περίπτωση, η Α.Δ.Α.Ε. οφείλει να μην αποκαλύπτει πληροφορίες και δεδομένα για φυσικά ή νομικά πρόσωπα, τα οποία ενδέχεται να προσβάλλουν την προσωπικότητά τους ή να επηρεάσουν δυσμενώς την επαγγελματική ή την κοινωνική τους θέση, εκτός εάν προκύπτει σχετική υποχρέωσή της από το νόμο.

Τα μέλη της Α.Δ.Α.Ε. κατά την άσκηση των καθηκόντων τους ενεργούν συλλογικά. Στον Πρόεδρο ανατίθενται καθήκοντα συντονισμού και διοίκησης των υπηρεσιών της Α.Δ.Α.Ε., καθώς και παρακολούθησης της εκτέλεσης των αποφάσεων, ορισμάτων και οποιωνδήποτε άλλων πράξεων της Α.Δ.Α.Ε. Με απόφαση του Προέδρου και σύμφωνη γνώμη της Α.Δ.Α.Ε. μπορούν να ανατίθενται, στα μέλη ή στο προσωπικό της, συγκεκριμένα καθήκοντα, μεταξύ των οποίων καθήκοντα διοίκησης ή διαχείρισης. Ο Πρόεδρος με απόφασή του μπορεί να εξουσιοδοτεί μέλη ή άλλα όργανά της να υπογράφουν "με εντολή Προέδρου" έγγραφα η άλλες πράξεις της Α.Δ.Α.Ε. Η Α.Δ.Α.Ε. εκπροσωπείται έναντι τρίτων δικαστικώς και εξωδίκως από τον Πρόεδρό της και όταν αυτός κωλύεται από τον Αντιπρόεδρο. Σε περίπτωση κωλύματος και του Αντιπροέδρου, η Α.Δ.Α.Ε. δύναται να αναθέτει την εκπροσώπηση για συγκεκριμένη πράξη ή ενέργεια ή κατηγορία πράξεων ή ενεργειών σε άλλο μέλος της.

Οι αναγκαίες για τη λειτουργία της Α.Δ.Α.Ε. πιστώσεις εγγράφονται υπό ίδιο φορέα στον προϋπολογισμό του Υπουργείου Δικαιοσύνης. Τον προϋπολογισμό εισηγείται στον Υπουργό Οικονομίας και Οικονομικών ο Πρόεδρος της Α.Δ.Α.Ε., ο οποίος είναι και διατάκτης των δαπανών της. Οι σχετικές δαπάνες εκκαθαρίζονται από την αρμόδια Υπηρεσία Δημοσιονομικού Ελέγχου (Υ.Δ.Ε.) και υπόκεινται στον προληπτικό και κατασταλτικό έλεγχο του Ελεγκτικού Συνεδρίου σύμφωνα με τις κείμενες διατάξεις.

Β. ΣΤΕΛΕΧΩΣΗ ΤΗΣ ΑΔΑΕ

1. Τα μέλη της ΑΔΑΕ

Σύμφωνα με τις διατάξεις του άρθρου 2 του Ν.3115/2003, η ΑΔΑΕ συγκροτείται από τον Πρόεδρο, τον Αντιπρόεδρο και άλλα πέντε (5) μέλη, καθώς και από αντίστοιχους αναπληρωτές, οι οποίοι πρέπει να διαθέτουν τις αυτές ιδιότητες και προσόντα. Ο Πρόεδρος, ο Αντιπρόεδρος και τα άλλα μέλη της ΑΔΑΕ, καθώς και οι αναπληρωτές τους επιλέγονται από τη Βουλή σύμφωνα με την παράγραφο 2 του άρθρου ιοιΑ του Συντάγματος και την προβλεπόμενη από τον Κανονισμό της Βουλής διαδικασία και διορίζονται με απόφαση του Υπουργού Δικαιοσύνης εντός προθεσμίας δεκαπέντε (15) ημερών από την κοινοποίηση σε αυτόν της απόφασης της Διάσκεψης των Προέδρων της Βουλής. Με την υπ'αριθμ. 125807/30-7-2003 Απόφαση του Υπουργού Δικαιοσύνης (ΦΕΚ Β' 1072/1-8-2003) διορίστηκαν τα μέλη της ΑΔΑΕ ως εξής:

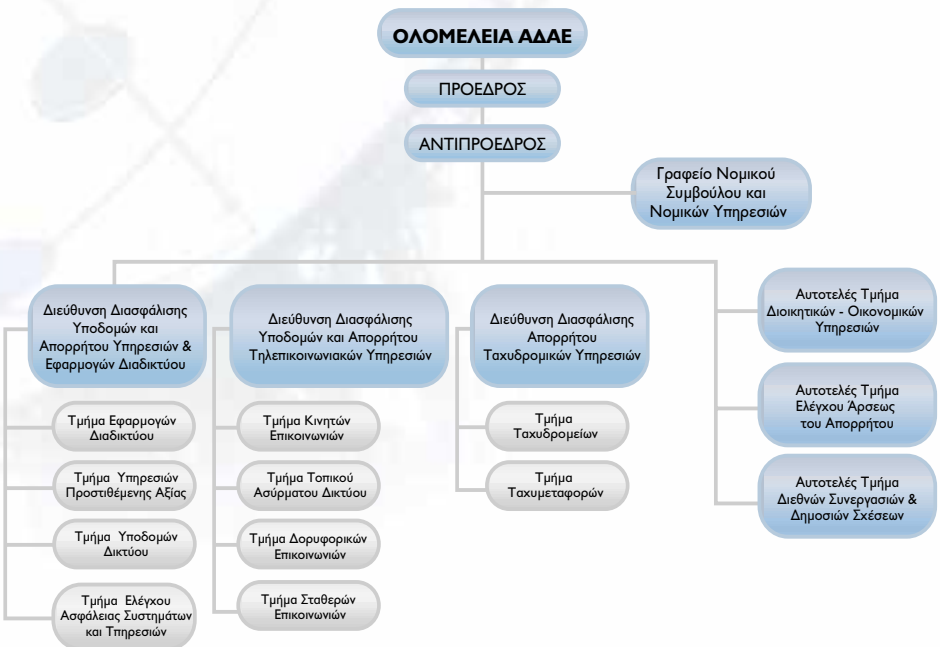
1. **Ανδρέας Λαμπρινόπουλος,** Μηχανολόγος- Ηλεκτρολόγος, ως Πρόεδρος
2. **Βασίλης Κούτρης,** τ. Αναπληρωτής Γενικός Διευθυντής του ΟΤΕ ως Αντιπρόεδρος
3. **Μιχαήλ Καρατζάς,** Αρεοπαγίτης ε.τ. , ως τακτικό μέλος
4. **Χρήστος Καψάλης,** Καθηγητής Ε.Μ.Π., ως τακτικό μέλος
5. **Ιάκωβος Βενιέρης,** Καθηγητής Ε.Μ.Π., ως τακτικό μέλος
6. **Σταύρος Σκοπετέας,** επίτ. Δικηγόρος, ως τακτικό μέλος
7. **Κωνσταντίνος Μαραβέλας,** τ. Διευθυντής του ΟΤΕ, ως τακτικό μέλος

Ως αναπληρωτές διορίστηκαν οι:

1. **Δημήτριος Δεδούσης,** επίτ. Σύμβουλος του Ελεγκτικού Συνεδρίου
2. **Γεώργιος Στασινόπουλος,** Καθηγητής Ε.Μ.Π.
3. **Χρήστος Δουληγέρης,** Αναπληρωτής Καθηγητής του Πανεπιστημίου του Πειραιά
4. **Αικατερίνη Καραμάνου,** επίτ. Δικηγόρος
5. **Κωνσταντίνος Βρεττός,** τ. Διευθυντής του ΟΤΕ

2. Το προσωπικό της ΑΔΑΕ

Για τη στελέχωση της ΑΔΑΕ συστήθηκαν με το Ν.3115/2003 συνολικά σαράντα (40) θέσεις, από τις οποίες οι είκοσι πέντε (25) είναι θέσεις τακτικού προσωπικού, οι δώδεκα (12) θέσεις Ειδικού Επιστημονικού Προσωπικού, οι δύο (2) θέσεις δικηγόρων



παρ'εφέταις με έμμισθη εντολή και μία (1) θέση Νομικού Συμβούλου.

α. Οι είκοσι πέντε (25) θέσεις του τακτικού προσωπικού κατανέμονται κατά κατηγορίες και κλάδους ως εξής:

Πανεπιστημιακής εκπαίδευσης (ΠΕ):
Κλάδος ΠΕ Διοικητικού Οικονομικού, θέσεις τέσσερις (4).

Πανεπιστημιακής εκπαίδευσης (ΠΕ):
Κλάδος ΠΕ Μηχανικών, θέσεις δύο (2).

Πανεπιστημιακής εκπαίδευσης (ΠΕ):
Κλάδος ΠΕ Πληροφορικής, θέσεις δύο (2).

Τεχνολογικής εκπαίδευσης (ΤΕ):
Κλάδος ΤΕ Διοικητικός Λογιστικός, θέσεις τρεις (3),

Κλάδος ΤΕ2 Τεχνολογικών Εφαρμογών,
θέσεις πέντε (5).

Δευτεροβάθμιας εκπαίδευσης (ΔΕ):
Κλάδος ΔΕ, θέσεις έξι (6).

Πρωτοβάθμιας εκπαίδευσης (ΥΕ):
Κλάδος ΥΕ Βοηθητικού Προσωπικού, θέσεις τρεις (3).

β. Οι δώδεκα (12) θέσεις του Ειδικού Επιστημονικού Προσωπικού κατανέμονται ως εξής:

- Δέκα (10) θέσεις διπλωματούχων ηλεκτρολόγων μηχανικών και μηχανικών Η/Υ ή ηλεκτρονικών μηχανικών ή τηλεπικοινωνιακών μηχανικών ή μηχανικών πληροφορικής ή πληροφορικής ή φυσικών και
- Δύο (2) θέσεις πτυχιούχων νομικής, οι οποίες συνεπάγονται την αναστολή άσκησης του δικηγορικού λειτουργήματος.

γ. Οι θέσεις των δικηγόρων με έμμισθη εντολή είναι δύο (2).

δ. Ο Νομικός Σύμβουλος πρέπει να είναι δικηγόρος παρ' Αρείω Πάγω και κάτοχος τουλάχιστον μεταπτυχιακού τίτλου σπουδών σε συναφές με τους σκοπούς της Α.Δ.Α.Ε. αντικείμενο.

Την 31η Δεκεμβρίου 2005 το ανθρώπινο δυναμικό της Α.Δ.Α.Ε. αριθμούσε 28 υπαλλήλους έναντι 8 στο τέλος του 2004, στους οποίους προσμετράται και ένας αποσπασμένος υπάλληλος της ΕΘΕΛ Α.Ε. για την κάλυψη σχετικών αναγκών της Αρχής.

Ειδικότερα, το προσωπικό που υπηρετούσε στην ΑΔΑΕ στο τέλος του 2005 κατανέμεται ως εξής:

α) 16 άτομα Τακτικό Προσωπικό (2 ΠΕ Διοικητικού – Οικονομικού, 5 ΤΕ Τεχνολογικών Εφαρμογών, 3 ΤΕ Διοικητικού – Λογιστικού, 5 ΔΕ Διοικητικού – Λογιστικού, 1 ΔΕ

Οδηγών Αυτοκινήτων) και
β) 11 άτομα Ειδικό Επιστημονικό Προσωπικό (9 διπλωματούχοι ηλεκτρολόγοι μηχανικοί, μηχανικοί Η/Υ ή πτυχιούχοι πληροφορικής και 4 πτυχιούχοι νομικής).

Περαιτέρω, το α΄εξάμηνο του 2006 αναμενόταν να ολοκληρωθεί η διαδικασία πρόσληψης στην ΑΔΑΕ του Νομικού Συμβούλου, ενός δικηγόρου παρ' εφέταις με έμμισθη εντολή και ενός Ειδικού Επιστήμονα για την πλήρωση μιας θέσεως στην Διεύθυνση Διασφάλισης Υποδομών και Απορρήτου Τηλεπικοινωνιακών Υπηρεσιών αλλά και ο διορισμός ενός υπαλλήλου του κλάδου ΥΕ Βοηθητικό Προσωπικό. Με την ολοκλήρωση της προαναφερθείσας διαδικασίας πρόσληψης των παραπάνω υπολείπονται σύμφωνα με τις διατάξεις του Ν. 3115/2003 (ΦΕΚ 47 Α/27.2.2003) οι ακόλουθες 9 θέσεις:
α. Οκτώ (8) θέσεις του τακτικού προσωπικού ως εξής:

Πανεπιστημιακής εκπαίδευσης (ΠΕ):
Κλάδος ΠΕ Διοικητικού Οικονομικού, θέσεις δύο (2).

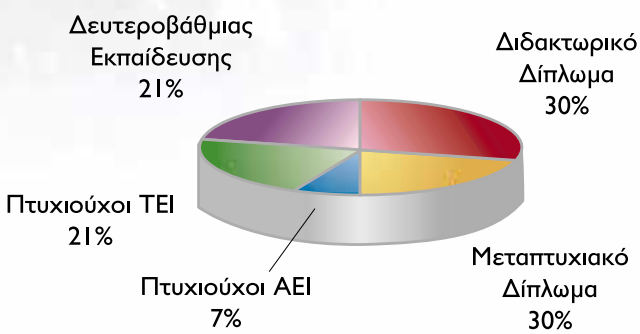
Πανεπιστημιακής εκπαίδευσης (ΠΕ):
Κλάδος ΠΕ Μηχανικών, θέσεις δύο (2).

Πανεπιστημιακής εκπαίδευσης (ΠΕ):
Κλάδος ΠΕ Πληροφορικής, θέσεις δύο (2).
Πρωτοβάθμιας εκπαίδευσης (ΥΕ):
Κλάδος ΥΕ Βοηθητικού Προσωπικού, θέσεις τρεις (2).

β. Μία (1) θέση δικηγόρου με έμμισθη εντολή, στην πλήρωση των οποίων η Α.Δ.Α.Ε. προτίθεται να προχωρήσει ει δυνατόν εντός του 2006.
Παρατήρηση: Με το ν.3472/2006 τροποποιήθηκε η αναλογία ειδικού επιστημονικού προσωπικού και τακτικού προσωπικού.

Τέλος, το μορφωτικό επίπεδο του προσωπικού που υπηρετούσε στην Α.Δ.Α.Ε. στο τέλος του 2005 απεικονίζεται στο ακόλουθο διάγραμμα :

ΜΟΡΦΩΤΙΚΟ ΕΠΙΠΕΔΟ ΠΡΟΣΩΠΙΚΟΥ Α.Δ.Α.Ε.



Γ. ΕΔΡΑ ΤΗΣ ΑΔΑΕ

Η έδρα της Αρχής βρίσκεται στο Μαρούσι Αττικής, επί της οδού Ιερού Λόχου 3.

Δ. ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ ΤΗΣ Α.Δ.Α.Ε.

1. Παρούσα Κατάσταση

Η ιστοσελίδα της Α.Δ.Α.Ε. (www.adae.gr) έχει κατασκευαστεί με την βοήθεια του Πανεπιστημίου Πειραιώς και διαθέτει πλούσιο ηλεκτρονικό και ενημερωτικό υλικό, το οποίο πλέον διαχειρίζεται το προσωπικό της Αρχής και είναι δομημένο ως εξής:

- **Πληροφοριακά στοιχεία για την Α.Δ.Α.Ε. :**
  Τι είναι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, ποιο είναι το θεσμικό πλαίσιο που διέπει την λειτουργία και την εσωτερική της διάρθρωση, ποιο είναι το αντικείμενο και το πεδίο δράσης της.
- Κανονισμοί, σχέδια κανονισμών και προεδρικά διατάγματα σχετικά με την άρση και την διασφάλιση του απορρήτου, όπως και όλα τα θέματα που σχετίζονται με την Α.Δ.Α.Ε., θετικές και αρνητικές γνωμοδοτήσεις και αποφάσεις της Α.Δ.Α.Ε. που πάρθηκαν μετά από σχετικές με το αντικείμενό της αιτήσεις παρόχων.
- Νέα και ανακοινώσεις που αφορούν τους διαγωνισμούς για τη στελέχωση της Α.Δ.Α.Ε., ημερίδες και σεμινάρια εκπαίδευσης και ενημέρωσης του προσωπικού της Αρχής και του ευρύτερου κοινού, όπως και το υλικό των παρουσιάσεων των εν λόγω εκδηλώσεων.
- Χρήσιμοι σύνδεσμοι και επικοινωνία – διάλογος με τους ενδιαφερόμενους για θέματα που εμπίπτουν στις αρμοδιότητες της Α.Δ.Α.Ε.

2. Δικτυακή και Πληροφοριακή Υποδομή της ΑΔΑΕ

Κατά τη διάρκεια του έτους 2005 έγινε αναβάθμιση της δικτυακής και πληροφοριακής υποδομής της ΑΔΑΕ, με έμφαση στην ασφάλεια δικτύων και πληροφοριών. Η σχετική μελέτη πραγματοποιήθηκε από το προσωπικό της Διεύθυνσης Διασφάλισης Υποδομών, Απορρήτου Υπηρεσιών και Εφαρμογών Διαδικτύου και έλαβε υπόψη τις απαιτήσεις που περιγράφονται στην Πολιτική Ασφάλειας της ΑΔΑΕ.

Το δίκτυο προσφέρει στους υπαλλήλους της ΑΔΑΕ υπηρεσίες πρόσβασης στο διαδίκτυο, ηλεκτρονικό ταχυδρομείο με προστασία από κακόβουλο λογισμικό και ενοχλητική αλληλογραφία, δυνατότητα για διαμοιρασμό αρχείων μέσω ενός κεντρικού εξυπηρετητή, ψηφιακά πιστοποιητικά, και ασύρματη κρυπτογραφημένη πρόσβαση στη δικτυακή και πληροφοριακή υποδομή. Επιπρόσθετα προσφέρει παρουσία με δικτυακό τόπο στο διαδίκτυο, καθώς και ασύρματη πρόσβαση στο διαδίκτυο για επισκέπτες χωρίς να επιτρέπεται η πρόσβαση στο εσωτερικό δίκτυο.

Τα επιθυμητά επίπεδα ασφάλειας επιτυγχάνονται με το διαμοιρασμό του δικτύου σε κατάλληλα διαμορφωμένες ζώνες μέσω ενός συστήματος προστασίας firewall. Παράλληλα, γίνεται χρήση ενός συστήματος ανίχνευσης εισβολών (IDS).

Το προσωπικό της ΑΔΑΕ έχει καταγράψει σε τεχνικά εγχειρίδια τη διαμόρφωση των

δικτυακών και πληροφοριακών συστημάτων που έχουν εγκατασταθεί, και είναι υπεύθυνο για τη διαχείριση και τον έλεγχο αυτών, σύμφωνα με τους ρόλους που ορίζει η Πολιτική Ασφάλειας της ΑΔΑΕ.

Για τη διασύνδεση με το Διαδίκτυο, η γραμμή ISDN στα 128Kbps αναβαθμίστηκε σε δύο (2) γραμμές ADSL των 1024Kbps η κάθε μία, στις οποίες πραγματοποιείται διαμοιρασμός φορτίου (load balancing).

3. Πολιτική Ασφάλειας της ΑΔΑΕ

Το προσωπικό των τεχνικών διευθύνσεων της ΑΔΑΕ, κατά τη διάρκεια του έτους 2005, ανέπτυξε και υλοποίησε μια ολοκληρωμένη Πολιτική Ασφάλειας για τη πληροφοριακή και δικτυακή υποδομή της ΑΔΑΕ, με σκοπό να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των αποθηκευμένων πληροφοριών όπως επίσης και των πληροφοριών που ανταλλάσσονται με οντότητες εκτός της Αρχής.

Η γενική Πολιτική Ασφάλειας καθορίζει τις επιμέρους πολιτικές, τις σχετικές διαδικασίες και τους ρόλους και αρμοδιότητες αυτών. Οι επιμέρους Πολιτικές είναι επιγραμματικά οι εξής:

- Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας
- Πολιτική Προστασίας Πληροφορίας
- Πολιτική Διαχείρισης Περιστατικών Ασφάλειας
- Πολιτική Παρακολούθησης και Ελέγχου Ασφάλειας
- Πολιτική Ασφάλειας Διαδικτύου και Ηλεκτρονικού Ταχυδρομείου
- Πολιτική Κρυπτογράφησης
- Πολιτική Πρόσβασης και Αποδεκτής Χρήσης
- Πολιτική Ασφάλειας Δικτύων και Συστημάτων
- Πολιτική Προστασίας από Κακόβουλο Λογισμικό
- Πολιτική Διαχείρισης Επιχειρηματικής Συνέχειας.

Το site της Α.Δ.Α.Ε.

ΚΕΦΑΛΑΙΟ ΙΙ.
ΑΠΟΛΟΓΙΣΜΟΣ ΤΟΥ ΕΡΓΟΥ ΤΗΣ ΑΔΑΕ ΚΑΤΑ ΤΟ ΕΤΟΣ 2005

ΚΕΦΑΛΑΙΟ ΙΙ.
ΑΠΟΛΟΓΙΣΜΟΣ ΤΟΥ ΕΡΓΟΥ ΤΗΣ ΑΔΑΕ ΚΑΤΑ ΤΟ ΕΤΟΣ 2005

Α. Άσκηση της Κανονιστικής Αρμοδιότητας της ΑΔΑΕ

Άσκηση Κανονιστικης Αρμοδιότητας

Κανονισμός για τη Διασφάλιση του Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών	ΦΕΚ Β' 87/26-1-2005
Κανονισμός για τη Διασφάλιση του Απορρήτου κατά την Παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών	
Κανονισμός για τη Διασφάλιση του Απορρήτου κατά την Παροχή Ασύρματων Τηλεπικοινωνιακών Υπηρεσιών	
Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές	ΦΕΚ Β' 88/26-1-2005
Κανονισμός για τη Διασφάλιση του Απορρήτου Διαδικτυακών Εφαρμογών	
Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και χρήστη Διαδικτύου	
Κανονισμός για τη Διασφάλιση του Απορρήτου κατά τη χρήση Αυτόματων Ταμειολογιστικών Μηχανών	ΦΕΚ Β' 298/8-3-2005
Κανονισμός για τη Διασφάλιση του Απορρήτου των Ταχυδρομικών Υπηρεσιών	ΦΕΚ Β' 384/24-3-2005

1. Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών (Απόφαση ΑΔΑΕ 629α, ΦΕΚ Β' 87/26-1-2005)

Σκοπός του Κανονισμού είναι:

- Η θέσπιση των υποχρεώσεων των φορέων παροχής κινητών τηλεπικοινωνιακών υπηρεσιών για τη διασφάλιση του απορρήτου των κινητών τηλεπικοινωνιακών υπηρεσιών στο πλαίσιο της σχετικής νομοθεσίας (Ν. 2225/94 «Περί προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Ν. 3115/03 "Περί

Διασφάλισης του Απορρήτου των Επικοινωνιών").

- Η παρουσίαση βασικών χαρακτηριστικών ασφαλείας των τεχνολογιών κινητών επικοινωνιών δεύτερης και τρίτης γενιάς.
- Η θέσπιση διαδικασιών ελέγχου στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του εν λόγω Κανονισμού υπάγονται όλοι οι τηλεπικοινωνιακοί οργανισμοί οι οποίοι παρέχουν Κινητές Τηλεπικοινωνιακές Υπηρεσίες.

Ο Κανονισμός καθορίζει ως πρωταρχικό στοιχείο για τη διασφάλιση του απορρήτου των κινητών επικοινωνιών την ύπαρξη στους παρόχους Πολιτικής Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΚΤΥ), που αποτελεί το σύνολο των κριτηρίων και κανόνων που καθορίζουν τις απαιτήσεις, τις υποχρεώσεις και τα δικαιώματα που διέπουν τη λειτουργία των τηλεπικοινωνιακών παρόχων, το προσωπικό τους, τους συνεργάτες τους και των χρηστών των τηλεπικοινωνιακών υπηρεσιών, με σκοπό την προστασία του απορρήτου των επικοινωνιών που διεξάγονται μέσω δικτύων κινητών επικοινωνιών και του απορρήτου των ευαίσθητων προσωπικών δεδομένων των χρηστών των κινητών τηλεπικοινωνιακών υπηρεσιών.

Η ΠΔΑΚΤΥ αποτελείται από επί μέρους πολιτικές όπως είναι η Πολιτική Προστασίας των Δικτύων Κινητών Επικοινωνιών, η Πολιτική επεξεργασίας Δεδομένων Επικοινωνίας, η Πολιτική σε σχέση με το Προσωπικό και τους Συνεργάτες των Τηλεπικοινωνιακών Παρόχων, η Πολιτική Πρόσβασης, η Πολιτική Αποδεκτής Χρήσης και η Πολιτική Άρσης του Απορρήτου από τις οποίες απορρέουν τα δικαιώματα και οι υποχρεώσεις των εμπλεκομένων στη λειτουργία, τη διαχείριση και τη χρήση των τηλεπικοινωνιακών υπηρεσιών.

Στη συνέχεια αναφέρονται χαρακτηριστικά τεχνικά στοιχεία ασφαλείας για τις τεχνολογίες κινητών επικοινωνιών 2ης και 3ης γενιάς, τα ευάλωτα σημεία των τεχνολογιών αυτών καθώς και οι πληροφορίες που πρέπει να προστατεύονται.

Στον Κανονισμό αναλύονται οι υποχρεώσεις των παρόχων αναφορικά με την ΠΔΑΚΤΥ Ασφάλειας. Επιπρόσθετα καθορίζεται η διαδικασία ελέγχου και η άσκηση εποπτείας από την ΑΔΑΕ.

Το πλήρες κείμενο του ως άνω Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

2. Κανονισμός για την Διασφάλιση Απορρήτου κατά την Παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών (Απόφαση ΑΔΑΕ 630α, ΦΕΚ Β' 87/26-1-2005)

Σκοπός του Κανονισμού είναι:

- Η θέσπιση των υποχρεώσεων παρόχων σταθερών τηλεπικοινωνιακών υπηρεσιών για τη διασφάλιση του απορρήτου των κινητών τηλεπικοινωνιακών υπηρεσιών στο πλαίσιο της σχετικής νομοθεσίας (Ν. 2225/94 «Περί προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Ν. 3115/03 "Περί Διασφάλισης του Απορρήτου των Επικοινωνιών").
- Ο καθορισμός της διαδικασίας ελέγχου στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του εν λόγω Κανονισμού υπάγονται όλοι οι τηλεπικοινωνιακοί οργανισμοί οι οποίοι παρέχουν Σταθερές Τηλεπικοινωνιακές Υπηρεσίες.

Ο Κανονισμός καθορίζει ως πρωταρχικό στοιχείο για τη διασφάλιση του απορρήτου των κινητών επικοινωνιών την ύπαρξη στους παρόχους Πολιτικής Διασφάλισης του Απορρήτου των Σταθερών Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΣΤΥ), που αποτελεί το σύνολο των κριτηρίων και κανόνων που καθορίζουν τις απαιτήσεις, τις υποχρεώσεις και τα δικαιώματα που διέπουν τη λειτουργία των τηλεπικοινωνιακών παρόχων, το προσωπικό τους, τους συνεργάτες τους και των χρηστών των τηλεπικοινωνιακών υπηρεσιών, με σκοπό την προστασία του απορρήτου της τηλεπικοινωνίας μέσω σταθερών δικτύων και του απορρήτου των ευαίσθητων προσωπικών δεδομένων των χρηστών των σταθερών τηλεπικοινωνιακών υπηρεσιών.

Η ΠΔΑΣΤΥ αποτελείται από επί μέρους πολιτικές όπως είναι η Πολιτική Προστασίας των Σταθερών Τηλεπικοινωνιακών Δικτύων, η Πολιτική Επεξεργασίας Δεδομένων Επικοινωνίας, η Πολιτική σε σχέση με το Προσωπικό και τους Συνεργάτες των Τηλεπικοινωνιακών Παρόχων, η Πολιτική Πρόσβασης, η Πολιτική Αποδεκτής Χρήσης και η Πολιτική Άρσης του Απορρήτου, από τις οποίες απορρέουν τα δικαιώματα και οι υποχρεώσεις των εμπλεκομένων στη λειτουργία, τη διαχείριση και τη χρήση των σταθερών τηλεπικοινωνιακών υπηρεσιών.

Στη συνέχεια αναφέρονται χαρακτηριστικά τεχνικά στοιχεία ασφαλείας για τις τεχνολογίες σταθερών επικοινωνιών (σταθερή τηλεφωνία), τα ευάλωτα σημεία των τεχνολογιών αυτών, καθώς και οι πληροφορίες που πρέπει να προστατεύονται.

Στον Κανονισμό αναλύονται επιπλέον οι υποχρεώσεις των παρόχων αναφορικά με την ΠΔΑΣΤΥ Ασφάλειας. Επιπρόσθετα καθορίζεται η διαδικασία ελέγχου και η άσκηση εποπτείας από την ΑΔΑΕ.
Το πλήρες κείμενο του ως άνω Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

3. Κανονισμός για την Διασφάλιση Απορρήτου κατά την Παροχή Ασυρμάτων Τηλεπικοινωνιακών Υπηρεσιών (Απόφαση ΑΔΑΕ 631α , ΦΕΚ Β' 87/26-1-2005)

Σκοπός του Κανονισμού είναι:

- Η θέσπιση των υποχρεώσεων των φορέων παροχής κινητών τηλεπικοινωνιακών υπηρεσιών για τη διασφάλιση του απορρήτου των ασυρμάτων τηλεπικοινωνιακών υπηρεσιών στο πλαίσιο της σχετικής νομοθεσίας (Ν. 2225/94 «Περί προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Ν. 3115/03 "Περί Διασφάλισης του Απορρήτου των Επικοινωνιών").
- Η παρουσίαση βασικών χαρακτηριστικών ασφαλείας των τεχνολογιών ασυρμάτων δικτύων.
- Η θέσπιση διαδικασιών ελέγχου στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του εν λόγω Κανονισμού υπάγονται όλοι οι τηλεπικοινωνιακοί οργανισμοί οι οποίοι παρέχουν Ασύρματες Τηλεπικοινωνιακές Υπηρεσίες.

Ο Κανονισμός καθορίζει ως πρωταρχικό στοιχείο για τη διασφάλιση του απορρήτου των κινητών επικοινωνιών την ύπαρξη στους παρόχους Πολιτικής Διασφάλισης του Απορρήτου των Ασυρμάτων Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΑΤΥ), που αποτελεί το σύνολο των κριτηρίων και κανόνων που καθορίζουν τις απαιτήσεις, τις υποχρεώσεις και τα δικαιώματα που διέπουν τη λειτουργία των τηλεπικοινωνιακών παρόχων, το προσωπικό τους, τους συνεργάτες τους και των χρηστών των τηλεπικοινωνιακών υπηρεσιών, με σκοπό την προστασία του απορρήτου της τηλεπικοινωνίας μέσω σταθερών δικτύων και του απορρήτου των ευαίσθητων προσωπικών δεδομένων των χρηστών των σταθερών τηλεπικοινωνιακών υπηρεσιών.

Η ΠΔΑΑΤΥ αποτελείται από επί μέρους πολιτικές όπως είναι η Πολιτική Προστασίας των Ασυρμάτων Τηλεπικοινωνιακών Δικτύων, η Πολιτική Επεξεργασίας Δεδομένων Επικοινωνίας, η Πολιτική σε σχέση με το Προσωπικό και τους Συνεργάτες των Τηλεπικοινωνιακών Παρόχων, η Πολιτική Πρόσβασης, η Πολιτική Αποδεκτής Χρήσης και η Πολιτική Άρσης του Απορρήτου, από τις οποίες απορρέουν τα δικαιώματα και οι υποχρεώσεις των εμπλεκομένων στη λειτουργία, τη διαχείριση και τη χρήση των ασυρμάτων τηλεπικοινωνιακών υπηρεσιών.

Στη συνέχεια αναφέρονται χαρακτηριστικά τεχνικά στοιχεία ασφαλείας για τις τεχνολογίες ασυρμάτων επικοινωνιών (Τεχνολογία Bluetooth, Ασύρματα Τοπικά Δίκτυα IEEE 802.11, Δίκτυα Σταθερής Ασύρματης Πρόσβασης, Δορυφορικά Δίκτυα Επικοινωνιών), τα ευάλωτα σημεία των τεχνολογιών αυτών, καθώς και οι πληροφορίες που πρέπει να προστατεύονται.

Στον Κανονισμό αναλύονται επιπλέον οι υποχρεώσεις των παρόχων αναφορικά με την ΠΔΑΑΤΥ Ασφάλειας. Επιπρόσθετα καθορίζεται η διαδικασία ελέγχου και η άσκηση εποπτείας από την ΑΔΑΕ.
Τέλος, στο Παράρτημα Α, ο Κανονισμός παραθέτει την αναλυτική περιγραφή διαδικασίας ελέγχου παρόχου, ενώ στο Παράρτημα Β περιγράφεται το Ελάχιστο περιεχόμενο του εντύπου με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Τηλεπικοινωνιακό Πάροχο αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Ασυρμάτων Τηλεπικοινωνιακών Υπηρεσιών».
Το πλήρες κείμενο του ως άνω Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

Στους τρεις παραπάνω Κανονισμούς για τη Διασφάλιση του Απορρήτου κατά την Παροχή Τηλεπικοινωνιακών Υπηρεσιών, περιγράφονται τρόποι με τους οποίους ο τηλεπικοινωνιακός πάροχος κατά τη χάραξη της πολιτικής του μπορεί:

- Να προσδιορίσει τις πληροφορίες που πρέπει να προστατευτούν.
- Να προσδιορίσει τα ευάλωτα σημεία του τηλεπικοινωνιακού δικτύου.
- Να προσδιορίσει τους κινδύνους και τις απειλές .
- Να προσδιορίσει τα μέτρα διασφάλισης της προστασίας του απορρήτου στις Τηλεπικοινωνιακές Υπηρεσίες που παρέχει.
- Να καθορίσει τις υποχρεώσεις των υπαλλήλων και συνεργατών του.
- Να καθορίσει τις δεσμεύσεις και υποχρεώσεις του έναντι των πελατών του.

- Να καταρτίσει σχέδιο αναθεώρησης και βελτίωσης των επιμέρους πολιτικών κάθε φορά που θα εντοπίζεται νέος κίνδυνος ή αδυναμία ή που θα προκύπτουν νέες τεχνολογικές διευκολύνσεις διαχείρισης ασφάλειας.
- Κάθε τηλεπικοινωνιακός πάροχος πρέπει να τεκμηριώνει με σχέδια την προστασία του απορρήτου για να αντιμετωπίσει προβλήματα που πιθανώς να εμφανισθούν σε έκτακτες περιστάσεις, όπως είναι η άρση του απορρήτου μετά από εντολή δικαστικών ή εισαγγελικών αρχών και η προβληματική λειτουργία των τηλεπικοινωνιακών ή/και των μηχανογραφικών συστημάτων του ή των συστημάτων των συνεργατών του.
- Εφόσον ο πάροχος διαθέτει γενικότερη πολιτική ασφάλειας πληροφοριών και πληροφοριακών συστημάτων (π.χ. η γενικότερη πολιτική ασφάλειας μπορεί να αφορά πρόσβαση σε φυσικούς χώρους όπως κτίρια, δωμάτια, κτλ στα οποία αποθηκεύονται στοιχεία συνδρομητών), θα πρέπει να ενσωματώνει σε αυτήν τη γενικότερη πολιτική και την πολιτική διασφάλισης του απορρήτου που αποτελεί αντικείμενο των εν λόγω Κανονισμών.

Επιπλέον, η κάθε επιμέρους Πολιτική Διασφάλισης Απορρήτου Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΚΤΥ, ΠΔΑΣΤΥ και ΠΔΑΑΤΥ) για να θεωρείται επαρκής θα πρέπει να διαθέτει τουλάχιστον τα ακόλουθα χαρακτηριστικά:

1. Να υλοποιείται μέσω διαδικασιών διαχείρισης συστημάτων, δημοσιοποίησης οδηγιών αποδεκτής χρήσης ή άλλων αντίστοιχων κατάλληλων μεθόδων.
2. Οι διαδικασίες, οι οποίες σχετίζονται με την υλοποίηση της πολιτικής, πρέπει να περιλαμβάνουν τουλάχιστον τον προσδιορισμό ταυτότητας, την αυθεντικότητα, την εξουσιοδότηση, τον έλεγχο πρόσβασης, την εμπιστευτικότητα, την ακεραιότητα, την προστασία του απορρήτου, και τον έλεγχο παραβίασης του απορρήτου.
3. Να εφαρμόζεται μέσω εργαλείων ασφάλειας, ή όταν αυτό δεν είναι εφικτό, με την εφαρμογή αυστηρών κυρώσεων που θα έχουν αποτρεπτικό χαρακτήρα.
4. Να καθορίζει τα όρια ευθύνης των χρηστών, του προσωπικού, των συνεργατών και της διοίκησης του παρόχου. Επιπλέον οι μηχανισμοί μεταβολής της πολιτικής διασφάλισης του απορρήτου πρέπει να είναι καλά ορισμένοι, περιλαμβάνοντας τη διαδικασία, τους εμπλεκόμενους, καθώς και τους υπεύθυνους προς έγκριση.
5. Επίσης, συνιστάται:
   α) Να είναι ανεξάρτητη, στο μέτρο που είναι δυνατόν από τεχνικής απόψεως, από συγκεκριμένο εξοπλισμό (υλικό, λογισμικό) και
   β) Να βασίζεται σε μια ανοικτή αρχιτεκτονική ώστε να καθίσταται βιώσιμη μακροπρόθεσμα.

4. Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές (Απόφαση ΑΔΑΕ 632α, ΦΕΚ Β'88/26-1-2005)

Σκοπός του Κανονισμού είναι:

- Η διασφάλιση του απορρήτου των διαδικτυακών επικοινωνιών.
- Η ασφάλεια των διαδικτυακών τηλεπικοινωνιακών φορέων και Δημοσίων οργανισμών.

- Η θέσπιση των υποχρεώσεων των εν λόγω φορέων αναφορικά με την ασφάλεια και το απόρρητο των επικοινωνιών.
- Ο έλεγχος στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:

- Πάροχοι πρόσβασης στο διαδίκτυο (σταθεροί και κινητοί τηλεπικοινωνιακοί πάροχοι κλπ.)
- Πάροχοι διαδικτυακών υπηρεσιών
- Πάροχοι διαδικτυακών υπηρεσιών προστιθέμενης αξίας

Ο Κανονισμός καθορίζει ως πρωταρχικό στοιχείο για τη διασφάλιση του απορρήτου των επικοινωνιών στο διαδίκτυο την ύπαρξη στους παρόχους Πολιτικής Ασφάλειας. Η Πολιτική Ασφάλειας ορίζεται ως το «σύνολο των τεχνικών, οργανωτικών και κανονιστικών μέτρων, τα οποία εφαρμόζονται από πάροχο διαδικτυακών επικοινωνιών και αποβλέπουν στη διασφάλιση του απορρήτου και γενικά στην ασφαλή λειτουργία των δικτύων διαδικτυακών επικοινωνιών».

Σύμφωνα με τον Κανονισμό, αναπόσπαστο μέρος της Πολιτικής Ασφάλειας αποτελούν η Πολιτική Πρόσβασης και η Πολιτική Αποδεκτής Χρήσης. Η Πολιτική Πρόσβασης (access policy) καθορίζει το επίπεδο πρόσβασης χρηστών και χρηστών παρόχου, καθώς και των εργαλείων λογισμικού εποπτείας σε καθένα από τα συστήματα υλικού και λογισμικού από τα οποία αποτελείται ο εξοπλισμός του παρόχου. Η Πολιτική Αποδεκτής Χρήσης (Acceptable or Appropriate Use Policy) περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών και των χρηστών παρόχου των υπολογιστικών και τηλεπικοινωνιακών συστημάτων ενός παρόχου.

Περαιτέρω, ο Κανονισμός αναφέρεται στο απόρρητο των επικοινωνιών, και ειδικότερα αναφέρει ότι οι επικοινωνίες αυτές καλύπτουν τις πληροφορίες και τα δεδομένα τα οποία διακινούνται πάνω σε δημόσια δίκτυα επικοινωνιών και εξυπηρετούνται από τις αντίστοιχες υπηρεσίες επικοινωνιών. Συγκεκριμένα, απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των πληροφοριών και δεδομένων από άλλα πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια.

Στον Κανονισμό αναλύονται οι υποχρεώσεις των παρόχων αναφορικά με την Πολιτική Ασφάλειας. **Πιο συγκεκριμένα, οι πάροχοι υποχρεούνται:**

- Να διαθέτουν ανά πάσα στιγμή καθορισμένη Πολιτική Ασφάλειας για τη διασφάλιση του απορρήτου διαδικτυακών επικοινωνιών.
- Να εφαρμόζουν την εν λόγω πολιτική.

Επιπρόσθετα καθορίζεται η διαδικασία ελέγχου και η άσκηση εποπτείας από την ΑΔΑΕ. Πιο συγκεκριμένα, η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε πάροχο που εμπίπτει στις διατάξεις του Κανονισμού. Επίσης, στο πλαίσιο της άσκησης εποπτείας, κάθε πάροχος στο τέλος του ημερολογιακού έτους υποβάλλει στην ΑΔΑΕ ετήσια έκθεση με στοιχεία που αφορούν στην ασφάλεια των διαδικτυακών επικοινωνιών και τη διασφάλιση του απορρήτου.

Το πλήρες κείμενο του ως άνω Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

5. Κανονισμός για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών (Απόφαση ΑΔΑΕ 633α , ΦΕΚ Β' 88/26-1-2005)

Σκοπός του Κανονισμού είναι:

- Η ασφάλεια των Διαδικτυακών υποδομών των παρόχων και η διασφάλιση του απορρήτου αυτών.
- Η θέσπιση των υποχρεώσεων των εν λόγω παρόχων αναφορικά με την ασφάλεια και το απόρρητο των Διαδικτυακών τους υποδομών.
- Ο έλεγχος στους εν λόγω παρόχους σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του εν λόγω Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Πάροχοι Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:

- Πάροχοι σταθερής και κινητής πρόσβασης στο διαδίκτυο
- Πάροχοι Διαδικτυακών υπηρεσιών, υπηρεσιών προστιθέμενης αξίας και υπηρεσιών εφαρμογών.

Ο Κανονισμός αυτός αναφέρει μια σειρά από πολιτικές και διαδικασίες ασφαλείας καθώς και τη διαδικασία ελέγχου και εποπτείας που ασκείται από την ΑΔΑΕ και η οποία περιγράφεται λεπτομερειακά στον Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές.

Η Πολιτική Ασφάλειας Περιμέτρου έχει ως σκοπό να προστατεύσει τους διάφορους δικτυακούς πόρους του παρόχου διαδικτύου από εισβολείς, δηλαδή να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του παρόχου διαδικτύου (σε υλικό ή λογισμικό), καθώς και τη διακοπή της ομαλής παροχής των υπηρεσιών του παρόχου διαδικτύου.

Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού εξασφαλίζει ότι τυχόν αλλαγές στον υπάρχοντα εξοπλισμό καθώς και η εισαγωγή καινούργιου εξοπλισμού στη λειτουργία του παρόχου διαδικτύου γίνεται κατά τέτοιο τρόπο ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών και να μην παραβιάζεται η Πολιτική Ασφάλειας του παρόχου διαδικτύου.

Η Πολιτική Αντιγράφων Ασφαλείας περιλαμβάνει τις διαδικασίες και τους ελέγχους που θα εξασφαλίσουν ότι ο τηλεπικοινωνιακός εξοπλισμός μπορεί να ανακτήσει τη λειτουργία εντός μιας λογικής χρονικής περιόδου μετά από οποιαδήποτε ζημιά που μπορεί να οφείλεται σε κακόβουλες επιθέσεις στο δικτυακό εξοπλισμό.

Η Διαδικασία Χειρισμού Περιστατικών Ασφαλείας έχει ως στόχους να καταγραφούν όλες οι λεπτομέρειες του περιστατικού, να ενημερωθούν οι αρμόδιοι και οι χρήστες, να διασφαλιστεί το δυνατόν συντομότερο το απόρρητο, και να διερευνηθούν τα αίτια και να βρεθούν τα πιθανά σφάλματα του παρόχου διαδικτύου ή και άλλων προσώπων.

Η Διαδικασία Ελέγχου Ασφάλειας Δικτύου πραγματοποιείται με σκοπό να εξακριβώσει ότι διασφαλίζεται η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα πληροφοριών και πόρων.

Η Διαδικασία Αποτίμησης Κινδύνων έχει ως στόχο να βοηθήσει τον πάροχο διαδικτύου να επιλέξει τις διαδικασίες και πρακτικές που ελαχιστοποιούν την πιθανότητα παραβίασης του απορρήτου επικοινωνιών των χρηστών καθώς και το κόστος εφαρμογής τους.

Το πλήρες κείμενο του ως άνω Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

6. Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου (Απόφαση ΑΔΑΕ 634α, ΦΕΚ Β' 88/26-1-2005)

Σκοπός του Κανονισμού είναι:

- Η διασφάλιση του απορρήτου των εφαρμογών στο διαδίκτυο και των χρηστών τους.
- Η ασφάλεια των παρόχων υπηρεσίας εφαρμογής ως προς τις προσφερόμενες υπηρεσίες και εφαρμογές.
- Η θέσπιση των υποχρεώσεων των εν λόγω παρόχων αναφορικά με την ασφάλεια και το απόρρητο των εφαρμογών Διαδικτύου και των χρηστών.
- Ο έλεγχος στους εν λόγω παρόχους σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:

- Πάροχοι σταθερής και κινητής πρόσβασης στο διαδίκτυο.
- Πάροχοι Διαδικτυακών υπηρεσιών, υπηρεσιών προστιθέμενης αξίας και υπηρεσίας εφαρμογών.

Ο Κανονισμός αναφέρει επιμέρους πολιτικές που σχετίζονται με τη διασφάλιση του απορρήτου εφαρμογών και χρηστών Διαδικτύου, και συνοδεύουν την Πολιτική Ασφάλειας, όπως αυτή ορίζεται στον Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές.

Η Πολιτική Ασφάλειας Χρήστη Διαδικτύου έχει ως σκοπό να ορίσει τους κανόνες και τις απαιτήσεις ασφάλειας για τη χρήση του Διαδικτύου ως ασφαλές μέσο για τη μετάδοση ευαίσθητων πληροφοριών και να διασφαλίσει την χρήση του.

Η Πολιτική Ορθής (Δεοντολογικής) Συμπεριφοράς Χρήστη περιλαμβάνει την πολιτική ορθής συμπεριφοράς παρόχων και την πολιτική ορθής συμπεριφοράς χρηστών.

Η Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων καθορίζει ότι οι πάροχοι διαδικτύου οφείλουν να εφαρμόζουν αλγόριθμους και τεχνικές κρυπτογράφησης τόσο στα συστήματα μετάδοσης δεδομένων που χρησιμοποιούν, όσο και στις εφαρμογές και τις υπηρεσίες του Διαδικτύου που παρέχουν, με σκοπό να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η μη-αποποίηση ευθύνης στις συναλλαγές και τις επικοινωνίες μέσω Διαδικτύου, τα οποία και αποτελούν αναπόσπαστα στοιχεία της ιδιωτικότητας του χρήστη.

Η Πολιτική Χρήσης Κωδικών Ασφάλειας (Passwords) καθορίζει την αναγκαιότητα εφαρμογής μιας πολιτικής δημιουργίας και διαχείρισης κωδικών ασφάλειας σε έναν πάροχο διαδικτύου και παραθέτει τα βασικά χαρακτηριστικά δημιουργίας και διαχείρισης κωδικών ασφάλειας. Επίσης καθορίζει τη δημιουργία και διαχείριση κωδικών

ασφάλειας αναφορικά με την πρόσβαση από απόσταση (μέσω Διαδικτύου) σε εφαρμογές, καθώς και την προστασία των κωδικών ασφάλειας.

Η Πολιτική Προστασίας και Αποτροπής Ιών (Anti-virus Policy) περιγράφει τις διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης ιών, που απαιτούνται προκειμένου να εξασφαλίζεται στο μέγιστο δυνατό βαθμό η προστασία του συνόλου του δικτύου του παρόχου διαδικτύου και των χρηστών του από ιούς.

Η Πολιτική Ασφάλειας Παρόχου Υπηρεσίας Εφαρμογής ορίζει το σύνολο των εγγυήσεων που οφείλει να λαμβάνει ο πάροχος διαδικτύου από τον πάροχο υπηρεσίας εφαρμογής, προκειμένου να εξασφαλιστεί το απόρρητο των επικοινωνιών των χρηστών. Η πολιτική αυτή ισχύει σε περίπτωση που ο πάροχος διαδικτύου και ο πάροχος υπηρεσίας εφαρμογής έχουν συμβατική σχέση, ανεξαρτήτως της τοποθεσίας όπου φιλοξενείται η υποδομή που υποστηρίζει τις εν λόγω υπηρεσίες και εφαρμογές.

Τέλος, καθορίζεται η διαδικασία ελέγχου και η άσκηση εποπτείας από την ΑΔΑΕ.

Το πλήρες κείμενο του ως άνω Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

7. Κανονισμός για τη Διασφάλιση του Απορρήτου κατά τη χρήση Αυτόματων Ταμειολογιστικών Μηχανών (Απόφαση ΑΔΑΕ 969, ΦΕΚ Β' 298/8-3-2005)

Σκοπός του Κανονισμού είναι ο καθορισμός ενός ελάχιστου επιπέδου προστασίας του απορρήτου των επικοινωνιών κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών από το κοινό, με τη θέσπιση υποχρεώσεων για κάθε πιστωτικό ίδρυμα ή άλλο φυσικό ή νομικό πρόσωπο, το οποίο, σύμφωνα με την κείμενη νομοθεσία, παρέχει στο κοινό υπηρεσίες διενέργειας συναλλαγών μέσω αυτόματων ταμειολογιστικών μηχανών.

Στο πλαίσιο αυτό, κάθε υπόχρεος Φορέας εντός του πρώτου τριμήνου εκάστοτε ημερολογιακού έτους, καλείται να υποβάλει στην Α.Δ.Α.Ε. Ετήσια Έκθεση, η οποία αφορά στο προηγούμενο έτος, με στοιχεία που σχετίζονται με την διασφάλιση του απορρήτου των επικοινωνιών κατά τη χρήση των αυτόματων ταμειολογιστικών μηχανών.

Το ελάχιστο περιεχόμενο της Ετήσιας Έκθεσης ορίζεται ως εξής:

1. Περιστατικά που απείλησαν την ασφάλεια του απορρήτου των επικοινωνιών κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών.
2. Εκτίμηση της ζημιάς που υπέστη ο Υπόχρεος Φορέας εξαιτίας αυτών των περιστατικών.
3. Εκτίμηση της ζημιάς που υπέστησαν οι χρήστες των μηχανών εξαιτίας αυτών των περιστατικών
4. Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών από τον Υπόχρεο Φορέα.
5. Ο Προγραμματισμός Επιβολής Μέτρων Προστασίας.

Ο Προγραμματισμός Επιβολής Μέτρων Προστασίας περιλαμβάνει το σύνολο των μέτρων που λαμβάνουν οι υπόχρεοι φορείς με σκοπό την ενημέρωση και προστασία των χρηστών αλλά και την προστασία, αναβάθμιση και κατηγοριοποίηση των Αυτόματων Ταμειολογιστικών Μηχανών.

Η ενημέρωση του χρήστη επιτυγχάνεται, με την εκτέλεση από το φορέα κάθε απα-

ραίτητης ενέργειας (π.χ. ενημέρωση με ανακοινώσεις αναρτημένες απευθείας πάνω στις ταμειολογιστικές μηχανές, ενημερωτικά φυλλάδια, μέσω διαδικτύου, μέσω του περιοδικού ή ημερήσιου τύπου, ή άλλων μέσων) για τη σαφή και έγκυρη ενημέρωση των χρηστών.

Η προστασία του χρήστη, επιτυγχάνεται, μεταξύ άλλων, περιορίζοντας στο ελάχιστο τους κινδύνους παρατήρησης και καταγραφής από τρίτους του αριθμού και του κωδικού πρόσβασης της κάρτας του χρήστη.

Η προστασία και αναβάθμιση των αυτόματων ταμειολογιστικών μηχανών επιτυγχάνεται κυρίως με τη λήψη προληπτικών μέτρων από τους υπόχρεους φορείς, η οποία στοχεύει

- στη φυσική προστασία των μηχανών από κάθε είδους ενέργεια η οποία ενδέχεται να απειλήσει το απόρρητο της επικοινωνίας κατά τη χρήση αυτών,
- στο υλικό (hardware) των χρησιμοποιούμενων για την παροχή των υπηρεσιών τους αυτόματων ταμειολογιστικών μηχανών, ώστε να συμβάλλει στην διασφάλιση του απορρήτου της επικοινωνίας κατά τη χρήση αυτών,
- στο λογισμικό (software) των χρησιμοποιούμενων για την παροχή των υπηρεσιών τους αυτόματων ταμειολογιστικών μηχανών ώστε, να αναβαθμίζεται και να συμβάλλει στη διασφάλιση του απορρήτου της επικοινωνίας κατά τη χρήση αυτών καθώς και στην έγκαιρη διαπίστωση περιστατικών παραβίασης του απορρήτου,
- στην κατηγοριοποίηση των χρησιμοποιούμενων αυτόματων ταμειολογιστικών μηχανών με βάση την πιθανότητα παραβίασης του απορρήτου κατά τη χρήση αυτών.

Η διαδικασία ελέγχου και άσκησης εποπτείας από την ΑΔΑΕ περιγράφονται αναλυτικά στο κείμενο του Κανονισμού.
Το πλήρες κείμενο του Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

8. Κανονισμός για τη Διασφάλιση του Απορρήτου των Ταχυδρομικών Υπηρεσιών (Απόφαση ΑΔΑΕ 1001, ΦΕΚ Β' 384/24-3-2005)

Η ΑΔΑΕ, στο πλαίσιο των αρμοδιοτήτων της, έδωσε προτεραιότητα και στην διασφάλιση του απορρήτου κατά την παροχή ταχυδρομικών υπηρεσιών. Για το λόγο αυτό, συνέταξε «Κανονισμό για τη Διασφάλιση του Απορρήτου των Τξαχυδρομικών Υπηρεσιών», ο οποίος καλύπτει τις υπηρεσίες που παρέχονται μέσω του ταχυδρομικού δικτύου (αλληλογραφία, ταχυδρομικά αντικείμενα ταχυμεταφορές κλπ), εστιάζοντας σε θέματα διασφάλισης του απορρήτου.

Στόχος του εν λόγω κανονισμού είναι η θέσπιση υποχρεώσεων των Ταχυδρομικών Επιχειρήσεων, του προσωπικού τους καθώς και των τρίτων που συνεργάζονται με αυτές, δυνάμει οποιασδήποτε έννομης σχέσης για την παροχή ταχυδρομικών υπηρεσιών, σχετικά με το απόρρητο, όπως αυτό προβλέπεται στο άρθρο 22 του Ν. 2668/1998, όπως ισχύει, και με τους όρους ασφαλείας των ταχυδρομικών υπηρεσιών, καθορίζοντας παράλληλα και τη διαδικασία ελέγχου αυτών.

Για την επίτευξη αυτού του σκοπού, κάθε Ταχυδρομική Επιχείρηση οφείλει να εκπονήσει την Πολιτική Διασφάλισης του Απορρήτου των Ταχυδρομικών Υπηρεσιών

(ΠΔΑΤΥ), η οποία περιλαμβάνει:

Α. Την Πολιτική Προστασίας του Απορρήτου, στη σφαίρα της οποίας εμπίπτουν τα αντικείμενα αλληλογραφίας, αλλά και κάθε ταχυδρομική επικοινωνία, ανεξαρτήτως του προσωπικού ή του εμπορικού χαρακτήρα της.

Β. Την Πολιτική Ασφάλειας, ως προϋπόθεση για τη διασφάλιση του απορρήτου των ταχυδρομικών υπηρεσιών.

Γ. Την Πολιτική Διασφάλισης της Εχεμύθειας τόσο του προσωπικού των Ταχυδρομικών Επιχειρήσεων όσο και τρίτων προσώπων που συνδέονται με αυτές με κάποια έννομη σχέση.

Οι Ταχυδρομικές Επιχειρήσεις υποχρεούνται να ενημερώνουν την ΑΔΑΕ σχετικά με την εφαρμοζόμενη ΠΔΑΤΥ και να την υποβάλουν σε αυτήν προς έγκριση. Η ΑΔΑΕ είναι αρμόδια να προβαίνει σε ελέγχους ορθής εφαρμογής της ΠΔΑΤΥ κάθε Ταχυδρομικής Επιχείρησης και να ασκεί εποπτεία επ΄αυτής.

Στο κείμενο του Κανονισμού περιγράφεται αναλυτικά η σχετική διαδικασία ελέγχου.

Οι Ταχυδρομικές Επιχειρήσεις εντός του πρώτου τριμήνου εκάστου ημερολογιακού έτους υποβάλλουν στην ΑΔΑΕ Ετήσια Έκθεση με στοιχεία που αφορούν στη διασφάλιση του απορρήτου των Ταχυδρομικών Υπηρεσιών. Το ελάχιστο περιεχόμενο της Ετήσιας Έκθεσης, ορίζεται ως εξής:

α) πλήρης φάκελος ΠΔΑΤΥ,

β) περιστατικά που απείλησαν τη διασφάλιση του απορρήτου των Ταχυδρομικών Υπηρεσιών, καθώς και εκτίμηση της ζημίας που υπέστη η ταχυδρομική επιχείρηση και οι χρήστες εξαιτίας αυτών των περιστατικών,

γ) μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.

Το πλήρες κείμενο του ως άνω Κανονισμού παρατίθεται στο Παράρτημα Α' της παρούσας Έκθεσης.

Β. Παραλαβή Πολιτικών Διασφάλισης του Απορρήτου των Επικοινωνιών – Αξιολόγηση - Ποσοστά Εταιρειών που κατέθεσαν Πολιτική Ασφάλειας στην ΑΔΑΕ το έτος 2005

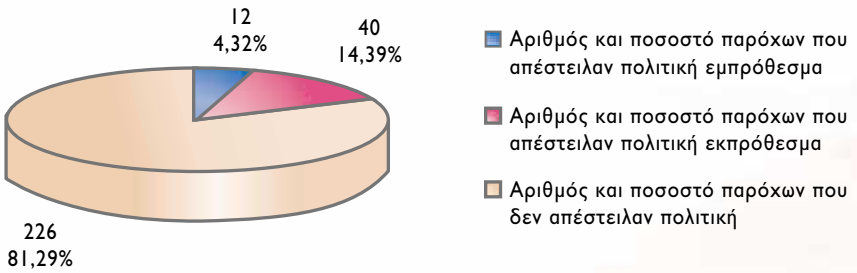
1) Τομέας Ηλεκτρονικών Επικοινωνιών

Σύμφωνα με τους Κανονισμούς της Α.Δ.Α.Ε., (ΦΕΚ 87 Β'/26-1-2005 και 88 Β'/26-1-2006), όλοι οι τηλεπικοινωνιακοί πάροχοι υποχρεούντο να ενημερώσουν την Αρχή ως προς τις εφαρμοζόμενες από αυτούς Πολιτικές Διασφάλισης του Απορρήτου εντός έξι μηνών από τη δημοσίευση των Κανονισμών, δηλαδή έως τα τέλη Ιουλίου 2005.

Σύμφωνα με το Μητρώο Παρόχων Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών του έτους 2005 της Εθνικής Επιτροπής Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ), οι αδειοδοτημένοι πάροχοι που ήταν υπόχρεοι προς την ΑΔΑΕ για να αποστείλουν Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών ήταν 278. Από αυτούς, οι 52 κατέθεσαν πολιτική εντός του έτους 2005, 12 εμπρόθεσμα (έως τις 26/7/2005) και 40 εκπρόθεσμα (μέχρι το τέλος του έτους).

Το παρακάτω γράφημα απεικονίζει τους σχετικούς αριθμούς και τα αντίστοιχα ποσοστά.

Στατιστικά στοιχεία υπόχρεων παρόχων



Στη συνέχεια ξεκίνησε η διαδικασία αξιολόγησής τους από το τεχνικό προσωπικό και τους νομικούς της Αρχής. Μέχρι το τέλος του έτους είχε ολοκληρωθεί το μεγαλύτερο μέρος της αξιολόγησης των Πολιτικών Διασφάλισης του Απορρήτου που υπεβλήθησαν στην Α.Δ.Α.Ε..

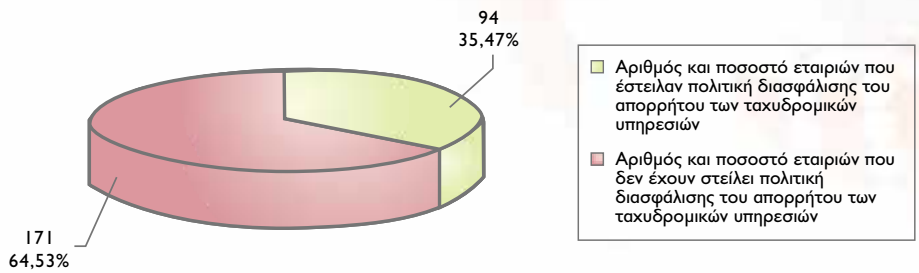
Τα αποτελέσματα της αξιολόγησης κάθε υποβληθείσας Πολιτικής καταγράφονται σε μία «Έκθεση Ελέγχου Συμμόρφωσης», η οποία στη συνέχεια εγκρίνεται από την Αρχή.

Στην «Έκθεση Ελέγχου Συμμόρφωσης» κάθε υποβληθείσας Πολιτικής περιλαμβάνονται οι παρατηρήσεις των τεχνικών Διευθύνσεων και της Νομικής Υπηρεσίας της Αρχής που πραγματοποιούν την αξιολόγηση εκάστης Πολιτικής Ασφάλειας, ως προς την πληρότητα και τη νομιμότητά της. Οι τηλεπικοινωνιακοί πάροχοι καλούνται να λάβουν υπόψη τις παρατηρήσεις αυτές, αναθεωρώντας και τροποποιώντας αντίστοιχα τις Πολιτικές τους.

Η αποστολή προς τους τηλεπικοινωνιακούς παρόχους των «Εκθέσεων Ελέγχου Συμμόρφωσης» από την Α.Δ.Α.Ε. αναμένεται να γίνει εντός του πρώτου διμήνου του 2006.

2) Τομέας Ταχυδρομείων

Μετά τη δημοσίευση του Κανονισμού για τη διασφάλιση του απορρήτου στις ταχυδρομικές υπηρεσίες, η ΑΔΑΕ προέβη σε σχετική ενημέρωση των υπόχρεων ταχυδρομικών επιχειρήσεων μέσω επιστολών. Παράλληλα, δόθηκαν διευκρινίσεις και απαντήσεις σε όλα τα ερωτήματα που ετέθησαν από παρόχους ταχυδρομικών υπηρεσιών, γεγονός που διευκόλυνε και επέσπευσε τη συμμόρφωση των ταχυδρομικών επιχειρήσεων με το κανονιστικό κείμενο.



Συμπερασματικά, σύμφωνα με τις αποσταλείσες στην ΑΔΑΕ Ετήσιες Εκθέσεις των ταχυδρομικών επιχειρήσεων, ο αριθμός των εταιρειών που συμμορφώθηκαν με τον Κανονισμό για τη διασφάλιση του απορρήτου των ταχυδρομικών υπηρεσιών, κατά το έτος 2005, ανέρχεται σε 94 επί συνόλου 265 εταιρειών, κατόχων γενικής και ειδικής άδειας παροχής ταχυδρομικών υπηρεσιών.

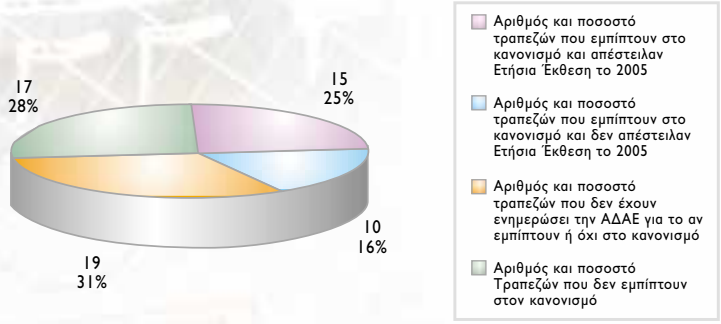
Ο έλεγχος των Ετήσιων Εκθέσεων, ανατέθηκε σε ομάδα εργασίας.

3)Αυτόματες Ταμειολογιστικές Μηχανές (ΑΤΜ)

Σύμφωνα με το Κανονισμό της ΑΔΑΕ για τη Διασφάλιση του Απορρήτου κατά τη χρήση Αυτόματων Ταμειολογιστικών Μηχανών (Απόφαση ΑΔΑΕ 969, ΦΕΚ Β' 298/8-3-2005), κάθε υπόχρεος Φορέας (Πιστωτικό Ίδρυμα) εντός του πρώτου τριμήνου εκάστοτε ημερολογιακού έτους, καλείται να υποβάλει στην Α.Δ.Α.Ε. Ετήσια Έκθεση, η οποία αφορά στο προηγούμενο έτος, με στοιχεία που σχετίζονται με την διασφάλιση του απορρήτου των επικοινωνιών κατά τη χρήση των αυτόματων ταμειολογιστικών μηχανών.

Σύμφωνα με τον Πίνακα Πιστωτικών Ιδρυμάτων που διατηρεί η Τράπεζα της Ελλάδος στον επίσημο ιστοχώρο της, υπάρχουν συνολικά 61 πιστωτικά ιδρύματα. Τα πιστωτικά ιδρύματα που εμπίπτουν στο Κανονισμό και έχουν αποστείλει στην ΑΔΑΕ την Ετήσια Έκθεση με στοιχεία που σχετίζονται με την διασφάλιση του απορρήτου των επικοινωνιών κατά τη χρήση των αυτόματων ταμειολογιστικών μηχανών είναι 15, ενώ αυτά που δεν έχουν αποστείλει ενώ υποχρεούνται είναι 10. Περεταίρω τα πιστωτικά ιδρύματα που δεν έχουν ενημερώσει καθόλου την ΑΔΑΕ για το αν εμπίπτουν ή όχι στο κανονισμό είναι 19 και τέλος τα πιστωτικά ιδρύματα που δεν εμπίπτουν στο κανονισμό είναι 17.

Το παρακάτω γράφημα απεικονίζει τους σχετικούς αριθμούς και τα αντίστοιχα ποσοστά.



Στατιστικά στοιχεία για το σύνολο των Πιστωτικών Ιδρυμάτων με έδρα την Ελλάδα
(Πηγή Πληροφορίας: Τράπεζα της Ελλάδος)

Τα αποτελέσματα της αξιολόγησης κάθε υποβληθείσας Ετήσιας Έκθεσης καταγράφονται σε μία «Έκθεση Ελέγχου Συμμόρφωσης», η οποία στη συνέχεια εγκρίνεται από την Αρχή.

Στην «Έκθεση Ελέγχου Συμμόρφωσης» κάθε υποβληθείσας Ετήσιας Έκθεσης περιλαμβάνονται οι παρατηρήσεις των τεχνικών Διευθύνσεων και της Νομικής Υπηρεσίας της Αρχής, που πραγματοποιούν την αξιολόγηση, ως προς την πληρότητα και τη νομι-

μότητά της. Τα πιστωτικά ιδρύματα καλούνται να λάβουν υπόψη τις παρατηρήσεις αυτές.

Η αποστολή των «Εκθέσεων Ελέγχου Συμμόρφωσης» από την Α.Δ.Α.Ε. προς τα πιστωτικά ιδρύματα αναμένεται να γίνει εντός του 2006.

Γ. Διαχείριση καταγγελιών σχετικών με την παραβίαση του απορρήτου των επικοινωνιών

Η ΑΔΑΕ στο πλαίσιο των αρμοδιοτήτων της, δέχθηκε καταγγελίες ιδιωτών που αφορούσαν περιπτώσεις πιθανής παραβίασης του απορρήτου των τηλεφωνικών και των διαδικτυακών επικοινωνιών τους, καθώς και καταγγελίες ιδιωτών που αφορούσαν κυρίως περιπτώσεις διάνοιξης κλειστού φακέλου, πλημμελούς επίδοσης επιστολών και απώλειας των ταχυδρομικών αντικειμένων κατά τη διαχείρισή τους από τις ταχυδρομικές επιχειρήσεις, με αποτέλεσμα να παραβιάζεται το απόρρητο της επικοινωνίας μέσω επιστολών. Κατά τον έλεγχο των καταγγελιών, η ΑΔΑΕ προέβη σε ενδελεχή έρευνα των καταγγελλόμενων περιστατικών, προβαίνοντας, κατά περίπτωση, σε επιτόπιους ελέγχους στις εγκαταστάσεις των εμπλεκόμενων παρόχων, σε συναντήσεις με τα εμπλεκόμενα μέρη, και σε διατύπωση συστάσεων και οδηγιών προς τους παρόχους υπηρεσιών επικοινωνιών .

Τα αποτελέσματα των ελέγχων που πραγματοποιήθηκαν διατυπώθηκαν σε εκθέσεις ελέγχου, οι οποίες εγκρίθηκαν από την Ολομέλεια και στη συνέχεια ενημερώθηκαν οι καταγγέλοντες.

Ο αριθμός των καταγγελιών που δέχθηκε η Α.Δ.Α.Ε. κατά το έτος 2005 είναι συνολικά δεκαοκτώ (18), εκ των οποίων δώδεκα (12) για παραβίαση του απορρήτου ηλεκτρονικών επικοινωνιών και έξι (6) για παραβίαση του απορρήτου της επικοινωνίας μέσω επιστολών.

Δ. Παραλαβή Διατάξεων Άρσης του Απορρήτου των Επικοινωνιών

Σύμφωνα με το άρθρο 5 παρ. 4 του Ν. 2225/94, όπως τροποποιήθηκε με το άρθρο 12 του Ν. 3115/03, παραδίδεται στην ΑΔΑΕ μέσα σε κλειστό φάκελο, όλο το κείμενο της διάταξης που επιβάλλει την άρση του απορρήτου.

Η ΑΔΑΕ παρέλαβε κατά το έτος 2005 διατάξεις άρσης απορρήτου, ως εξής:

Α. 406 διατάξεις του Εισαγγελέα Εφετών για λόγους εθνικής ασφάλειας, εκ των οποίων οι 351 αφορούν χρονικές παρατάσεις προγενέστερων διατάξεων άρσης του απορρήτου, ενώ 55 αφορούσαν νέες περιπτώσεις άρσης του απορρήτου.

Β. 144 βουλεύματα Συμβουλίων Πλημμελειοδικών τα οποία αφορούν τις αξιόποινες πράξεις της ανθρωποκτονίας εκ προθέσεως, βιασμού, ληστείας, έκρηξης, απάτης με ηλεκτρονικό υπολογιστή, πλαστογραφίας, κλοπής, εμπορίας ναρκωτικών, εμπρησμού, πορνογραφίας ανηλίκων, απάτης μέσω διαδικτύου, παιδικής πορνογραφίας μέσω διαδικτύου, αγοράς όπλων μέσω διαδικτύου, υπεξαίρεσης, αρπαγής, εκβίασης, διακίνησης λαθρομεταναστών, κυκλοφορίας παραχαραγμένων νομισμάτων, εμπορίας ανθρώπων, διατάραξης ασφάλειας αεροσκαφών, έκρηξης, εκρηκτικών υλών και οργανωμένου εγκλήματος.

Γ. 23 βουλεύματα Συμβουλίων Εφετών, τα οποία αφορούν την διάπραξη αδικημάτων από

αστυνομικούς υπαλλήλους σύμφωνα με τις προβλέψεις του Ν. 2713/99.

Η ΑΔΑΕ κοινοποίησε τα παραπάνω βουλεύματα, όπως προβλέπεται από τον νόμο, στον Υπουργό Δικαιοσύνης, ενώ παράλληλα ενημέρωσε σχετικά τους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή.

Κατόπιν διασταύρωσης των διατάξεων που κοινοποιήθηκαν στην ΑΔΑΕ κατά το έτος 2005 από τις αρμόδιες αρχές με αντίστοιχα στοιχεία που της γνωστοποιήθηκαν από τους τηλεπικοινωνιακούς παρόχους, διαπιστώθηκε ότι η πλειοψηφία των διατάξεων άρσης του απορρήτου που κοινοποιήθηκαν στην ΑΔΑΕ προερχόταν από την Εισαγγελία Πρωτοδικών Αθηνών, ενώ η Αρχή δεν ελάμβανε γνώση διατάξεων άρσης απορρήτου από τα Πρωτοδικεία της Περιφέρειας, αν και είχαν σταλεί αποδεδειγμένα σε παρόχους τηλεπικοινωνιακών υπηρεσιών προς εκτέλεση.

Η ΑΔΑΕ ενημέρωσε σχετικά τον Εισαγγελέα του Αρείου Πάγου ζητώντας την άμεση παρέμβασή του, ούτως ώστε να εκλείψουν αντίστοιχα φαινόμενα, που αφορούν στο ευαίσθητο πεδίο της διαφύλαξης του συνταγματικά κατοχυρωμένου ατομικού δικαιώματος του απορρήτου των επικοινωνιών.

Ε. Έκδοση γνωμοδότησης αναφορικά με την προστατευτική σφαίρα του απορρήτου των επικοινωνιών και την ακολουθητέα διαδικασία άρσης αυτού (Γνωμοδότηση υπ'αριθμ. 1 /2005)

Η ΑΔΑΕ είχε δεχτεί αναφορές από εταιρείες παροχής υπηρεσιών κινητής τηλεφωνίας, σύμφωνα με τις οποίες οι εταιρείες αυτές δέχονταν αιτήματα δημοσίων αρχών για παροχή στοιχείων επικοινωνίας των συνδρομητών τους (αναλυτική κατάσταση εισερχομένων και εξερχομένων κλήσεων, χρόνο συνδιάλεξης κλπ), χωρίς να τηρείται η διαδικασία που προβλέπεται στο Ν.2225/1994 «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας», όπως ισχύει. Τα προβαλλόμενα από τις δημόσιες αρχές αιτήματα βασίζονταν στον ισχυρισμό ότι τα λεγόμενα «εξωτερικά στοιχεία της επικοινωνίας» συνιστούν προσωπικά δεδομένα, που δεν εμπίπτουν στην έννοια του προστατευμένου από το άρθρο 19 του Συντάγματος απορρήτου της ελεύθερης ανταπόκρισης και επικοινωνίας.

Κατόπιν τούτου, τον Φεβρουάριο του 2005 η Αρχή προχώρησε στην έκδοση γνωμοδότησης, η οποία καταλήγει στα ακόλουθα συμπεράσματα:

1. στην προστατευτική σφαίρα του απορρήτου εμπίπτουν και τα εξωτερικά στοιχεία της επικοινωνίας,
2. η διαδικασία άρσης του απορρήτου ρυθμίζεται ειδικά από το Ν.2225/94, όπως ισχύει, και διατάσσεται μόνο από τη δικαστική αρχή, σύμφωνα με τη ρητή Συνταγματική επιταγή του άρθρου 19,
3. δεν είναι παραδεκτό, σε περιπτώσεις που γίνεται έρευνα για τη διακρίβωση των κακουργημάτων που αναφέρονται στο άρθρο 4 του Ν.2225/94 όπως ισχύει, οι αρμόδιες δικαστικές ή προανακριτικές αρχές, που ενεργούν κατ'άρθρο 243 ΚΠΔ, να ζητούν από τους τηλεπικοινωνιακούς φορείς τη χορήγηση εξωτερικών στοιχείων επικοινωνίας των συνδρομητών τους, χωρίς να τηρείται η προβλεπόμενη στο Ν.2225/94 διαδικασία,

4. σε περιπτώσεις αξιόποινων πράξεων που δεν αναφέρονται στο Ν.2225/94, όπως ισχύει, ή το άρθρο 253Α του ΚΠΔ, δεν δικαιολογείται η απαίτηση των αρμοδίων αρχών να χορηγούνται από τους τηλεπικοινωνιακούς φορείς εξωτερικά στοιχεία επικοινωνίας των συνδρομητών τους.

Επισημαίνεται ότι ένα μήνα μετά την έκδοση της υπ'αριθμ.1/2005 γνωμοδότησης της Α.Δ.Α.Ε., δημοσιεύθηκε το Π.Δ.47/2005 (ΦΕΚ Α' 64/10-3-2005), στο άρθρο 4 του οποίου υπάρχει πλέον ρητή και σαφής αναφορά στα στοιχεία επικοινωνίας, συμπεριλαμβανομένων και των εξωτερικών στοιχείων, που είναι δυνατόν να αποτελέσουν το αντικείμενο διάταξης άρσης του απορρήτου και, κατά συνέπεια, σύμφωνα και με τη θέση της Αρχής όπως διατυπώθηκε στη γνωμοδότησή της, εμπίπτουν στην προστατευτική σφαίρα του απορρήτου.

ΣΤ. Έκδοση του Π.Δ. 47/2005 «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του» (ΦΕΚ Α' 64/10-3-2005) - Δράσεις της ΑΔΑΕ σχετικά με την εφαρμογή του Προεδρικού Διατάγματος 47/2005

Σύμφωνα με το άρθρο 9 του Ν.3115/2003, με προεδρικό διάταγμα που εκδίδεται ύστερα από πρόταση των Υπουργών Οικονομίας και Οικονομικών, Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Δικαιοσύνης, Δημόσιας Τάξης και Μεταφορών και Επικοινωνιών και γνώμη της Α.Δ.Α.Ε., ρυθμίζονται οι διαδικασίες, καθώς και οι τεχνικές και οργανωτικές εγγυήσεις, για την άρση του απορρήτου των επικοινωνιών, όταν αυτή διατάσσεται από τις αρμόδιες δικαστικές και εισαγγελικές αρχές.

Σε εφαρμογή του άρθρου αυτού εκδόθηκε το Π.Δ.47/2005 («Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του»), το οποίο δημοσιεύθηκε στο ΦΕΚ Α'64 της 10ης Μαρτίου του 2005.

Το πλήρες κείμενο του Π.Δ.47/2005 περιλαμβάνεται στο Παράρτημα Β' της παρούσας Έκθεσης.

Με το Π.Δ.47/2005 καθορίζονται, μεταξύ άλλων, τα στοιχεία στα οποία επιτρέπεται η πρόσβαση, η τεχνική μέθοδος πρόσβασης στα στοιχεία και το είδος του χρησιμοποιούμενου εξοπλισμού, οι υποχρεώσεις των παρόχων υπηρεσιών επικοινωνίας, η τεχνική μέθοδος λήψης, αναπαραγωγής και μεταβίβασης των στοιχείων, η διασφάλιση του απορρήτου των επικοινωνιών από άποψη τεχνική και από άποψη αρμόδιων εξουσιοδοτημένων προσώπων και ο καταμερισμός του κόστους αφ'ενός του εξοπλισμού και αφ'ετέρου της διαδικασίας μεταξύ των παρόχων υπηρεσιών επικοινωνίας και των αρμόδιων αρχών.

Σε περίπτωση που κατά το χρόνο δημοσίευσης του Π.Δ.47/2005, το τηλεπικοινωνιακό σύστημα ενός παρόχου δεν διέθετε τον αναγκαίο εξοπλισμό και λογισμικό για την άρση του απορρήτου και την παροχή στις αρμόδιες αρχές των στοιχείων επικοινωνίας, όπως αυτά καθορίζονται στο προεδρικό διάταγμα, ο πάροχος υποχρεούτο να προμηθευτεί, εγκαταστήσει και θέσει σε λειτουργία στο σύστημά του, τον προς τούτο απαιτούμενο εξοπλισμό ή και λογισμικό εντός προθεσμίας εννέα (9) μηνών από την δημοσίευσή του, δηλαδή μέχρι τις 11 Δεκεμβρίου του 2005.

Κατά το διάστημα αυτό, και με σκοπό να συνδράμει στην έγκαιρη και ορθή εφαρμογή του προεδρικού διατάγματος, η Α.Δ.Α.Ε. προέβη στις ακόλουθες δράσεις :

(α) Η Αρχή ήλθε σε επαφή με τις αρχές που είναι αρμόδιες, σύμφωνα με το νόμο, να υποβάλλουν αίτηση για την άρση του απορρήτου επικοινωνιών και να λαμβάνουν τα σχετικά στοιχεία της επικοινωνίας, καθώς και με τους μεγαλύτερους παρόχους ηλεκτρονικών επικοινωνιών που δραστηριοποιούνται στην Ελλάδα.
Πραγματοποιήθηκαν συνολικά έξι συναντήσεις, δύο (2) μεταξύ της Α.Δ.Α.Ε. και των αρμόδιων αρχών (στις 29/7/05 και 14/9/05), και τέσσερις (4) με τη συμμετοχή της ΑΔΑΕ, των αρμόδιων αρχών και των εν λόγω παρόχων (στις 8/9/05, 20/9/05, 7/11/05 και 15/11/05).
Σκοπός των συναντήσεων ήταν η έκδοση τεχνικών κειμένων που θα καταγράφουν τις απαιτήσεις, αλλά και θα επισημαίνουν και επιλύουν, όπου είναι εφικτό, τα ανοιχτά τεχνικά ζητήματα των συστημάτων που θα εγκαθίσταντο στις αρμόδιες αρχές και στους παρόχους ηλεκτρονικών επικοινωνιών, προκειμένου να υλοποιηθεί η άρση του απορρήτου σύμφωνα με το Π.Δ.47/2005.
Κατά την πρώτη συνάντηση μεταξύ των τριών εμπλεκόμενων φορέων εκφράστηκαν γενικοί προβληματισμοί σε τεχνικά, νομικά και διαδικαστικά ζητήματα από τους παρόχους.
Κατόπιν τούτου, αποφασίστηκε οι επόμενες συναντήσεις να επικεντρωθούν σε τεχνικά ζητήματα ανά κατηγορία υπηρεσιών επικοινωνιών, δηλαδή ως προς τις κινητές επικοινωνίες, τις σταθερές επικοινωνίες, και τις επικοινωνίες Διαδικτύου.
Οι επόμενες τρεις συναντήσεις που πραγματοποιήθηκαν είχαν ως αποτέλεσμα την επίτευξη συμφωνίας μεταξύ των παρόχων αυτών και των αρμόδιων αρχών ως προς ένα γενικό τεχνικό πλαίσιο υλοποίησης της διαδικασίας άρσης του απορρήτου.
Καταρχάς συμφωνήθηκε να ακολουθηθούν τα πρότυπα που έχουν αναπτυχθεί από το Ευρωπαϊκό Ινστιτούτο Προτυποποίησης Τηλεπικοινωνιών (European Telecommunications Standards Institute, ETSI) σχετικά με την υλοποίηση της άρσης του απορρήτου στο διαδίκτυο. Τα πρότυπα αυτά καλύπτουν, συνοπτικά, τα εξής τεχνικά θέματα:

- Ζητήματα διασύνδεσης των συστημάτων άρσης απορρήτου των παρόχων και των αρμοδίων αρχών (μεταξύ άλλων, διεπαφές, στοιχεία, επικεφαλίδες, και πρωτόκολλα).
- Στοιχεία επικοινωνίας και τρόπους στόχευσης για τις υπηρεσίες (ανά κατηγορία υπηρεσιών ηλεκτρονικών επικοινωνιών).

Η ΑΔΑΕ εξέδωσε σχετικά κείμενα και για τις τρεις κατηγορίες υπηρεσιών (κινητές, σταθερές, Διαδικτύου).
Επίσης, συμφωνήθηκε ότι σε επόμενο στάδιο, μετά την επιλογή προμηθευτών για τα συστήματά τους, οι αρμόδιες αρχές και οι πάροχοι θα πραγματοποιήσουν νέες συναντήσεις ώστε να καθοριστούν συγκεκριμένες λεπτομέρειες λειτουργίας αλλά και διαλειτουργικότητας, ούτως ώστε να προκύψει ένα τελικό εθνικό πρότυπο άρσης απορρήτου ηλεκτρονικών επικοινωνιών.

(β) Στελέχη της Αρχής πραγματοποίησαν συναντήσεις στην έδρα της Α.Δ.Α.Ε. με τον πρόεδρο της Τεχνικής Επιτροπής σχετικά με την άρση του απορρήτου στις ηλεκτρονικές επικοινωνίες

του Ευρωπαϊκού Ινστιτούτου Προτυποποίησης Τηλεπικοινωνιών (European Telecommunications Standards Institute - ETSI),
κ. Peter van der Arend.
Στις συναντήσεις αυτές συζητήθηκαν εκτενώς τα πρότυπα που έχει εκδώσει το ETSI, καθώς και οι μελλοντικές δράσεις της Τεχνικής Επιτροπής. Επιπρόσθετα, ο κ. Peter van der Arend, ο οποίος συμμετείχε ενεργά στην επιτροπή για την εφαρμογή της άρσης του απορρήτου στις ηλεκτρονικές επικοινωνίες στην Ολλανδία, παρουσίασε τον τρόπο με τον οποίο αυτή υλοποιήθηκε σε αυτή τη χώρα της Ευρωπαϊκής Ένωσης.

(γ) Πραγματοποιήθηκαν συναντήσεις με τον κ. Ralf Schmalbach, στέλεχος της Ρυθμιστικής Αρχής της Γερμανίας (http://www.bundesnetzagentur.de) και υπεύθυνο, μεταξύ άλλων, για την υλοποίηση της άρσης του απορρήτου στις ηλεκτρονικές επικοινωνίες στη Γερμανία.
Συζητήθηκαν εκτενώς πολλά σχετικά ζητήματα και αντλήθηκαν πολύτιμα συμπεράσματα από την εμπειρία της εφαρμογής της άρσης του απορρήτου στη Γερμανία.

(δ) Η ΑΔΑΕ συμμετείχε στη συνάντηση της τεχνικής επιτροπής σχετικά με την άρση του απορρήτου στις ηλεκτρονικές επικοινωνίες του Ευρωπαϊκού Ινστιτούτου Προτυποποίησης Τηλεπικοινωνιών (ETSI) (ETSI TC LI Meeting LI#10) που πραγματοποιήθηκε 4-6/10/2005 στο Sorrento στην Ιταλία. Στη συνάντηση αυτή πραγματοποιήθηκε παρουσίαση των αρμοδιοτήτων και δράσεων της Αρχής και έγιναν σημαντικές επαφές με εκπροσώπους σχετικών Αρχών άλλων κρατών, καθώς και με εκπροσώπους κατασκευαστών συστημάτων άρσης του απορρήτου. Η έναρξη της συνάντησης έγινε από τον πρόεδρο της τεχνικής επιτροπής TC LI, κ. Peter Van der Arend. Τη συνάντηση παρακολούθησαν 52 εκπρόσωποι οι οποίοι προέρχονταν από αρχές άλλων κρατών, παρόχους ηλεκτρονικών επικοινωνών, κατασκευαστές ηλεκτροτεχνικών και τηλεπικοινωνιακών προϊόντων, καθώς και από ερευνητικά ινστιτούτα.

Η ατζέντα της συνάντησης περιλάμβανε μια μεγάλη λίστα θεμάτων προς συζήτηση, της οποίας βασικές ενότητες ήταν:

- Οι αναφορές από συναντήσεις άλλων σχετικών τεχνικών επιτροπών (π.χ. 3GPP S3-LI, TC TETRA, TC TISPAN, PTSC LAES SC)
- Τα ανοιχτά θέματα από τις ήδη δημοσιευμένες προδιαγραφές και αναφορές του TC LI (π.χ. TS 101 331, TS 101 671, TS 102 234)
- Η πρόοδος των προσχεδίων προδιαγραφών και αναφορών του TC LI (π.χ. DTS/LI-00024, DTR/LI-00014),
- Προτάσεις για νέες προδιαγραφές και αναφορές,
- Άλλες συνεισφορές.

Αξίζει να γίνει αναφορά στο "plugtest event", το οποίο προγραμματιζόταν για το Μάρτιο του 2006, και στο οποίο οι κατασκευαστές προϊόντων άρσης του απορρήτου θα μπορούσαν να ελέγχουν τη διαλειτουργικότητα των προϊόντων τους. Οι προδιαγραφές

του ETSI που θα ελέγχονταν με δοκιμές σε πραγματικά δίκτυα θα ήταν οι:

- ETSI TS 102 232 - Handover of intercepted IP Traffic
- ETSI TS 102 233 - Service specific details for E-mail services
- ETSI TS 102 234 - Service specific details for Internet Access services

Η ΑΔΑΕ σκοπεύει να συμμετάσχει σε μελλοντικές συναντήσεις της τεχνικής επιτροπής ώστε να είναι συνεχώς ενημερωμένη για τα πρότυπα και τις σχετικές υλοποιήσεις στα άλλα κράτη μέλη καθώς και να έχει ενεργό ρόλο στη διαμόρφωση των προτύπων αυτών. Η τεχνική επιτροπή συνεδριάζει τακτικά τρεις φορές το χρόνο, ενώ γίνονται και έκτακτες συναντήσεις πάνω σε συγκεκριμένα τεχνικά ζητήματα.

(ε) Πραγματοποιήθηκαν συναντήσεις με κατασκευαστές συστημάτων άρσης απορρήτου ηλεκτρονικών επικοινωνιών με σκοπό την κατανόηση τεχνικών λεπτομερειών σχετικά με τα συστήματα αυτά, αλλά και προκειμένου να συζητηθούν οι εμπειρίες και τα προβλήματα που προέκυψαν από την εγκατάσταση των συστημάτων αυτών σε παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών άλλων κρατών. Στο πλαίσιο των συναντήσεων αυτών έγινε παρουσίαση συστημάτων από τις ακόλουθες εταιρείες: Nokia, Ericsson, Cisco, Siemens, SS8, PINE. Πέραν των παρουσιάσεων αυτών, η Αρχή προέβη στην εξέταση του χαρτοφυλακίου προϊόντων και διάφορων άλλων εταιρειών.

Ζ. Συναντήσεις εκπροσώπων της Α.Δ.Α.Ε. με τη Νομοπαρασκευαστική Επιτροπή για την ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

Εκπρόσωποι της Α.Δ.Α.Ε. πραγματοποίησαν σειρά συναντήσεων με τη Νομοπαρασκευαστική Επιτροπή του Υπουργείου Δικαιοσύνης για την ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Με την κατάθεση προτάσεων και υπομνημάτων, η Α.Δ.Α.Ε. συνέβαλε στη διαπίστωση τεχνικών παραμέτρων, αναγκαίων για την εφαρμογή των προβλεπόμενων στην Οδηγία διαδικασιών διασφάλισης του απορρήτου των ηλεκτρονικών επικοινωνιών και στην επισήμανση των ιδιαιτεροτήτων που εμφανίζει η ελληνική έννομη τάξη λόγω της ύπαρξης δύο Ανεξάρτητων Αρχών, της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Α.Δ.Α.Ε., που διαχειρίζονται θέματα προστασίας της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Η. Δράση της Α.Δ.Α.Ε. κατά τις διαβουλεύσεις για την έκδοση της Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη διατήρηση των δεδομένων ηλεκτρονικών επικοινωνιών (data retention)

Στο πλαίσιο των ομάδων εργασίας της Ευρωπαϊκής Ένωσης στον τομέα «Δικαιοσύνη και Εσωτερικές Υποθέσεις» είχε αρχίσει επί Ολλανδικής Προεδρίας συζήτηση επί ενός σχεδίου απόφασης–πλαίσιο για τη διατήρηση των δεδομένων που υποβάλλονται σε επε-

ξεργασία και αποθηκεύονται σε συνάρτηση με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, με σκοπό την πρόληψη, διερεύνηση, εντοπισμό και δίωξη του εγκλήματος και των εν γένει ποινικών αδικημάτων, συμπεριλαμβανομένης της τρομοκρατίας.

Δεδομένης της σοβαρότητας του θέματος, η Α.Δ.Α.Ε. συμμετείχε σε συσκέψεις των εμπλεκόμενων μερών (Υπουργείων Μεταφορών και Επικοινωνιών και Δημόσιας Τάξης, Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων, παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών) που πραγματοποιήθηκαν με πρωτοβουλία του Υπουργείου Δικαιοσύνης το Μάρτιο, Αύγουστο και Οκτώβριο του 2005, με αντικείμενο την οριστικοποίηση των ελληνικών θέσεων επί του ζητήματος της διατήρησης δεδομένων ηλεκτρονικών επικοινωνιών.

Σε συνέχεια των συσκέψεων αυτών, και ανταποκρινόμενη σε αίτημα του Υπουργείου Δικαιοσύνης για κατάθεση των επίσημων θέσεων όλων των συμμετεχόντων μερών αναφορικά με το σχέδιο απόφασης–πλαίσιο της Ομάδας Εργασίας της Ευρωπαϊκής Ένωσης, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) απέστειλε τις θέσεις της, όπως αυτές εμπεριέχονται στην υπ' αριθμ.: 54/24-8-2005 απόφαση της Ολομέλειας της Αρχής. Το κείμενο της απόφασης έχει ως ακολούθως:

Ενόψει των διεθνών εξελίξεων, κάθε περαιτέρω περιορισμός του ατομικού δικαιώματος του απορρήτου της επικοινωνίας, που αποσκοπεί στη δίωξη του εγκλήματος και την αντιμετώπιση της τρομοκρατίας, θα πρέπει να υιοθετηθεί μόνον εφόσον αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μία δημοκρατική κοινωνία, και υπό την προϋπόθεση ότι δεν θίγεται ο πυρήνας του συνταγματικά κατοχυρωμένου ατομικού δικαιώματος του απορρήτου της επικοινωνίας.

Για το λόγο αυτό η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) εκφράζει τις επιφυλάξεις της αναφορικά με το περιεχόμενο του σχεδίου της απόφασης-πλαίσιο της ομάδας εργασίας της Ευρωπαϊκής Ένωσης, ιδιαίτερα δε με την πρόθεση διεύρυνσης του αριθμού των δεδομένων Ηλεκτρονικών Επικοινωνιών, που προτείνει να φυλάσσονται, και σημαντικής επιμήκυνσης του χρονικού διαστήματος διατήρησής τους, καθόσον από τεχνικής και διαδικαστικής πλευράς δυσχεραίνεται η διασφάλιση του Απορρήτου των Επικοινωνιών.

Θ. Συγκρότηση Ομάδων Εργασίας

- Με την με αρ. 33/10.3.2005 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε. (ΦΕΚ 412 Β/31.3.2005) συγκροτήθηκε Ομάδα Εργασίας με σκοπό:

α. τη λεπτομερή αναγνώριση και καταγραφή των κινδύνων που υπάρχουν στην παροχή υπηρεσιών ηλεκτρονικού εμπορίου μέσω του Διαδικτύου, και την αποτίμηση της σοβαρότητας των κινδύνων (αποτίμηση ρίσκου) γενικότερα, αλλά και ειδικά για τον Ελληνικό χώρο (για παράδειγμα σε σχέση με την εισχώρηση του ηλεκτρονικού εμπορίου στην γενικότερη εμπορική πρακτική),

β. την έκδοση οδηγιών και συστάσεων για την προστασία (μέτρα προφύλαξης) των χρηστών υπηρεσιών ηλεκτρονικού εμπορίου μέσω Διαδικτύου, τα οποία σχετίζονται τόσο με τον τελικό χρήστη όσο και με τον πάροχο της υπηρεσίας.

γ. την αναγνώριση και καταγραφή των απαιτήσεων από τους παρόχους υπηρεσιών ηλεκτρονικού εμπορίου, αλλά και των παρόχων πρόσβασης στο διαδίκτυο που τους εξυ-

πηρετούν, σε άμεση σχέση με τους Κανονισμούς της ΑΔΑΕ που εκδόθηκαν πρόσφατα (ΦΕΚ 88/26.1.2005). Η Ομάδα Εργασίας θα εξειδικεύσει όσο μπορεί τις απαιτήσεις και τις υποχρεώσεις των παρόχων που δραστηριοποιούνται στο χώρο του ηλεκτρονικού εμπορίου.

- Με την με αρ. 34/10.3.2005 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε. (ΦΕΚ 1135 Β/17.8.2005) συγκροτήθηκε Ομάδα Εργασίας με σκοπό την εξέταση του νομικού πλαισίου για ασφάλεια που ισχύει για το ηλεκτρονικό εμπόριο μέσω Διαδικτύου.

- Με την με αρ. 52/15.7.2005 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε. (ΦΕΚ 412 Β/31.3.2005) συγκροτήθηκε Ομάδα Εργασίας με αντικείμενο τη λεπτομερειακή επεξεργασία των ζητημάτων που είχαν τεθεί τόσο από τεχνικής όσο και από νομικής πλευράς αναφορικά με ενδεχόμενη επικάλυψη αρμοδιοτήτων μεταξύ της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Α.Δ.Α.Ε.. Η Ομάδα Εργασίας, αφού εντόπισε τα κυριότερα ζητήματα, συμμετείχε σε συναντήσεις με στελέχη της Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, κατά τις οποίες, αφού αναπτύχθηκαν οι απόψεις των δύο Αρχών, ακολούθησε εποικοδομητικός διάλογος.

- Με την με αρ. 65/24.10.2005 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε. (ΦΕΚ 1549 Β/9.11.2005) συγκροτήθηκε Ομάδα Εργασίας με σκοπό την οργάνωση στην ΑΔΑΕ της δεύτερης ημερίδας για την εκπόνηση Εθνικής Στρατηγικής σχετικά με την ασφάλεια ηλεκτρονικών δικτύων και πληροφοριών περί τα τέλη Ιουνίου 2006.

- Με την με αρ. 73/12.12.2005 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε. (ΦΕΚ 1822 Β/23.12.2005) συγκροτήθηκε Ομάδα Εργασίας με αντικείμενο τον έλεγχο συμμόρφωσης των Ταχυδρομικών Επιχειρήσεων στην «Πολιτική Διασφάλισης του Απορρήτου των Ταχυδρομικών Υπηρεσιών» σύμφωνα με την υπ΄αριθμ. 1001/Φ.21 Απόφαση της Α.Δ.Α.Ε «Έγκριση του Κανονισμού για τη Διασφάλιση του Απορρήτου των Ταχυδρομικών Υπηρεσιών».

Ι. Οργάνωση Εκπαιδευτικών Σεμιναρίων για την εκπαίδευση του προσωπικού.

Η ΑΔΑΕ έδωσε προτεραιότητα στην εκπαίδευση του προσωπικού της. Και τούτο διότι κρίθηκε απαραίτητο, με την ανάληψη των καθηκόντων του, το προσωπικό της Αρχής να έχει σαφή εικόνα της δράσης, των στόχων και του τρόπου λειτουργίας της νεοσύστατης Αρχής. Η οργάνωση και ο συντονισμός των εν λόγω σεμιναρίων ανετέθη σε Ομάδα Εργασίας.

Τα σεμινάρια έλαβαν χώρα στην έδρα της Αρχής στο Μαρούσι και διήρκεσαν από την 14η Φεβρουαρίου 2005 έως την 11η Μαρτίου 2005.

Η επιλογή των εισηγητών έγινε με γνώμονα, αφενός την πληρέστερη κάλυψη του ευρύτατου πεδίου των τηλεπικοινωνιών σε θέματα τεχνολογικής εξέλιξης και σκιαγράφησης της αγοράς των τηλεπικοινωνιών και, αφετέρου, την ευρύτερη ενημέρωση σε θέματα ρυθμιστικού και θεσμικού ενδιαφέροντος λόγω του ιδιαίτερου ρόλου της ΑΔΑΕ, ως Ανεξάρτητης Αρχής προβλεπόμενης από το άρθρο 19 παρ. 2 του Συντάγματος.

Στα σεμινάρια παρέστησαν, μεταξύ άλλων, καθηγητές των Ανωτάτων Εκπαιδευτικών Ιδρυμάτων της χώρας στον τομέα της τεχνολογίας των επικοινωνιών, οι οποίοι αναφέρθηκαν στη διασφάλιση του απορρήτου, στις πολιτικές ασφάλειας των δικτύων και πλη-

ροφοριών τόσο στην τηλεφωνία όσο και στο διαδίκτυο, στην ανάλυση των νέων συστημάτων και τους τρόπους αντιμετώπισης των συνεχώς εξελισσόμενων προκλήσεων, καθώς και καθηγητές Πανεπιστημίου με ειδίκευση στον τομέα των τηλεπικοινωνιών, οι οποίοι κάλυψαν θέματα νομικού και οικονομικού ενδιαφέροντος.

Στο σκέλος αυτό έγινε ενημέρωση αναφορικά με τον ιδρυτικό νόμο της ΑΔΑΕ και τα σχετικά με τη δράση της Αρχής νομοθετήματα, τα κανονιστικά κείμενα της Αρχής που είχαν ήδη δημοσιευθεί, θέματα διεθνούς θεσμικού πλαισίου, καθώς και θέματα οικονομίας της αγοράς και της επικοινωνίας.

Τα σεμινάρια ολοκληρώθηκαν με ανοιχτή συζήτηση με τους εκπροσώπους των παρόχων. Ακολουθεί το πρόγραμμα των Εκπαιδευτικών Σεμιναρίων.

ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗΣ ΚΑΙ ΕΞΕΙΔΙΚΕΥΣΗΣ ΝΕΟΠΡΟΣΛΗΦΘΕΝΤΩΝ ΣΤΗΝ ΑΔΑΕ
ΦΕΒΡΟΥΑΡΙΟΣ-ΜΑΡΤΙΟΣ 2005

με γενικό θέμα
Το περιβάλλον δραστηριοποίησης της ΑΔΑΕ και σχετικές τεχνολογίες

1. Δίκτυο ΟΤΕ

Ε. Μπίλλης, Επικ. καθ. Ε.Μ.Π.

2. Αρμοδιότητες ΑΔΑΕ και Ανάλυση Κανονισμών

Αρμοδιότητες ΑΔΑΕ
Ι. Βενιέρης, καθ. Ε.Μ.Π.
Χ. Καψάλης, καθ. Ε.Μ.Π.
Χ. Δουληγέρης, καθ. Πανεπ. Πειραιώς
Γ. Στασινόπουλος, καθ. Ε.Μ.Π.

Πολιτικές Ασφαλείας
Α Μαυρουδέας, MSc Information Security

Ανάλυση των εκπονηθέντων Κανονισμών σχετικά με την ασφάλεια στο Διαδίκτυο
Α Μαυρουδέας, MSc Information Security

Ασφάλεια Κινητών, Ασύρματων και Δορυφορικών Συστημάτων
Α. Παναγόπουλος, ΕΕΠ ΑΔΑΕ
Π. Μπάμπαλης, ΕΕΠ ΑΔΑΕ
Π. Τρακάδας, ΕΕΠ ΑΔΑΕ

Ανάλυση των εκπονηθέντων Κανονισμών σχετικά με την ασφάλεια στις τηλεπικοινωνίες
Α. Παναγόπουλος, ΕΕΠ ΑΔΑΕ

Πρόταση Εθνικής Στρατηγικής για ασφάλεια δικτύων και πληροφοριών
Κ. Μαραβέλας, Μέλος ΑΔΑΕ

Πολιτικές Ασφαλούς Συνδεσιμότητας
Γ. Μπράνης, ΕΕΠ ΑΔΑΕ

3. Τεχνικό Υπόβαθρο

Υπηρεσίες και Εφαρμογές Υποδομής Δημόσιας Κλείδας (ΥΔΚ)
Ν. Πολέμη, καθ. Πανεπ. Πειραιώς

Ασφάλεια Ασύρματων Δικτύων
Χ. Καψάλης, καθ. Ε.Μ.Π.

Η έννοια της ασφάλειας σε μεγάλους τηλεπικοινωνιακούς οργανισμούς (ασφ. Περιμέτρου, ασφ. Εφαρμογών, τηλ. εξοπλισμός, ασφ. σε σχέση με προσωπικό και χρήστες)
Γ. Πρεζεράκος, Αναπλ. καθ. Τ.Ε.Ι. Πειραιώς

Επιθέσεις Άρνησης Υπηρεσίας
Χ. Δουληγέρης, καθ. Πανεπ. Πειραιώς

Ασφάλεια και Διαδίκτυο
Ιακ. Βενέρης, καθ. Ε.Μ.Π.

Χρησιμοποίηση PGP για την εξασφάλιση απορρήτου των επικοινωνιών
Χαρ. Πατρικάκης, Διδάκτωρ Ε.Μ.Π.

Τεχνολογίες XML και ασφάλεια εφαρμογών
Γ, Στασινόπουλος, καθ. Ε.Μ.Π.

4. Θεσμικά Θέματα

Δρ. Β. Ζαρκάδης, Δ/ντης Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Δρ. Ζωή Καρδασιάδου, Νομική Ελέγκτρια Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Β. Κονδύλης, Νομικός Σύμβουλος ΕΕΤΤ

Κ. Μαραβέλας, μέλος ΑΔΑΕ

Μ. Καρατζάς, μέλος ΑΔΑΕ

5. Τεχνοοικονιμικό υπόβαθρο

Ρυθμιστικά Θέματα
Κ. Λεβέντη, Προϊσταμένη Νομικής Υπηρεσίας ΕΕΤΤ

Οικονομία της αγοράς και σχέση με την Ασφάλεια
Γ. Μπήτρος, καθ. Οικονομικού Πανεπιστημίου

Ζητήματα Διοικητικής Διαδικασίας και Προστασίας
Χ. Χρυσανθάκης, καθ. Δημοσίου Δικαίου ΕΚΠΑ

Διεθνές Θεσμικό Πλαίσιο
Χρυσάφης (Ε.Ε.)

Θέματα Επικοινωνίας
Ι. Μεταξάς, καθ. ΕΚΠΑ

ΙΑ. ΔΙΟΡΓΑΝΩΣΗ ΗΜΕΡΙΔΑΣ ΑΠΟ ΤΗΝ Α.Δ.Α.Ε.

Στις 11 Απριλίου 2005 διοργανώθηκε από την Α.Δ.Α.Ε. σε κεντρικό ξενοδοχείο της Αθήνας ημερίδα με θέμα : «Γενικές Αρχές Εθνικής Στρατηγικής για το Απόρρητο και την Ασφάλεια Δικτύων και Πληροφοριών».

Κύριος σκοπός της ημερίδας ήταν η παρουσίαση και συζήτηση προτάσεων για μια Εθνική Στρατηγική για το Απόρρητο και την Ασφάλεια Δικτύων και Πληροφοριών, που θα διασφαλίζει το απόρρητο των επικοινωνιών των πολιτών, σύμφωνα με τις επιταγές του Συντάγματος, θα καλύπτει τις ανάγκες θωράκισης της ελληνικής δημόσιας διοίκησης και μεγάλων οργανισμών από επιθέσεις στην πληροφοριακή και δικτυακή τους υποδομή, και θα προωθεί το αίσθημα ασφαλείας και τη διαφύλαξη του κεφαλαίου γνώσης προς όφελος της επιχειρηματικότητας όλων των παραγωγικών τάξεων της χώρας. Η ημερίδα αποσκοπούσε στη συγκρότηση διαρκούς forum, με την ευρύτερη δυνατή συμμετοχή, για τη συνεχή αντιμετώπιση των σχετικών προκλήσεων αλλά και δυνατοτήτων στο διεθνές περιβάλλον.

Η ημερίδα χωριζόταν σε τρεις ενότητες οι οποίες ήταν οι εξής :

1η ενότητα : Διεθνής περίγυρος και ελληνικές προοπτικές
2η ενότητα : Συμμετοχή παρόχων, χρηστών, συνδρομητών και καταναλωτών
3η ενότητα : Ασφάλεια, εμπιστοσύνη και ανάπτυξη

Μετά το πέρας των ομιλιών, οι παριστάμενοι οργανώθηκαν σε τρεις αντίστοιχες ομάδες εργασίας, οι οποίες κατέληξαν σε συμπεράσματα και προτάσεις.

Ακολουθούν οι ομιλητές και τα θέματα για τα οποία μίλησαν :

κ. Ανδρέας Λαμπρινόπουλος, Πρόεδρος ΑΔΑΕ
Αναγκαιότητα και Σκοπιμότητα Χάραξης Εθνικής Στρατηγικής

1η Ενότητα: Διεθνής Περίγυρος και Ελληνικές Προοπτικές

Εισηγητής : κ. Σωκράτης Κάτσικας, Πρύτανης Πανεπιστημίου Αιγαίου
Ασφάλεια Πληροφορίας και Δικτύων: Άξονες μιας Εθνικής Στρατηγικής

κ. Θανάσης Χρυσάφης, Ευρωπαϊκή Ένωση, Ευρωπαϊκή Επιτροπή, Γενική Διεύθυνση Κοινωνίας της Πληροφορίας και Μαζικών Μέσων
Διαχείριση Ταυτότητας στην Ηλεκτρονική Διακυβέρνηση στην Ευρωπαϊκή Ένωση

κ. Δημήτριος Γκρίτζαλης, αναπληρωτής καθηγητής, Οικονομικό Πανεπιστήμιο Αθηνών
Ασφάλεια Κρίσιμων Υποδομών: Διεθνές Τοπίο και Προοπτικές

κ. Ανδρέας Μητράκας, Δικηγόρος Αθηνών
Ασφάλεια Δικτύων και Πληροφοριών : Ρυθμιστικές πρωτοβουλίες

κ. Διομήδης Σπινέλλης, αναπληρωτής καθηγητής, Οικονομικό Πανεπιστήμιο Αθηνών
Ο Ρόλος Ανοικτών Προτύπων και Τεχνολογιών στην Επίτευξη της Ασφάλειας

κ. Παντελής Αγγελίδης, Γενικός Διευθυντής ΙΝΑ
Το Πλαίσιο Συνεργασίας στην Ν.Α. Ευρώπη για την Ασφάλεια Δικτύων και Πληροφοριών

2η Ενότητα: Συμμετοχή Παρόχων, Χρηστών, Συνδρομητών και Καταναλωτών

Εισηγήτρια : κα Δέσποινα Πολέμη, Πανεπιστήμιο Πειραιώς
Ασφάλεια σε Υπηρεσίες και Εφαρμογές

κ. Δημοσθένης Γαλλής, Τράπεζα της Ελλάδος
Αρχές Ασφαλούς και Αποτελεσματικής Λειτουργίας των Συστημάτων Πληροφορικής στα Πιστωτικά Ιδρύματα

κ. Κώστας Ταβλαρίδης, Ένωση Ελληνικών Τραπεζών
Συστήματα Πληρωμών και Ηλεκτρονικής Τραπεζικής

κ. Στέλιος Μαΐστρος, Πανεπιστήμιο Αιγαίου
Ασφάλεια και Αντιμετώπιση Περιστατικών Χρηστών ΕΔΕΤ

κ. Νίκος Βασιλάκος και κα Έλενα Σπυροπούλου, Ένωση Ελλήνων Χρηστών Internet
Συμμετοχική Αυτοδιαχείριση στο διαδίκτυο: Αυτορρύθμιση, Συρύθμιση ή Απορρύθμιση,

κ. Ανέστης Στάθης, Γενική Συνομοσπονδία Εργατών Ελλάδος
Ασφάλεια Δικτύων – Προστασία Καταναλωτών

3η Ενότητα: Ασφάλεια, Εμπιστοσύνη και Ανάπτυξη

Εισηγητής : κ. Δρακούλης Μαρτάκος, αναπληρωτής καθηγητής, Πανεπιστήμιο Αθηνών
Κυβερνοεγκληματικότητα

κ. Γιώργος Επιτήδειος, Πρόεδρος Ένωσης Ελλήνων Επαγγελματιών Internet
Ασφάλεια Δεδομένων: Επιδράσεις στην Δημόσια Εικόνα της Επιχείρησης

κ. Νίκος Κυρλόγλου, Εμπορικό και Βιομηχανικό Επιμελητήριο Αθηνών
Το ασφαλές ηλεκτρονικό εμπόριο από την πλευρά των επιχειρήσεων

Στην ημερίδα συμμετείχαν πάνω από 400 άτομα από όλο το φάσμα των εμπλεκομένων στις ηλεκτρονικές επικοινωνίες. Παραβρέθηκαν εκπρόσωποι τηλεπικοινωνιακών παρόχων, παραγωγικών φορέων, δημοσίων υπηρεσιών και κοινωνικών εταίρων.

Στις ομάδες εργασίας που συστήθηκαν αντίστοιχα με τις ενότητες της ημερίδας, συζητήθηκαν εκτενώς τα αντίστοιχα θέματα και προέκυψαν συμπεράσματα και προτάσεις τα, συνοπτικά, οποία είναι τα εξής :

1η Ενότητα: Διεθνής Περίγυρος και Ελληνικές Προοπτικές

Η συγκεκριμένη ενότητα είχε ως θέμα την κατάθεση προβληματισμών σχετικά με την ελληνική πραγματικότητα και το διεθνή περίγυρο. Η συζήτηση και οι προτάσεις κινήθηκαν σε τέσσερεις κατευθύνσεις, οι οποίες είναι οι εξής :

Κατεύθυνση Ι

- Αποσαφήνιση του νομικού πλαισίου και των αρμοδιοτήτων (ασφάλεια/ τηλεπικοινωνίες / προσωπικά δεδομένα / καταναλωτές)
- Συμμετοχή στη διαδικασία και ενθάρρυνση στην ανάπτυξη προτύπων και βέλτιστων πρακτικών
- Πρότυπα που απορρέουν από το κανονιστικό πλαίσιο
- Προαιρετικά πρότυπα (βιομηχανικά, de facto)
- Ενημέρωση χρηστών με μέτρο τη διείσδυση της τεχνολογίας
- Πιστοποίηση και έλεγχος ποιότητας (ISO 17799, Basel II, Common Criteria κλπ.)

Κατεύθυνση ΙΙ

Σύνδεση με:
- φυσική ασφάλεια & υποδομές (CIP vs CIIP)
- Δημόσια τάξη / κυβερνοέγκλημα (απάτη, IPR, παιδική πορνογραφία) Ομαδοποίηση προϋποθέσεων
- ανά κλάδο οικονομικής δραστηριότητας (eGov, eCom, eBank)
- Ανά εφαρμογή (Προμήθειες, διαχείριση ταυτότητας, βιομετρικά διαβατήρια, ταχογράφοι, υγεία κλπ.)

Κατεύθυνση ΙΙΙ

- Πρόσκληση προς τους εμπλεκόμενους φορείς
- Εκπαίδευση και ενημέρωση των ασχολούμενων με την ασφάλεια
- Σχολεία, εκπαιδευτικά προγράμματα, δια βίου εκπαίδευση
- Εφαρμογή των πολιτικών ασφαλείας από χρήστες
- Προληπτικές ενέργειες από τους χρήστες

Κατεύθυνση ΙV

- Συνεργασία δημόσιου – ιδωτικού τομέα (private public partnerships -- PPP)

2η Ενότητα: Συμμετοχή Παρόχων, Χρηστών, Συνδρομητών και Καταναλωτών

Η συγκεκριμένη ενότητα είχε ως θέμα την κατάθεση προβληματισμών και σκέψεων σχετικά με την ασφάλεια που παρέχεται από υπηρεσίες του ευρύτερου δημόσιου τομέα, από χρηματοπιστωτικούς φορείς, και από παρόχους τηλεπικοινωνιακών υπηρεσιών. Στην ομάδα εργασίας συμμετείχαν εκπρόσωποι από όλους τους προαναφερθέ-

ντες φορείς, καθώς επίσης και χρήστες διαδικτυακών υπηρεσιών, οι οποίοι κατέθεσαν τους προβληματισμούς τους σχετικά με την ασφάλεια των επικοινωνιών τους.

Θέματα Συζήτησης :

Δημόσια Διοίκηση

Τα κύρια προβλήματα που εντοπίστηκαν είναι τα ακόλουθα:

- Έλλειψη κοινού πλαισίου διαβάθμισης πληροφορίας στον Δημόσιο τομέα. Δηλαδή, ο χαρακτηρισμός της πληροφορίας σε επίπεδα εμπιστευτικότητας, καθώς και η ερμηνεία των επιπέδων εμπιστευτικότητας πληροφορίας δεν είναι κοινή σε όλους τους δημόσιους φορείς.
- Έλλειψη φορέα ο οποίος εκδίδει κανονισμούς ή συστάσεις ασφάλειας για τους φορείς του δημοσίου, καθώς και έλλειψη φορέα ο οποίος ελέγχει την ασφάλεια των οργανισμών του δημόσιου τομέα.

Προτάσεις

Για την εξέταση των παραπάνω προβληματισμών προτάθηκε η δημιουργία ομάδας εργασίας με την συμμετοχή αρμοδίων από διάφορα υπουργεία (Υπ. Δικαιοσύνης, Υπ. Επικοινωνιών και Μεταφορών, Υπ. Εσωτερικών κλπ.) με σκοπό την διερεύνηση των προαναφερθέντων και την πρόταση λύσεων για την θωράκιση των δημοσίων δικτύων.

Χρηματοπιστωτικός τομέας

Η Τράπεζα της Ελλάδος, για την ενίσχυση της ασφάλειας των ιδρυμάτων που ελέγχει, έχει ήδη δημοσιεύσει κανονισμό που αναφέρεται στις Αρχές Ασφαλούς και Αποτελεσματικής Λειτουργίας των συστημάτων Πληροφορικής στα πλαίσια της Διαχείρισης του Λειτουργικού τους Κινδύνου. Το κυρίως ζητούμενο από την ΑΔΑΕ είναι η συνεισφορά της στην αύξηση της εμπιστοσύνης των χρηστών για την πραγματοποίηση ηλεκτρονικών τραπεζικών συναλλαγών και ιδιαίτερα μέσω του διαδικτύου. Για την επίτευξη αυτού του σκοπού προτάθηκαν οι ακόλουθες ενέργειες:

- Οι τράπεζες πρέπει να ακολουθούν πολιτικές ασφάλειας οι οποίες θα στηρίζονται σε διεθνώς αναγνωρισμένα πρότυπα ασφάλειας αλλά και σε συστάσεις, οδηγίες που εκδίδονται ειδικά για την ασφάλεια του χρηματοπιστωτικού τομέα (π.χ. Επιτροπή Βασιλείας). Προς αυτή την κατεύθυνση θα συνεισφέρει η εφαρμογή του κανονισμού ασφαλούς λειτουργίας της Τράπεζας της Ελλάδος.
- Θα πρέπει να υποστηρίζεται η διαλειτουργικότητα (interoperability) στις τεχνολογίες που χρησιμοποιούν οι τράπεζες, κυρίως για την παροχή WEB-Banking υπηρεσιών, και ιδιαίτερα στις τεχνολογίες ασφάλειας, κρυπτογράφησης και δημιουργίας/επαλήθευσης υπογραφής.
- Θα πρέπει να ενισχυθεί η πεποίθηση του καταναλωτή ότι σε περίπτωση λάθους ή σε περιπτώσεις εξαπάτησης για τις οποίες δεν ευθύνεται ο ίδιος σε συναλλαγές ηλε-

κτρονικής τραπεζικής, δεν πρόκειται να επωμισθεί το κόστος.

Προτάσεις

Προτάθηκε η δημιουργία μίας μόνιμης επιτροπής με την συνεργασία της Τράπεζας της Ελλάδος, εκπροσώπων τραπεζών, της ΕΕΤΤ και της Α.Δ.Α.Ε., με σκοπό την διερεύνηση και επίλυση των προαναφερθέντων συμπερασμάτων .

3η Ενότητα: Ασφάλεια, Εμπιστοσύνη και Ανάπτυξη

Θέματα Συζήτησης :

Ψηφιακά Πιστοποιητικά

Συζητήθηκε το ζήτημα των ψηφιακών πιστοποιητικών των ιστοσελίδων. Η συζήτηση προσανατολίστηκε στην ασφάλεια που προσφέρουν, και στην περίπτωση χρήσης πέραν της χρονικής περιόδου ισχύος τους.

Ψηφιακές Υπογραφές

Συζητήθηκαν οι υποχρεώσεις των φορέων πιστοποίησης.

Αποτίμηση Κινδύνων e-commerce

Συζητήθηκε διεξοδικά το αποδεκτό επίπεδο κινδύνου στη χρήση e-services και οι τρόποι μείωσής του. Οι συμμετέχοντες συμφώνησαν ότι ο κίνδυνος δεν μπορεί να εξαλειφθεί και ότι θα πρέπει να καταβληθούν προσπάθειες σε ευρωπαϊκό επίπεδο για συνεργασία και ανταλλαγή πληροφοριών σχετικά με την ισχύουσα νομοθεσία σε κάθε κράτος-μέλος. Ιδιαιτέρως συζητήθηκε ο τρόπος που χρησιμοποιείται για την ηλεκτρονική τιμολόγηση και την ασφάλεια που προσφέρουν οι αντίστοιχοι αλγόριθμοι. Τέλος, συζητήθηκε η ασφάλεια του τρόπου πληρωμής μέσω πιστωτικών καρτών και ο τρόπος αποστολής αποδεικτικών (τιμολογίων, δελτίων αποστολής) στην Ελλάδα και στα υπόλοιπα κράτη (Ε.Ε., Η.Π.Α.).

ΙΒ. Διεθνείς Δραστηριότητες

- Συνάντηση με στελέχη της Φινλανδικής Αρχής Finnish Communications Regulatory Authority (FICORA)- Ελσίνκι, 16η Σεπτεμβρίου 2005.

Στο πλαίσιο των διεθνών συνεργασιών που επιδιώκει να έχει η Α.Δ.Α.Ε. με αντίστοιχες αρχές χωρών της Ευρωπαϊκής Ένωσης, αντιπροσωπεία της ΑΔΑΕ πραγματοποίησε επίσκεψη στη Finnish Communications Regulatory Authority (FICORA), στην έδρα της Αρχής στο Ελσίνκι, την 16η Σεπτεμβρίου 2005. Κατά την διάρκεια της συνάντησης, αφού πρώτα έγινε παρουσίαση των αρμοδιοτήτων των δύο αρχών, αντηλλάγησαν απόψεις σχετικά με τους κινδύνους που απειλούν την ασφάλεια των τηλεπικοινωνιακών δικτύων καθώς και τη θωράκιση του θεσμικού πλαισίου για την ασφάλεια των δικτύων και την διασφάλιση του απορρήτου των επικοινωνιών. Τέλος, πραγματοποιήθηκε ανταλλαγή απόψεων σχετικά με τον ρόλο που έχουν οι δύο αρχές κατά την την υλο-

ποίηση και τον έλεγχο των συστημάτων νόμιμης συνακρόασης και συμφωνήθηκε η συστηματική συνεργασία μεταξύ των δύο αρχών.

- Συμμετοχή της Α.Δ.Α.Ε. ως τεχνικού συμβούλου του Υπουργείου Δικαιοσύνης κατά τις διαβουλεύσεις στην Ευρωπαϊκή Ένωση αναφορικά με τη διατήρηση των δεδομένων ηλεκτρονικών επικοινωνιών

Όπως αναφέρθηκε, κατά την διάρκεια του 2005 μείζον ζήτημα για την Ευρωπαϊκή Ένωση υπήρξε η διαμόρφωση ενός νομοθετικού πλαισίου για τη διατήρηση των δεδομένων που υποβάλλονται σε επεξεργασία και αποθηκεύονται σε συνάρτηση με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, με σκοπό την πρόληψη, διερεύνηση, εντοπισμό και δίωξη του εγκλήματος και των εν γένει ποινικών αδικημάτων, συμπεριλαμβανομένης της τρομοκρατίας . Η Α.Δ.Α.Ε., μετά από την αίτηση του Υπουργείου Δικαιοσύνης, λειτούργησε ως τεχνικός σύμβουλος του Υπουργείου κατά τις εν λόγω διαβουλεύσεις.

ΙΓ. Σύνταξη Σχεδίου Προϋπολογισμού 2006

Η Αρχή συνέταξε έγκαιρα και υπέβαλε στα αρμόδια Υπουργεία, όπως προβλέπει ο νόμος, τον Προϋπολογισμό της (ΑΔΑΕ) για το έτος 2006 προκειμένου αυτός να ενταχθεί στον Προϋπολογισμό του Υπουργείου Δικαιοσύνης με ίδιο φορέα.

ΚΕΦΑΛΑΙΟ ΙΙΙ.
ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΔΡΑΣΗΣ ΕΤΟΥΣ 2006

ΚΕΦΑΛΑΙΟ ΙΙΙ.
ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΔΡΑΣΗΣ ΕΤΟΥΣ 2006

Η δράση της ΑΔΑΕ κατά το 2006 προγραμματίζεται να καλύψει τα ακόλουθα θέματα:

1. Ολοκλήρωση της διαδικασίας ελέγχου και έγκρισης Πολιτικών Ασφάλειας των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών σύμφωνα με τους Κανονισμούς της Αρχής.
2. Κλήση σε ακρόαση και επιβολή κυρώσεων σε παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών που δεν έχουν συμμορφωθεί με τους Κανονισμούς της Αρχής.
3. Διενέργεια ελέγχου σε παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών προς διαπίστωση της τήρησης των όρων που διασφαλίζουν το απόρρητο των επικοινωνιών.
4. Ενημέρωση και αποστολή κατάλληλων συστάσεων σε φορείς – παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών επί θεμάτων σχετικών με τη λήψη μέτρων διαφύλαξης του απορρήτου.
5. Εξέταση καταγγελιών που αναφέρονται σε ζητήματα διασφάλισης ή άρσης του απορρήτου των επικοινωνιών.
6. Παρακολούθηση και έλεγχος της τήρησης της ορθής διαδικασίας άρσης του απορρήτου των επικοινωνιών σύμφωνα με τα προβλεπόμενα στους Ν.2225/94, Ν.3115/2003 και το Π.Δ.47/2005.
7. Ολοκλήρωση της διαδικασίας επίλυσης των ανοικτών τεχνικών ζητημάτων διασύνδεσης και λειτουργίας των συστημάτων άρσης του απορρήτου των αρμόδιων αρχών και των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.
8. Έλεγχος και έγκριση των Πολιτικών Διασφάλισης του Απορρήτου κατά τη χρήση των Αυτόματων Ταμειολογιστικών Μηχανών των υπόχρεων φορέων, σύμφωνα με τον αντίστοιχο Κανονισμό της Αρχής.
9. Έλεγχος και έγκριση των Πολιτικών Διασφάλισης του Απορρήτου των Ταχυδρομικών Υπηρεσιών των Ταχυδρομικών Επιχειρήσεων, σύμφωνα με τον αντίστοιχο Κανονισμό της Αρχής.
10. Αξιολόγηση και προμήθεια εξοπλισμού και λογισμικού αναγκαίου για την διενέργεια ελέγχων στους παρόχους δικτύου ή/και υπηρεσιών επικοινωνιών.
11. Συνεργασία με άλλες αρμόδιες Αρχές και Υπηρεσίες του κράτους για την αντιμετώπιση προβλημάτων που αφορούν στο απόρρητο και στην ασφάλεια των επικοινωνιών (π.χ. συμμετοχή στο Εθνικό Συμβούλιο για θέματα Ηλεκτρονικώς Επιχειρείν).
12. Ανάπτυξη σχέσεων με αντίστοιχες ευρωπαϊκές Ρυθμιστικές Αρχές και συμμετοχή σε Ημερίδες, Συνέδρια, Τεχνικές Επιτροπές.
13. Υποβολή προτάσεων για νομοθετικές ρυθμίσεις που κρίνονται αναγκαίες για τη λειτουργία της Αρχής και την εκπλήρωση του θεσμικού της ρόλου.
14. Εκπαίδευση του προσωπικού επί θεμάτων σχετικών με τις διαδικασίες και τους τρόπους διενέργειας ελέγχων καθώς και με τη λειτουργία τηλεπικοινωνιακών συστημάτων.
15. Σύσταση ομάδων εργασίας με στόχο την ορθή εφαρμογή του Π.Δ. 47/2005, τη μελέτη αρχείων καταγραφής τηλεπικοινωνιακών συστημάτων, τη μελέτη λογισμικού τηλεπικοινωνιακών κέντρων και την ανάλυση κλήσεων.
15. Ολοκλήρωση της διαδικασίας πρόσληψης του προσωπικού της Αρχής.
17. Ενημέρωση του κοινού επί των θεμάτων που σχετίζονται με την τήρηση του απορρήτου των επικοινωνιών.

ΚΕΦΑΛΑΙΟ IV.
ΝΟΜΟΘΕΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ

ΕΚΘΕΣΗ ΠΕΠΡΑΓΜΕΝΩΝ
ΕΤΟΥΣ 2005

ΚΕΦΑΛΑΙΟ IV.
ΝΟΜΟΘΕΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ

Η διαρκής εξέλιξη της τεχνολογίας και των κινδύνων που αυτή συνεπάγεται απαιτεί τη συνεχή επαγρύπνηση όλων μας και την υιοθέτηση εκείνων των λύσεων που διασφαλίζουν τα ευεργετικά αποτελέσματα της τεχνολογίας και αποτρέπουν την ανάπτυξη των δυσμενών συνεπειών της, προς όφελος τελικά του κάθε πολίτη και της ασφάλειας της χώρας.

Προς αυτήν την κατεύθυνση παρίσταται άμεση ανάγκη θωράκισης του υφιστάμενου νομικού πλαισίου που διέπει το απόρρητο των επικοινωνιών και την ασφάλεια των δικτύων.

Η έγκαιρη, ορθή και συνολική ικανοποίηση των προτάσεων που ακολουθούν αποτελεί την ελάχιστη αναγκαία προϋπόθεση για να ανταποκριθεί η Α.Δ.Α.Ε. με επιτυχία στις μεγάλες απαιτήσεις που δημιουργεί το σύγχρονο περιβάλλον της απελευθερωμένης αγοράς στο θέμα της ασφάλειας των δικτύων τηλεπικοινωνιών και πληροφορικής και της διασφάλισης του απορρήτου.

1. Ασφάλεια δικτύων ηλεκτρονικών επικοινωνιών

Η ασφάλεια των δικτύων ηλεκτρονικών επικοινωνιών περιλαμβάνει στον ορισμό της τις παραμέτρους α) ιδιωτικότητα (ότι η επικοινωνία δεν υποκλέπτεται), β) ακεραιότητα (ότι τα στοιχεία της επικοινωνίας φθάνουν στους αποδέκτες χωρίς αλλοίωση), γ) αυθεντικότητα (ότι τα πρόσωπα που συνδιαλέγονται είναι πραγματικά αυτά), δ) διαθεσιμότητα (ότι τα δίκτυα μπορούν να αντιμετωπίσουν και καταστάσεις κρίσεως) . Όπως προκύπτει και εκ των παραμέτρων αυτών, 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 και ρητά στην Α.Δ.Α.Ε., η οποία έχει εκδώσει ήδη σχετικούς Κανονισμούς. Η Ε.Ε.Τ.Τ. διατηρεί την αρμοδιότητα της διαθεσιμότητας και της φυσικής ασφάλειας των δικτύων.

2. Εθνική Στρατηγική για την Ασφάλεια των Δικτύων

Για την αντιμετώπιση των σημαντικών κινδύνων από κακόβουλες προσβάσεις στα αρχεία υπολογιστικών συστημάτων φορέων στρατηγικής σημασίας της χώρας (π.χ. ΔΕΗ, αερομεταφορές, τραπεζικά συστήματα κλπ.) απαιτείται η εκπόνηση από την Α.Δ.Α.Ε. εθνικής στρατηγικής για την ασφάλεια των δικτύων και η μέριμνα για τη συνεχή επικαιροποίησή της. Η εθνική στρατηγική θα εγκρίνεται από τους αρμόδιους Υπουργούς και θα εντάσσεται στην Πολιτική Ασφαλείας Δικτύων της Πολιτείας. Σχετική πρόταση έχει υποβληθεί στα συναρμόδια Υπουργεία.

3. Εποπτεία Δικτύων

Θα πρέπει να διαμορφωθεί ρυθμιστικό πλαίσιο για την εποπτεία της ασφάλειας των δικτύων των φορέων στρατηγικής σημασίας της χώρας και να θεσπιστεί η υποχρέωση των φορέων αυτών να αποκτήσουν αυστηρή πολιτική ασφαλείας. Η εποπτεία της πολιτικής αυτής θα πρέπει να ανατεθεί στην Α.Δ.Α.Ε., η οποία παράλληλα θα ενημερώνεται για τους νέους κινδύνους που παρουσιάζονται διεθνώς και θα μεταφέρει την ενημέρωση αυτή, σε όλους τους φορείς στρατηγικής σημασίας της χώρας για να επικαιροποιούν τις πολιτικές ασφάλειάς τους.

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

Οι απειλές ασφάλειας των επικοινωνιών δεν περιορίζονται μόνο σε οργανισμούς και επιχειρήσεις που ασχολούνται με τις επικοινωνίες. Προτείνεται να προβλεφθεί και ρητά η αρμοδιότητα της Α.Δ.Α.Ε. να προβαίνει σε ελέγχους και επί των νομικών ή φυσικών προσώπων που διαθέτουν εσωτερικά δίκτυα (intranet) ή ιδιωτικά τηλεφωνικά κέντρα (π.χ. ξενοδοχεία, επιχειρήσεις, κλπ.), πέραν εκείνων που ασχολούνται με τηλεπικοινωνιακές, ταχυδρομικές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία, καθώς και σε φυσικά ή νομικά πρόσωπα που προμηθεύουν εξοπλισμό ηλεκτρονικών επικοινωνιών ή παρέχουν υπηρεσίες σχετικές με δραστηριότητες ηλεκτρονικών επικοινωνιών στους οργανισμούς και επιχειρήσεις που υπάγονται ήδη, σύμφωνα με την ισχύουσα νομοθεσία, στην ελεγκτική αρμοδιότητα της Α.Δ.Α.Ε..

Τούτο προκύπτει άλλωστε από το γεγονός ότι το δικαίωμα που προστατεύεται από το άρθρο 19 του Συντάγματος αποτελεί απόλυτο δικαίωμα, το οποίο κατοχυρώνεται έναντι πάντων (δημόσιων φορέων και ιδιωτών).

5. Έλεγχος Ε.Υ.Π. και άλλων Αρχών που έχουν τη δυνατότητα να ζητούν άρση του απορρήτου.

Οι Αρχές αυτές θα πρέπει να οριοθετήσουν τους τομείς δραστηριότητάς τους σε σχέση με τον τομέα των επικοινωνιών. Θα πρέπει επίσης να προσαρμοστούν άμεσα, νομικά και τεχνικά στις διατάξεις του ΠΔ 47/2005. Τέλος, θα πρέπει να διευκολύνουν τον έλεγχο του ελεγκτικού φορέα στον οποίον υπάγονται.

6. Πιστοποίηση Ασφάλειας του εξοπλισμού των παρόχων ηλεκτρονικών επικοινωνιών

Η Α.Δ.Α.Ε. θα πρέπει να πιστοποιεί την ύπαρξη μέτρων ασφαλείας του εξοπλισμού και του λογισμικού που χρησιμοποιούνται ή μπορούν να χρησιμοποιηθούν από τις υπαγόμενες στον έλεγχό της υπηρεσίες, οργανισμούς και επιχειρήσεις, σε σχέση με τις κανονιστικές πράξεις για τη διασφάλιση του απορρήτου των επικοινωνιών που εκδίδει. Η διάθεση και χρήση του εξοπλισμού αυτού χωρίς την εν λόγω πιστοποίηση θα καθίστανται παράνομες.

7. Ενημέρωση Α.Δ.Α.Ε. κατά την προμήθεια εξοπλισμού

Οι προμηθευτές εξοπλισμού παραβίασης του απορρήτου θα πρέπει να ενημερώνουν την Α.Δ.Α.Ε. για οποιοδήποτε αίτημα αγοράς σχετικού εξοπλισμού ή και ανταλλακτικών του.

8. Έλεγχος καταγγελιών για παραβίαση του απορρήτου των επικοινωνιών

Με βάση το ισχύον θεσμικό πλαίσιο, η Α.Δ.Α.Ε. 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.

9. Δυνατότητα της Α.Δ.Α.Ε. 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. Για το σκοπό αυτό μεσολαβεί είτε βούλευμα του Συμβουλίου Εφετών ή του Συμβουλίου Πλημμελειοδικών, ανάλογα με τη βαρύτητα του υπό διερεύνηση αδικήματος, είτε εισαγγελική διάταξη που επικυρώνεται με αντίστοιχο βούλευμα. Για λόγους εθνικής ασφάλειας απαιτείται απλώς διάταξη του Εισαγγελέα Εφετών. Η Α.Δ.Α.Ε. προβλέπεται να ενημερώνεται σε κάθε περίπτωση, ανεξαρτήτως της Αρχής που υποβάλλει το σχετικό αίτημα άρσης του απορρήτου. Στο πλαίσιο αυτό, η Α.Δ.Α.Ε., 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 περιπτώσεις αυτές θα πρέπει να προβλεφθεί η δυνατότητα της Α.Δ.Α.Ε. να ζητεί 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 Α.Δ.Α.Ε..

10. 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 παράβασης της κείμενης νομοθεσίας σχετικά με την προστασία του απορρήτου των επικοινωνιών. Περαιτέρω, εφόσον κρίνεται σκόπιμο από τη δικαστική αρχή, η ΑΔΑΕ θα καλείται να λάβει γνώση της σχετικής δικογραφίας και το αργότερο εντός τριάντα ημερών από την επίδοση της κλήσεως να υποβάλει, εφόσον επιθυμεί, έκθεση με τις απόψεις της για όλες τις καταγγελλόμενες πράξεις που διερευνώνται.

11. Αποφασιστική αρμοδιότητα της Α.Δ.Α.Ε. κατά την εφαρμογή του Π.Δ.47/2005

Θα πρέπει να προβλεφθεί ρητά στο εν λόγω Π.Δ. ότι η Α.Δ.Α.Ε. 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 του προεδρικού αυτού διατάγματος, για κάθε θέμα σχετικό με τη διαδικασία άρσης του απορρήτου των επικοινωνιών.

12. Διατύπωση γνώμης της Α.Δ.Α.Ε. για την έκδοση του Κανονισμού Γενικών Αδειών της Ε.Ε.Τ.Τ.

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

13. Διατύπωση γνώμης της Α.Δ.Α.Ε. για την έκδοση της Κ.Υ.Α. του άρθρου 24 παρ.19 του Ν.3431/2006.

Η γνώμη της Α.Δ.Α.Ε. προτείνεται να διατυπώνεται 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. Περαιτέρω, προτείνεται να ανατεθεί στην Α.Δ.Α.Ε. η αρμοδιότητα να διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, ελέγχους σχετικούς με τη διάθεση, κατοχή και χρήση του εν λόγω εξοπλισμού, ενημερώνοντας σχετικά την Ε.Ε.Τ.Τ..

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

Μεταξύ των αδικημάτων για τα οποία προβλέπεται άρση απορρήτου δεν περιλαμβάνεται το αδίκημα της πορνογραφίας ανηλίκων μέσω του διαδικτύου (άρθρο 348Α ΠΚ), παρά το γεγονός ότι το αδίκημα αυτό λαμβάνει πλέον επικίνδυνες διαστάσεις. Προτείνεται, στο τέλος της πρώτης παραγράφου του άρθρου 4 του Ν. 2225/94, να προστεθούν και τα αδικήματα των άρθρων 348Α και 370 , 370 Α, Β, Γ του Ποινικού Κώδικα.

15. Άσκηση ελέγχου από το προσωπικό της Α.Δ.Α.Ε.

Θα πρέπει να προβλεφθεί η δυνατότητα άσκησης ελέγχου όχι μόνο από μέλη της Ολομελείας της Α.Δ.Α.Ε., αλλά και από το προσωπικό της, κατόπιν σχετικής απόφασης της Ολομελείας, λόγω του όγκου των ελέγχων που καλείται να διενεργήσει η Α.Δ.Α.Ε..

16. Υποκείμενα Ακρόασης από την Α.Δ.Α.Ε.

Θα πρέπει να διευρυνθεί ο κύκλος των προσώπων τα οποία μπορεί να καλέσει σε ακρόαση η Α.Δ.Α.Ε., υπό την προϋπόθεση ότι συμβάλλουν στην εκπλήρωση της αποστολής της.

17. Αυστηρότερες διοικητικές κυρώσεις

Οι διοικητικές κυρώσεις που μπορεί να επιβάλει η Α.Δ.Α.Ε. 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 εν λόγω επιχειρήσεων, δεν μπορούν να έχουν αποτρεπτικό χαρακτήρα, αν και η ίδρυση ανεξαρτήτων διοικητικών αρχών επιβάλλεται κυρίως λόγω του προληπτικού χαρακτήρα του ελέγχου

τους. Υπό την έννοια αυτή, χωρίς την πρόβλεψη αυστηρότερων διοικητικών κυρώσεων, αναιρείται ο δικαιολογητικός λόγος ύπαρξης των ανεξαρτήτων διοικητικών αρχών.

Προτείνεται η επιβολή διοικητικών κυρώσεων σε κυμαινόμενο ποσοστό, αναλόγως του κύκλου εργασιών των ελεγχομένων επιχειρήσεων και της βαρύτητας της παραβάσεως.

Επιπλέον, πρέπει να προβλεφθούν αυξημένες διοικητικές κυρώσεις σε περίπτωση διάπραξης αδικήματος εις βάρος της εθνικής ασφάλειας της χώρας.

Οι κυρώσεις αυτές θα πρέπει να συνδέονται με το σύνολο της αρμοδιότητας της Α.Δ.Α.Ε. και να μη σχετίζονται μόνο με το απόρρητο των επικοινωνιών και τους όρους και τη διαδικασία άρσης αυτού.

18. Ελεγκτικός ρόλος της Α.Δ.Α.Ε. 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 διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ

Η προβλεπόμενη από την Οδηγία αυτή διατήρηση δεδομένων επικοινωνίας για μακρά χρονική περίοδο καθιστά αναγκαία, κατά τη διαδικασία ενσωμάτωσής της στην εθνική έννομη τάξη, την πρόβλεψη ελέγχου από την Α.Δ.Α.Ε. 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.

19. Ενίσχυση των μέσων για την υλοποίηση του θεσμικού ρόλου της Α.Δ.Α.Ε..

α. Προϋπολογισμός της Α.Δ.Α.Ε.

Ο προϋπολογισμός της Α.Δ.Α.Ε. το έτος 2003 ανήλθε στο ποσό των 400.000 ευρώ, το έτος 2004 στο ποσό των 708.979 ευρώ, και το έτος 2005 στο ποσό των 1.997.024 . Υπό τα δεδομένα αυτά παρίσταται άμεση ανάγκη αναλογικής αύξησης του προϋπολογισμού της Α.Δ.Α.Ε. στο πλαίσιο των αρμοδιοτήτων της, προκειμένου να αντεπεξέλθει στην αυξημένη ελεγκτική της αρμοδιότητα, να εξοπλισθεί με τα κατάλληλα τεχνικά μέσα και να στελεχωθεί με το αναγκαίο εξειδικευμένο προσωπικό.

β. Στελέχωση της Α.Δ.Α.Ε.

i) Το προσωπικό της Αρχής άρχισε να προσλαμβάνεται από το Νοέμβριο του 2004 και εφεξής. Μέχρι τότε, η Α.Δ.Α.Ε. λειτουργούσε με την Ολομέλειά της. Με βάση τις σημερινές ανάγκες αλλά και τις νέες απαιτήσεις εκτιμάται ότι για τη στελέχωση της ΑΔΑΕ απαιτούνται τουλάχιστον εκατό (100) θέσεις, από τις οποίες πενήντα έξι (56) είναι θέσεις ειδικού επιστημονικού προσωπικού, οι τριάντα οκτώ (38) είναι θέσεις τακτικού προσωπικού, οι πέντε (5) είναι θέσεις δικηγόρων παρ' εφέταις με έμμισθη εντολή και μία (1) θέση Νομικού Συμβούλου.

ii) Το προσωπικό αυτό της Α.Δ.Α.Ε. 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 Α.Δ.Α.Ε., το είδος των πρόσθετων απολαβών και το

ύψος αυτών να καθορίζονται με κοινή απόφαση των Υπουργών Οικονομίας και Οικονομικών και Δικαιοσύνης, κατά παρέκκλιση από τις κείμενες διατάξεις.

iii) Με την υπάρχουσα στελέχωση της Α.Δ.Α.Ε. 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 η ανάγκη να προβλεφθεί με νομοθετική ρύθμιση ότι κατά την πρώτη εφαρμογή συγκρότησης του υπηρεσιακού συμβουλίου και του δευτεροβάθμιου πειθαρχικού συμβουλίου της Αρχής, η Ολομέλεια της Α.Δ.Α.Ε. μπορεί με απόφασή της να αναθέτει καθήκοντα προϊσταμένου των διοικητικών υπηρεσιών της στο προσωπικό της.

γ. Τεχνολογικός εξοπλισμός

Η διαρκής εξέλιξη της τεχνολογίας επιβάλλει τον ανάλογο εξοπλισμό των ελεγκτικών αρχών με σύγχρονα μέσα.

Ο εξοπλισμός αυτός ενδεικτικά αναφέρεται 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, κτλ.)

δ. Υποδομές

Η αναγνώριση του θεσμικού ρόλου της Α.Δ.Α.Ε. πρέπει να συνοδεύεται από τις αναγκαίες κτηριακές και υλικοτεχνικές υποδομές (π.χ. πληροφοριακά συστήματα, οχήματα για τη μετάβαση στις περιοχές ελέγχου κλπ.).

ε. Οικονομική ευελιξία

Για τη διευκόλυνση του έργου της, η Α.Δ.Α.Ε. θα πρέπει να μπορεί να συνάπτει συμβάσεις παροχής υπηρεσιών, μελετών και προμηθειών για θέματα που άπτονται των σκοπών της και της λειτουργίας της. Η σύναψη και η υλοποίηση των συμβάσεων αυτών θα διέπονται από τους σχετικούς κανονισμούς της Α.Δ.Α.Ε., 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 Α.Δ.Α.Ε. ειδικός λογαριασμός.

Στον ειδικό λογαριασμό θα αποδίδονται και περιέρχονται έσοδα και κάθε άλλο ποσό το οποίο εισπράττεται από οποιαδήποτε διοικητική ή δικαστική αρχή ή άλλον νόμιμο τίτλο ως χρηματική ποινή, δικαστικό πρόστιμο ή προϊόν δήμευσης σε σχέση με τις αρμοδιότητες της Α.Δ.Α.Ε. σύμφωνα με το νόμο.

Ο ειδικός λογαριασμός της Α.Δ.Α.Ε. θα υπόκειται στον έλεγχο ορκωτών ελεγκτών και ο τρόπος της οικονομικής του διαχείρισης θα καθορίζεται με κοινή απόφαση των συναρμοδίων Υπουργών μετά από εισήγηση της Α.Δ.Α.Ε..

Σε κάθε περίπτωση θα πρέπει να προβλεφθεί αρμοδιότητα της Ολομέλειας της Α.Δ.Α.Ε. να καθορίζει με αποφάσεις της τη σύσταση και τις αμοιβές ομάδων εργασίας, καθώς και την αποζημίωση για τη διενέργεια ελέγχου. Ως γνωστόν, ο έλεγχος αυτός είναι χρονοβόρος και απαιτεί διαρκή ετοιμότητα και συχνή μετακίνηση των ελεγκτών.

στ. Ίδια έσοδα

Η ανεξαρτησία της Αρχής 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 Ε.Ε.Τ.Τ., θα περιέρχονται στον ειδικό λογαριασμό αυτής και θα εισπράττονται σύμφωνα με τις διατάξεις του Κ.Ε.Δ.Ε.. Οι πόροι του λογαριασμού αυτού θα είναι: έσοδα από διοικητικές κυρώσεις (πρόστιμα) που επιβάλλονται από την Αρχή, αμοιβές από εργασίες πιστοποιήσεων, διοικητικά τέλη στο πλαίσιο ελέγχου της εφαρμογής της διαδικασίας άρσης του απορρήτου σύμφωνα με το Π.Δ.47/2005 κ.α.

ΠΑΡΑΡΤΗΜΑ Α

Ν. 3115/2003

άρθρου 19 του Συντάγματος.

Προστασία του απορρήτου των επικοινωνιών

οφάσεις της Α.Δ.Α.Ε. κοινοποιούνται με μέριμνά της στον Υπουργό Δικαιοσύνη

σύμφωνα με το άρθρο 1 του ιδρυτικού της νόμου, σκοπός της είναι

η προστασία του απορρήτου των επιστολών

ελεύθερης ανταπόκρισης

ΕΚΘΕΣΗ ΠΕΠΡΑΓΜΕΝΩΝ
ΕΤΟΥΣ 2005

ΠΑΡΑΡΤΗΜΑ Α

Αριθμ: 629 α

ΑΠΟΦΑΣΗ

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

΄Εχοντας υπόψη:
α. Το Ν. 3115/27.02.2003, άρθρο 1 παραγρ.1
β. Το Ν. 3115/27.02.2003, άρθρο 6 παράγρ.1
γ. Ὀτι εκ της παρούσας Αποφάσεως δεν προκύπτει δαπάνη για το Δημόσιο
δ. Τη σχετική εισήγηση της Υπηρεσίας

Α π ο φ ά σ ι σ ε,
κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ
Άρθρο 1
Σκοπός – Πεδίο Εφαρμογής

Σκοπός του παρόντος Κανονισμού είναι:

1. Η θέσπιση των υποχρεώσεων των φορέων παροχής κινητών τηλεπικοινωνιακών υπηρεσιών για τη διασφάλιση του απορρήτου των κινητών τηλεπικοινωνιακών υπηρεσιών στα πλαίσια της σχετικής Νομοθεσίας Ν. 2225/94 «Περί προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Ν. 3115/03 "Περί Διασφάλισης του Απορρήτου των Επικοινωνιών").
2. Η παρουσίαση βασικών χαρακτηριστικών ασφαλείας των τεχνολογιών κινητών επικοινωνιών δεύτερης και τρίτης γενιάς.
3. Η θέσπιση διαδικασιών ελέγχου στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του παρόντος Κανονισμού υπάγονται όλοι οι τηλεπικοινωνιακοί πάροχοι οι οποίοι παρέχουν Κινητές Τηλεπικοινωνιακές Υπηρεσίες.

Άρθρο 2
Ορισμοί

Για τις ανάγκες του παρόντος Κανονισμού χρησιμοποιούνται οι παρακάτω ορισμοί.

ακεραιότητα: Η επιβεβαίωση ότι τα δεδομένα τα οποία έχουν σταλεί, έχουν παραληφθεί ή έχουν αποθηκευθεί είναι πλήρη και αμετάβλητα.

αντίγραφα ασφάλειας: Τα αντίγραφα των ηλεκτρονικών αρχείων πληροφοριών που αφορούν σε δεδομένα επικοινωνίας και χρησιμοποιούνται σε περιπτώσεις καταστροφής των πρωτευόντων αρχείων για την ανάκτησή τους.

απειλή: Η εν δυνάμει παραβίαση της ασφάλειας ενός συστήματος

αυθεντικότητα: Η επιβεβαίωση της εγκυρότητας της ταυτότητας.

δεδομένα θέσης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία στο τηλεπικοινωνιακό δίκτυο και υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας.

δεδομένα κίνησης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία για να επιτευχθεί η επικοινωνία μέσω του τηλεπικοινωνιακού δικτύου ή για την τιμολόγησή της.

δημόσιο δίκτυο κινητών επικοινωνιών: Τηλεπικοινωνιακό Δίκτυο αποτελούμενο από τα συστήματα μετάδοσης, τον εξοπλισμό μεταγωγής και τα λοιπά μέσα που επιτρέπουν την μεταφορά σημάτων πληροφορίας με χρήση ραδιοκυμάτων, οπτικών ή άλλων ηλεκτρομαγνητικών μέσων, των οποίων η χρήση είναι εν μέρει ή καθολική για την παροχή διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών σε τερματικά που δεν βρίσκονται σε σταθερές θέσεις.

δημόσιο τηλεπικοινωνιακό δίκτυο 3ης γενιάς: Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κινητών Επικοινωνιών 3ης Γενιάς (IMT-2000), το οποίο είναι σε θέση να υποστηρίζει καινοτόμες πολυμεσικές υπηρεσίες (πέραν των δυνατοτήτων των δικτύων 2ης Γενιάς όπως το GSM) με την υψηλή ταχύτητα επικοινωνίας που εξασφαλίζει μεταξύ τερματικών και δικτύου.

δημόσιες κινητές τηλεπικοινωνιακές υπηρεσίες: Τηλεπικοινωνιακές υπηρεσίες των οποίων η παροχή συνίσταται, συνολικά ή εν μέρει, στην εγκατάσταση ραδιοεπικοινωνίας με έναν κινητό χρήστη και οι οποίες χρησιμοποιούν, ολικώς ή εν μέρει, ένα Δημόσιο Δίκτυο Κινητών Επικοινωνιών.

δημόσιες κινητές τηλεπικοινωνιακές υπηρεσίες 2ης γενιάς : οι δημόσιες Τηλεπικοινωνιακές Υπηρεσίες Κινητών

Επικοινωνιών που χρησιμοποιούν καθολικά ή εν μέρει ένα Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κινητών Επικοινωνιών 2ης Γενιάς, όπως αυτές οι υπηρεσίες προσδιορίζονται στις Συστάσεις των Τηλεπικοινωνιακών Δικτύων Κινητών Επικοινωνιών όπως το GSM1800 /GSM900.

δημόσιες κινητές τηλεπικοινωνιακές υπηρεσίες 3ης γενιάς : οι δημόσιες Τηλεπικοινωνιακές Υπηρεσίες Κινητών Επικοινωνιών που χρησιμοποιούν καθολικά ή εν μέρει ένα Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κινητών Επικοινωνιών 3ης Γενιάς, όπως αυτές οι υπηρεσίες προσδιορίζονται στις Συστάσεις των Τηλεπικοινωνιακών Δικτύων Κινητών Επικοινωνιών 3ης Γενιάς, UMTS (IMT-2000) που εκδίδονται από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προδιαγραφών (ETSI) και το Διεθνή Οργανισμό Τηλεπικοινωνιών (ITU).

έλεγχος πρόσβασης: Η πρόληψη μη εξουσιοδοτημένης χρήσης ενός πόρου, συμπεριλαμβανομένης της πρόληψης της χρήσης του πόρου με μη εξουσιοδοτημένο τρόπο.

εμπιστευτικότητα: Η προστασία των επικοινωνιών ή των αποθηκευμένων δεδομένων από την υποκλοπή και την ανάγνωση από μη εξουσιοδοτημένα άτομα.

εξουσιοδότηση: Η διαδικασία χορήγησης δικαιώματος πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από την οντότητα που ελέγχει τον πόρο για τον οποίο ζητάται η πρόσβαση.

επίθεση: Οι δραστηριότητες που αναπτύσσονται με σκοπό την παράκαμψη ή την εκμετάλλευση των ατελειών των μηχανισμών ασφάλειας ενός συστήματος. Διακρίνονται σε άμεσες (εκμετάλλευση ατελειών αλγορίθμων, αρχών και ιδιοτήτων του μηχανισμού ασφάλειας) και εμμεσες επιθέσεις (υποχρέωση του συστήματος να χρησιμοποιήσει το μηχανισμό ασφάλειας με λανθασμένο τρόπο, παράκαμψη μηχανισμών).

επικοινωνία: περιλαμβάνει κάθε είδους επικοινωνία μεταξύ ανθρώπων, αντικειμένων, ανθρώπων και αντικειμένων η οποία γίνεται είτε με τη μορφή του προφορικού ή γραπτού λόγου, είτε με τη μορφή μουσικής, ήχων και εικόνων, είτε με τη μορφή σημάτων είτε και με οποιοδήποτε συνδυασμό όλων αυτών των μορφών.

κινητό τερματικό: Περιλαμβάνει την κινητή συσκευή και την κάρτα ταυτότητας συνδρομητή (SIM ή USIM) που περιέχει όλα τις πληροφορίες και τα δεδομένα που αφορούν τον συνδρομητή, ενώ η Κινητή Συσκευή ή κινητό τηλέφωνο, μπορεί να είναι κοινή για οποιοδήποτε δίκτυο χρησιμοποιεί ο συνδρομητής.

Προστασία του απορρήτου: Η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων επικοινωνίας από άλλα πρόσωπα, χωρίς την συγκατάθεσή τους, εξαιρουμένων των περιπτώσεων που προβλέπονται στο σύνταγμα και τους νόμους.

σταθερές τηλεπικοινωνιακές υπηρεσίες: Οι υπηρεσίες των οποίων η παροχή συνίσταται συνολικά ή εν μέρει στη μετάδοση και δρομολόγηση σημάτων μέσω σταθερών τηλεπικοινωνιακών δικτύων εξαιρουμένων των ραδιοφωνικών και τηλεοπτικών εκπομπών.

συνδρομητής: Κάθε φυσικό η νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών για την παροχή των υπηρεσιών αυτών.

σταθμός βάσης: Σταθερός σταθμός του δικτύου κινητών επικοινωνιών που χρησιμοποιείται για την ασύρματη επικοινωνία με τα κινητά τερματικά.

ταυτότητα: Οι πληροφορίες που προσδιορίζουν το χρήστη με μοναδικό τρόπο.

τηλεπικοινωνία: Η μεταφορά ήχων, σημάτων, εικόνων, δεδομένων, και εν γένει κάθε φύσης πληροφοριών μεταδιδόμενων εν όλω ή εν μέρει μέσω ενσύρματων, ασύρματων, ηλεκτρομαγνητικών, φωτοηλεκτρονικών ή φωτοοπτικών συστημάτων.

τηλεπικοινωνιακός πάροχος: Κάθε φυσικό ή νομικό πρόσωπο που παρέχει τηλεπικοινωνιακές υπηρεσίες στο κοινό ή δημόσιο τηλεπικοινωνιακό δίκτυο. Όπου στο κείμενο αναφέρεται ο όρος χωρίς επεξήγηση θα εννοείται ο Πάροχος τηλεπικοινωνιακών υπηρεσιών.

υπηρεσία κλήσης έκτακτης ανάγκης: Η υπηρεσία λήψης και διαχείρισης κλήσεων έκτακτης ανάγκης που γίνονται προς έναν τηλεφωνικό αριθμό και δρομολογούνται προς ειδικές κρατικές και μη Υπηρεσίες όπως είναι η Αστυνομία, η Πυροσβεστική Υπηρεσία, τα Νοσοκομεία, κλπ.

χρήστης: Κάθε φυσικό πρόσωπο ή νομική οντότητα που χρησιμοποιεί ή ζητά διαθέσιμη στο κοινό τηλεπικοινωνιακή υπηρεσία.

Χρήστης Παρόχου: Κάθε φυσικό πρόσωπο που ανήκει στο προσωπικό ή τους συνεργάτες του Παρόχου και χρησιμοποιεί τα συστήματα και τις υποδομές του Παρόχου.

ΚΕΦΑΛΑΙΟ ΙΙ

Πολιτική Διασφάλισης Απορρήτου Κινητών Τηλεπικοινωνιακών Υπηρεσιών

Άρθρο 3

Ορισμός - Γενικές Απαιτήσεις και Συστάσεις

1. Πολιτική Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΚΤΥ), είναι το σύνολο των κριτηρίων και κανόνων που καθορίζουν τις απαιτήσεις, τις υποχρεώσεις και τα δικαιώματα που διέπουν τη λειτουργία των τηλεπικοινωνιακών παρόχων και των χρηστών των τηλεπικοινωνιακών υπηρεσιών, με σκοπό την προστασία του απορρήτου των επικοινωνιών που διεξάγονται μέσω δικτύων κινητών τηλεπικοινωνιακών επικοινωνιών.
2. Η ΠΔΑΚΤΥ θα εκπονείται από τους τηλεπικοινωνιακούς παρόχους διαθέσιμων στο κοινό κινητών τηλεπικοινωνιακών υπηρεσιών με βάση τις απαιτήσεις και τις υποδείξεις του παρόντος Κανονισμού και θα εφαρμόζεται από αυτούς μετά την έγκρισή της από την ΑΔΑΕ.
3. Η ΠΔΑΚΤΥ αποτελείται από επί μέρους πολιτικές όπως είναι η Πολιτική προστασίας των Δικτύων Κινητών Επικοινωνιών, η Πολιτική επεξεργασίας δεδομένων Επικοινωνίας, η Πολιτική σε σχέση με το προσωπικό και τους συνεργάτες των τηλεπικοινωνιακών παρόχων, η Πολιτική πρόσβασης, η Πολιτική αποδεκτής χρήσης και η Πολιτική άρσης του απορρήτου από τις οποίες απορρέουν τα δικαιώματα και οι υποχρεώσεις των εμπλεκομένων στη λειτουργία, τη διαχείριση και τη χρήση των τηλεπικοινωνιακών υπηρεσιών.
4. Η ΠΔΑΚΤΥ για να θεωρείται επαρκής θα πρέπει να διαθέτει τουλάχιστον τα ακόλουθα χαρακτηριστικά:

α) Να υλοποιείται μέσω διαδικασιών διαχείρισης συστημάτων, δημοσιοποίησης οδηγιών αποδεκτής χρήσης ή άλλων αντίστοιχων κατάλληλων μεθόδων.

β) Οι διαδικασίες οι οποίες σχετίζονται με την υλοποίηση της πολιτικής πρέπει να περιλαμβάνουν τουλάχιστον τον προσδιορισμό ταυτότητας, την αυθεντικότητα, την εξουσιοδότηση, τον έλεγχο πρόσβασης, την εμπιστευτικότητα, την ακεραιότητα, την προστασία του απορρήτου και τον έλεγχο παραβίασης της ασφάλειας του απορρήτου.

γ) Να εφαρμόζεται μέσω εργαλείων ασφάλειας ή/και μέσω διαδικασιών ασφάλειας.

δ) Να καθορίζει τις περιοχές ευθύνης των χρηστών και των χρηστών παρόχου. Επιπλέον οι μηχανισμοί μεταβολής της πολιτικής διασφάλισης του απορρήτου πρέπει να είναι καλά ορισμένοι, περιλαμβάνοντας τη διαδικασία, τους εμπλεκόμενους, καθώς και τους υπεύθυνους προς έγκριση.

5. Επίσης, συνιστάται η ΠΔΑΚΤΥ:

α) Να είναι ανεξάρτητη, στο μέτρο που είναι δυνατόν από τεχνικής απόψεως, από συγκεκριμένο εξοπλισμό (υλικό, λογισμικό) και

β) Να βασίζεται σε μια ανοικτή αρχιτεκτονική έτσι ώστε να καθίσταται βιώσιμη μακροπρόθεσμα.

6. Η ΠΔΑΚΤΥ υπόκειται σε έλεγχο από την ΑΔΑΕ, τόσο ως προς την πληρότητα και αποτελεσματικότητά της, όσο και ως προς τον βαθμό εφαρμογής της.

Άρθρο 4
Χάραξη και στοιχεία Πολιτικής Διασφάλισης Απορρήτου Κινητών Τηλεπικοινωνιακών Υπηρεσιών

ι. Ένας τηλεπικοινωνιακός πάροχος προκειμένου να χαράξει την πολιτική του μπορεί, χωρίς να υποχρεώνεται ή να περιορίζεται, να ακολουθήσει τα παρακάτω βήματα:

α) Να προσδιορίσει τις πληροφορίες που πρέπει να προστατευτούν.
β) Να προσδιορίσει τα ευάλωτα σημεία του τηλεπικοινωνιακού δικτύου.
γ) Να προσδιορίσει τους κινδύνους και τις απειλές για τα α), β).
δ) Να προσδιορίσει τα μέτρα διασφάλισης της προστασίας του απορρήτου στις κινητές Τηλεπικοινωνιακές Υπηρεσίες.
ε) Να καθορίσει τις υποχρεώσεις των υπαλλήλων και συνεργατών του.
στ) Να καθορίσει τις δεσμεύσεις και υποχρεώσεις του έναντι των πελατών του.
ζ) Να καταρτίσει σχέδιο αναθεώρησης και βελτίωσης της ΠΔΑΚΤΥ κάθε φορά που θα εντοπίζεται νέος κίνδυνος ή αδυναμία ή που θα προκύπτουν νέες τεχνολογικές διευκολύνσεις διαχείρισης ασφάλειας.

2. Κάθε τηλεπικοινωνιακός πάροχος πρέπει, και σε περίπτωση που απαιτείται σε συνεργασία με τους παρόχους τηλεπικοινωνιακού δικτύου, να τεκμηριώνει με σχέδια την προστασία του απορρήτου για να αντιμετωπίσει προβλήματα που πιθανώς να εμφανισθούν σε έκτακτες περιστάσεις, όπως είναι η άρση του απορρήτου μετά από εντολή δικαστικών ή εισαγγελικών αρχών (Νόμος 2225) και η προβληματική λειτουργία των τηλεπικοινωνιακών ή/και των μηχανογραφικών συστημάτων του ή των συστημάτων των συνεργατών του.

Άρθρο 5
Προστατευόμενα στοιχεία κινητών επικοινωνιών

1. Κάθε πάροχος κινητών τηλεπικοινωνιακών υπηρεσιών οφείλει να διασφαλίζει και να προστατεύει το απόρρητο των διαφόρων δεδομένων Επικοινωνίας του περιεχόμενου της επικοινωνίας, και εν γένει κάθε πληροφορίας που αφορά τους συνδρομητές του και χρησιμοποιείται για την παροχή της τηλεπικοινωνιακής υπηρεσίας, τη διεκπεραίωση της επικοινωνίας, κ.τ.λ.

2. Σε συγκεκριμένο φυσικό ή νομικό πρόσωπο, που είναι συνδρομητής ή χρήστης ενός παρόχου κινητών τηλεπικοινωνιακών υπηρεσιών πρέπει να προστατεύεται το απόρρητο των ακόλουθων στοιχείων εισερχομένων και εξερχομένων κλήσεων:

α) Καλών και καλούμενος αριθμός,
β) Καλών και καλούμενος συνδρομητής-χρήστης,
γ) Χρόνος και διάρκεια επικοινωνίας,
δ) Εντοπισμός καλούντος ή και καλούμενου χρήστη,
ε) Στοιχεία που αφορούν στη χρέωση της επικοινωνίας,
στ) Περιεχόμενο και δεδομένα επικοινωνίας,
ζ) Ταυτότητα κινητής τερματικής συσκευής και ταυτότητα σύνδεσης.

3. Οι πάροχοι κινητών τηλεπικοινωνιακών υπηρεσιών θα πρέπει να προσδιορίζουν τους κινδύνους και τις ενδεχόμενες απειλές για τα παραπάνω στοιχεία. Ο πάροχος οφείλει να διασφαλίζει το απόρρητο της μετάδοσης και αποθήκευσης των δεδομένων Επικοινωνίας που χρησιμοποιούνται σε ένα δίκτυο κινητών επικοινωνιών. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να ενημερώνει τους συνδρομητές του με συγκεκριμένους τρόπους και μέσα της επιλογής του για οποιουσδήποτε ειδικούς κινδύνους σχετικά με την ασφάλεια των υπηρεσιών που παρέχει καθώς επίσης και οποιωνδήποτε δυνατοτήτων για την απομάκρυνση των κινδύνων και του κόστους των μέτρων που περιλαμβάνονται.

Άρθρο 6
Ευάλωτα Σημεία Δικτύου Κινητών Επικοινωνιών

Ενδεικτικά αναφέρονται ευάλωτα σημεία σε επιθέσεις και παραβιάσεις:

1. Τερματικών συσκευών χρηστών:

α) Η ίδια η συσκευή
β) Το αρχείο των εξερχόμενων ή εισερχόμενων κλήσεων
γ) Το αρχείο των καλούντων και καλούμενων αριθμών
δ) Ο τυχόν ενσωματωμένος αυτόματος τηλεφωνητής
ε) Τυχόν μνήμη καταγραφής
στ) Κάρτα Ταυτότητας Συνδρομητή (SIM)

2. Δικτύου:

α) Σταθμός Βάσης
β) Μικροκυματικές Ραδιοζεύξεις (μεταξύ σταθμών βάσης, κ.α.)
γ) Αλγόριθμοι Κρυπτογράφησης
δ) Διακομιστές (servers)
ε) Το φωνητικό ταχυδρομείο (Voice mail).
στ) Κεντρικοί κατανεμητές Παρόχου
ζ) Κέντρα μεταγωγής και συνδέσεις του δικτύου κινητών επικοινωνιών με το σταθερό τηλεπικοινωνιακό δίκτυο
η) Οι δρομολογητές κλήσεων όταν υπάρχει εκτροπή των κλήσεων σε εναλλακτικό φορέα παροχής τηλεπικοινωνιακών υπηρεσιών
θ) Η αποκάλυψη κλειδιών που χρησιμοποιούνται για κρυπτογράφηση.

Ο πάροχος κινητών τηλεπικοινωνιακών υπηρεσιών θα πρέπει να ενημερώνει τους χρήστες με συγκεκριμένα μέσα (γραπτές οδηγίες κλπ.) για τα ευάλωτα σημεία που ανήκουν στην περιοχή ευθύνης τους και θα λαμβάνει όλα τα προσήκοντα μέτρα για την προστασία των ευάλωτων σημείων που ανήκουν στην δικαιοδοσία του.

ΚΕΦΑΛΑΙΟ ΙΙΙ
Επιμέρους Πολιτικές Διασφάλισης Απορρήτου Κινητών Τηλεπικοινωνιακών Υπηρεσιών

Άρθρο 7
Ασφάλεια Δικτύων Κινητών Επικοινωνιών Δεύτερης Γενιάς

1. Η ασφάλεια ενός δικτύου κινητών επικοινωνιών δεύτερης γενιάς θα πρέπει να καλύπτει τις απαιτήσεις τόσο του παρόχου όσο και του συνδρομητή.
2. Ένας τηλεπικοινωνιακός πάροχος, διαχειριστής ενός δικτύου κινητών επικοινωνιών 2ης γενιάς, πρέπει να χρησιμοποιεί τις προτεινόμενες διαδικασίες ασφαλείας σχετικές με: α) την δημιουργία και διανομή των κλειδιών, β) την ανταλλαγή πληροφοριών με άλλους διαχειριστές και γ) το απόρρητο των αλγορίθμων.
3. Οι βασικοί στόχοι ασφάλειας για ένα πάροχο κινητών τηλεπικοινωνιακών υπηρεσιών μέσων ενός δικτύου κινητών επικοινωνιών 2ης γενιάς είναι:

α) Το απόρρητο της ταυτότητας του συνδρομητή, ώστε να μην μπορεί κάποιος τρίτος να γνωρίζει πότε και από που χρησιμοποιεί ο συνδρομητής το δίκτυο. Για να επιτευχθεί το απόρρητο της ταυτότητας του συνδρομητή, του αποδίδονται προσωρινές ταυτότητες. Κάθε συνδρομητής έχει μία Διεθνή Ταυτότητα Συνδρομητή η οποία είναι παγκοσμίως μοναδική και είναι αποθηκευμένη στην κάρτα SIM (Subscriber Identity Module). Η Διεθνής Ταυτότητα Συνδρομητή χρησιμοποιείται μόνο όταν δεν υπάρχει άλλος τρόπος να αναγνωρισθεί ο Συνδρομητής. Αυτό μπορεί να συμβεί κατά την διαδικασία δημιουργία της πρώτης σύνδεσης ενός καινούριου Συνδρομητή ή εφόσον υπάρξει κάποια απώλεια δεδομένων στο δίκτυο. Επιπλέον, στην διάρκεια της σύνδεσης στο δίκτυο, δίνεται σε τακτά χρονικά διαστήματα καινούρια Προσωρινή Ταυτότητα στον Κινητό Σταθμό, κάτι που καθιστά αρκετά δύσκολη την προσπάθεια γεωγραφικού εντοπισμού του Συνδρομητή. Εφόσον δεν υπάρχει κάποιο πρόβλημα με το δίκτυο, με κανένα τρόπο δεν πρέπει να μεταδίδεται η Διεθνής Ταυτότητα μέσω του αέρα σε καμιά άλλη περίπτωση εκτός από την διαδικασία της αρχικής σύνδεσης.

β) Η πιστοποίηση της ταυτότητας του συνδρομητή, ώστε ο διαχειριστής να είναι σίγουρος ότι χρεώνει το σωστό άτομο. Η διαδικασία πιστοποίησης στις κινητές επικοινωνίες 2ης γενιάς είναι μια μονομερής διαδικασία αφού ο Συνδρομητής δεν μπορεί να πιστοποιήσει την ταυτότητα του δικτύου. Βασικό ρόλο στη διαδικασία πιστοποίησης διαδραματίζει ο Αλγόριθμος Πιστοποίησης Α3, ο οποίος δεν είναι απαραίτητα κοινός για όλα τα δίκτυα αλλά για να υπάρχει συμβατότητα μεταξύ τους, οι βασικές του παράμετροι καθορίζονται από την κοινοπραξία GSM.

γ) Η προστασία των δεδομένων σηματοδοσίας, ώστε δεδομένα όπως αριθμοί τηλεφώνου να μην μπορούν να υποκλαπούν.

δ) Η προστασία της συνομιλίας, ώστε να προστατευτεί το απόρρητο της συνομιλίας. Η προστασία των δεδομένων Επικοινωνίας είναι επίσης απαραίτητη.Η χρησιμοποίηση ή μη της κρυπτογράφησης εξαρτάται από το δίκτυο κινητών επικοινωνιών και όχι από τον συνδρομητή. Μόνο ο σταθμός βάσης μπορεί να στείλει εντολή στον κινητό τερματικό σταθμό ώστε να ξεκινήσει η κρυπτογράφηση και από τις δύο πλευρές. Οι αλγόριθμοι, που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων, είναι γνωστοί ως Α8 και Α5 και είναι αποθηκευμένοι, ο μεν πρώτος στην κάρτα SIM και ο δεύτερος στην κινητή συσκευή. Συνήθως ο αλγόριθμος Α8 συνδυάζεται μαζί με το Α3 σε ένα νέο αλγόριθμο, τον Α3/8. Εφόσον υπάρχουν διαφορετικές εκδόσεις του αλγόριθμου Α5, πριν αρχίσει η κρυπτογράφηση είναι απαραίτητο να ενημερωθεί ο Σταθμός Βάσης για την έκδοση του αλγορίθμου που χρησι-

μοποιεί ο Κινητός Σταθμός. Το κλειδί κρυπτογράφησης πρέπει να ανανεώνεται κάθε φορά που πιστοποιείται η ταυτότητα του Συνδρομητή από το Δίκτυο και αυτό πρέπει να γίνεται πριν από κάθε κλήση ή κάθε φορά που ο Συνδρομητής επιθυμεί να συνδεθεί στο δίκτυο εκ νέου. Η συχνότητα της πιστοποίησης από τον Διαχειριστή του Δικτύου Κινητών Επικοινωνιών πρέπει να είναι τέτοια ώστε να ελαχιστοποιούνται οι πιθανότητες υποκλοπής δεδομένων συνομιλίας και σηματοδοσίας. .

4. Περιπτώσεις απειλών του συστήματος ασφαλείας ενός δικτύου κινητών επικοινωνιών δεύτερης γενιάς:

α) Απόκτηση πρόσβασης στο δίκτυο κορμού
β) Επιθέσεις στην κάρτα SIM
γ) Επίθεση στο αλγόριθμο A5
δ) Επίθεση με απομίμηση σταθμού βάσης
ε) Άρνηση των υπηρεσιών για ένα συνδρομητή λόγω παρεμβολής.

Άρθρο 8
Ασφάλεια Δικτύων Κινητών Επικοινωνιών Τρίτης Γενιάς

ι. Η ασφάλεια ενός δικτύου κινητών επικοινωνιών τρίτης γενιάς περιλαμβάνει τις παρακάτω βασικές αρχές:

α) Τα δεδομένα που σχετίζονται ή δημιουργούνται από τον χρήστη είναι επαρκώς προστατευμένα από κακή χρήση ή κατάχρηση
β) Οι υπηρεσίες που παρέχονται από τα δίκτυα εξυπηρέτησης και τους καταχωρητές στους σταθμούς βάσης είναι επαρκώς προστατευμένες από κακή χρήση ή κατάχρηση.
γ) Οι διαδικασίες ασφαλείας πρέπει να είναι επαρκώς ορισμένες ώστε να διασφαλιστεί η παγκόσμια χρήση τους και η περιαγωγή μεταξύ διαφορετικών δικτύων εξυπηρέτησης.
δ) Οι διαδικασίες και οι μηχανισμοί ασφαλείας πρέπει να μπορούν να επεκταθούν ή να αναθεωρηθούν ανάλογα με τις καινούριες απαιτήσεις που θα προκύψουν στο μέλλον.

2. Ένα δίκτυο κινητών επικοινωνιών τρίτης γενιάς πρέπει να χαρακτηρίζεται από όλες τις τεχνικές ασφαλείας που προστέθηκαν σε σχέση με τα δίκτυα κινητών επικοινωνιών δεύτερης γενιάς δηλαδή: πιστοποίηση της ταυτότητας του δικτύου και από τον συνδρομητή ώστε να αποκλείονται έτσι τις επιθέσεις «ψεύτικου σταθμού βάσης», αύξηση του μήκους των κλειδιών πιστοποίησης και κρυπτογράφησης με αποτέλεσμα τη δημιουργία ισχυρότερων αλγόριθμων, εισαγωγή μηχανισμών ασφαλείας τόσο μέσα στο δίκτυο όσο και μεταξύ των δικτύων και τέλος, προστασία των διασυνδέσεων μεταξύ Σταθμού Βάσης και Ελεγκτή. Σε ένα δίκτυο κινητών επικοινωνιών τρίτης γενιάς οι διαδικασίες ασφαλείας πρέπει να αντιμετωπίζονται με ενιαίο τρόπο.

3. Περιπτώσεις απειλών του συστήματος ασφαλείας ενός δικτύου κινητών επικοινωνιών τρίτης γενιάς:

α) Επιθέσεις στην κάρτα USIM
β) Επίθεση στο αλγόριθμο f8
γ) Επίθεση στο αλγόριθμο f9
δ) Επίθεση στην σηματοδοσία και στην διαδικασία επανασυγχρονισμού
ε) Επίθεση στις διαδικασίες που χρησιμοποιούνται για την πιστοποίηση και τη διευθέτησης κλειδιών

ζ) Επίθεση στους διαδοχικούς αριθμούς (SQN) οι οποίοι εξασφαλίζουν στο συνδρομητή ότι τα δεδομένα πιστοποίησης δεν έχουν ξαναχρησιμοποιηθεί.

4. Σε ένα δίκτυο κινητών επικοινωνιών με μικτά τμήματα δεύτερης και τρίτης γενιάς, θα εφαρμοστεί η διαδικασία Πιστοποίησης και Διευθέτησης Κλειδιών δεύτερης γενιάς αν ένα τουλάχιστον τμήμα, εξαιρουμένου του Υποσυστήματος Σταθμού Βάσης, είναι δεύτερης γενιάς. Αντίθετα για να πραγματοποιηθεί η διαδικασία Πιστοποίησης και Διευθέτησης Κλειδιών τρίτης γενιάς θα πρέπει όλα τα τμήματα, εξαιρουμένου του Υποσυστήματος Σταθμού Βάσης, να είναι τρίτης γενιάς.
5. Οι πάροχοι κινητών τηλεπικοινωνιακών υπηρεσιών 3ης γενιάς υποχρεούνται να ενημερώνουν τους συνδρομητές τους για την αλληλεπίδραση μεταξύ καρτών SIM, USIM και κινητών συσκευών με αποτέλεσμα την ενδεχόμενη έλλειψη ασφαλείας στις επικοινωνίες τους.

Άρθρο 9
Προστασία δικτύων κινητών επικοινωνιών

1. Η ασφάλεια δικτύων επικοινωνίας περιλαμβάνει: α) τις απειλές που οφείλονται στην εμπεριεχόμενη αξιοπιστία του ίδιου του δικτύου κινητών επικοινωνιών, και β) την ευαισθησία του στις απειλές από κακόβουλες πράξεις. Η ΑΔΑΕ αναγνωρίζει ότι η πηγή απειλής μπορεί να προέλθει από ένα άλλο διασυνδεόμενο δίκτυο τηλεπικοινωνιών (σταθερό, ασύρματο) και αυτό είναι εφικτό για το λόγο ότι η σηματοδοσία στο σταθερό τηλεφωνικό δίκτυο δεν είναι κρυπτογραφημένη. Για αυτό το λόγο η πολιτική ασφάλειας των παρόχων πρέπει να επιδιώκει να εντοπίζει τα σημεία που πρέπει να δοθεί ιδιαίτερη προσοχή.
2. Απαιτείται να λαμβάνονται τα απαραίτητα μέτρα για τη σωστή χωροθέτηση του τηλεπικοινωνιακού εξοπλισμού του παρόχου, την προστασία των γραμμών μεταφοράς του δικτύου καθώς και όλων των στοιχείων του δικτύου, συμπεριλαμβανομένων των ιστών των κεραιών, ώστε να εξασφαλίζονται έναντι κακοβούλων επιθέσεων και έναντι άλλων μορφών φυσικών παρεμβάσεων.
3. Τα σημεία εισόδου από άλλα τηλεπικοινωνιακά δίκτυα πρέπει να ελέγχονται επισταμένως.
4. Πρέπει να λαμβάνονται όλα τα απαραίτητα μέτρα προστασίας για τα ευάλωτα σημεία του δικτύου που αναφέρονται στο άρθρο 7 του παρόντος.

Άρθρο 10
Προστασία επεξεργασίας των δεδομένων Επικοινωνίας

Οι πάροχοι κινητών τηλεπικοινωνιακών υπηρεσιών οφείλουν να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της κείμενης νομοθεσίας για την προστασία της επεξεργασίας των δεδομένων Επικοινωνίας.

Άρθρο 11
Ασφάλεια σε σχέση με τους Χρήστες Παρόχου

Οι χρήστες παρόχου οφείλουν να συμμορφώνονται με τις διατάξεις της νομοθεσίας περί προστασίας του απορρήτου.

Ειδικότερα:

α) Απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία που συνδέονται με: i) το περιεχόμενο ή την ουσία της επικοινωνίας που πραγματοποιείται μέσω παρόχου υπηρεσιών επικοινωνιών ή ii) υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο μέσω ενός παρόχου υπηρεσιών επικοινωνιών ή iii) τα δεδομένα Επικοινωνίας που υποπίπτουν στην αντίληψη ή στην κατοχή του ως αποτέλεσμα της φύσης της εργασίας του.

β) Όσοι διαχειρίζονται ή έχουν πρόσβαση στη βάση δεδομένων των συνδρομητών απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία που συνδέονται με: i) υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο μέσω ενός παρόχου υπηρεσιών επικοινωνιών ή ii) τα δεδομένα Επικοινωνίας που υποπίπτουν στην αντίληψη ή στην κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

γ) Οι χρήστες παρόχου που διαχειρίζονται κλήσεις έκτακτης ανάγκης απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία συνδέονται με: i) το περιεχόμενο ή την ουσία της επικοινωνίας που πραγματοποιείται μέσω του τηλεπικοινωνιακού παρόχου ή ii) τα δεδομένα Επικοινωνίας (όπως μη ανακοινώσιμες συνδέσεις και διευθύνσεις) που υποπίπτουν στην αντίληψη ή στην κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

Οι εξαιρέσεις των προηγούμενων γενικών κανόνων, που επιβάλλονται για λόγους λειτουργίας του παρόχου ή προβλέπονται στην ισχύουσα νομοθεσία, θα περιγράφονται με σαφήνεια στην πολιτική ασφάλειας του τηλεπικοινωνιακού παρόχου.

Άρθρο 12
Πολιτική πρόσβασης

1. Η Πολιτική Πρόσβασης καθορίζει το επίπεδο πρόσβασης χρηστών παρόχου και διεργασιών λογισμικού σε καθένα από τα συστήματα υλικού και λογισμικού από τα οποία αποτελείται ο εξοπλισμός του παρόχου για την παροχή των κινητών τηλεπικοινωνιακών υπηρεσιών.
2. Η Πολιτική Πρόσβασης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΚΤΥ.
3. Ο πάροχος οφείλει να διαθέτει και να εφαρμόζει Πολιτική Πρόσβασης για τα συστήματα τα οποία αναφέρονται σε εξωτερικές συνδέσεις, επικοινωνίες φωνής και δεδομένων, τηλεπικοινωνιακές συσκευές και προγράμματα λογισμικού.
4. Η Πολιτική Πρόσβασης περιγράφει για κάθε σύστημα, με τρόπο λεπτομερή και σαφή, τουλάχιστον τις ακόλουθες διαδικασίες:

(α) Διαδικασίες προσθήκης νέων χρηστών και χρηστών παρόχου στο συγκεκριμένο δίκτυο κινητών επικοινωνιών

(β) Διαδικασίες εξουσιοδότησης σχετικά με την προσθήκη, διαγραφή και αλλαγή των επιπέδων πρόσβασης των χρηστών παρόχου σε τηλεπικοινωνιακές υπηρεσίες του εν λόγω συστήματος.

(γ) Διαδικασίες ταυτοποίησης χρηστών

(δ) Τρόπους ελέγχου των παραπάνω διαδικασιών και διαχείρισης του επιπέδου πρόσβασης που παραχωρείται στους χρήστες παρόχου

(ε) Διαδικασίες πρόσβασης των χρηστών παρόχου των κινητών τηλεπικοινωνιακών υπηρεσιών σε συστήματα που διατηρούν δεδομένα κίνησης και θέσης χρηστών

(στ) Σε περίπτωση που χρησιμοποιείται κρυπτογράφηση, η Πολιτική Πρόσβασης θα πρέπει να περιέχει τις διαδικασίες πρόσβασης των χρηστών παρόχου σε συστήματα κρυπτογράφησης/αποκρυπτογράφησης καθώς και σε διαδικασίες σχετικά με την διαχείριση, διανομή, εισαγωγή και αρχειοθέτηση των κλειδιών κρυπτογράφησης. Οι πληροφορίες αυτές θα αναφέρονται σε καταλλήλως διαβαθμισμένο παράρτημα των εγγράφων που περιέχουν την Πολιτική Πρόσβασης.

Άρθρο 13
Πολιτική Αποδεκτής Χρήσης

1. Η Πολιτική Αποδεκτής Χρήσης περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών και χρηστών παρόχου των συστημάτων μετάδοσης του δικτύου κινητών επικοινωνιών ενός παρόχου.
2. Η Πολιτική Αποδεκτής Χρήσης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΚΤΥ.
3. Σκοπός της είναι να διασφαλίσει ότι οι χρήστες και οι χρήστες παρόχου δεν θα εκμεταλλευτούν την πρόσβαση που τους παρέχεται σύμφωνα με την Πολιτική Πρόσβασης σε παντός είδους τηλεπικοινωνιακά δίκτυα προκειμένου να προβούν σε ενέργειες που παραβιάζουν οποιονδήποτε νόμο του κράτους.
4. Η Πολιτική Αποδεκτής Χρήσης πρέπει να είναι προσαρμοσμένη στην κατηγορία χρηστών στην οποία απευθύνεται (χρηστών και χρηστών παρόχου) και να είναι σύμφωνη με την Πολιτική Πρόσβασης για κάθε κατηγορία χρηστών.
5. Η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει, με όσο το δυνατόν πιο λεπτομερή και κατανοητό τρόπο ώστε να αποφεύγονται οι παρερμηνείες, το ακόλουθο ελάχιστο περιεχόμενο:

(α) Δικαιώματα χρήστη και χρήστη παρόχου. Σε αυτή την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης.

(β) Υποχρεώσεις χρήστη και χρήστη παρόχου. Σε αυτή την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα μη αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης, καθώς και συνέπειες μη συμμόρφωσης με αυτές τις υποχρεώσεις.

(γ) Δικαιώματα του παρόχου κινητών τηλεπικοινωνιακών υπηρεσιών.

(δ) Υποχρεώσεις του τηλεπικοινωνιακού παρόχου κινητών υπηρεσιών.

6. Επιπλέον στην ενότητα που αναφέρεται στις υποχρεώσεις των χρηστών, η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει τις παρακάτω διατάξεις οι οποίες σχετίζονται με την ασφάλεια του συστήματος:

(α) Οι χρήστες οφείλουν να λαμβάνουν όλα τα ενδεικνυόμενα μέτρα για την διασφάλιση του απορρήτου επικοινωνιών τους.

(β) Οι χρήστες οφείλουν να ενημερώνουν αμέσως τους υπευθύνους του παρόχου αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέτει σε κίνδυνο το απόρρητο επικοινωνιών των ίδιων ή άλλων χρηστών.

(γ) Οι χρήστες οφείλουν να αποκτούν πρόσβαση αποκλειστικά και μόνο σε δεδομέ-

να κίνησης ή θέσης τα οποία αναφέρονται στους ίδιους ή είναι Δημοσίως Ανακοινώσιμα κατά την Πολιτική Ευαισθησίας Πληροφοριών ή για τα οποία τους έχει δοθεί πρόσβαση κατά την Πολιτική Πρόσβασης.

(δ) Οι χρήστες απαγορεύεται να επιχειρούν να εκμεταλλευτούν πιθανά κενά ασφάλειας των συστημάτων του παρόχου προκειμένου να αποκτήσουν πρόσβαση σε πληροφορίες άλλων χρηστών, να διαταράξουν την ομαλή λειτουργία των δικτύων, να εκτελέσουν κακόβουλο λογισμικό και γενικά να υποβαθμίσουν το επίπεδο ασφάλειας του συστήματος.

7. Ο πάροχος οφείλει να δίνει στο χρήστη πρόσβαση στα συστήματά του μόνο εφόσον ο χρήστης έχει λάβει γνώση και ακολούθως έχει αποδεχθεί την Πολιτική Αποδεκτής Χρήσης. Το γεγονός αυτό αποδεικνύεται είτε με έγγραφη δήλωση του χρήστη η οποία φέρει την πρωτότυπη υπογραφή του ή εφόσον ο χρήστης έχει συμπληρώσει το αντίστοιχο πεδίο σε σχετική φόρμα αποδοχής στην περίπτωση που η Πολιτική Αποδεκτής Χρήσης παρουσιάζεται ηλεκτρονικά.

ΚΕΦΑΛΑΙΟ IV
Υποχρεώσεις φορέων ,Έλεγχος και Εποπτεία

Άρθρο 14
Υποχρεώσεις φορέων αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών

1. Όλοι οι τηλεπικοινωνιακοί πάροχοι υποχρεούνται:

(α) Να διαθέτουν ανά πάσα στιγμή καθορισμένη πολιτική για τη διασφάλιση του απορρήτου τηλεπικοινωνιακών υπηρεσιών παρεχομένων από δημόσια τηλεπικοινωνιακά δίκτυα κινητών επικοινωνιών.

(β) Να εφαρμόζουν την εν λόγω πολιτική.

(γ) Να ενημερώσουν σχετικά ως προς την εφαρμοζόμενη πολιτική την ΑΔΑΕ εντός έξι μηνών από την δημοσίευση του παρόντος.

(δ) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική εντός ενός έτους από την έγκρισή της.

2. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβλέπει στο οργανόγραμμά του ξεχωριστή διοικητική οντότητα η οποία θα είναι επιφορτισμένη με την κατάρτιση και την εφαρμογή της ΠΔΑΚΤΥ με επικεφαλής κατάλληλα καταρτισμένο στέλεχός του που θα φέρει τον τίτλο του Υπευθύνου Ασφαλείας.

3. Για την αποτελεσματική εφαρμογή της Πολιτικής Πρόσβασης ο κάθε τηλεπικοινωνιακός πάροχος οφείλει να ορίζει τουλάχιστον:

(α) Έναν Υπεύθυνο Πρόσβασης, ο οποίος θα καθορίζει το είδος της πρόσβασης των χρηστών στα συστήματα.

(β) Έναν Υπεύθυνο Συστήματος, ο οποίος θα υλοποιεί τις αποφάσεις του Υπευθύνου Πρόσβασης.

(γ) Έναν Υπεύθυνο Αντιγράφων Ασφαλείας, ο οποίος πάντα σε συνεννόηση με τον Υπεύθυνο Πρόσβασης θα καθορίζει ποιος έχει πρόσβαση στα αντίγραφα ασφάλειας καθώς και το χρονικό διάστημα λήψης τους.

4. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβαίνει σε τακτικές επισκοπήσεις και

αναθεωρήσεις της πολιτικής διασφάλισης του απορρήτου, είτε αυτόβουλα (μετά από έγκριση της ΑΔΑΕ σε περίπτωση αναθεώρησης) είτε ύστερα από σχετική εντολή της ΑΔΑΕ όπως μπορεί να προκύψει από πιθανή διαδικασία ελέγχου ή έκδοση σχετικής οδηγίας.

5. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου ο πάροχος οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους ασφάλειας και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους) και να παρέχει στοιχεία για την αποτροπή ή αντιμετώπισή τους.
6. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου που δεν είναι δυνατό να αντιμετωπιστεί με τα τρέχοντα μέσα που διαθέτει ο τηλεπικοινωνιακός πάροχος, αυτός οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους ασφάλειας και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους).
7. Ο πάροχος οφείλει να ενημερώνει τους χρήστες για την ύπαρξη και τον τρόπο χρήσης τεχνολογιών-πόρων σχετικών με την ασφάλεια των μεταδιδομένων πληροφοριών.
8. Ο πάροχος οφείλει να ορίζει συνέπειες για τη μη συμμόρφωση των χρηστών παρόχου με τα προβλεπόμενα από την ΠΔΑΚΤΥ του Απορρήτου (συμπεριλαμβανομένων των Πολιτικών Πρόσβασης και Αποδεκτής χρήσης).

Άρθρο 15
Διαδικασία Ελέγχου από την ΑΔΑΕ-Κυρώσεις

1. Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε πάροχο που εμπίπτει στις διατάξεις του παρόντος. Η συχνότητα των ελέγχων θα καθοριστεί από την ΑΔΑΕ με μεταγενέστερη Απόφαση της.
2. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες υπηρεσίες της ΑΔΑΕ ή από ειδικούς που τελούν υπό την άμεση επίβλεψη της ΑΔΑΕ, με την παρουσία εξουσιοδοτημένου προσώπου του παρόχου, σύμφωνα με τη διαδικασία που περιγράφεται στο Παράρτημα Α του παρόντος Κανονισμού.
3. Κατά την διάρκεια του ελέγχου η ΑΔΑΕ καταγράφει αναλυτικά τις ενέργειες σε ειδικό έντυπο με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Πάροχο Κινητών Τηλεπικοινωνιακών Υπηρεσιών αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών». Τα ελάχιστα απαραίτητα στοιχεία του εν λόγω εντύπου παρατίθενται στο Παράρτημα Β του παρόντος Κανονισμού.
4. Η ομάδα ελέγχου κοινοποιεί το πόρισμά της στην Ολομέλεια της ΑΔΑΕ. Η Ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου λαμβάνοντας υπόψη και τις πιθανές ενστάσεις του παρόχου και είτε εγκρίνει τις ενέργειες που προβλέπονται στην εκάστοτε πολιτική προστασίας του απορρήτου του παρόχου που έχει εγκριθεί από την ΑΔΑΕ είτε επιβάλλει κυρώσεις εφόσον κρίνει ότι δεν έχουν ληφθεί τα προσήκοντα μέτρα, με βάση τα αναφερόμενα στην εγκεκριμένη ΠΔΑΚΤΥ.
5. Η ΑΔΑΕ διενεργεί έκτακτους ελέγχους σε περίπτωση δημόσιων καταγγελιών ή έγγραφων καταγγελιών εκ μέρους των χρηστών. Εφόσον πρόκειται για δημόσιες

καταγγελίες, ακολουθείται η διαδικασία που προβλέπεται για τους τακτικούς ελέγχους, ενώ στην περίπτωση εμπιστευτικών έγγραφων καταγγελιών εκ μέρους χρηστών, ο έλεγχος μπορεί κατά την κρίση της ΑΔΑΕ να γίνει αιφνιδιαστικά.

6. Ως προς τη διαδικασία και τις κυρώσεις της παραγράφου 5, ισχύουν οι διατάξεις του Νόμου 3115, άρθρο 11 και άρθρο 6, παράγραφος 4, καθώς και τα προβλεπόμενα στον εσωτερικό κανονισμό της ΑΔΑΕ (ΦΕΚ 1642/Β/7-11-2003).

Άρθρο 16
Άσκηση Εποπτείας

Κάθε πάροχος κινητών τηλεπικοινωνιακών υπηρεσιών στο τέλος του ημερολογιακού έτους υποβάλλει στην ΑΔΑΕ ετήσια έκθεση με στοιχεία που αφορούν στην ασφάλεια των κινητών επικοινωνιών και τη διασφάλιση του απορρήτου.

Το ελάχιστο περιεχόμενο της ετήσιας έκθεσης ορίζεται ως εξής:

(α) Περιστατικά που απείλησαν την ασφάλεια του παρόχου και τη διασφάλιση του απορρήτου καθώς και τυχόν βλάβες που υπέστη ο πάροχος και οι χρήστες του εξαιτίας αυτών.

(β) Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.

Η ΑΔΑΕ με Απόφασή της δύναται να μεταβάλλει το ελάχιστο περιεχόμενο της ετήσιας έκθεσης.

Η ΑΔΑΕ δύναται να ζητήσει εκτάκτως από τους φορείς οποιεσδήποτε πληροφορίες θεωρεί αναγκαίες στα πλαίσια των αρμοδιοτήτων της για την ασφάλεια των κινητών επικοινωνιών και τη διασφάλιση του απορρήτου.

Άρθρο 17
Προστασία Επεξεργασίας Αρχείων

Σε περιπτώσεις παραβίασης των διατάξεων προστασίας του απορρήτου των επικοινωνιών, οι οποίες περιλαμβάνουν και επεξεργασία αρχείων που αφορούν την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η ΑΔΑΕ θα την ενημερώνει σχετικά προκειμένου να επιλαμβάνεται στο πλαίσιο των δικών της αρμοδιοτήτων.

ΚΕΦΑΛΑΙΟ V
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 18
Έναρξη Ισχύος

Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

ΠΑΡΑΡΤΗΜΑ Α

Αναλυτική περιγραφή διαδικασίας Ελέγχου Τηλεπικοινωνιακού Παρόχου Κινητών Υπηρεσιών

Η διαδικασία ελέγχου παρόχου διενεργείται με βάση τα ακόλουθα βήματα:

(α) Η ΑΔΑΕ με Απόφασή της ορίζει ομάδα ελέγχου που αποτελείται από τρία (3)

τουλάχιστον άτομα με σκοπό τον έλεγχο συγκεκριμένου παρόχου. Η ελαχίστη στελέχωση της ομάδας ελέγχου περιλαμβάνει τον υπεύθυνο της ομάδας, έναν νομικό σύμβουλο και έναν τεχνικό σύμβουλο.

(β) Σε χρόνο που αποφασίζει η ομάδα ελέγχου, επικοινωνεί με τον πάροχο και ζητεί να έρθει σε άμεση επικοινωνία με τον υπεύθυνο ασφάλειας όπως αυτός ορίζεται στο κεφάλαιο IV του παρόντος. Τυχόν καθυστέρηση ή κώλυμα που παρουσιάζεται κατά την προσπάθεια επικοινωνίας με τον υπεύθυνο ασφάλειας καταγράφεται και φέρει τις ανάλογες κυρώσεις.

(γ) Ο υπεύθυνος ασφάλειας παραδίδει στην ομάδα ελέγχου πλήρες αντίγραφο της ΠΔΑΚΤΥ και των τυχών συνοδευτικών εγγράφων. Από τα παραδιδόμενα έγγραφα θα πρέπει να προκύπτουν οι ημερομηνίες έκδοσης και έγκρισης των συγκεκριμένων πολιτικών. Τυχόν καθυστέρηση επίδοσης σημειώνεται και φέρει τις ανάλογες κυρώσεις.

(δ) Η ομάδα ελέγχου προβαίνει σε αναλυτική εξέταση όλων των σχετικών εγγράφων ώστε κα καταγραφούν οι τυχόν ελλείψεις που παρουσιάζονται στην πολιτική του παρόχου. Κατά την διαδικασία αυτή δύναται να ζητηθεί η συνδρομή του παρόχου έτσι ώστε να διασαφηνιστούν τυχόν ασάφειες και προβλήματα που παρουσιάζονται στην πολιτική προστασίας του απορρήτου.

(ε) Κατά την διάρκεια του ελέγχου ο πάροχος δεν έχει την δυνατότητα να αντικαταστήσει την πολιτική προστασίας του απορρήτου με νέα ούτε να προβεί σε τυχόν διορθώσεις αυτής.

(στ) Σε περίπτωση ασαφειών ως προς την πολιτική προστασίας του απορρήτου οι πάροχοι, μετά από σχετική σύσταση της ΑΔΑΕ θα προβαίνουν στις απαραίτητες διορθώσεις στην πολιτική τους

(ζ) Η ομάδα ελέγχου προβαίνει σε αυτοψία των εγκαταστάσεων του παρόχου για να διαπιστώσει σε ποιο βαθμό εφαρμόζονται οι διαδικασίες που προβλέπονται από τα προσκομισθέντα έγγραφα. Η αυτοψία δύναται να περιλαμβάνει και επαφή με το προσωπικό του παρόχου. Η ομάδα ελέγχου καταγράφει αναλυτικά τις ελλείψεις και τα σφάλματα που τυχόν διαπιστώνονται.

(η) Ο πάροχος οφείλει να υποβάλλει στην ομάδα ελέγχου οποιοδήποτε στοιχείο θεωρηθεί απαραίτητο από την ομάδα για την επιτυχή ολοκλήρωση του ελέγχου.

(θ) Τυχόν διαπίστωση έλλειψης συνεργασίας από τον πάροχο ή/και προσπάθειας παραπλάνησης της ομάδας ελέγχου καταγράφεται και φέρει τις ανάλογες κυρώσεις.

Ελάχιστο περιεχόμενο του εντύπου με τίτλο
«Έκθεση Διενέργειας Ελέγχου σε Πάροχο Διαδικτυακών Επικοινωνιών αναφορικά με την Πολιτική Ασφάλειας και τη Διασφάλιση του Απορρήτου»

Το ως άνω έντυπο θα περιέχει απαραιτήτως τουλάχιστον τα ακόλουθα στοιχεία:
(α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε ο έλεγχος.
(β) Τα ονοματεπώνυμα και τις ιδιότητες των στελεχών της ΑΔΑΕ που απαρτίζουν την ομάδα ελέγχου καθώς και την ημερομηνία σύστασής της.
(γ) Το όνομα του υπό έλεγχο παρόχου καθώς και το όνομα του υπευθύνου ασφάλειάς του.
(δ) Το χρόνο που απαιτήθηκε έως ότου να αποδοθεί στην ομάδα ελέγχου η πλήρης Πολιτική Ασφάλειας του παρόχου.
(ε) Ημερολόγιο ενεργειών και ερωτήσεων της ομάδας ελέγχου και καταγραφή της ανταπόκρισης του ελεγχόμενου παρόχου.
(στ) Το αποτέλεσμα της αυτοψίας για την αποτίμηση της εφαρμογής της Πολιτικής Ασφάλειας με καταγραφή τυχόν ελλείψεων και ασαφειών.
(ζ) Τις ημερομηνίες έναρξης και περάτωσης του ελέγχου.
(η) Το τελικό πόρισμα του ελέγχου και την εισήγηση προς την Ολομέλεια της ΑΔΑΕ.

Αριθμ: 633 α

ΑΠΟΦΑΣΗ
Έχοντας υπόψη :
α. Το Ν. 3115/27-02-2003, άρθρο 1 παραγρ. 1,
β. Το Ν. 3115/27-02-2003, άρθρο 6, παραγρ. 1,
γ. Ότι εκ της αποφάσεως δεν προκύπτει δαπάνη για το δημόσιο
δ. Τη σχετική εισήγηση της Υπηρεσίας

Α π ο φ ά σ ι σ ε
Κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004 , την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ
Άρθρο 1
Σκοπός – Πεδίο Εφαρμογής
1. Σκοπός του παρόντος Κανονισμού είναι:
(α) Η ασφάλεια των Διαδικτυακών υποδομών των παρόχων και η διασφάλιση του απορρήτου αυτών.
(β) Η θέσπιση των υποχρεώσεων των εν λόγω παρόχων αναφορικά με την ασφάλεια και το απόρρητο των Διαδικτυακών τους υποδομών.
(γ) Ο έλεγχος στους εν λόγω παρόχους σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

2. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Πάροχοι Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:
(α) Πάροχοι σταθερής και κινητής πρόσβασης στο Διαδίκτυο,
(β) Πάροχοι Διαδικτυακών υπηρεσιών, υπηρεσιών προστιθέμενης αξίας και υπηρεσιών εφαρμογών.
3. Ο παρών Κανονισμός συμπληρώνει τον «Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές» καθώς και τον «Κανονισμό για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου» που προηγήθηκαν .

Άρθρο 2
Ορισμοί

Για την εφαρμογή του παρόντος Κανονισμού ισχύουν οι ορισμοί των προαναφερθέντων Κανονισμών της ΑΔΑΕ, που επαναλαμβάνονται εδώ για λόγους πληρότητας. Επιπρόσθετα, οι ακόλουθοι όροι έχουν την έννοια που τους αποδίδεται κατωτέρω:

Αντίγραφα ασφαλείας – Τα εφεδρικά αντίγραφα που προκύπτουν μετά την εφαρμογή των κατάλληλων μεθόδων αντιγραφής και σχετίζονται με τα δεδομένα διάρθρωσης των δικτυακών στοιχείων.

Απειλή (Threat): Κάθε άτομο, δραστηριότητα ή συμβάν που είναι δυνατόν να προκαλέσει παραβίαση της διαθεσιμότητας, ακεραιότητας ή εμπιστευτικότητας σε οποιοδήποτε σύστημα το οποίο χρησιμοποιείται για την παρακολούθηση, αποθήκευση, επεξεργασία, εξαγωγή, διαβίβαση, ανακοίνωση και δημοσιοποίηση δεδομένων επικοινωνίας. Οι απειλές μπορεί να είναι τυχαίες ή σκόπιμες και μπορεί να προέρχονται είτε από το εσωτερικό είτε από το εξωτερικό του παρόχου.

Αποστρατιωτικοποιημένη Ζώνη (Demilitarized Zone): Το υποδίκτυο του παρόχου που βρίσκεται μεταξύ των εξωτερικών δικτύων (π.χ. το Διαδίκτυο) και του έμπιστου εσωτερικού δικτύου του παρόχου. Τυπικά σε αυτή τη ζώνη τοποθετούνται συστήματα που παρέχουν υπηρεσίες προσβάσιμες από οποιονδήποτε μέσω του Διαδικτύου ή άλλων εξωτερικών δικτύων (π.χ. διακομιστές παγκόσμιου ιστού και ηλεκτρονικού ταχυδρομείου).

Ασύμμετρη Κρυπτογραφία: Κρυπτογραφία που στηρίζεται στη χρήση ενός ζευγαριού κλειδιών, ενός ιδιωτικού και ενός δημόσιου. Όταν η κρυπτογράφηση γίνεται με το ένα κλειδί, η αποκρυπτογράφηση γίνεται με το άλλο. Είναι γνωστή και ως Κρυπτογραφία Δημόσιου Κλειδιού.

Ακεραιότητα: Ιδιότητα της διαδικασίας ασφάλειας, με την οποία ελέγχεται αν τα δεδομένα έχουν τροποποιηθεί ή καταστραφεί κατά μη εξουσιοδοτημένο τρόπο.

Αυξητική Αντιγραφή (incremental backup): Αντιγραφή μόνο των αρχείων τα οποία έχουν προστεθεί ή τροποποιηθεί πρόσφατα. Εξυπηρετεί την επιτάχυνση της διαδικασίας αντιγραφής αφού αποθηκεύονται μόνο τα αρχεία που έχουν αλλάξει μετά από την εκτέλεση της τελευταίας αντιγραφής.

Δεδομένα Διάρθρωσης (configuration data): Τα απαραίτητα στοιχεία δεδομένων που σχετίζονται με τη διάρθρωση, τον προγραμματισμό και τη σωστή λειτουργία των δικτυακών διατάξεων του παρόχου.

Δεδομένα Θέσης: Τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

Δεδομένα Κίνησης: Τα δεδομένα που υποβάλλονται σε επεξεργασία με σκοπό τη διαβίβαση μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της.

Διαδικτυακές Επικοινωνίες: Υπηρεσίες ηλεκτρονικών επικοινωνιών οι οποίες παρέχονται από δίκτυο μετάδοσης δεδομένων και φωνής με πακετομεταγωγή το οποίο είτε έχει τη μορφή ενδοδικτύου (Intranet) είτε είναι ολόκληρο το διαδίκτυο (Internet).

Διακομιστής (server): Πληροφοριακό σύστημα το οποίο παρέχει δεδομένα και υπηρεσίες σε άλλα υπολογιστικά συστήματα, γνωστά ως πελάτες (clients), τα οποία συνδέονται σε αυτόν από απόσταση και με δική τους πρωτοβουλία.

Διαμόρφωση ή Διάρθρωση (configuration): Διαδικασία κατά την οποία αρχικοποιούνται ή μεταβάλλονται τα δεδομένα διάρθρωσης.

Διαφορική Αντιγραφή (differential backup): Αντιγραφή που αποθηκεύει όλα τα αρχεία που έχουν αλλάξει από την τελευταία πλήρη αντιγραφή. Δεν αποθηκεύει τα αρχεία της τελευταίας πλήρους αντιγραφής.

Δικτυακή Σύνοδος (session): Η ακολουθία αλληλεπιδράσεων μεταξύ δύο άκρων επικοινωνίας που λαμβάνει χώρα κατά τη διάρκεια μιας δικτυακής επικοινωνίας.

Δικτυακοί Πόροι: Τα συστήματα (υπολογιστές, εξυπηρετητές, δικτυακοί κόμβοι, κ.α.) που απαρτίζουν το δίκτυο του παρόχου ή είναι συνδεδεμένα σε αυτό, αλλά και τα δεδομένα που αποθηκεύονται και διακινούνται καθώς και οι υπηρεσίες που προσφέρονται από το δίκτυο του παρόχου.

Δίκτυο Ηλεκτρονικών

Επικοινωνιών: Τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, συμπεριλαμβανομένου του Διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών.

Δοκιμαστικά Δεδομένα: Δεδομένα που απαιτούνται από τον τηλεπικοινωνιακό εξοπλισμό του παρόχου για την παροχή υπηρεσιών (ενδεικτικά αναφέρονται ονόματα χρήστη, αριθμοί κλήσης κλπ.) και τα οποία είτε δεν αντιστοιχούν σε χρήστες είτε αντιστοιχούν σε στελέχη ή / και χρήστες του οργανισμού οι οποίοι εν γνώσει τους συμμετέχουν σε δοκιμές τηλεπικοινωνιακού εξοπλισμού (φιλικοί χρήστες).

Δοκιμές Αποδοχής: Διαδικασία εκτέλεσης δοκιμών της λειτουργίας ενός προϊόντος ή υπηρεσίας, μέσω της οποίας ελέγχεται κατά πόσον το προϊόν συμμορφώνεται αφενός με την περιγραφή του κατασκευαστή και αφετέρου με τις απαιτήσεις του αγοραστή.

Δρομολογητής (router): Τηλεπικοινωνιακός εξοπλισμός που παρέχει υπηρεσίες δρομολόγησης δεδομένων στο στρώμα δικτύου με βάση τη στοίβα πρωτοκόλλων του Διαδικτύου.

Εμπιστευτικότητα: Η ιδιότητα της διαδικασίας ασφάλειας με την οποία αποτρέπεται η διάθεση ή η αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα, οντότητες ή διεργασίες.

Εξουσιοδότηση: Η διαδικασία χορήγησης δικαιώματος πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από την οντότητα που ελέγχει τον πόρο για τον οποίο ζητείται η πρόσβαση.

Επαλήθευση Ταυτότητας (Authentication): Οι αυτοματοποιημένες και τυποποιημένες μέθοδοι για την πιστοποίηση της ταυτότητας του χρήστη στο διαδίκτυο. Αναφέρεται και ως αυθεντικοποίηση.

Επισύνδεση ή Εισβολή (Intrusion): Απόπειρα παραβίασης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των υπολογιστικών συστημά-

των και των δικτύων του παρόχου, καθώς και προσπάθεια παράκαμψης των μηχανισμών ασφάλειας αυτών.

Ευπάθεια (vulnerability): Αδυναμία ή ελάττωμα στο υλικό (hardware), στο λογισμικό (software) ή στην αρχιτεκτονική ενός συστήματος, καθώς και στις διαδικασίες ασφαλείας που ακολουθούνται, που μπορεί κάποιος να εκμεταλλευτεί προκειμένου να παραβιάσει τη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα του εν λόγω συστήματος.

Θύρα (port): Άκρο μιας λογικής σύνδεσης του στρώματος μεταφοράς όπως αυτό ορίζεται με βάση τη στοίβα πρωτοκόλλων του Διαδικτύου.

Ιός (virus): Στοιχείο λογισμικού το οποίο εισβάλλει σε ένα υπολογιστικό σύστημα με σκοπό να προκαλέσει ανεπιθύμητα αποτελέσματα, όπως καταστροφή δεδομένων χρήστη, άρνηση υπηρεσίας (denial-of-service), παραβίαση του συστήματος ασφάλειας κτλ. Κύριο χαρακτηριστικό του είναι το γεγονός ότι μεταδίδεται μεταξύ των υπολογιστικών συστημάτων με τη μορφή εκτελέσιμων προγραμμάτων (executables), εγγραφών συστήματος (system or boot records) και μακρο-εντολών (macros). Οι ιοί είναι δυνατόν να επιτεθούν κατά προσωπικών υπολογιστών, διακομιστών, δρομολογητών κτλ.

Κλειδί Κρυπτογράφησης: Σειρά από bits συγκεκριμένου μήκους που χρησιμοποιείται για να κρυπτογραφήσει ή να αποκρυπτογραφήσει τα δεδομένα σε έναν αλγόριθμο κρυπτογράφησης.

Λογισμικό Ελέγχου: Το λογισμικό το οποίο χρησιμοποιείται για τη διεξαγωγή ελέγχων και μετρήσεων με σκοπό τον έλεγχο ασφάλειας δικτύου.

Λογισμικό Προστασίας από Ιούς (anti-virus software): Κατηγορία εφαρμογών λογισμικού που αποσκοπεί στην ανίχνευση και απομάκρυνση ιών που έχουν προσβάλλει ένα υπολογιστικό σύστημα.

Μη Αποποίηση Ευθύνης: Διαδικασία που εξασφαλίζει ότι οι συναλλασσόμενοι σε εφαρμογές και υπηρεσίες Διαδικτύου που προσφέρονται είτε από πάροχους διαδικτύου είτε από πάροχους υπηρεσίας εφαρμογής δεν μπορούν να αρνηθούν τη συμμετοχή τους στη συναλλαγή.

Ομάδα Ελέγχου Ασφάλειας Δικτύου: Ομάδα Εργασίας του παρόχου, η οποία πρόκειται να πραγματοποιήσει έλεγχο ασφάλειας δικτύου σε υπολογιστικό και δικτυακό εξοπλισμό.

Παροχή Δικτύου Διαδικτυακών Επικοινωνιών: Η σύσταση, η λειτουργία, ο έλεγχος και η διάθεση τέτοιου δικτύου.

Πάροχος Δικτύου Διαδικτυακών Επικοινωνιών (Internet Service Provider): Η επιχείρηση ή το νομικό πρόσωπο που παρέχει δίκτυο διαδικτυακών επικοινωνιών ή/και το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του. Για τις ανάγκες του παρόντος ο πάροχος δικτύου διαδικτυακών επικοινωνιών θα αναφέρεται στη συνέχεια του κειμένου ως «πάροχος διαδικτύου».

Πάροχος Υπηρεσίας Εφαρμογής (Application Service Provider): μία οντότητα (οργανισμός, εταιρεία κτλ), η οποία διαθέτει εφαρμογές λογισμικού (software), υλική υποδομή (hardware) και δικτυακή υποδομή, προκειμένου να παρέχει υπηρεσίες και εφαρμογές στον πάροχο δικτύου διαδικτυακών επικοινωνιών και τους χρήστες του.

Περιβάλλον Δοκιμής: Τμήμα του εξοπλισμού του παρόχου, το οποίο είναι δικτυακά απομονωμένο από το Περιβάλλον Παραγωγής και χρησιμοποιείται για δοκιμές, εκπαίδευση, παρουσιάσεις κλπ.

Περιβάλλον Παραγωγής: Το σύνολο του εξοπλισμού του παρόχου το οποίο χρησιμοποιείται για ανταλλαγή δεδομένων και παροχή υπηρεσιών στους υπαλλήλους, στους πελάτες και στους συνεργάτες του παρόχου και βρίσκεται συνήθως εντός της περιμέτρου του παρόχου και προστατευόμενο από το εταιρικό firewall.

Περίμετρος Δικτύου: Όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα (διαδίκτυο, δίκτυα άλλων υποκαταστημάτων του παρόχου, δίκτυα συνεργατών του, ασύρματα δίκτυα, κτλ)

Πηγαίος Κώδικας: Η μορφή στην οποία βρίσκεται το λογισμικό (συνήθως σε μορφή εντολών κάποιας γλώσσας προγραμματισμού υψηλού επιπέδου κατανοητή στον άνθρωπο) προτού περάσει από διαδικασία μεταγλώττισης και μετατραπεί σε μορφή κατανοητή από το εκάστοτε υπολογιστικό σύστημα.

Πλήρης Αντιγραφή (full backup): Πλήρης αποθήκευση κάθε αρχείου ενός διακομιστή ή δικτυακού στοιχείου.

Πολιτική Ασφάλειας: Το σύνολο τεχνικών, οργανωτικών και κανονιστικών μέτρων, τα οποία εφαρμόζονται από πάροχο διαδικτύου και αποβλέπουν στη διασφάλιση του απορρήτου και γενικά στην ασφαλή λειτουργία των δικτύων διαδικτυακών επικοινωνιών.

Πόροι Δεδομένων Επικοινωνιών: οι πόροι λογισμικού (software), υλικού (hardware), συστημάτων, υπηρεσιών και δικτύων όπου αποθηκεύονται, επεξεργάζονται, διαβιβάζονται και ανακοινώνονται δεδομένα επικοινωνιών χρηστών.

Προσδιορισμός Ταυτότητας: Αναφέρεται σε λιγότερο τυποποιημένες μεθόδους (σε σχέση με τη διαδικασία επαλήθευσης ταυτότητας) για την πιστοποίηση της φύσης του χρήστη, που είναι συνήθως μη αυτόματες και απαιτούν ανθρώπινη παρέμβαση.

Προστασία του Απορρήτου: Η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων επικοινωνίας από άλλα πρόσωπα, χωρίς τη συγκατάθεσή τους, εξαιρουμένων των νόμιμα εξουσιοδοτημένων.

Συγκατάθεση του Χρήστη ή του Συνδρομητή: Η συγκατάθεση του προσώπου που αφορούν τα δεδομένα επικοινωνιών, κατά την έννοια της οδηγίας 95/46/ΕΚ.

Συμμετρική Κρυπτογραφία: Κρυπτογραφία στην οποία η κρυπτογράφηση και αποκρυπτογράφηση πραγματοποιούνται με ένα κλειδί.

Σύστημα Ανίχνευσης Επισύνδεσης (Intrusion Detection System): Το σύστημα που παρακολουθεί τα διάφορα γεγονότα στα υπολογιστικά συστήματα και δίκτυα του παρόχου και τα αναλύει για να εντοπίσει σημάδια επισυνδέσεων.

Ταυτότητα: Οι πληροφορίες που προσδιορίζουν τον χρήστη με μοναδικό τρόπο.

Τοίχος Προστασίας (Firewall): Το σύστημα που υλοποιείται με λογισμικό ή/και υλικό για την προστασία του εσωτερικού δικτύου του παρόχου από εξωτερικές επιθέσεις.

Υπεργολάβος: Όπως ορίζεται από την ισχύουσα νομοθεσία.

Υπηρεσία Προστιθέμενης Αξίας: Υπηρεσία μη τηλεπικοινωνιακή η οποία μπορεί να παρέχεται ή να υποστηρίζεται από δίκτυο διαδικτυακών επικοινωνιών.

Υπηρεσίες Ηλεκτρονικών Επικοινωνιών: Οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοι-

νωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχόμενου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και υπηρεσίες της κοινωνίας της πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του ΠΔ39/2001 (Α'28), και που δεν αφορούν, εν όλω ή εν μέρει, τη μεταφορά σημάτων σε δίκτυα επικοινωνιών.

Υπολειπόμενος Κίνδυνος (Residual Risk): Κίνδυνος που εξακολουθεί να υφίσταται ακόμα και μετά την υλοποίηση μέτρων ασφαλείας που αντιμετωπίζουν ένα κίνδυνο παραβίασης του απορρήτου επικοινωνιών των χρηστών.

Χρήστης: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

Χρήστης Παρόχου: κάθε φυσικό πρόσωπο που εργάζεται στην επιχείρηση ή το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του.

ΚΕΦΑΛΑΙΟ ΙΙ
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΕΡΙΜΕΤΡΟΥ

Άρθρο 3
Γενικά

1. Ο πρωταρχικός σκοπός της πολιτικής ασφάλειας περιμέτρου είναι να προστατεύσει τους διάφορους δικτυακούς πόρους του παρόχου διαδικτύου από εισβολείς, δηλαδή να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του παρόχου διαδικτύου (σε υλικό ή λογισμικό), καθώς και τη διακοπή της ομαλής παροχής των υπηρεσιών του παρόχου διαδικτύου. Δεδομένου ότι οι κίνδυνοι και οι απειλές της ασφάλειας των δικτυακών πόρων δεν μπορούν να ελεγχθούν εξ ολοκλήρου, σκοπός της πολιτικής ασφάλειας περιμέτρου είναι να διατηρήσει ένα ικανοποιητικό επίπεδο ασφάλειας, ιδιαίτερα όσον αφορά την πρόσβαση από/προς το διαδίκτυο, ανάλογα με την Αποτίμηση Κινδύνου (Κεφάλαιο VII) που οφείλει πρώτα ο πάροχος διαδικτύου να έχει πραγματοποιήσει.
2. Η πολιτική ασφάλειας περιμέτρου ορίζει τους μηχανισμούς (σε υλικό και λογισμικό) που χρησιμοποιούνται για τον σκοπό που περιγράφηκε παραπάνω, καθώς και τους τρόπους διαμόρφωσης και ανανέωσης αυτών. Ενδεικτικά και όχι περιοριστικά αναφέρονται τα εξής συστήματα: Τοίχος Προστασίας (firewall), Σύστημα Προστασίας Αποστρατιωτικοποιημένης Ζώνης, και Σύστημα Ανίχνευσης Επισυνδέσεων (Intrusion

Detection System), μεταξύ άλλων.

3. Προκειμένου η πολιτική ασφάλειας περιμέτρου να εξασφαλίζει το επιθυμητό επίπεδο ασφάλειας των δικτυακών πόρων ενός παρόχου διαδικτύου, πρέπει ο πάροχος διαδικτύου να ακολουθεί τις διεθνώς, ευρέως αποδεκτές πρακτικές που αφορούν την πολιτική ασφάλειας περιμέτρου. Αυτό συνεπάγεται την κατάλληλη επιλογή, διαμόρφωση, και ανανέωση των συστημάτων που υλοποιούν την ασφάλεια περιμέτρου.
4. Ο πάροχος διαδικτύου οφείλει να ορίζει Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου, ο οποίος είναι υπεύθυνος για τον καθορισμό της πολιτικής ασφάλειας περιμέτρου και για τη σωστή εφαρμογή της. Για τον σκοπό αυτό, ο πάροχος διαδικτύου οφείλει να αναγνωρίζει ότι η διαχείριση των συστημάτων περιμετρικής ασφάλειας απαιτεί σημαντικό χρόνο και κατάλληλη εκπαίδευση, και να εξασφαλίζει αυτά στον Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου.

Άρθρο 4
Συστήματα Firewalls

1. Ο πάροχος διαδικτύου υποχρεούται να χρησιμοποιεί συστήματα firewall για την προστασία των συνδέσεων του δικτύου του με το διαδίκτυο ή με άλλα δίκτυα, σύμφωνα με την πολιτική ασφάλειας περιμέτρου που έχει ορίσει, χωρίς διακοπή (24 ώρες το 24ωρο). Διακοπή της λειτουργίας των συστημάτων επιτρέπεται σε περιπτώσεις συντήρησης ή αναβάθμισης, ύστερα όμως από έγκαιρη ενημέρωση των χρηστών και αναβολή της συνδεσιμότητας του δικτύου με εξωτερικά δίκτυα και το διαδίκτυο για όσο χρόνο διαρκούν οι διαδικασίες αυτές.
2. Ο πάροχος διαδικτύου πρέπει ιδιαίτερα να εξασφαλίζει την ασφάλεια των ιδίων συστημάτων firewall, όπως για παράδειγμα μέσω της χρήσης ενός πολύ ασφαλούς λειτουργικού συστήματος για τα συστήματα αυτά.
3. Οι πάροχοι διαδικτύου οφείλουν να αντιμετωπίζουν τα συστήματα firewall ως την πρώτη γραμμή άμυνας από εξωτερικές απειλές, τα οποία όμως δεν διασφαλίζουν πλήρως την ασφάλεια των εσωτερικών συστημάτων, τα οποία πρέπει να προστατεύονται αυτόνομα και διαρκώς.
4. Η αρχιτεκτονική των συστημάτων firewall που θα αναπτυχθεί σε έναν πάροχο διαδικτύου πρέπει να διακρίνει το εσωτερικό δίκτυο σε δύο βασικές περιοχές: (α) εσωτερικό έμπιστο (trusted) δίκτυο και (β) δίκτυο αποστρατικοποιημένης ζώνης. Το σύστημα firewall επιβάλλεται να μην επιτρέπει την απευθείας πρόσβαση σε δεδομένα που υπάρχουν στα πληροφοριακά συστήματα και τα δικτυακά στοιχεία του εσωτερικού έμπιστου δικτύου.
5. Η επιλογή, διαμόρφωση και ανανέωση των συστημάτων firewall γίνεται με βάση τις διεθνώς, ευρέως αποδεκτές πρακτικές, οι οποίες περιλαμβάνουν αλλά δεν περιορίζονται στις εξής:

(α) Η βασική πολιτική διαμόρφωσης ενός firewall σχετικά με την εισερχόμενη κίνηση είναι να μην επιτρέπει την είσοδο σε κανένα πακέτο και σύνδεση εκτός εάν ο τύπος της κίνησης και της σύνδεσης έχει ρητώς επιτραπεί. Αυτή η προσέγγιση θεωρείται περισσότερο ασφαλής από το να επιτρέπει αρχικά την είσοδο σε όλες τις συνδέσεις και πακέτα, εξαιρώντας κατόπιν συγκεκριμένους τύπους σύνδεσης

και κίνησης.

(β) Η διαμόρφωση των firewalls γίνεται με βάση την αποτίμηση κινδύνων δικτύου και οφείλει να ανανεώνεται (αν χρειάζεται) κάθε φορά που τροποποιείται η Αναφορά Αποτίμησης Κινδύνων ή και σε προγραμματισμένα, τακτά χρονικά διαστήματα. Η πολιτική ασφάλειας περιμέτρου καθορίζει μια τυπική διαδικασία για τη διαχείριση των προσθέσεων και αφαιρέσεων των κανόνων του firewall.

(γ) Ο πάροχος διαδικτύου θα επιτρέπει την είσοδο από το διαδίκτυο προς το εσωτερικό έμπιστο δίκτυο μέσω του firewall εκείνων μόνο των δικτυακών συνόδων που έχουν ισχυρή ταυτοποίηση και κρυπτογράφηση.

(δ) Το firewall πρέπει να ελέγχεται και παρακολουθείται συνεχώς για τον εντοπισμό παραβιάσεων ή κακής διαχείρισης, πιθανώς και με τη χρήση Συστημάτων Ανίχνευσης Επισυνδέσεων.

(ε) Το firewall πρέπει να ενημερώνει τον Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου σε σχεδόν πραγματικό χρόνο σχετικά με κάθε στοιχείο που ενδέχεται να χρειάζεται άμεσης εξέτασης (όπως μια εισβολή στο σύστημα) και αντιμετώπισης.

(στ) Η δρομολόγηση με βάση τη διεύθυνση πηγής (source routing) πρέπει να είναι απενεργοποιημένη σε όλα τα συστήματα firewall και τους εξωτερικούς δρομολογητές.

(ζ) Το σύστημα firewall πρέπει να καταγράφει λεπτομερώς και να αποθηκεύει για ικανοποιητικό χρονικό διάστημα όλες τις δικτυακές συνόδους ώστε να μπορούν να εξεταστούν για ανωμαλίες offline. Στο αποθηκευμένο αυτό υλικό έχει πρόσβαση μόνο ο Υπεύθυνος Πολιτικής Ασφάλειας Περιμέτρου.

(η) Ο Υπεύθυνος Πολιτικής Ασφάλειας Περιμέτρου οφείλει να κρατά γραπτώς τεκμηρίωση της διαμόρφωσης και λειτουργίας του συστήματος firewall, συμπεριλαμβανόμενων πληροφοριών σχετικά με τη λειτουργία του δικτύου (διάγραμμα δικτύου, διευθύνσεις IP, και άλλα), καθώς και όλων των υπηρεσιών και των τύπων κίνησης που εξουσιοδοτούνται να διατρέξουν το firewall.

(θ) Ο Υπεύθυνος Πολιτικής Ασφάλειας Περιμέτρου οφείλει να αξιολογεί κάθε νέα έκδοση του λογισμικού του συστήματος firewall και να αποφασίζει εάν η ανανέωσή του είναι αναγκαία. Όλες οι προτεινόμενες από τον κατασκευαστή τροποποιήσεις (patches), που είναι σχετικές με την ασφάλεια του συστήματος firewall, πρέπει να υλοποιούνται άμεσα.

Άρθρο 5
Συστήματα Ανίχνευσης Επισυνδέσεων

1. Ο πάροχος διαδικτύου υποχρεούται να χρησιμοποιεί συστήματα ανίχνευσης επισυνδέσεων για την ενίσχυση της προστασίας του δικτύου του, σύμφωνα με την πολιτική ασφάλειας περιμέτρου που έχει ορίσει, χωρίς διακοπή (24 ώρες το 24ωρο). Διακοπή της λειτουργίας των συστημάτων αυτών επιτρέπεται μόνο για διαδικασίες συντήρησης ή αναβάθμισής τους, εκτός εάν συντρέχουν περιπτώσεις ανωτέρας βίας (π.χ. βλάβες) ή η διακοπή οφείλεται σε λόγους που δεν άγονται στο πεδίο δραστηριότητας και ευθύνης του παρόχου.
2. Η λειτουργικότητα των συστημάτων ανίχνευσης επισυνδέσεων πρέπει τουλάχιστον να περιλαμβάνει την παρακολούθηση των επισφαλών γεγονότων στο δίκτυο, καθώς και την παθητική (passive) αντίδρασή τους σε περίπτωση διαπίστωσης επισύνδεσης. Η παθητική αντίδραση περιλαμβάνει τουλάχιστον την ενεργοποίηση των συναγερμών που υποστηρίζει το σύστημα και την ειδοποίηση του Υπεύθυνου Πολιτικής Ασφάλειας Περιμέτρου. Συνιστάται όμως το σύστημα ανίχνευσης επισύνδεσης να ορίζει και να μπορεί να επιτελέσει επιπλέον ενεργές (active) αντιδράσεις σε περίπτωση διαπίστωσης επισύνδεσης. Ενδεικτικά και όχι περιοριστικά αναφέρονται τα εξής παραδείγματα ενεργής αντίδρασης: συλλογή επιπλέον πληροφοριών, μεταβολή του δικτυακού περιβάλλοντος, και απευθείας αντίδραση κατά των εισβολέων.
3. Η διαμόρφωση των συστημάτων ανίχνευσης επισυνδέσεων γίνεται με βάση την αποτίμηση κινδύνων δικτύου και οφείλει να ανανεώνεται (αν χρειάζεται) κάθε φορά που τροποποιείται η Αναφορά Αποτίμησης Κινδύνων ή και σε προγραμματισμένα, τακτά χρονικά διαστήματα. Η πολιτική ασφάλειας περιμέτρου καθορίζει μια τυπική διαδικασία για τη διαμόρφωση των συστημάτων ανίχνευσης επισυνδέσεων.
4. Τα συστήματα ανίχνευσης θα πρέπει να ελέγχονται σε τακτά χρονικά διαστήματα, από το προσωπικό που είναι υπεύθυνο για το χειρισμό και τη λειτουργία τους, ώστε το λογισμικό τους να είναι ενημερωμένο.
5. Τα διάφορα γεγονότα που ανιχνεύονται από το σύστημα ανίχνευσης επισυνδέσεων πρέπει να καταγράφονται και να αποθηκεύονται από το σύστημα για περαιτέρω επεξεργασία. Σημαντικά γεγονότα που καταγράφονται από το σύστημα, θα αναλύονται διεξοδικά από τον Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου και θα καταγράφονται σε ειδική Φόρμα Καταγραφής Επισυνδέσεων που θα ορίζεται από την πολιτική ασφάλειας περιμέτρου. Περιοδικά, ή ύστερα από έλεγχο από την ΑΔΑΕ, ο πάροχος διαδικτύου είναι υποχρεωμένος να αποστέλλει τις φόρμες αυτές στην ΑΔΑΕ.

ΚΕΦΑΛΑΙΟ ΙΙΙ
ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΟΥ ΕΞΟΠΛΙΣΜΟΥ

Άρθρο 6
Ανάγκη Ύπαρξης Πολιτικής Εγκατάστασης και Διαχείρισης Τηλεπικοινωνιακού Εξοπλισμού

1. Κάθε πάροχος διαδικτύου υποχρεούται να διαθέτει Πολιτική Διαχείρισης και

Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού ως μέρος της Πολιτικής Ασφάλειάς του.

2. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού εξασφαλίζει ότι τυχόν αλλαγές στον υπάρχοντα εξοπλισμό (υλικό, λογισμικό και διαμόρφωση αυτών) καθώς και η εισαγωγή καινούργιου εξοπλισμού στη λειτουργία του παρόχου διαδικτύου γίνεται κατά τέτοιο τρόπο ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών και να μην παραβιάζεται η Πολιτική Ασφάλειας του παρόχου διαδικτύου.
3. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού μπορεί να είναι κοινή για όλες τις οργανικές μονάδες του παρόχου διαδικτύου ή να διαφοροποιείται ανάλογα με τις ειδικές ανάγκες κάθε οργανικής μονάδας. Σε κάθε περίπτωση όμως θα πρέπει να τηρούνται οι βασικές αρχές εγκατάστασης και διαχείρισης που περιγράφονται στον παρόντα Κανονισμό.

Άρθρο 7
Σκοπός και Περιεχόμενο της Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού

1. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού, στο πλαίσιο της απαίτησης για διασφάλιση του απορρήτου των επικοινωνιών και της τήρησης της Πολιτικής Ασφαλείας του παρόχου διαδικτύου αλλά και γενικότερα στο πλαίσιο της εύρυθμης λειτουργίας του παρόχου διαδικτύου, καθορίζει ένα συστηματικό τρόπο για:

(α) Τη δημιουργία πλήρους ιστορικού αναφορικά με τις αλλαγές που έχουν πραγματοποιηθεί στον τηλεπικοινωνιακό εξοπλισμό του παρόχου διαδικτύου.
(β) Την εκτίμηση του χρόνου διακοπής της παροχής διαφόρων υπηρεσιών που σχετίζονται με πραγματοποιούμενες αλλαγές.
(γ) Τον συντονισμό των αλλαγών που πραγματοποιούνται στον τηλεπικοινωνιακό εξοπλισμό έτσι ώστε αλλαγές σε κάποιο στοιχείο του εξοπλισμού να μην επηρεάζουν / επιφέρουν αλλαγές σε άλλα στοιχεία του εξοπλισμού.
(δ) Την ελαχιστοποίηση της πιθανότητας για εκδήλωση επισυνδέσεων και άλλων παρόμοιων απειλών εναντίον του τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου.

2. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού σε έναν πάροχο διαδικτύου περιλαμβάνει κατ' ελάχιστο:

(α) Διαδικασίες για τη δοκιμή και την εγκατάσταση νέου τηλεπικοινωνιακού εξοπλισμού.
(β) Διαδικασίες για την καταγραφή των αλλαγών που πραγματοποιούνται σε υπάρχοντα τηλεπικοινωνιακό εξοπλισμό.
(γ) Διαδικασίες για την ενημέρωση του παρόχου διαδικτύου αναφορικά με την πραγματοποίηση αλλαγών σε υπάρχοντα τηλεπικοινωνιακό εξοπλισμό.
(δ) Διαδικασίες για το καθορισμό αρμοδιοτήτων αναφορικά με την διαχείριση και τη διαμόρφωση τηλεπικοινωνιακού εξοπλισμού.
(ε) Διαδικασίες για την εξουσιοδότηση μελών του προσωπικού του παρόχου διαδικτύου, τα οποία θα εφαρμόζουν την εν λόγω πολιτική συνολικά για όλες τις οργανικές μονάδες του παρόχου διαδικτύου ή/και ανά οργανική μονάδα ξεχωριστά.

Άρθρο 8
Εγκατάσταση Τηλεπικοινωνιακού Εξοπλισμού

1. Ο τηλεπικοινωνιακός εξοπλισμός ενός παρόχου διαδικτύου εγκαθίσταται εντός των ορίων της περιμέτρου του παρόχου διαδικτύου και σύμφωνα με τα όσα ορίζονται στην αντίστοιχη Πολιτική Ασφαλείας Περιμέτρου. Εξαιρούνται περιπτώσεις για τις οποίες τεκμηριώνεται απαίτηση για εγκατάσταση εκτός της περιμέτρου προκειμένου να επιτευχθεί ορθή λειτουργία του εξοπλισμού ή/και των υπηρεσιών που βασίζονται στη λειτουργία του.
2. Η εγκατάσταση του εξοπλισμού γίνεται σε δύο τουλάχιστον στάδια και περιλαμβάνει κατ' ελάχιστο τα ακόλουθα βήματα:

Στάδιο Προετοιμασίας:

(α) Ελέγχονται η πληρότητα και η έκταση της προσφερόμενης τεκμηρίωσης αναφορικά με την εγκατάσταση, τη διαμόρφωση, τη χρήση και τη συντήρηση του εξοπλισμού δίνοντας έμφαση σε ότι αφορά στα χαρακτηριστικά ασφάλειάς του και τις δυνατότητες προστασίας και άρσης του απορρήτου. Η τεκμηρίωση θα πρέπει να περιλαμβάνει ένα καλά καθορισμένο σύνολο από δοκιμές αποδοχής του εξοπλισμού. Εφόσον ο υπό εγκατάσταση εξοπλισμός περιλαμβάνει λογισμικό το οποίο έχει αναπτυχθεί εσωτερικά τότε η τεκμηρίωση θα πρέπει να περιλαμβάνει ανάλυση / σχολιασμό σε επίπεδο πηγαίου κώδικα.

(β) Εφόσον η εγκατάσταση εξοπλισμού περιλαμβάνει και εγκατάσταση λογισμικού τότε ελέγχεται η συμμόρφωση του λογισμικού με καθιερωμένα διεθνή πρότυπα ή διεθνώς διαδεδομένες πρακτικές.

(γ) Αποτιμάται ο κίνδυνος, αναφορικά με την ορθή λειτουργία του παρόχου διαδικτύου, που μπορεί να προκύψει από ενδεχόμενη δυσλειτουργία του υπό εγκατάσταση τηλεπικοινωνιακού εξοπλισμού. Η αποτίμηση του κινδύνου περιλαμβάνει και την καταγραφή των αλληλεξαρτήσεων του υπό εγκατάσταση τηλεπικοινωνιακού εξοπλισμού με τα υπάρχοντα τμήματα του τηλεπικοινωνιακού εξοπλισμού που βρίσκονται σε λειτουργία στον πάροχο διαδικτύου. Επίσης η διαδικασία αποτίμησης του κινδύνου καθορίζει κατά πόσον οι δοκιμές αποδοχής του εξοπλισμού θα πρέπει να διεξαχθούν σε ξεχωριστό περιβάλλον δοκιμών ή όχι. Η αποτίμηση του κινδύνου γίνεται τόσο σε επίπεδο υλικού και λογισμικού όσο και σε επίπεδο δικτυακής επικοινωνίας.

(δ) Στην περίπτωση αναβάθμισης λογισμικού αποτιμάται η εξάρτηση του εν λόγω λογισμικού από το λειτουργικό σύστημα που είναι εν χρήσει στο αντίστοιχο υλικό καθώς και από βιβλιοθήκες λογισμικού οι οποίες είναι τυχόν εν χρήσει στο αντίστοιχο υλικό.

(ε) Καθορίζεται ποια χαρακτηριστικά του εξοπλισμού, που σχετίζονται με την ασφάλεια και τη διασφάλιση του απορρήτου, πρέπει να ενεργοποιηθούν και με ποιο τρόπο.

Στάδιο Εγκατάστασης και Ελέγχου Ορθής Λειτουργίας:

(στ) Ο εξοπλισμός εγκαθίσταται είτε στο ξεχωριστό περιβάλλον δοκιμής είτε στο περιβάλλον παραγωγής του παρόχου διαδικτύου σύμφωνα με τη διαδικασία απο-

τίμησης κινδύνου. Ελέγχονται οι λειτουργίες του εξοπλισμού και διαπιστώνονται τυχόν προβλήματα. Τα προβλήματα συζητούνται με τον προμηθευτή του εξοπλισμού και γίνεται προσπάθεια επίλυσής τους.

(ζ) Εφόσον οι δοκιμές του υπό εγκατάσταση εξοπλισμού γίνονται σε συνεργασία με τηλεπικοινωνιακό εξοπλισμό ο οποίος ευρίσκεται σε περιβάλλον παραγωγής τότε είναι επιθυμητό οι δοκιμές αυτές να λαμβάνουν χώρα σε περιόδους χαμηλής τηλεπικοινωνιακής κίνησης (περιόδους μη αιχμής). Για την πραγματοποίηση των δοκιμών θα πρέπει να χρησιμοποιούνται όπου αυτό είναι δυνατό, δοκιμαστικά δεδομένα.

3. Οι ενέργειες που περιγράφονται στις παραγράφους 1 και 2 του παρόντος Άρθρου πραγματοποιούνται από εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου, σύμφωνα με τις αρμοδιότητες που έχουν καθορισθεί από την Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού. Σε περίπτωση σύμβασης υπεργολαβίας, η τελική ευθύνη της τήρησης της Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού παραμένει στον πάροχο διαδικτύου.
4. Το εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου με αιτιολογημένη έκθεσή του προτείνει την αποδοχή ή απόρριψη του εξοπλισμού στις ενδιαφερόμενες μονάδες του παρόχου διαδικτύου. Ο Υπεύθυνος Ασφάλειας του παρόχου διαδικτύου λαμβάνει γνώση της εκθέσεως. Στην περίπτωση που στην έκθεση προτείνεται η αποδοχή του εξοπλισμού τότε αυτός τίθεται σε λειτουργία στο περιβάλλον παραγωγής.

Άρθρο 9
Διαχείριση Τηλεπικοινωνιακού Εξοπλισμού

1. Η πρόσβαση στον εγκατεστημένο εξοπλισμό καθορίζεται από την ισχύουσα Πολιτική Ασφάλειας Περιμέτρου.
2. Το εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου θα πρέπει να ενημερώνεται αναφορικά με κάθε πρόβλημα ασφάλειας ή/και αναθεώρησης υλικού και λογισμικού που σχετίζεται με την ασφάλεια του τηλεπικοινωνιακού εξοπλισμού το οποίο διαπιστώνεται από κατασκευαστή ή από έγκυρους οργανισμούς σχετιζόμενους με την ασφάλεια, να αξιολογεί άμεσα κάθε σχετική πληροφορία αυτής της μορφής και, εφόσον διαπιστώνει ότι αφορά στον εξοπλισμό του παρόχου, να προβαίνει στις κατάλληλες αναβαθμίσεις.
3. Κατά τη διαδικασία διευθυνσιοδότησης του τηλεπικοινωνιακού εξοπλισμού δεν θα πρέπει να ενθαρρύνεται η χρήση δημοσίως γνωστών δικτυακών αναγνωριστικών (ενδεικτικά αναφέρονται διευθύνσεις IP, hostnames κ.λ.π.) εκτός από τις περιπτώσεις στις οποίες τεκμηριώνεται σχετική απαίτηση προκειμένου να επιτευχθεί ορθή λειτουργία του εξοπλισμού ή/και των υπηρεσιών που βασίζονται στη λειτουργία του.
4. Κάθε διακομιστής που αποτελεί μέρος τηλεπικοινωνιακού εξοπλισμού παρόχου θα πρέπει, κατά προτίμηση:

(α) Να χρησιμοποιείται για την παροχή μίας μόνο υπηρεσίας, ώστε να ελαχιστοποιείται η πιθανότητα διαχειριστικών λαθών και να μειώνονται τα περιθώρια για παραβίαση της ασφάλειας του διακομιστή με εκδήλωση επισυνδέσεων και άλλων αντί-

στοιχων απειλών. Η χρήση εξοπλισμού για περισσότερες από μία υπηρεσίες επιτρέπεται μόνο εφόσον ο κίνδυνος που προκύπτει από τέτοια κοινή χρήση έχει εξεταστεί από την διαδικασία αποτίμησης κινδύνου. Στην περίπτωση που ο διακομιστής χρησιμοποιείται για την παροχή περισσότερων της μιας υπηρεσιών, θα πρέπει να καταβάλλεται κάθε δυνατή προσπάθεια για απενεργοποίηση υπηρεσιών που δεν χρησιμοποιούνται, ιδιαίτερα εφόσον οι εν λόγω υπηρεσίες σχετίζονται με τη διαδικτυακή πρόσβαση.

(β) Να μη χρησιμοποιείται ως σταθμός εργασίας.

5. Σε κάθε δρομολογητή που αποτελεί μέρος τηλεπικοινωνιακού εξοπλισμού θα πρέπει, όποτε είναι εφικτό, να λαμβάνει χώρα:

(α) Απενεργοποίηση υπηρεσιών που δεν χρησιμοποιούνται.

(β) Αποτίμηση των δικτυακών διευθύνσεων, θυρών και πρωτοκόλλων με βάση τα οποία δρομολογούνται δεδομένα από το δρομολογητή.

(γ) Απενεργοποίηση της υπηρεσίας δρομολόγησης για δικτυακές διευθύνεις, θύρες και πρωτόκολλα που δεν περιλαμβάνονται στην ως άνω αποτίμηση.

6. Τυχόν διαχείριση τηλεπικοινωνιακού εξοπλισμού από απόσταση θα πρέπει να γίνεται μέσα από ασφαλείς διαύλους επικοινωνίας (ενδεικτικά αναφέρονται μισθωμένη γραμμή με κρυπτογράφηση, σύνδεση VPN κλπ.).

7. Ο χειρισμός των κωδικών ασφαλείας του τηλεπικοινωνιακού εξοπλισμού υπάγεται στην Πολιτική Κωδικών Ασφάλειας σύμφωνα με τον Κανονισμό για τη Διασφάλιση του Απορρήτου Εφαρμογών Διαδικτύου και Χρήστη.

8. Η διαμόρφωση του τηλεπικοινωνιακού εξοπλισμού θα πρέπει να ενεργοποιεί τις αντίστοιχες δυνατότητες καταγραφής ώστε να καθίσταται εφικτή η άρση του απορρήτου σύμφωνα με την κείμενη νομοθεσία.

9. Σε περίπτωση που ο τηλεπικοινωνιακός εξοπλισμός παρέχει τη δυνατότητα υλοποίησης πολλαπλών επιπέδων δικαιωμάτων πρόσβασης σε πόρους και δεδομένα του, πέραν της χρήσης κωδικών ασφαλείας, η διαμόρφωση του εξοπλισμού θα πρέπει να αξιοποιεί αυτή τη δυνατότητα. Με τον τρόπο αυτό μειώνεται η πιθανότητα παραβίασης της ασφαλείας και του απορρήτου είτε από τυχαία ενέργεια μη εξουσιοδοτημένου χρήστη ή από προσχεδιασμένη απειλή.

10. Στον εξοπλισμό επιτρέπεται η εγκατάσταση λογισμικού μόνο από το εξουσιοδοτημένο προσωπικό και μόνο για τους σκοπούς υποστήριξης του εξοπλισμού και των υπηρεσιών που προσφέρει.

11. Στα πλαίσια της Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού το ειδικά εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου καταγράφει σε μόνιμη βάση όλες τις πράξεις που σχετίζονται με εγκατάσταση, απεγκατάσταση, αναβάθμιση, αλλαγή διαμόρφωσης του τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου. Η καταγραφή γίνεται εντύπως σε ειδικό βιβλίο ή/και ηλεκτρονικά σε βάση δεδομένων του παρόχου διαδικτύου.

12. Με την ως άνω καταγραφή θα εξασφαλίζεται επίσης ότι στον τηλεπικοινωνιακό εξοπλισμό του παρόχου διαδικτύου δεν έχει εγκατασταθεί παράνομο ή επικίνδυνο λογισμικό.

13. Πρόσβαση στην ως άνω καταγραφή έχει μόνο το εξουσιοδοτημένο προσωπικό του

παρόχου.

14. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού θα πρέπει να προβλέπει τη διατήρηση των παλαιών εκδόσεων του λογισμικού για ορισμένο χρονικό διάστημα με σκοπό την επαναφορά τους στα συστήματα του παρόχου διαδικτύου στην περίπτωση που διαπιστωθεί πρόβλημα λειτουργίας το οποίο οφείλεται σε εγκατάσταση νέας έκδοσης λογισμικού ή σε αναβάθμιση λογισμικού. Οι ακριβείς διαδικασίες διατήρησης και επαναφοράς των παλαιών εκδόσεων του λογισμικού ορίζονται κατά περίπτωση από τον κάθε πάροχο διαδικτύου.
15. Τα τμήματα του τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου, τα οποία είναι δυνατό να τρωθούν από ιούς, θα πρέπει να προστατεύονται από κατάλληλο λογισμικό κατά των ιών.
16. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού προβλέπει συγκεκριμένες ενέργειες αναφορικά με την ασφάλεια και το απόρρητο κατά τη διαδικασία απεγκατάστασης τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου. Με τις ενέργειες αυτές θα πρέπει να διασφαλίζεται ότι η πληροφορία που έχει εγγραφεί μόνιμα στον εν λόγω εξοπλισμό (π.χ. σε μνήμες ROM, σκληρούς δίσκους, μαγνητικές ταινίες κλπ.) διαγράφεται οριστικά και δεν μπορεί να χρησιμοποιηθεί από τρίτους προκειμένου να παραβιασθεί η ασφάλεια του παρόχου διαδικτύου.

ΚΕΦΑΛΑΙΟ IV
ΠΟΛΙΤΙΚΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

Άρθρο 10
Γενικά

1. Η Πολιτική Αντιγράφων Ασφάλειας περιλαμβάνει τις διαδικασίες και τους ελέγχους που θα εξασφαλίσουν ότι ο τηλεπικοινωνιακός εξοπλισμός μπορεί να ανακτήσει τη λειτουργία εντός μιας λογικής χρονικής περιόδου μετά από οποιαδήποτε ζημιά που μπορεί να οφείλεται σε κακόβουλες επιθέσεις στο δικτυακό εξοπλισμό.
2. Ο σκοπός της πολιτικής αυτής είναι να καθορίζει τους κανόνες και τις διαδικασίες αντιγράφων ασφάλειας και ανάκτησης δεδομένων για να αποτραπεί η απώλεια στοιχείων στην περίπτωση διακοπής της λειτουργίας του συστήματος του παρόχου διαδικτύου.

Άρθρο 11
Περιεχόμενο

1. Τα Αντίγραφα Ασφάλειας στην παρούσα πολιτική αναφέρονται στα δεδομένα διάρθρωσης των δικτυακών στοιχείων.
2. Κάθε πάροχος διαδικτύου πρέπει να αναπτύξει και να συντηρήσει ένα σχέδιο για να μπορεί να ανταποκρίνεται σε περιπτώσεις εκτάκτου ανάγκης του συστήματος μετά από κακόβουλες επιθέσεις περιλαμβάνοντας την εκτέλεση αντιγράφων ασφαλείας, την παροχή διαδικασιών που μπορούν να χρησιμοποιηθούν για να διευκολύνουν τη συνέχιση της λειτουργίας σε περίπτωση ανάγκης και την ανάκτηση από μια επίθεση. Πιο συγκεκριμένα:

(α) Πρέπει να αναπτυχθεί και να τεκμηριωθεί μια διαδικασία ανάλυσης της ευαισθησίας, των ευπαθειών, και της ασφάλειας των προγραμμάτων και των πληροφοριών που λαμβάνουν, χειρίζονται, αποθηκεύουν, ή/και μεταδίδουν τα δικτυακά στοιχεία ώστε να προσδιοριστούν τα στοιχεία για τα οποία θα πρέπει να αποθηκεύονται.

(β) Η συχνότητα και η έκταση των αντιγράφων ασφαλείας πρέπει να είναι σύμφωνα με τη σημασία των πληροφοριών και του αποδεκτού κινδύνου όπως καθορίζεται μετά από την αντίστοιχη ανάλυση.

(γ) Ένα σχέδιο ανάκτησης δεδομένων πρέπει να τεκμηριωθεί και να ενημερώνεται σε τακτά χρονικά διαστήματα για να δημιουργήσει και να διατηρήσει, για μια συγκεκριμένη χρονική περίοδο, ανακτήσιμα ακριβή αντίγραφα των πληροφοριών.

(δ) Ένα σχέδιο αποκατάστασης πρέπει να αναπτυχθεί και να τεκμηριωθεί, έτσι ώστε να επιτρέπει στον πάροχο διαδικτύου να αποκαταστήσει οποιαδήποτε απώλεια στοιχείων σε περίπτωση αποτυχίας του συστήματος και των δικτυακών πόρων μετά από κακόβουλη επίθεση.

(ε) Ένα σχέδιο λειτουργίας τρόπου έκτακτης ανάγκης πρέπει να αναπτυχθεί και να τεκμηριωθεί, το οποίο να επιτρέπει στον πάροχο διαδικτύου να συνεχίσει να λειτουργεί σε περίπτωση αποτυχίας του συστήματος.

(στ) Διαδικασίες δοκιμών και αναθεώρησης πρέπει να αναπτυχθούν και να τεκμηριωθούν, οι οποίες να απαιτούν την περιοδική δοκιμή των σχεδίων έκτακτης ανάγκης (contingency plans) για να ανακαλύψουν τυχόν αδυναμίες.

(ζ) Στα αντίγραφα ασφαλείας πρέπει να διατίθεται το ίδιο επίπεδο προστασίας με τα αρχικά στοιχεία.

(η) Τα εφεδρικά αντίγραφα ασφαλείας και οι διαδικασίες αντιγραφής θα πρέπει να εξετάζονται περιοδικά για να εξασφαλισθεί ότι είναι δυνατό να ανακτηθούν.

Άρθρο 12
Ασφάλεια Αντιγράφων Δικτυακών Στοιχείων

1. Σε περίπτωση βλάβης κάποιας δικτυακής διάταξης, όπως δρομολογητές, μεταγωγείς (switch), κόμβοι (hub) και firewalls ή ακόμα και σε περίπτωση κακόβουλης αλλαγής της διάρθρωσης των διατάξεων αυτών, είναι απαραίτητος ο επαναπρογραμματισμός των στοιχείων αυτών στην αρχική τους κατάσταση. Για αυτό το λόγο θα πρέπει διάφορα αρχεία που προσδιορίζουν την κατάσταση και τη διάρθρωση των συσκευών αυτών να αντιγράφονται, και συγκεκριμένα:

(α) Τα δεδομένα διάρθρωσης μιας δικτυακής διάταξης (λογισμικό συστήματος, αρχεία σύνθεσης του λογισμικού, αρχεία βάσεων δεδομένων, κλπ.) πρέπει να αντιγράφονται ημερησίως, εβδομαδιαίως και μηνιαίως, έτσι ώστε σε περίπτωση αποτυχίας του συστήματος, τα δεδομένα και τα αρχεία σύνθεσης του λογισμικού (configuration files) να μπορούν να ανακτηθούν.

(β) Τα εφεδρικά αντίγραφα πρέπει να αποθηκεύονται με ασφαλή τρόπο σε αρχεία μόνο αναγνώσιμα έτσι ώστε τα αποθηκευμένα δεδομένα να μην επεγγράφονται (overwrite) ακούσια και πρέπει να κλειδώνονται ώστε τα δεδομένα να είναι προσβάσιμα μόνο σε εξουσιοδοτημένο προσωπικό.

(γ) Μια λύση θα ήταν η ύπαρξη ενός εφεδρικού firewall, που θα έχει την ίδια σύνθεση με το firewall που χρησιμοποιείται. Το firewall αυτό θα μπορούσε να τεθεί σε λειτουργία σε περίπτωση βλάβης του αρχικού και να χρησιμοποιείται ενώ το άλλο είναι υπό επισκευή. Τουλάχιστον ένα firewall πρέπει να έχει διαρθρωθεί και να διαφυλάσσεται, ώστε σε περίπτωση αποτυχίας, αυτό το εφεδρικό firewall να μπορεί να χρησιμοποιηθεί για την προστασία του δικτύου.

2. Σημαντικό για τον πάροχο διαδικτύου είναι επίσης η παροχή προστασίας στους διακομιστές του δίκτυου του και η ανάκτηση αρχείων στην περίπτωση απώλειας αυτών. Οι διαχειριστές δικτύων μπορεί να παρέχουν διάφορες μεθόδους παροχής εφεδρικών αντιγράφων, όπως πλήρη, αυξητική και διαφορική αντιγραφή αρχείων. Μια διαφορετική μέθοδος αντιγραφής είναι η Δικτυακή Αντιγραφή αρχείων, στην οποία κρυπτογραφημένα δεδομένα με αυτόματο και ασφαλή τρόπο αντιγράφονται και αποθηκεύονται σε μια περιοχή εκτός του εσωτερικού δικτύου του παρόχου διαδικτύου.

ΚΕΦΑΛΑΙΟ V
ΔΙΑΔΙΚΑΣΙΑ ΧΕΙΡΙΣΜΟΥ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Άρθρο 13
Γενικά

1. Κάθε πάροχος διαδικτύου οφείλει να διαθέτει σαφή Διαδικασία Χειρισμού Περιστατικών Ασφάλειας (Δ.Χ.Π.Α) τα οποία απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και τη διασφάλιση του απορρήτου των επικοινωνιών που διεξάγονται μέσω του παρόχου.
2. Σε κάθε περίπτωση όπου:

(α) διαπιστώνεται κίνδυνος για την διασφάλιση του απορρήτου,
(β) έχει καταγγελθεί παραβίαση απορρήτου,
(γ) υπάρχουν σοβαρές υπόνοιες ότι δε διασφαλίζεται το απόρρητο των επικοινωνιών,

ο πάροχος διαδικτύου οφείλει να ενεργοποιεί άμεσα την Δ.Χ.Π.Α.

3. Στόχοι της διαδικασίας είναι να:

(α) Καταγραφούν όλες οι λεπτομέρειες του περιστατικού.
(β) Να ενημερωθούν οι αρμόδιοι (του παρόχου διαδικτύου αλλά και φορείς όπως η ΑΔΑΕ) και οι χρήστες.
(γ) Να διασφαλιστεί το δυνατόν συντομότερο το απόρρητο.
(δ) Να διερευνηθούν τα αίτια και να βρεθούν τα πιθανά σφάλματα του παρόχου διαδικτύου ή και άλλων προσώπων.

Άρθρο 14
Περιεχόμενο

1. Η Δ.Χ.Π.Α. πρέπει να περιέχει τουλάχιστον τα σημεία που περιγράφονται στο παρόν άρθρο.
2. Πρέπει να ορίζεται ομάδα άμεσου χειρισμού του συμβάντος αποτελούμενη από εξειδικευμένους τεχνικούς αλλά και διοικητικά στελέχη. Τα τεχνικά στελέχη έχουν την ευθύνη να επιβεβαιώσουν το συμβάν και να προβούν άμεσα στην αποκατάσταση του προβλήματος. Τα διοικητικά στελέχη φέρουν την ευθύνη αξιολόγησης και

διαχείρισης του συμβάντος σε συνεργασία με την τεχνική ομάδα.

3. Κάθε συμβάν θα πρέπει να αναφέρεται ώστε να είναι δυνατή η άμεση αντιμετώπισή του. Για αυτό το λόγο θα πρέπει να οριστεί ένα ή περισσότερα άτομα στα οποία θα πρέπει να αναφέρεται άμεσα η εκδήλωση ενός περιστατικού ασφάλειας, από οποιοδήποτε μέλος του προσωπικού του παρόχου, όταν αυτό γίνεται αντιληπτό. Το άτομο ή τα άτομα αυτά θα πρέπει να γνωστοποιούνται σε όλο το προσωπικό, μαζί με πιθανούς τρόπους επικοινωνίας (τηλέφωνα, fax, email ή ό,τι άλλο κρίνεται αναγκαίο).
4. Κάθε συμβάν πρέπει να αξιολογείται και με βάση την αξιολόγησή του, κρίνεται ο τρόπος με τον οποίο πρέπει να αντιμετωπιστεί. Ανάλογα με την κρισιμότητα του περιστατικού ενεργοποιείται και η κατάλληλη διάταξη της Δ.Χ.Π.Α.
5. Επίσης πρέπει να ορίζεται η επικοινωνιακή πολιτική για κάθε περίπτωση ανάλογου περιστατικού. Αναλόγως με την κρισιμότητα του συμβάντος ειδοποιούνται τα κατάλληλα στελέχη του παρόχου διαδικτύου. Σε περίπτωση κρίσιμου περιστατικού πρέπει να ειδοποιούνται σταδιακά υψηλόβαθμα στελέχη του παρόχου διαδικτύου, τα οποία φέρουν και την ευθύνη καταγγελίας του περιστατικού στους αρμόδιους φορείς και την ΑΔΑΕ.
6. Ο παρακάτω πίνακας είναι ενδεικτικός για τον τρόπο με τον οποίο αντιμετωπίζονται αντίστοιχα συμβάντα με βάση την κρισιμότητά τους.

Κρισιμότητα	**Ομάδα άμεσης επέμβασης**	**Ενέργειες**	**Επικοινωνιακή πολιτική**
	Περιλαμβάνει στοιχεία επικοινωνίας και ρόλο κάθε προσώπου	Περιλαμβάνουν τόσο τεχνικές επιταγές και σχέδιο αποκατάστασης του απορρήτου όσο και διοκητικές ενέργειες	Περιλαμβάνει λίστα των φορέων και ατόμων οι οποίοι πρέπει να λάβουν γνώση του συμβάντος καθώς και τη συχνότητα ενημέρωσης του κάθε φορέα ή προσώπου
Κρίσιμη	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς
Σοβαρή	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς
Πιθανή	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς
Ελάχιστη	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς

7. Ο πάροχος διαδικτύου οφείλει να διατηρεί την Δ.Χ.Π.Α. ενημερωμένη με σωστά στοιχεία επικοινωνίας για όλους του εμπλεκόμενους. Τα στοιχεία των προσώπων και φορέων που πρέπει να ειδοποιηθούν άμεσα στην περίπτωση που διαπιστώνεται κάποιο συμβάν πρέπει να επαρκούν για την άμεση ειδοποίησή τους.
8. Ακόμα, πρέπει να υπογραμμιστεί η αναγκαιότητα καταγραφής όλων των ενεργειών που εκτελέστηκαν από την τεχνική ομάδα, όλων των τεχνικών ευρημάτων, καθώς και όλων των επικοινωνιών κατά τη διάρκεια καταστολής του περιστατικού. Η καταγραφή των στοιχείων πρέπει να γίνεται με τρόπο σαφή και σε ειδικά έντυπα τα οποία περιγράφονται στην Δ.Χ.Π.Α. του παρόχου διαδικτύου.
9. Επίσης ο πάροχος διαδικτύου πρέπει να ελέγχει σε τακτά χρονικά διαστήματα την ετοιμότητα ενεργοποίησης όλων τον μηχανισμών και προσώπων που περιγράφονται στην Δ.Χ.Π.Α.

ΚΕΦΑΛΑΙΟ VI
ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

Άρθρο 15
Γενικά

1. Η διαδικασία ελέγχου ασφάλειας δικτύου πραγματοποιείται από την ομάδα ελέγχου ασφάλειας δικτύου του παρόχου διαδικτύου. Η ομάδα ελέγχου ασφάλειας δικτύου θα χρησιμοποιήσει συγκεκριμένο λογισμικό ελέγχου για τη διεξαγωγή ηλεκτρονικής ανίχνευσης των δικτύων ή/και των συστημάτων προστασίας επιθέσεων ή οποιουδήποτε άλλου πληροφοριακού και δικτυακού συστήματος στον πάροχο διαδικτύου.
2. Ο έλεγχος ασφάλειας δικτύου πραγματοποιείται με σκοπό :

(α) Την εξακρίβωση ότι διασφαλίζεται η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα πληροφοριών και πόρων.

(β) Την εξακρίβωση ότι διασφαλίζεται η συμφωνία των πιθανών περιστατικών που σχετίζονται με την ασφάλεια με την πολιτική ασφάλειας του παρόχου διαδικτύου.

(γ) Την παρακολούθηση ενεργειών των χρηστών, των χρηστών παρόχου και του συστήματος όπου αυτό κρίνεται αναγκαίο, ύστερα από σχετική ενημέρωση του χρήστη ή χρήστη παρόχου.

3. Η ομάδα ελέγχου ασφάλειας δικτύου επιτελεί τη διαδικασία ελέγχου ασφάλειας με τέτοιο τρόπο ώστε να μην εμποδίζεται η παροχή των υπηρεσιών του παρόχου διαδικτύου προς τους χρήστες ή χρήστες παρόχου.
4. Η ομάδα ελέγχου ασφάλειας δικτύου μπορεί να είναι εσωτερική, δηλαδή να απαρτίζεται από εργαζόμενους στον πάροχο διαδικτύου, ή εξωτερική, δηλαδή να απαρτίζεται από εξειδικευμένο προσωπικό άλλου φορέα, με τον οποίο συνάπτεται η κατάλληλη συμφωνία.

Άρθρο 16
Υποχρεώσεις Παρόχου

1. Κατά τη διαδικασία ελέγχου ασφάλειας δικτύου, ο πάροχος διαδικτύου επιτρέπει στην ομάδα ελέγχου ασφάλειας δικτύου την πρόσβαση στο δίκτυο και τα συστήματα προστασίας επιθέσεων, έως το επίπεδο το οποίο κρίνεται αναγκαίο ώστε να γίνει

δυνατή η εκτέλεση των καθορισμένων ελέγχων.

2. Ο πάροχος διαδικτύου παρέχει τα αναγκαία πρωτόκολλα, τις δικτυακές συνδέσεις και τις πληροφορίες διευθυνσιοδότησης που είναι αναγκαία στην ομάδα ελέγχου ασφάλειας δικτύου για την εκτέλεση του λογισμικού ελέγχου και διάγνωσης του δικτύου. Η πρόσβαση αυτή μπορεί να συμπεριλαμβάνει:

(α) Πρόσβαση επιπέδου χρήστη ή/και συστήματος σε οποιαδήποτε διάταξη υπολογιστή και επικοινωνίας.

(β) Πρόσβαση σε πληροφορία (ηλεκτρονικής ή έντυπης μορφής) η οποία μπορεί να παραχθεί, μεταδοθεί ή αποθηκευτεί σε εξοπλισμό ή σε εγκαταστάσεις οι οποίες ανήκουν στον πάροχο διαδικτύου. Σε περίπτωση που η πληροφορία αυτή αφορά κάποιον χρήστη ή χρήστη παρόχου, ο πάροχος οφείλει να ενημερώνει το χρήστη ή χρήστη παρόχου για τη διαδικασία αυτή.

(γ) Πρόσβαση σε χώρους εργασίας (εργαστήρια, γραφεία, αποθηκευτικούς χώρους, κ.λ.π.)

(δ) Πρόσβαση με σκοπό την ενεργή παρακολούθηση και καταγραφή κίνησης πάνω από τα δίκτυα του παρόχου διαδικτύου.

Άρθρο 17
Έλεγχος Δικτύου

1. Η ομάδα ελέγχου ασφάλειας δικτύου πραγματοποιεί τον έλεγχο μόνο κατά τη διάρκεια των επιτρεπόμενων ημερομηνιών και ωραρίων που έχουν προσυμφωνηθεί με τον πάροχο διαδικτύου.
2. Σε περίπτωση που ο πάροχος διαδικτύου δε διαθέτει τον πλήρη έλεγχο πάνω στα δίκτυά του, ή η πρόσβαση στις υπηρεσίες διαδικτύου παρέχεται μέσω άλλων παρόχων διαδικτύου, οι τελευταίοι θα πρέπει να παράσχουν έγγραφη αποδοχή της διαδικασίας ελέγχου ασφάλειας δικτύου, κατά τη διάρκεια των προκαθορισμένων ημερομηνιών και ωραρίων.
3. Οι επιδόσεις ή/και η διαθεσιμότητα του δικτύου ενδέχεται να επηρεαστούν κατά τη διάρκεια των δοκιμών και των ελέγχων που θα πραγματοποιηθούν. Η ομάδα ελέγχου ασφάλειας δικτύου οφείλει να λαμβάνει όλα τα δυνατά μέτρα ώστε να ελαχιστοποιούνται όσο είναι δυνατό τέτοιες επιδράσεις. Όμως, η ομάδα ελέγχου ασφάλειας δικτύου απαλλάσσεται από οποιαδήποτε ευθύνη σχετικά με ζημιές οι οποίες ενδέχεται να προκύψουν ως αποτέλεσμα της μη διαθεσιμότητας του δικτύου η οποία μπορεί να προκληθεί από τις δοκιμές και τους ελέγχους που θα πραγματοποιηθούν, με εξαίρεση την περίπτωση που οι ζημιές αυτές είναι το αποτέλεσμα αμέλειας ή σκόπιμης κακόβουλης ενέργειας της ομάδας ελέγχου ασφάλειας δικτύου.

Άρθρο 18
Εφαρμογή

1. Ο πάροχος διαδικτύου πραγματοποιεί διαδικασία ελέγχου ασφάλειας δικτύου είτε αυτόβουλα, σε τακτά χρονικά διαστήματα, είτε ύστερα από αιτιολογημένο αίτημα της ΑΔΑΕ.

ΚΕΦΑΛΑΙΟ VII
ΔΙΑΔΙΚΑΣΙΑ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ

Άρθρο 19
Γενικά

1. Ως Διαδικασία Αποτίμησης Κινδύνων ορίζεται η διαδικασία εντοπισμού, ελέγχου και αξιολόγησης των τρωτών σημείων και απειλών ασφαλείας των πληροφοριακών και δικτυακών συστημάτων του παρόχου διαδικτύου σε ότι αφορά στην εμπιστευτικότητα και ακεραιότητα των δεδομένων και τη διαθεσιμότητα των παρεχόμενων υπηρεσιών.
2. Ειδικότερα για το τηλεπικοινωνιακό απόρρητο, η Διαδικασία Αποτίμησης Κινδύνων εστιάζεται στις απειλές που σχετίζονται με την προστασία των δεδομένων επικοινωνίας των χρηστών των υπηρεσιών ηλεκτρονικών επικοινωνιών.
3. Σκοπός της είναι να βοηθήσει τον πάροχο διαδικτύου να επιλέξει τις διαδικασίες και πρακτικές που ελαχιστοποιούν την πιθανότητα παραβίασης του απορρήτου επικοινωνιών των χρηστών καθώς και το κόστος εφαρμογής τους.

Άρθρο 20
Περιεχόμενο

1. Ο πάροχος διαδικτύου οφείλει να συγκροτεί Ομάδα Αποτίμησης Κινδύνων, η οποία θα αναλαμβάνει να αναλύει τους κινδύνους που υφίστανται για το απόρρητο επικοινωνιών των χρηστών. Συνιστάται η Ομάδα να περιλαμβάνει τόσο τεχνικό προσωπικό (προγραμματιστές, μηχανικούς ασφαλείας κτλ) όσο και ανώτερα στελέχη, ώστε η αποτίμηση να είναι ολοκληρωμένη και να λαμβάνει υπόψη όλες τις αναγκαίες πτυχές.
2. Η Ομάδα Αποτίμησης Κινδύνων οφείλει να συνέρχεται τουλάχιστον μια φορά κάθε 12 μήνες και να συντάσσει την Αναφορά Αποτίμησης Κινδύνων σύμφωνα με το άρθρο 21. Επιπλέον, συνιστάται η ομάδα να συνέρχεται όποτε παρουσιάζεται κάποιο σημαντικό θέμα ασφαλείας, όπως νέες απειλές, αλλαγή/ανανέωση τηλεπικοινωνιακού υλικού, ενεργοποίηση καινούργιας εφαρμογής λογισμικού, μεταξύ άλλων.
3. Ο πάροχος διαδικτύου οφείλει να ορίζει Υπεύθυνο Αποτίμησης Κινδύνων. Συνιστάται να είναι στέλεχος του παρόχου διαδικτύου και να μην συμμετέχει στην Ομάδα Αποτίμησης Κινδύνων. Ο Υπεύθυνος Αποτίμησης Κινδύνων οφείλει:

(α) Να ελέγχει την ποιότητα των εργασιών της Ομάδας Αποτίμησης Κινδύνων.

(β) Να ελέγχει την Αναφορά Αποτίμησης Κινδύνων και να την παραδίδει εγκαίρως στον Υπεύθυνο Ασφάλειας του παρόχου διαδικτύου.

4. Σε περίπτωση ανάθεσης του έργου σε τρίτο με σύμβασης υπεργολαβίας, η τελική ευθύνη της Διαδικασίας Αποτίμησης Κινδύνων παραμένει στον πάροχο διαδικτύου. Τυχόν αμέλεια του Υπευθύνου Αποτίμησης Κινδύνων συνεπάγεται κυρώσεις κατά του ιδίου αλλά και κατά του παρόχου διαδικτύου, ο οποίος εν τέλει είναι υπεύθυνος για την διασφάλιση του απορρήτου.

Άρθρο 21
Αναφορά Αποτίμησης Κινδύνων

1. Η Διαδικασία Αποτίμησης Κινδύνων οφείλει να περιγράφει λεπτομερώς και να ακο-

λουθεί κατ' ελάχιστον τα παρακάτω βήματα:

(α) Καταγραφή των Πόρων Δεδομένων Επικοινωνιών: πρόκειται για την πλήρη καταγραφή όλων των πόρων που χρησιμοποιούνται για την παρακολούθηση, αποθήκευση, επεξεργασία, εξαγωγή, διαβίβαση, ανακοίνωση και δημοσιοποίηση δεδομένων επικοινωνίας. Συνιστάται επίσης η καταγραφή των μέτρων ασφαλείας που ισχύουν ήδη.

(β) Κατηγοριοποίηση των Πόρων Δεδομένων Επικοινωνιών: κάθε πόρος δεδομένων επικοινωνιών πρέπει να χαρακτηριστεί ως «κρίσιμος», «βασικός» ή «κανονικός» με κριτήριο τη σημασία ως προς το απόρρητο των δεδομένων επικοινωνιών που διαχειρίζεται ο κάθε πόρος.

(γ) Καταγραφή Ευπαθειών: για κάθε Πόρο Δεδομένων Επικοινωνιών πρέπει να καταγράφονται όλες οι ευπάθειες (αδυναμίες, ελαττώματα) που είναι δυνατόν να θέσουν σε κίνδυνο το απόρρητο επικοινωνιών των χρηστών.

(δ) Κατηγοριοποίηση Ευπαθειών: κάθε ευπάθεια που καταγράφηκε στο προηγούμενο βήμα οφείλει να ορισθεί με σαφήνεια και να χαρακτηρισθεί ως «κρίσιμη», «σημαντική» ή «δευτερεύουσα» με κριτήριο το πόσο επικίνδυνη είναι για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών.

(ε) Καταγραφή Απειλών: για κάθε Πόρο Δεδομένων Επικοινωνιών πρέπει να καταγράφονται όλες οι απειλές που είναι δυνατόν να εκμεταλλευτούν μια ευπάθεια και να θέσουν σε κίνδυνο το απόρρητο επικοινωνιών των χρηστών.

(στ) Κατηγοριοποίηση Απειλών: κάθε απειλή που καταγράφηκε στο προηγούμενο βήμα οφείλει να ορισθεί με σαφήνεια και να χαρακτηρισθεί ως «κρίσιμη», «σημαντική» ή «δευτερεύουσα» με κριτήριο το πόσο επικίνδυνη είναι για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών. Πρέπει να λαμβάνονται υπόψη τόσο τα αποτελέσματα μιας τέτοιας απειλής καθώς και η πιθανότητα να συμβεί.

(ζ) Ιεράρχηση Κινδύνου: πρόκειται για την ταξινόμηση όλων των συνδυασμών «Πόρος Δεδομένων Επικοινωνιών – Ευπάθεια – Απειλή» ως προς την κρισιμότητα του κινδύνου. Στο βήμα αυτό, οποιαδήποτε μεθοδολογία αποτίμησης και αν ακολουθείται, πρέπει να αναφέρεται ξεκάθαρα ποιοι συνδυασμοί παρουσιάζουν μεγαλύτερο κίνδυνο για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών και ποιοι μικρότερο.

(η) Προτάσεις Αντιμετώπισης Κινδύνου: για κάθε συνδυασμό «Πόρος Δεδομένων Επικοινωνιών – Ευπάθεια – Απειλή» του προηγούμενου βήματος πρέπει να προτείνεται και να περιγράφεται λεπτομερώς τουλάχιστον μία λύση. Η λύση αυτή είναι πιθανόν να αφορά είτε συγκεκριμένα τεχνικά βήματα είτε πολιτικές - διαδικασίες αντιμετώπισης του κινδύνου. Για κάθε λύση συνιστάται επίσης να καθορίζονται το σκεπτικό, τα προτερήματα και μειονεκτήματά της έναντι των άλλων λύσεων, το πιθανό κόστος και ο χρονικός ορίζοντας υλοποίησής της. Ιδιαίτερη προσοχή πρέπει να δίνεται στις περιπτώσεις υψηλού κινδύνου.

(θ) Προτεινόμενη λύση: για κάθε συνδυασμό «Πόρος Δεδομένων Επικοινωνιών – Ευπάθεια – Απειλή» πρέπει να επιλέγεται μία λύση ανάμεσα σε αυτές που αναφέρθηκαν στο προηγούμενο βήμα (εφόσον οι λύσεις είναι περισσότερες από μία). Για αυτήν τη λύση πρέπει να αναφέρονται τόσο οι λόγοι που οδήγησαν στην

επιλογή αυτή όσο και τον υπολειπόμενο κίνδυνο.

2. Η Αναφορά Αποτίμησης Κινδύνων οφείλει επίσης να αναφέρει τα μέλη της Ομάδας Αποτίμησης Κινδύνων, τον Υπεύθυνο Αποτίμησης Κινδύνων και την ημερομηνία δημιουργίας της.

ΚΕΦΑΛΑΙΟ VIII
ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 22
Γενικά

1. Οι πολιτικές και οι διαδικασίες που ορίστηκαν στον κανονισμό αυτό αποτελούν μέρος της γενικότερης Πολιτικής Ασφάλειας του παρόχου διαδικτύου, όπως αυτή ορίστηκε στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».
2. Κατά συνέπεια, η ΑΔΑΕ στα πλαίσια ελέγχου και εποπτείας που καθορίστηκαν στον «Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές», μπορεί ανά πάσα στιγμή να προβεί σε έλεγχο του καθορισμού, επιβολής και σωστής λειτουργίας των πολιτικών που ορίστηκαν στον παρόντα Κανονισμό.
3. Σχετικά με τις λεπτομερείς διαδικασίες διενέργειας του ελέγχου καθώς και τις προβλεπόμενες διοικητικές κυρώσεις ισχύουν, κατ' αναλογία, τα αναγραφόμενα στον «Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».

Άρθρο 23
Πολιτική Ασφάλειας Περιμέτρου

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου εφαρμόζει Πολιτική Ασφάλειας Περιμέτρου και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.
2. Ο πάροχος διαδικτύου υποχρεούται να παραδίδει στα στελέχη της ΑΔΑΕ την πιο πρόσφατη Πολιτική Ασφάλειας Περιμέτρου είτε κατά τη διάρκεια ελέγχου είτε κάθε φορά που πραγματοποιείται κάποια σημαντική αλλαγή σε αυτή. Επιπρόσθετα, ο πάροχος διαδικτύου υποχρεούται περιοδικά να αποστέλλει στην ΑΔΑΕ τις τελευταίες Φόρμες Καταγραφής Επισυνδέσεων.
3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Ασφάλειας Περιμέτρου. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την Πολιτική Ασφάλειας Περιμέτρου αναλόγως, εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 24
Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού

1. Το εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου διενεργεί περιοδικούς ελέγχους προκειμένου να διαπιστώσει κατά πόσον τηρείται η Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού στις διάφορες οργανικές μονάδες

του παρόχου διαδικτύου. Σε όσες περιπτώσεις είναι δυνατό θα πρέπει να γίνεται χρήση αυτοματοποιημένων εργαλείων τα οποία π.χ. συλλέγουν και αναλύουν δεδομένα από αρχεία καταγραφής ή/και πραγματοποιούν εικονικές επιθέσεις στον εξοπλισμό του παρόχου διαδικτύου για διαπίστωση πιθανών κενών ασφαλείας. Η διαδικασία των περιοδικών ελέγχων θα πρέπει να έχει σχεδιαστεί με τέτοιο τρόπο έτσι ώστε να τελεί υπό την άμεση εποπτεία του Υπεύθυνου Ασφάλειας του παρόχου διαδικτύου.

2. Η ΑΔΑΕ διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου διατηρεί και εφαρμόζει επαρκή και ενημερωμένη Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού, η οποία συμφωνεί με τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.
3. Ο υπό έλεγχο πάροχος διαδικτύου οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ την εν ενεργεία Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού καθώς και να παρέχει πρόσβαση στην έντυπη ή/και ηλεκτρονική καταγραφή των πράξεων που σχετίζονται με εγκατάσταση, απεγκατάσταση, αναβάθμιση, αλλαγή διαμόρφωσης του τηλεπικοινωνιακού εξοπλισμού του.
4. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού αναλόγως.

Άρθρο 25
Πολιτική Αντιγράφων Ασφάλειας

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου εφαρμόζει την Πολιτική Αντιγράφων Ασφάλειας και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.
2. Ο πάροχος διαδικτύου υποχρεούται να παραδίδει στα στελέχη της ΑΔΑΕ την πιο πρόσφατη Πολιτική Αντιγράφων Ασφάλειας είτε κατά τη διάρκεια ελέγχου είτε κάθε φορά που πραγματοποιείται κάποια σημαντική αλλαγή σε αυτή.
3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Αντιγράφων Ασφάλειας. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την Πολιτική Αντιγράφων Ασφάλειας αναλόγως, εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 26
Διαδικασία Χειρισμού Περιστατικών Ασφάλειας

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου διατηρεί επαρκή και ενημερωμένη Δ.Χ.Π.Α. η οποία συμφωνεί με τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.
2. Ο υπό έλεγχο πάροχος διαδικτύου οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ την τελευταία Δ.Χ.Π.Α. Η ΑΔΑΕ μπορεί επιπλέον να ζητήσει την ενεργοποίηση της διαδικασίας είτε για να διαπιστώσει την ετοιμότητα του παρόχου είτε για να διερευνήσει καταγγελθέντα περιστατικά.

3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Δ.Χ.Π.Α.. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει τη Δ.Χ.Π.Α. αναλόγως.

Άρθρο 27
Διαδικασία Ελέγχου Ασφάλειας Δικτύου

1. Κατά τη διάρκεια ελέγχου ασφάλειας δικτύου, η ΑΔΑΕ μπορεί να διενεργήσει αυτοψία για να διαπιστώσει αν όντως τηρούνται οι διαδικασίες ελέγχου ασφάλειας δικτύου, και αν ο πάροχος διαδικτύου εφαρμόζει τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.
2. Κατά τη διάρκεια ελέγχου ασφάλειας δικτύου, οι εμπλεκόμενοι φορείς στη διαδικασία ελέγχου ασφάλειας δικτύου, οφείλουν να ενημερώσουν άμεσα την ΑΔΑΕ για οποιεσδήποτε αποκλίσεις ή παραβιάσεις της διαδικασίας ελέγχου ασφάλειας δικτύου.
3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν τη διαδικασία ελέγχου ασφάλειας δικτύου. Μετά από κάθε τέτοιου είδους τροποποίηση, η πραγματοποίηση οποιουδήποτε νέου ελέγχου ασφάλειας δικτύου, οφείλει να είναι σύμφωνη με το νέο τροποποιημένο Κανονισμό.

Άρθρο 28
Διαδικασία Αποτίμησης Κινδύνων

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου εφαρμόζει Διαδικασία Αποτίμησης Κινδύνων και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.
2. Ο υπό έλεγχο πάροχος διαδικτύου οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ την τελευταία Αναφορά Αποτίμησης Κινδύνων η οποία οφείλει να είναι ενημερωμένη και σύμφωνη με την υπάρχουσα κατάσταση σε ότι αφορά στους κινδύνους παραβίασης του απορρήτου επικοινωνιών των χρηστών.
3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Διαδικασία Αποτίμησης Κινδύνων. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει τη Διαδικασία Αποτίμησης Κινδύνων αναλόγως και να συγκαλεί την Ομάδα Αποτίμησης Κινδύνων εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

ΚΕΦΑΛΑΙΟ IX
ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 29
Μεταβατικές Διατάξεις

1. Όλοι οι πάροχοι διαδικτύου υποχρεούνται:

(α) Να ενημερώσουν ως προς την εφαρμοζόμενη πολιτική ασφάλειας την ΑΔΑΕ εντός έξι (6) μηνών από τη δημοσίευση του παρόντος.

(β) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική ασφάλειας εντός ενός (1) έτους από την έγκρισή της.

ΚΕΦΑΛΑΙΟ Χ
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 30
Έναρξη Ισχύος

ι. Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

Αριθμ: 634 α

ΑΠΟΦΑΣΗ
Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
Έχοντας υπόψη :

α. Το Ν. 3115/27-02-2003, άρθρο 1, παραγρ. 1,
β. Το Ν. 3115/27-02-2003, άρθρο 6, παραγρ. 1
γ. Ότι εκ της αποφάσεως δεν προκύπτει δαπάνη για το δημόσιο
δ. Τη σχετική εισήγηση της Υπηρεσίας

Α π ο φ ά σ ι σ ε,
κατά τη συνεδρίασή της την 1ον Νοεμβρίου 2004, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός – Πεδίο Εφαρμογής

4. Σκοπός του παρόντος Κανονισμού είναι:
(α) Η διασφάλιση του απορρήτου των εφαρμογών στο διαδίκτυο και των χρηστών τους.
(β) Η ασφάλεια των παρόχων υπηρεσίας εφαρμογής ως προς τις προσφερόμενες υπηρεσίες και εφαρμογές.
(γ) Η θέσπιση των υποχρεώσεων των εν λόγω παρόχων αναφορικά με την ασφάλεια και το απόρρητο των εφαρμογών Διαδικτύου και των χρηστών.
(δ) Ο έλεγχος στους εν λόγω παρόχους σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.
5. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:
(α) Πάροχοι σταθερής και κινητής πρόσβασης στο Διαδίκτυο
(β) Πάροχοι Διαδικτυακών υπηρεσιών, υπηρεσιών προστιθέμενης αξίας και υπηρεσίας εφαρμογών.

Άρθρο 2
Ορισμοί

Για την εφαρμογή του παρόντος Κανονισμού ισχύουν οι ορισμοί του «Κανονισμού για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές» της ΑΔΑΕ, που επαναλαμβάνονται για πληρότητα.

Επιπρόσθετα, οι ακόλουθοι όροι έχουν την έννοια που τους αποδίδεται κατωτέρω:

Ασύμμετρη Κρυπτογραφία: στηρίζεται στη χρήση ενός ζευγαριού κλειδιών, ενός ιδιωτικού και ενός δημόσιου. Όταν η κρυπτογράφηση γίνεται με το ένα κλειδί, η αποκρυπτογράφηση γίνεται με το άλλο. Είναι γνωστή και ως Κρυπτογραφία Δημόσιου Κλειδιού.

Ακεραιότητα: είναι ιδιότητα της διαδικασίας ασφάλειας με την οποία ελέγχεται αν τα δεδομένα έχουν τροποποιηθεί ή καταστραφεί κατά μη εξουσιοδοτημένο τρόπο.

Δεδομένα Θέσης: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

Δεδομένα Κίνησης: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της.

Διαδικτυακές Επικοινωνίες: Υπηρεσίες ηλεκτρονικών επικοινωνιών όπου το δίκτυο ηλεκτρονικών επικοινωνιών είναι δίκτυο μετάδοσης δεδομένων και φωνής με πακετομεταγωγή το οποίο είτε έχει τη μορφή ενδοδικτύου (Intranet) είτε είναι ολόκληρο το διαδίκτυο (Internet).

Δίκτυο Ηλεκτρονικών Επικοινωνιών: τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, συμπεριλαμβανομένου του Διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών.

Εμπιστευτικότητα: η ιδιότητα της διαδικασίας ασφάλειας με την οποία αποτρέπεται η διάθεση ή η αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα, οντότητες ή διεργασίες.

Εξουσιοδότηση: η διαδικασία χορήγησης δικαιώματος πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από

την οντότητα που ελέγχει τον πόρο για τον οποίο ζητάτε η πρόσβαση.

Επαλήθευση Ταυτότητας (Authentication): αναφέρεται στις αυτοματοποιημένες και τυποποιημένες μεθόδους για την πιστοποίηση της ταυτότητας του χρήστη στο διαδίκτυο. Αναφέρεται και ως αυθεντικοποίηση.

Ιός (virus): Ως ιός περιγράφεται ένα κομμάτι κώδικα λογισμικού το οποίο εισβάλλει σε ένα υπολογιστικό σύστημα με σκοπό να προκαλέσει ανεπιθύμητα αποτελέσματα, όπως καταστροφή δεδομένων χρήστη, άρνηση υπηρεσίας (denial-of-service), παραβίαση του συστήματος ασφαλείας του συστήματος κτλ. Κύριο χαρακτηριστικό του είναι το γεγονός ότι μεταδίδεται μεταξύ των υπολογιστικών συστημάτων με τη μορφή εκτελέσιμων προγραμμάτων (executables), εγγραφών συστήματος (system or boot records) και μακρο-εντολών (macros). Οι ιοί είναι δυνατόν να επιτεθούν κατά προσωπικών υπολογιστών, servers, routers κτλ.

Κλειδί Κρυπτογράφησης: μια σειρά από bits συγκεκριμένου μήκους που χρησιμοποιείται για να κρυπτογραφήσει ή να αποκρυπτογραφήσει τα δεδομένα σε έναν αλγόριθμο κρυπτογράφησης.

Λογισμικό Προστασίας από Ιούς (anti-virus software): Πρόκειται για μια κατηγορία εφαρμογών λογισμικού που αποσκοπεί στην ανίχνευση και απομάκρυνση ιών που έχουν προσβάλλει ένα υπολογιστικό σύστημα.

Μη Αποποίηση Ευθύνης: εξασφαλίζει ότι οι συναλλασσόμενοι σε εφαρμογές και υπηρεσίες Διαδικτύου που προσφέρονται είτε από πάροχους διαδικτύου είτε από πάροχους υπηρεσίας εφαρμογής δεν μπορούν να αρνηθούν τη συμμετοχή τους στη συναλλαγή.

Παροχή Δικτύου Διαδικτυακών Επικοινωνιών: η σύσταση, η λειτουργία, ο έλεγχος και η διάθεση τέτοιου δικτύου.

Πάροχος Δικτύου Διαδικτυακών Επικοινωνιών (Internet Service Provider): Η επιχείρηση ή το νομικό πρόσωπο που παρέχει δίκτυο διαδικτυακών επικοινωνιών ή/και το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του. Για τις ανάγκες του παρόντος ο πάροχος δικτύου διαδικτυακών επικοινωνιών θα αναφέρεται στη συνέχεια του κειμένου ως «πάροχος διαδικτύου».

Πάροχος Υπηρεσίας Εφαρμογής (Application Service Provider): μία οντότητα (οργανισμός, εταιρεία κτλ), η οποία διαθέτει εφαρμογές λογισμικού (software), υλική υποδομή (hardware) και δικτυακή υποδομή, προκειμένου να παρέχει υπηρεσίες και εφαρμογές στον πάροχο δικτύου διαδικτυακών επικοινωνιών και τους χρήστες του.

Πολιτική ασφάλειας: Το σύνολο τεχνικών, οργανωτικών και κανονιστικών μέτρων, τα οποία εφαρμόζονται από πάροχο διαδικτύου και αποβλέπουν στη διασφάλιση του απορρήτου και γενικά στην ασφαλή λειτουργία των δικτύων διαδικτυακών επικοινωνιών.

Προσδιορισμός ταυτότητας: αναφέρεται σε λιγότερο τυποποιημένες μεθόδους (σε σχέση με τη διαδικασία επαλήθευσης ταυτότητας) για την πιστοποίηση της φύσης του χρήστη, που είναι συνήθως μη αυτόματες και απαιτούν ανθρώπινη παρέμβαση.

Προστασία του απορρήτου: η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων επικοινωνίας από άλλα πρόσωπα, χωρίς τη συγκατάθεσή τους, εξαιρουμένων των νόμιμα εξουσιοδοτημένων.

Συγκατάθεση του Χρήστη ή του Συνδρομητή: η συγκατάθεση του προσώπου που αφορούν τα δεδομένα, κατά την έννοια της οδηγίας 95/46/ΕΚ.

Συμμετρική Κρυπτογραφία: η κρυπτογράφηση και αποκρυπτογράφηση πραγματοποιούνται με ένα κλειδί.

Ταυτότητα: είναι οι πληροφορίες που προσδιορίζουν το χρήστη με μοναδικό τρόπο.

Υπεργολάβος: όπως αυτός ορίζεται από την υπάρχουσα νομοθεσία.

Υπηρεσία Προστιθέμενης Αξίας: υπηρεσία μη τηλεπικοινωνιακή η οποία μπορεί να παρέχεται ή να υποστηρίζεται από δίκτυο διαδικτυακών επικοινωνιών.

Υπηρεσίες Ηλεκτρονικών Επικοινωνιών: οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχόμενου

που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και υπηρεσίες της κοινωνίας της πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του ΠΔ39/2001 (Α'28), και που δεν αφορούν, εν όλω ή εν μέρει, τη μεταφορά σημάτων σε δίκτυα επικοινωνιών.

Χρήστης: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

Χρήστης Παρόχου: κάθε φυσικό πρόσωπο που εργάζεται στην επιχείρηση ή το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του.

ΚΕΦΑΛΑΙΟ ΙΙ
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΧΡΗΣΤΗ ΔΙΑΔΙΚΤΥΟΥ

Άρθρο 3
Σκοπός, Κανόνες και Συνθήκες

1. Ο σκοπός της πολιτικής ασφάλειας χρήστη Διαδικτύου είναι να ορίσει τους κανόνες και τις απαιτήσεις ασφάλειας για τη χρήση του Διαδικτύου ως ασφαλές μέσο για τη μετάδοση ευαίσθητων πληροφοριών και να διασφαλίσει την χρήση του.
2. Οι πιο κάτω κανόνες και συνθήκες αφορούν όλους τους χρήστες που χρησιμοποιούν το διαδίκτυο ή έχουν κάποιο σημείο προσαρμογής σε αυτό, με σκοπό τη μετάδοση πληροφοριών. Η πολιτική αυτή δεν καλύπτει την προστασία υποδομών τοπικών δεδομένων ή τοπικών δικτύων (LAN κτλ).
3. Μια ολοκληρωμένη υλοποίηση Διαδικτυακής επικοινωνίας θα πρέπει να περιλαμβάνει επαρκείς μεθόδους κρυπτογράφησης (encryption), χρησιμοποίηση επαλήθευσης ή προσδιορισμού ταυτότητας (authentication or identification) από τους χρήστες και ένα σχέδιο διαχείρισης που θα ενσωματώνει αποδοτικές μεθόδους διαχείρισης κλειδιών και κωδικών πρόσβασης. Πιο συγκεκριμένα:

(α) Οι μέθοδοι που εφαρμόζονται από τους χρήστες θα πρέπει να περιλαμβάνουν μια μέθοδο κρυπτογράφησης και τουλάχιστον μία μέθοδο επαλήθευσης και προσδιορισμού ταυτότητας. Αυτές οι μέθοδοι πρέπει να είναι αρκετά γενικές και ανοικτές ώστε να παρέχουν μέγιστη προσαρμοστικότητα από την πλευρά του χρήστη και των εφαρμογών, μέσα όμως σε κάποια όρια ασφάλειας και εύκολης διαχείρισης.

(β) Οι τεχνικές θα πρέπει να παρέχουν στο χρήστη τη δυνατότητα να αποδεικνύει ότι είναι αυτός που δηλώνεται και να οργανώνουν έτσι τα δεδομένα προς μετάδοση ώστε να αποφεύγεται η ανάρμοστη γνωστοποίηση ή τροποποίηση των δεδομένων κατά τη μετάδοσή τους. Επομένως, τεχνικές επαλήθευσης και προσδιορισμού της ταυτότητας του χρήστη θα πρέπει να συνυπάρχουν με τεχνικές κρυπτογράφησης και μετάδοσης δεδομένων ώστε να εγγυηθούν ότι τα δεδομένα θα

μεταφερθούν με ασφαλή τρόπο και ότι μόνο οι εξουσιοδοτημένοι χρήστες θα μπορέσουν να τα διαβάσουν.

(γ) Υπάρχουν περιπτώσεις που "σταθεροί" κωδικοί πρόσβασης δεν επαρκούν, αλλά χρειάζεται ένα είδος δυναμικής πιστοποίησης των δεδομένων. Μια σειρά από διαφορετικές τεχνολογίες μπορούν να παρέχουν ένα είδος δυναμικής πιστοποίησης, όπως γεννήτριες δυναμικών κωδικών, τεχνικές βασισμένες στην κρυπτογραφία, καθώς και ψηφιακές υπογραφές και πιστοποιητικά.

(δ) Οι τεχνικές προσδιορισμού των κωδικών πρόσβασης παρέχουν ένα επίπεδο ασφάλειας. Η δυσκολία ανίχνευσης των κωδικών αυτών από τρίτα άτομα καθώς και ο τρόπος που αυτοί προστατεύονται καθορίζουν εμμέσως την ισχύ της διαδικασίας επαλήθευσης της ταυτότητας του χρήστη.

1. Οι χρήστες δεν θα πρέπει να δίνουν το λογαριασμό πρόσβασης καθώς και τους αντίστοιχους κωδικούς που έχουν σε άλλα μη εξουσιοδοτημένα άτομα.
2. Οι χρήστες δεν θα πρέπει να αλλάζουν χαρακτηριστικά των συστημάτων λογισμικού ή υλικού, καθώς και να μην εγκαθιστούν προγράμματα σε υπολογιστές ή στο δίκτυο που εν γνώσει τους μπορεί να προκαλέσουν ζημιές ή να δημιουργήσουν υπερβολικό φορτίο στο υπολογιστικό σύστημα ή στο δίκτυο.
3. Οι χρήστες πρέπει να συμμορφώνονται με τον τρόπο χρήσης του ηλεκτρονικού τους ταχυδρομείου όπως προσδιορίζεται από τους παρόχους διαδικτύου και το περιβάλλον εργασίας τους. Μπορεί να υπάρχουν κανόνες που να ορίζουν τόσο τη συμπεριφορά των χρηστών όσο και τις απαιτήσεις των εφαρμογών και των εξυπηρετητών ηλεκτρονικού ταχυδρομείου.

(α) Απαραίτητη θεωρείται η εξέταση των εισερχόμενων μηνυμάτων για ιούς και κακόβουλα δεδομένα

(β) Οι εξυπηρετητές (servers) του ηλεκτρονικού ταχυδρομείου μπορεί να είναι αρχικοποιημένοι ώστε κάθε μήνυμα να υπογράφεται χρησιμοποιώντας την ψηφιακή υπογραφή του αποστολέα, να απαγορεύουν την αποστολή μηνυμάτων σε μη κατάλληλους προορισμούς και να ανιχνεύουν τη χρήση με κατάλληλα προγράμματα για αποστολή / παραλαβή μηνυμάτων.

(γ) Οι χρήστες θα πρέπει να συμμορφώνονται με τους κανόνες ασφάλειας που ορίζονται από τους παρόχους διαδικτύου, ύστερα από ενημέρωσή τους από τον πάροχο διαδικτύου σχετικά με αυτούς τους κανόνες. Οι χρήστες δηλώνουν τη συμμόρφωσή τους με σαφή, ατελή και εύκολα προσβάσιμο τρόπο, είτε ενυπόγραφα είτε ηλεκτρονικά. Οι κανόνες αυτοί μπορεί να περιέχουν περιορισμούς ως προς το υλικό που θα μεταδώσουν, και να εξασφαλίζουν τη μη παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας, καθώς και τη μη εξουσιοδοτημένη πρόσβαση σε δικτυακούς πόρους.

(δ) Οι χρήστες δεν θα πρέπει να δημοσιοποιούν υλικό σε ηλεκτρονικούς τόπους, news groups ή mail lists, το οποίο είναι παράνομο, ή όχι κατάλληλο (π.χ. να στέλνουν electronic junk mail ή chain letters).

ΚΕΦΑΛΑΙΟ ΙΙΙ
ΠΟΛΙΤΙΚΗ ΟΡΘΗΣ (ΔΕΟΝΤΟΛΟΓΙΚΗΣ) ΣΥΜΠΕΡΙΦΟΡΑΣ ΧΡΗΣΤΗ

Άρθρο 4
Σκοπός και πεδίο εφαρμογής της πολιτικής ορθής συμπεριφοράς

1. Η ανάπτυξη της επικοινωνίας μέσω Διαδικτύου και συναφών υπηρεσιών είναι τόσο προς όφελος των παρόχων διαδικτύου και υπηρεσίας εφαρμογής όσο και προς όφελος των χρηστών. Αφενός διότι θα οδηγήσουν στην επιχειρηματική ανάπτυξη των παρόχων αυτών, αφετέρου διότι οι παρεχόμενες υπηρεσίες εξυπηρετούν τον χρήστη. Προϋπόθεση της ανάπτυξης και διάδοσής τους είναι να διέπονται από Κανόνες Δεοντολογίας. Ενδεικτικά θα μπορούσαμε να αναφέρουμε τους κανόνες (Netiquette) που ορίζονται από την παγκόσμια κοινότητα του Διαδικτύου IETF.
2. Για την επιτυχία του ως άνω σκοπού θα πρέπει οι κανόνες αυτοί να γίνουν αποδεκτοί από όλους ανεξαιρέτως τους εμπλεκόμενους στις δικτυακές επικοινωνίες, δηλαδή τους χρήστες, τους χρήστες παρόχου και τους παρόχους επικοινωνιακών συστημάτων και εφαρμογών.
3. Η εφαρμογή των κανόνων αυτών σε επίπεδο φυσικού ή νομικού προσώπου συνιστά την πολιτική ορθής συμπεριφοράς του εν λόγω προσώπου.

Άρθρο 5
Πολιτική ορθής συμπεριφοράς παρόχων

1. Οι πάροχοι διαδικτύου είναι απαραίτητο να δίνουν το παράδειγμα σε κάθε επιχειρηματικό τους βήμα, και κάθε επιχειρηματική τους πράξη να είναι νόμιμη, ειλικρινής και να διέπεται από διαφάνεια.
2. Ο πάροχος διαδικτύου και οι χρήστες παρόχου θα πρέπει να προσπαθούν να διαφυλάσσουν τους κανόνες ορθής συμπεριφοράς και να απαντούν άμεσα σε τυχόν ερωτήματα χρηστών.
3. Ο πάροχος διαδικτύου θα πρέπει να προσπαθήσει να αυξήσει την εμπιστοσύνη των χρηστών στις παρεχόμενες εφαρμογές εφαρμόζοντας τους κανόνες της καθημερινής ορθής συμπεριφοράς και στο διαδίκτυο.
4. Ο πάροχος διαδικτύου είναι υποχρεωμένος να καταγγέλλει άμεσα στην ΑΔΑΕ περιπτώσεις μη ορθής συμπεριφοράς μέσω των προσφερόμενων εφαρμογών που εμπίπτουν στην αντίληψή του όπως ορίζει κάθε φορά η ισχύουσα νομοθεσία.
5. Σε περιπτώσεις όπου η νομοθεσία αδυνατεί να επιβάλει όρους και κανόνες τότε η πολιτική ορθής συμπεριφοράς του παρόχου διαδικτύου θα πρέπει πάντοτε να διαφυλάσσει το χρήστη.
6. Η πολιτική ορθής συμπεριφοράς αποτελεί έννοια με ευρεία φιλοσοφική διάσταση και ως εκ τούτου καθίσταται δύσκολη η πλήρης καταγραφή της. Εν τούτοις, κάθε πάροχος διαδικτύου οφείλει να συμπεριλαμβάνει επίσημες αναφορές σε αυτήν σε κατάλληλα σημεία των επίσημων εγγράφων του (π.χ. γενικές αρχές λειτουργίας) όσο και στο υλικό που διανέμει στους χρήστες των διαδικτυακών υπηρεσιών του.

Άρθρο 6
Πολιτική ορθής συμπεριφοράς χρηστών

1. Οι χρήστες είναι υποχρεωμένοι να χρησιμοποιούν τις εφαρμογές, όπως αυτές παρέχονται από τον εκάστοτε πάροχο διαδικτύου, έχοντας υπόψη τους ότι οι κατά την κρατούσα αντίληψη κανόνες ορθής συμπεριφοράς, πρέπει να διαφυλάσσονται και κατά τη χρήση των εφαρμογών αυτών.
2. Σε κάθε περίπτωση που υποπίπτει στην αντίληψη του χρήστη μη ορθή συμπεριφορά και χρήση των εφαρμογών, είναι υποχρεωμένος να ειδοποιεί άμεσα τον πάροχο διαδικτύου ή και να καταγγέλλει το περιστατικό στις αρμόδιες υπηρεσίες.
3. Ο χρήστης πρέπει να κατανοήσει ότι είναι υπεύθυνος για κάθε πράξη του στο διαδίκτυο. Σε περιπτώσεις όπου ο χρήστης χρησιμοποιεί το διαδίκτυο και τις παρεχόμενες εφαρμογές για εκβιασμό, αποστολή μηνυμάτων ρατσιστικού ή προσβλητικού περιεχομένου κ.ο.κ, ο χρήστης διώκεται βάσει της υπάρχουσας νομοθεσίας.

Άρθρο 7
Ανήθικη συμπεριφορά

1. Οι πάροχοι διαδικτύου, οι χρήστες και οι χρήστες παρόχου θα πρέπει να αποφεύγουν κάθε είδους ανήθικη συμπεριφορά μέσω εφαρμογών Διαδικτύου.
2. Υπογραμμίζεται ότι η ανήθικη και παράνομη συμπεριφορά μέσω διαδικτυακών εφαρμογών δεν διαχωρίζεται νομικά από τις κανονικές περίπτωσης ανήθικης συμπεριφοράς, όπως αυτές προβλέπονται από την νομοθεσία.
3. Κάθε περίπτωση εκβιασμού, λιβελογραφίας, συκοφαντικής δυσφήμισης, ρατσιστικής μεταχείρισης, παιδοφιλίας, παρακολούθησης ή διαρροής απόρρητων πληροφοριών κ.ο.κ. καλύπτεται νομικά από την υπάρχουσα νομοθεσία, η οποία ισχύει και για τις περιπτώσεις στις οποίες χρησιμοποιήθηκαν διαδικτυακές επικοινωνίες και εφαρμογές. Ειδικά υπογραμμίζεται η περίπτωση όπου ο πάροχος διαδικτύου ή οι χρήστες παρόχου χρησιμοποιούν παράνομα και ανήθικα την προσφερόμενη στον χρήστη υπηρεσία.

ΚΕΦΑΛΑΙΟ IV
ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΑΛΓΟΡΙΘΜΩΝ

Άρθρο 8
Κρυπτογράφηση

1. Η κρυπτογράφηση έχει βασικό σκοπό να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και τη μη-αποποίηση ευθύνης στις συναλλαγές και τις επικοινωνίες μέσω Διαδικτύου, τα οποία και αποτελούν αναπόσπαστα στοιχεία της ιδιωτικότητας του χρήστη.
2. Οι πάροχοι διαδικτύου οφείλουν να εφαρμόζουν αλγόριθμους και τεχνικές κρυπτογράφησης τόσο στα συστήματα μετάδοσης δεδομένων που χρησιμοποιούν όσο και στις εφαρμογές και τις υπηρεσίες του Διαδικτύου που παρέχουν. Σχετικά με το τελευταίο, ενδεικτικά και όχι περιοριστικά αναφέρονται οι υπηρεσίες ηλεκτρονικού εμπορίου, οι τραπεζικές συναλλαγές μέσω Διαδικτύου και το ηλεκτρονικό ταχυδρομείο.

3. Σχετικά με τα συστήματα μετάδοσης, οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ακολουθούν τα διεθνή πρότυπα ανάλογα με τη τεχνολογία μετάδοσης που ακολουθείται. Οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ενημερώνουν την ΑΔΑΕ ως προς τις τεχνικές κρυπτογράφησης που ακολουθούν.
4. Ανεξάρτητα από το πεδίο στο οποίο εφαρμόζονται τεχνικές κρυπτογράφησης, το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο ώστε να εξασφαλίζει ότι η παραβίασή της δεν είναι δυνατή (σε λογικό χρόνο και με λογικούς υπολογιστικούς πόρους). Το επίπεδο της κρυπτογράφησης εκφράζεται συνήθως από το μέγεθος του κλειδιού κρυπτογράφησης. Στη γενική περίπτωση όσο μεγαλύτερο είναι το μήκος του κλειδιού τόσο δυσκολότερη γίνεται η παραβίαση της κρυπτογράφησης. Η ΑΔΑΕ θα εκδίδει τεχνικές οδηγίες και συστάσεις που θα καθορίζουν το μήκος του κλειδιού ανά πεδίο κρυπτογράφησης.
5. Ανεξάρτητα από το πεδίο στο οποίο εφαρμόζονται τεχνικές κρυπτογράφησης, οι αλγόριθμοι κρυπτογράφησης που θα χρησιμοποιούνται θα πρέπει να είναι οι ευρέως αποδεκτοί αλγόριθμοι. Ενδεικτικά και όχι περιοριστικά αναφέρονται οι αλγόριθμοι RSA, Diffie-Hellman και ElGamal για την ασύμμετρη κρυπτογραφία και οι 3DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish και CAST για τη συμμετρική κρυπτογραφία.

Άρθρο 9
Ασφάλεια Εφαρμογών Διαδικτύου

1. Για την ασφάλεια και τη διασφάλιση του απορρήτου των εφαρμογών Διαδικτύου έχουν αναπτυχθεί διάφορα πρωτόκολλα και εφαρμογές που βασίζονται στις γενικές αρχές της κρυπτογράφησης. Ανάλογα με τον τύπο εφαρμογής Διαδικτύου έχουν προταθεί και προτυποποιηθεί συγκεκριμένα πρωτόκολλα.
2. Οι πάροχοι υπηρεσίας εφαρμογής οφείλουν να κάνουν χρήση των ευρέως αποδεκτών τεχνικών και πρωτόκολλων ασφάλειας των εφαρμογών Διαδικτύου. Ενδεικτικά και όχι περιοριστικά αναφέρονται τα ακόλουθα πρωτόκολλα ανά τύπο εφαρμογής:

(α) Για εφαρμογές Παγκόσμιου Ιστού (WWW) (π.χ. ηλεκτρονικό εμπόριο, τραπεζικές συναλλαγές μέσω Διαδικτύου) χρησιμοποιούνται τα πρωτόκολλα Secure Sockets Layer (SSL) και Secure HTTP (S-HTTP). Εξασφαλίζουν αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα στην ανταλλαγή δεδομένων μεταξύ στοιχείων του παγκόσμιου ιστού (φυλλομετρητές και εξυπηρετητές).

(β) Για εφαρμογές ηλεκτρονικού ταχυδρομείου (e-mail) χρησιμοποιούνται τα πρωτόκολλα S/MIME και PEM (Privacy Enhanced Mail), τα οποία εν ολίγοις κάνουν χρήση ψηφιακών υπογραφών και κρυπτογράφησης στα μεταδιδόμενα ηλεκτρονικά μηνύματα. Η εφαρμογή PGP (Pretty Good Privacy) χρησιμοποιείται για παρόμοιο σκοπό.

(γ) Το πρωτόκολλο SET (Secure Electronic Transaction) χρησιμοποιείται για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών.

3. Δεδομένου ότι νέα πρωτόκολλα και τεχνολογίες θα ανακύπτουν με την πρόοδο της επιστήμης των υπολογιστών, η ΑΔΑΕ θα εκδίδει τεχνικές οδηγίες και συστάσεις προς

τους πάροχους διαδικτύου σχετικά με αυτά τα νέα πρωτόκολλα και τις τεχνολογίες. Οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ακολουθούν τα εκάστοτε ευρέως χρησιμοποιούμενα πρωτόκολλα και τεχνολογίες, είτε αυτόβουλα είτε έπειτα από έλεγχο και αντίστοιχη οδηγία από την ΑΔΑΕ.

ΚΕΦΑΛΑΙΟ V
ΧΡΗΣΗ ΚΩΔΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (PASSWORDS)

Άρθρο 10
Ανάγκη ύπαρξης πολιτικής κωδικών ασφάλειας

1. Οι κωδικοί ασφάλειας αποτελούν ένα από τα σημαντικότερα πεδία της ασφάλειας των επικοινωνιών. Αποτελούν την τελευταία γραμμή άμυνας ενάντια σε αυτούς που θα προσπαθήσουν να επιβουλευθούν ένα δίκτυο δεδομένων, δημόσιο ή ιδιωτικό, ή ένα υπολογιστικό σύστημα.
2. Τα παραπάνω καθίστανται ακόμα πιο σημαντικά στις ακόλουθες περιπτώσεις:

(α) Στην περίπτωση που ο κωδικός ασφάλειας αφορά χρήστη παρόχου ο οποίος συνδέεται με τα συστήματα του παρόχου διαδικτύου από απόσταση, μέσω Διαδικτύου.

(β) Στην περίπτωση που ο κωδικός ασφάλειας αφορά χρήστη παρόχου ο οποίος αποκτά πρόσβαση από σύστημα του παρόχου διαδικτύου προς το διαδίκτυο.

Και στις δύο περιπτώσεις ένας ακατάλληλος κωδικός ασφάλειας δύναται να οδηγήσει σε απώλεια σημαντικών δεδομένων καθώς και σε γενικότερη δυσλειτουργία των συστημάτων του παρόχου διαδικτύου.

3. Συνεπώς κάθε πάροχος διαδικτύου θα πρέπει να διαθέτει και να επιβάλλει κανόνες αναφορικά με τους κωδικούς ασφάλειας ούτως ώστε:

(α) Να δημιουργούνται συμπαγείς κωδικοί.

(β) Να προστατεύονται οι ως άνω κωδικοί.

(γ) Να μεταβάλλονται συχνά οι ως άνω κωδικοί.

4. Η πολιτική αυτή θα πρέπει να εφαρμόζεται από όλους τους χρήστες και χρήστες παρόχου, οι οποίοι διαθέτουν λογαριασμό με πρόσβαση από και προς το διαδίκτυο και ιδιαίτερα αν χειρίζονται ευαίσθητα, μη διαθέσιμα στο κοινό, δεδομένα.

Άρθρο 11
Δημιουργία και Διαχείριση κωδικών ασφάλειας

1. Της εφαρμογής μιας πολιτικής δημιουργίας και διαχείρισης κωδικών ασφάλειας σε έναν πάροχο διαδικτύου προηγείται ο διαχωρισμός των συστημάτων σε αυτά που χρειάζονται προστασία μέσω κωδικών ασφάλειας και σε αυτά που διατίθενται προς ελεύθερη πρόσβαση.
2. Προκειμένου οι χρήστες και χρήστες παρόχου να χρησιμοποιήσουν ένα εταιρικό δίκτυο ή υπολογιστικό σύστημα το οποίο προστατεύεται, θα πρέπει να διαθέτουν «όνομα χρήστη» (login name) και κατάλληλο κωδικό ασφάλειας (password). Ως εκ τούτου η πολιτική κωδικών ασφάλειας περιλαμβάνει:

(α) Περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία των ονομάτων χρηστών (user names)

(β) Περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία των κωδικών ασφάλειας (passwords).

(γ) Περιγραφή των διαδικασιών σύμφωνα με τις οποίες διανέμεται σε κάθε χρήστη ή χρήστη παρόχου το αντίστοιχο όνομα χρήστη καθώς και ο κωδικός ασφάλειας.

(δ) Περιγραφή των κανόνων σύμφωνα με τους οποίους επιτυγχάνεται η τακτική αλλαγή των κωδικών ασφάλειας και η εν γένει διαχείρισή τους.

(ε) Περιγραφή των κανόνων οι οποίοι καθορίζουν την ενδεδειγμένη συμπεριφορά των χρηστών και χρηστών παρόχου αναφορικά με την προστασία των κωδικών ασφάλειας. Το σύνολο των εν λόγων κανόνων, οι οποίοι αποτελούν υποσύνολο της πολιτικής δημιουργίας και διαχείρισης κωδικών ασφάλειας, συνιστούν την πολιτική προστασίας των κωδικών ασφάλειας.

(στ) Περιγραφή των διαδικασιών σύμφωνα με τις οποίες διενεργείται έλεγχος για την πιστή ή μη εφαρμογή της εν λόγω πολιτικής.

3. Η πολιτική δημιουργίας και διαχείρισης κωδικών ασφάλειας θα πρέπει να βρίσκεται καταγεγραμμένη σε αντίστοιχο επίσημο έντυπο του πάροχου διαδικτύου, στο οποίο πρέπει να υπάρχει ελεγχόμενη πρόσβαση.

4. Οι χρήστες και χρήστες παρόχου, μόλις παραλαμβάνουν τους κωδικούς ασφάλειάς τους, θα πρέπει να λαμβάνουν εγγράφως γνώση των υποχρεώσεών τους που απορρέουν από τις υφιστάμενες πολιτικές για τους κωδικούς ασφάλειας.

5. Η πολιτική δημιουργίας και διαχείρισης κωδικών ασφάλειας θα πρέπει να πληροί, κατ' ελάχιστον, τα ακόλουθα χαρακτηριστικά:

(α) Ὑπαρξη συμπαγών κωδικών ασφάλειας: Οι χρησιμοποιούμενοι κωδικοί ασφάλειας θα πρέπει να είναι συμπαγείς έτσι ώστε να μην μπορεί να τους «μαντέψει» όποιος επιβουλεύεται το σύστημα. Συνεπώς η πολιτική κωδικών ασφάλειας θα πρέπει να επιβάλλει τη δημιουργία κωδικών ασφάλειας με συνδυασμό γραμμάτων, αριθμών και μη αλφαριθμητικών χαρακτήρων. Επιπλέον θα πρέπει να επιβάλλεται ένα ικανό ελάχιστο μήκος.

(β) Περιορισμένη πρόσβαση στο αρχείο φύλαξης των κωδικών ασφάλειας: Η πρόσβαση στο αρχείο που φυλάσσονται οι κωδικοί πρόσβασης θα πρέπει να είναι περιορισμένη.

(γ) Περιοδική αλλαγή κωδικών ασφάλειας: Η πολιτική θα πρέπει να μην ευνοεί την συνεχή χρήση του ιδίου κωδικού ασφάλειας. Η συχνότητα με την οποία επιβάλλεται στους χρήστες και στους χρήστες παρόχου να αλλάζουν κωδικό εξαρτάται από τους διαχειριστές του συστήματος καθώς και από τη φύση της λειτουργίας του παρόχου διαδικτύου. Πάντως σε χαρακτηριστικές περιπτώσεις όπως είναι (ενδεικτικά) η αποχώρηση κάποιου χρήστη παρόχου ή η παραβίαση κάποιου λογαριασμού τότε θα πρέπει άμεσα να λαμβάνει χώρα αλλαγή του αντίστοιχου κωδικού ασφάλειας. Επιπλέον σε περιπτώσεις ευρείας παραβίασης της ασφάλειας του συστήματος, η οποία ενδέχεται να περιλαμβάνει και παραβίαση λογαριασμών διαχειριστών του συστήματος, θα πρέπει να λαμβάνει χώρα αλλαγή όλων των κωδικών ασφάλειας.

(δ) Αδρανοποίηση κωδικού ασφάλειας: Ως επιπλέον μέτρο ασφάλειας δύναται να επιβληθεί η αδρανοποίηση του λογαριασμού του χρήστη και του χρήστη παρό-

χου στην περίπτωση επαναλαμβανόμενης εισαγωγής κωδικών ασφάλειας (π.χ. μετά από τρεις συνεχόμενες αποτυχημένες απόπειρες).

6. Οι υπεύθυνοι ασφάλειας του συστήματος οφείλουν να πραγματοποιούν περιοδικούς ελέγχους προκειμένου να διαπιστώσουν κατά πόσον οι κωδικοί ασφάλειας είναι συμπαγείς με βάση τους αντιστοίχους κανόνες της πολιτικής δημιουργίας και διαχείρισης κωδικών ασφάλειας. Οι έλεγχοι θα περιλαμβάνουν δοκιμές της αντοχής στις μεθόδους αποκρυπτογράφησης των υφισταμένων κωδικών με αυτοματοποιημένο τρόπο μέσω καταλλήλων εργαλείων λογισμικού.
7. Εφόσον κατά τη διάρκεια των περιοδικών ελέγχων διαπιστωθεί η ύπαρξη μη συμπαγών κωδικών ασφάλειας, οι αντίστοιχοι χρήστες θα υποχρεώνονται να προβούν άμεσα στην αντικατάστασή τους.

Άρθρο 12
Δημιουργία και Διαχείριση κωδικών ασφάλειας αναφορικά με την πρόσβαση (μέσω Διαδικτύου) από απόσταση σε εφαρμογές

1. Εφόσον ένας πάροχος διαδικτύου παρέχει στους χρήστες και χρήστες παρόχου πρόσβαση από απόσταση (μέσω Διαδικτύου) σε εφαρμογές, θα πρέπει να λαμβάνει επιπλέον μέτρα σε σχέση με τη δημιουργία και διαχείριση των κωδικών ασφάλειας.
2. Στο βαθμό που είναι τεχνικά δυνατόν θα πρέπει να υφίσταται μία κοινή αρχιτεκτονική ταυτοποίησης για όλες τις εφαρμογές στις οποίες παρέχεται πρόσβαση μέσω Διαδικτύου. Η εν λόγω αρχιτεκτονική είναι προτιμότερο να βασίζεται σε διεθνώς αποδεκτά πρότυπα (π.χ. RADIUS)
3. Οι υπεύθυνοι ασφάλειας του παρόχου διαδικτύου θα πρέπει να προβαίνουν σε αποτίμηση κινδύνου αναφορικά με το κατά πόσον μια τέτοια εφαρμογή καθίσταται ασφαλής μέσω της χρήσης ονόματος χρήστη / κωδικού ασφάλειας ή κατά πόσον θα πρέπει να χρησιμοποιούνται πρόσθετες τεχνικές ταυτοποίησης. Χαρακτηριστικό παράδειγμα αποτελούν οι εφαρμογές μέσω των οποίων λαμβάνουν χώρα οικονομικές συναλλαγές.
4. Η εν λόγω αποτίμηση θα πρέπει μεταξύ άλλων να παρέχει κατευθύνσεις αναφορικά με τα ακόλουθα:

(α) Κατά πόσον οι εν λόγω εφαρμογές είναι σχεδιασμένες με βάση την εγκεκριμένη πολιτική για τους κωδικούς ασφάλειας.

(β) Ποιες εφαρμογές θα πρέπει να υποστηρίζουν την κρυπτογράφηση του ζεύγους αναγνωριστικών όνομα χρήστη / κωδικός ασφάλειας κατά την πρόσβαση στην εφαρμογή μέσω της χρήσης καταλλήλου πρωτοκόλλου βασισμένο σε αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού (π.χ. https).

(γ) Για ποιες εφαρμογές απαιτείται να παράγεται εκ νέου κωδικός ασφάλειας κάθε φορά που κάποιος χρήστης χρειάζεται να αποκτήσει πρόσβαση από απόσταση σε αυτές. Σε μια τέτοια περίπτωση θα πρέπει να προδιαγράφεται η διαδικασία δημιουργίας τέτοιων βραχύβιων κωδικών, π.χ. μέσω της χρήσης εξειδικευμένων συσκευών που διατίθενται στους χρήστες και στους χρήστες παρόχου.

5. Στις περιπτώσεις όπου υφίστανται εφαρμογές οι οποίες υποστηρίζουν αποκρυπτογράφηση δεδομένων με χρήση ιδιωτικού κλειδιού, οι πολιτικές που ισχύουν για τη

διαχείριση των κωδικών ασφάλειας έχουν εφαρμογή και στη διαχείριση των ιδιωτικών κλειδιών.

Άρθρο 13
Προστασία κωδικών ασφάλειας

1. Οι υπεύθυνοι ασφάλειας του δικτύου ή του συστήματος θα πρέπει να δίνουν έμφαση στην ενημέρωση των χρηστών αναφορικά με την πολιτική προστασίας των κωδικών ασφάλειας.
2. Συνιστάται η πολιτική προστασίας των κωδικών ασφάλειας να είναι καταγεγραμμένη με τη μορφή απλών κανόνων οι οποίοι θα είναι κατανοητοί από το σύνολο των χρηστών και χρηστών παρόχου έτσι ώστε να μπορούν να τους εφαρμόζουν.
3. Η πολιτική προστασίας των κωδικών ασφάλειας θα πρέπει να περιλαμβάνει, κατ' ελάχιστον, τους ακόλουθους κανόνες:

(α) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να μοιράζεται των κωδικό ασφάλειας του με άλλους χρήστες και χρήστες παρόχου εκτός αν ο λογαριασμός στον οποίο αντιστοιχεί ο εν λόγω κωδικός προορίζεται ρητώς για πρόσβαση πολλαπλών χρηστών.

(β) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να αποκαλύπτει σε οποιονδήποτε τον κωδικό ή τους κωδικούς ασφάλειας που του έχουν δοθεί. Η απαγόρευση αυτή περιλαμβάνει και άτομα που υπό άλλες συνθήκες θεωρούνται έμπιστα όπως π.χ. προϊσταμένους, υφισταμένους, φίλους και μέλη της οικογένειας του χρήστη και χρήστη παρόχου.

(γ) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να συμπεριλαμβάνει τους κωδικούς ασφάλειάς του σε μηνύματα ηλεκτρονικού ταχυδρομείου.

(δ) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να αναφέρει τους κωδικούς ασφάλειας του κατά τη διάρκεια τηλεφωνικών συνομιλιών.

(ε) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να καταγράφει τους κωδικούς ασφάλειας του σε ερωτηματολόγια ή άλλα έγγραφα ακόμα και αν αυτά αποτελούν επίσημα έγγραφα του παρόχου διαδικτύου.

(στ) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να χρησιμοποιεί τον κωδικό ασφάλειάς του προκειμένου να παρέχει πρόσβαση στο σύστημα σε μη εξουσιοδοτημένα άτομα.

(ζ) Ο χρήστης και χρήστης παρόχου οφείλει να απομνημονεύει τον κωδικό ασφάλειας του. Ως εκ τούτου, δεν θα πρέπει να καταγράφει τον κωδικό ασφάλειας του σε χαρτί ή άλλο μέσο καταγραφής ιδιαίτερα εφόσον το μέσο καταγραφής βρίσκεται κοντά στον υπολογιστή του. Σε περίπτωση που, για οποιονδήποτε λόγο, η απομνημόνευση είναι αδύνατη τότε το μέσο καταγραφής του κωδικού ασφάλειας θα πρέπει να τοποθετείται σε κάποιον προστατευμένο χώρο (π.χ. κλειδωμένη ντουλάπα)

(η) Ο χρήστης και χρήστης παρόχου οφείλει να αναφέρει στους υπευθύνους ασφάλειας οποιοδήποτε γεγονός ή ενέργεια υποπέσει στην αντίληψη του σχετικά με την παραβίαση της ασφάλειας του λογαριασμού του.

4. Η πολιτική προστασίας κωδικών ασφάλειας θα πρέπει να αναφέρει ρητώς τις επι-

βαλλόμενες κυρώσεις για τις περιπτώσεις που διαπιστωθεί παράβαση της εν λόγω πολιτικής εξ' υπαιτιότητος του χρήστη και χρήστη παρόχου.

ΚΕΦΑΛΑΙΟ VI
ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΠΟΤΡΟΠΗ ΙΩΝ

Άρθρο 14
Σκοπός και Αναγκαιότητα της Πολιτικής

1. Η Πολιτική Προστασίας και Αποτροπής Ιών (Anti-virus Policy) περιγράφει τις διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης ιών που απαιτούνται προκειμένου να εξασφαλίζεται στο μέγιστο δυνατό βαθμό η προστασία του συνόλου του δικτύου του παρόχου διαδικτύου και των χρηστών του από ιούς.
2. Σε ό,τι αφορά τη διασφάλιση απορρήτου επικοινωνιών ενός χρήστη και χρήστη παρόχου, πολλοί ιοί παραβιάζουν το σύστημα ασφάλειας του υπολογιστικού συστήματος και δημιουργούν αδυναμίες, μέσω των οποίων είναι δυνατόν να εγκατασταθούν προγράμματα πάσης φύσεως συμπεριλαμβανομένου και εφαρμογών που αποσκοπούν στην:

(α) Καταστροφή διαβαθμισμένων - απόρρητων πληροφοριών
(β) Υποκλοπή διαβαθμισμένων - απόρρητων πληροφοριών
(γ) Παρακολούθηση και καταγραφή των ενεργειών του χρήστη και χρήστη παρόχου
(δ) Υποκλοπή διαβαθμισμένων - απόρρητων επικοινωνιών
(ε) Αδυναμία πρόσβασης σε διαβαθμισμένες - απόρρητες πληροφορίες

3. Για να επιτευχθεί η προστασία από τους ιούς, ο πάροχος διαδικτύου, ο χρήστης και ο χρήστης παρόχου οφείλουν να ακολουθήσουν συγκεκριμένες διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης των ιών, όπως περιγράφεται στις παραγράφους που ακολουθούν.
4. Ο πάροχος διαδικτύου είναι υποχρεωμένος να διαθέτει «Πολιτική Προστασίας Ιών» στην οποία οφείλει να δημοσιεύει όλες τις διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης ιών που εφαρμόζει και είναι σύμφωνες με τις παραγράφους που ακολουθούν.

Άρθρο 15
Υποχρεώσεις του Παρόχου Διαδικτύου

1. Αποτροπή Ιών από τον πάροχο διαδικτύου: Ο πάροχος διαδικτύου οφείλει να:

(α) Διαθέτει δικτυακό εξοπλισμό ο οποίος περιορίζει την μετάδοση ιών. Για παράδειγμα, η μετάδοση ορισμένων ιών είναι δυνατόν να περιοριστεί μέσω χρήσης ειδικών φίλτρων (firewalls) στη δικτυακή υποδομή του παρόχου διαδικτύου. Η αναγκαία παραμετροποίηση των ειδικών αυτών φίλτρων πρέπει να εφαρμόζεται έγκαιρα και να διατηρείται έως ότου ο κίνδυνος από το συγκεκριμένο ιό έχει περιοριστεί. Ενδεικτικά, συνίσταται η διατήρηση των ειδικών παραμέτρων για δύο τουλάχιστον εβδομάδες.
(β) Διαθέτει το απαραίτητο λογισμικό για την προστασία από ιούς όλων των υπηρεσιών και εφαρμογών που προσφέρει στους χρήστες. Για παράδειγμα, υπηρεσίες όπως το ηλεκτρονικό ταχυδρομείο (e-mail) πρέπει να προστατεύονται από εξει-

δικευμένο λογισμικό (e-mail scanners).

(γ) Εγκαθιστά μονίμως στη μνήμη (memory resident) των υπολογιστικών συστημάτων λογισμικό προστασίας από ιούς, το οποίο να εξετάζει αυτομάτως όλα τα εισερχόμενα δεδομένα.

(δ) Εκπαιδεύει και ελέγχει τους χρήστες παρόχου σε τακτά χρονικά διαστήματα, ώστε να ακολουθούνται πάντα οι παραπάνω πολιτικές αποτροπής ιών.

(ε) Διατηρεί μια ομάδα ειδικών για την προστασία από ιούς, η οποία θα φροντίζει να ενημερώνεται σχετικά με την πιθανότητα επίθεσης από νέους ιούς (με σκοπό την έγκαιρη εγκατάσταση ή/και παραμετροποίηση των απαραίτητων μέσων προστασίας) και θα επανεξετάζει περιοδικά (τουλάχιστον 2 φορές το χρόνο) την πολιτική προστασίας ιών.

(στ) Ενημερώνει κι εκπαιδεύει τους χρήστες και χρήστες παρόχου σχετικά με το πώς μπορούν να προστατευθούν από τους ιούς.

2. Ανίχνευση Ιών από τον πάροχο διαδικτύου: Ο πάροχος διαδικτύου οφείλει να:

(α) Ανανεώνει τα συστήματα προστασίας από ιούς (ειδικό λογισμικό και ειδικός δικτυακός εξοπλισμός) ανά τακτά χρονικά διαστήματα ώστε να μπορούν να αποτρέψουν τη μετάδοση νέων ιών. Συνίσταται η αυτόματη ενημέρωση των συστημάτων του παρόχου διαδικτύου ανά δώδεκα (12) ώρες.

(β) Εξασφαλίζει ότι όλα τα αρχεία που είναι αποθηκευμένα στα συστήματα του παρόχου διαδικτύου και τα οποία είναι πιθανόν να περιλαμβάνουν ιούς εξετάζονται καθημερινά από προγράμματα ανίχνευσης ιών.

(γ) Ενημερώνει τους χρήστες και χρήστες παρόχου το δυνατόν συντομότερο σε περιπτώσεις όπου υπάρχει έξαρση μετάδοσης κάποιου επικίνδυνου ιού. Η ενημέρωση αυτή είναι δυνατόν να γίνεται με διάφορους τρόπους. Συνίσταται η ενημέρωση να γίνεται μέσω ηλεκτρονικού ταχυδρομείου, με ταυτόχρονη παρουσίαση του προβλήματος στην κεντρική σελίδα του δικτυακού του τόπου. Ο πάροχος διαδικτύου πρέπει να δίνει πληροφορίες για την αντιμετώπιση του ιού παρέχοντας links σε δικτυακούς τόπους μέσω των οποίων ο χρήστης και ο χρήστης παρόχου μπορεί να βρει το απαραίτητο λογισμικό για την αντιμετώπιση του ιού.

(δ) Ενημερώνει τους χρήστες και χρήστες παρόχου σχετικά με περιπτώσεις φάρσας, όπου ο χρήστης γίνεται συνήθως αποδέκτης ενός email που τον προειδοποιεί για την ύπαρξη κάποιου υποτιθέμενου ιού στο υπολογιστικό του σύστημα και τον παροτρύνει να προβεί σε ενέργειες, οι οποίες τελικά προκαλούν βλάβη στην σωστή λειτουργία του λειτουργικού συστήματος.

3. Αντιμετώπιση Ιών από τον πάροχο διαδικτύου: Ο πάροχος διαδικτύου οφείλει να:

(α) Ορίσει ομάδα αντιμετώπισης ιών, η οποία θα αναλαμβάνει την ανίχνευση και αφαίρεση όλων των ιών από τα υπολογιστικά συστήματα του παρόχου διαδικτύου.

(β) Απομονώνει εκτός δικτύου υπολογιστικά συστήματα στα οποία ανιχνεύθηκε κάποιος ιός. Το σύστημα είναι απαραίτητο να παραμείνει εκτός δικτύου ωσότου ο ιός αφαιρεθεί ολοκληρωτικά.

(γ) Στην περίπτωση που κάποιος χρήστης ζητήσει βοήθεια (είτε τηλεφωνικά είτε μέσω άλλου τρόπου επικοινωνίας) από τον πάροχο διαδικτύου για την αντιμετώπιση ιών, ο πάροχος διαδικτύου πρέπει να είναι προετοιμασμένος να παραπέμψει

τον χρήστη σε πληροφοριακές ιστοσελίδες και σε εταιρείες που προσφέρουν αντίστοιχες υπηρεσίες.

Άρθρο 16
Συστάσεις προς τον Χρήστη και Χρήστη Παρόχου

1. Αποτροπή Ιών: Ο χρήστης και ο χρήστης παρόχου συνίσταται να:

(α) Αναζητά βοήθεια από τον πάροχο διαδικτύου ή οποιονδήποτε άλλο οργανισμό μπορεί να βοηθήσει σχετικά με οποιαδήποτε μη φυσιολογική συμπεριφορά του λειτουργικού του συστήματος ή εφαρμογής.

(β) Έχει εγκατεστημένο μονίμως στην μνήμη (memory resident) ειδικό λογισμικό προστασίας από ιούς.

2. Ανίχνευση Ιών: Ο χρήστης και ο χρήστης παρόχου συνίσταται να:

(α) Χρησιμοποιεί την υπηρεσία αυτόματης ενημέρωσης του λογισμικού για νέους ιούς τουλάχιστον μια φορά το μήνα.

(β) Εξετάζει όλα τα αρχεία του προσωπικού υπολογιστή τουλάχιστον 2 φορές τον μήνα.

2. Αντιμετώπιση Ιών: Ο χρήστης και ο χρήστης παρόχου συνίσταται να:

(α) Αποσυνδέει το υπολογιστικό του σύστημα από το δίκτυο μέχρις ότου ο ιός αφαιρεθεί ολοκληρωτικά.

(β) Σε κάθε περίπτωση ο χρήστης και ο χρήστης παρόχου έχει το δικαίωμα να επικοινωνήσει με τον πάροχο διαδικτύου του και να ζητήσει πληροφορίες για την αντιμετώπιση των ιών. Ο πάροχος διαδικτύου σε αυτή την περίπτωση είναι υποχρεωμένος να παρέχει βοήθεια στο χρήστη και στο χρήστη παρόχου παραπέμποντας τον σε αντίστοιχες ιστοσελίδες ή και σε εταιρείες που προσφέρουν αντίστοιχες υπηρεσίες.

4. Υπενθυμίζεται ότι η σκόπιμη παραγωγή και μετάδοση ιών από συγκεκριμένο άτομο φέρει βαριές κυρώσεις μέσω της είδη υπάρχουσας νομοθεσίας.

ΚΕΦΑΛΑΙΟ VII
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΑΣ ΕΦΑΡΜΟΓΗΣ (APPLICATION SERVICE PROVIDER)

Άρθρο 17
Σκοπός και Εφαρμογή της Πολιτικής

1. Η πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής ορίζει το σύνολο των εγγυήσεων που οφείλει να λαμβάνει ο πάροχος διαδικτύου από τον πάροχο υπηρεσίας εφαρμογής, προκειμένου να εξασφαλιστεί το απόρρητο των επικοινωνιών των χρηστών. Η πολιτική αυτή ισχύει σε περίπτωση που ο πάροχος διαδικτύου και ο πάροχος υπηρεσίας εφαρμογής έχουν συμβατική σχέση, ανεξαρτήτως της τοποθεσίας όπου φιλοξενείται η υποδομή που υποστηρίζει τις εν λόγω υπηρεσίες και εφαρμογές.
2. Ο πάροχος διαδικτύου είναι υποχρεωμένος να διαθέτει και να εφαρμόζει πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής, η οποία να διασφαλίζει το απόρρητο των επικοινωνιών των χρηστών και να είναι σύμφωνη με τις παραγράφους που ακολουθούν.

3. Η ανάθεση μιας υπηρεσίας σε κάποιον πάροχο υπηρεσίας εφαρμογής πρέπει να γίνεται ύστερα από γραπτή έγκριση του Νομικού Εκπροσώπου του παρόχου διαδικτύου.
4. Ο πάροχος διαδικτύου οφείλει να ελέγχει διεξοδικά κατά πόσο ο πάροχος υπηρεσίας εφαρμογής δύναται να εφαρμόσει την πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής πριν την ανάθεση της υπηρεσίας και κατά τη διάρκεια λειτουργίας της υπηρεσίας. Ο πάροχος διαδικτύου είναι ο τελικός υπεύθυνος για την εφαρμογή της πολιτικής αυτής από τον πάροχο υπηρεσίας εφαρμογής.
5. Υπεύθυνος για τον ορισμό, έλεγχο εφαρμογής και οποιαδήποτε αλλαγή της πολιτικής ασφάλειας παρόχου υπηρεσίας εφαρμογής ορίζεται ο Υπεύθυνος Ασφάλειας του παρόχου διαδικτύου.
6. Ο πάροχος διαδικτύου επιτρέπεται να παραδίδει απόρρητα δεδομένα χρήστη στον πάροχο υπηρεσίας εφαρμογής μόνο εφόσον ο χρήστης έχει λάβει σαφείς πληροφορίες για τον σκοπό της επεξεργασίας, και πάντα με τη συγκατάθεση αυτού. Αυτό βέβαια δεν ισχύει στην περίπτωση που οι ενέργειες αυτές γίνονται για την εξυπηρέτηση της υπηρεσίας που έχει ρητά ζητήσει ο χρήστης.
7. Ο πάροχος διαδικτύου έχει το δικαίωμα να εξετάζει ανά τακτά χρονικά διαστήματα το κατά πόσο ο πάροχος υπηρεσίας εφαρμογής εφαρμόζει την πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής. Αν ο έλεγχος απαιτεί φυσική παρουσία στις εγκαταστάσεις του παρόχου υπηρεσίας εφαρμογής, ο πάροχος διαδικτύου οφείλει να ενημερώσει τον πάροχο υπηρεσίας εφαρμογής τουλάχιστον 24 ώρες πριν, ειδάλλως δεν απαιτείται καμία προειδοποίηση.
8. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να καταθέσει στον πάροχο διαδικτύου το πλήρες διάγραμμα δικτύου που χρησιμοποιεί για την υποστήριξη της εν λόγω υπηρεσίας, καθώς και τις τυχόν διασυνδέσεις του δικτύου αυτού με άλλα δίκτυα του παρόχου υπηρεσίας εφαρμογής και του παρόχου διαδικτύου. Θα πρέπει επίσης να κατατίθεται το πλήρες διάγραμμα ροής που αφορά στα απόρρητα δεδομένα επικοινωνιών, συμπεριλαμβανομένου των μέσων αποθήκευσης, εφαρμογών επεξεργασίας και μέτρων ασφάλειας των δεδομένων αυτών.
9. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να διακόπτει άμεσα τη λειτουργία της υπηρεσίας σε περίπτωση που εντοπιστεί οποιοδήποτε θέμα ασφάλειας των απόρρητων δεδομένων επικοινωνίας.
10. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να ενημερώνει τον Υπεύθυνο Ασφάλειας του παρόχου διαδικτύου σχετικά με όλα τα συμβάντα ασφάλειας που αφορούν στα απόρρητα δεδομένα επικοινωνιών.
11. Σε ό,τι αφορά θέματα πρόσβασης στις εφαρμογές λογισμικού, την υλική υποδομή και το δίκτυο του παρόχου υπηρεσίας εφαρμογής, η πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής πρέπει να περιλαμβάνει τουλάχιστον τα παρακάτω:

(α) Ο πάροχος υπηρεσίας εφαρμογής οφείλει να εφαρμόζει την Πολιτική Πρόσβασης του παρόχου διαδικτύου ως προς τα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

(β) Ο πάροχος διαδικτύου έχει τον τελικό λόγο σε θέματα πρόσβασης (φυσικής και μη) στα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

(γ) Ο πάροχος υπηρεσίας εφαρμογής οφείλει να γνωστοποιεί στον πάροχο διαδικτύου το προσωπικό το οποίο θα έχει φυσική και μη πρόσβαση στα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

12. Ο πάροχος υπηρεσίας εφαρμογής υποχρεούται να χρησιμοποιεί διαδικασίες και μεθόδους κρυπτογράφησης των απόρρητων δεδομένων επικοινωνίας, όπως αυτές ορίζονται στην Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων του παρόχου διαδικτύου.
13. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να εφαρμόζει την Πολιτική Κωδικών (Password Policy) του παρόχου διαδικτύου ως προς τα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.
14. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να ενημερώνει εγγράφως τον πάροχο διαδικτύου ως προς τις διαδικασίες ελέγχου ασφάλειας που ακολουθεί σχετικά με την επαλήθευση ταυτότητας (authentication), εξουσιοδότηση (authorization) και αποκάλυψη κενών ασφάλειας των εφαρμογών παγκόσμιου ιστού (WWW).
15. Ο πάροχος διαδικτύου οφείλει να έχει την έγγραφη διαβεβαίωση του παρόχου υπηρεσίας εφαρμογής σχετικά με την αποδοχή και πλήρη εφαρμογή των μέτρων διασφάλισης του απορρήτου των επικοινωνιών που περιγράφονται στις προηγούμενες παραγράφους.
16. Η πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής συνίσταται να ορίζει χρηματικές ποινές, ακόμα και την κατάργηση του συμβολαίου, για την περίπτωση κατά την οποία ο πάροχος υπηρεσίας εφαρμογής παραβεί τα μέτρα διασφάλισης του απορρήτου των επικοινωνιών.

ΚΕΦΑΛΑΙΟ VIII
ΔΙΑΔΙΚΑΣΙΑ ΣΥΜΒΑΣΗΣ ΥΠΕΡΓΟΛΑΒΙΑΣ

Άρθρο 18
Σύμβαση υπεργολαβίας με σκοπό την διασφάλιση απορρήτου

1. Σε κάθε περίπτωση όπου ο πάροχος διαδικτύου προβαίνει σε συμφωνία με τον εκάστοτε υπεργολάβο για την ανάληψη έργου το οποίο απαιτεί πρόσβαση σε εξοπλισμό ή λογισμικό το οποίο περιέχει ή παρέχει πρόσβαση σε διαβαθμισμένα, ευαίσθητα ή απόρρητα δεδομένα, ο πάροχος διαδικτύου είναι υποχρεωμένος να διαφυλάσσει το απόρρητο των πληροφοριών.
2. Για την διασφάλιση του απορρήτου υπό συνθήκες υπεργολαβίας απαιτείται η υπογραφή συμβάσεως προστασίας του απορρήτου των πληροφοριών. Ιδιαίτερη προσοχή πρέπει να δίνεται στη διασφάλιση του απορρήτου των επικοινωνιών, σε περιπτώσεις που απαιτείται πρόσβαση από τον υπεργολάβο σε εξοπλισμό ή λογισμικό το οποίο χρησιμοποιείται στις επικοινωνίες ή αποθηκεύει πληροφορίες επικοινωνιών.
3. Η σύμβαση μεταξύ παρόχου διαδικτύου και υπεργολάβου πρέπει να περιέχει τουλάχιστον τις παρακάτω παραγράφους.
4. Ο υπεργολάβος σε καμία περίπτωση δεν έχει το δικαίωμα να προβεί στην καταπάτηση του απορρήτου όπως αυτό περιγράφεται και διαφυλάσσεται από την είδη

υπάρχουσα πολιτική ασφάλειας του παρόχου διαδικτύου.

5. Ο υπεργολάβος έχει λάβει γνώση της υπάρχουσας πολιτικής προστασίας του απορρήτου των τηλεπικοινωνιών του παρόχου διαδικτύου, και ενυπόγραφα συμφωνεί με τους όρους, προϋποθέσεις και περιορισμούς που επιβάλλονται από την πολιτική αυτή.
6. Το εκάστοτε πρόσωπο το οποίο εν τέλει θα έχει πρόσβαση στον ευαίσθητο εξοπλισμό / λογισμικό έχει λάβει ειδική άδεια από τον πάροχο διαδικτύου (και όχι τον υπεργολάβο) αφού πρώτα έχει ενημερωθεί, συμφωνήσει και συνυπογράψει την σύμβαση διασφάλισης απορρήτου.
7. Ο υπεργολάβος πρέπει να έχει την άδεια του παρόχου διαδικτύου για να εκχωρήσει δικαιώματα χρήσης του ευαίσθητου εξοπλισμού σε τρίτους (εργολάβους). Κατά την εκάστοτε εκχώρηση δικαιωμάτων σε τρίτους επιβάλλεται να διατηρείται το ίδιο επίπεδο διασφάλισης του απορρήτου και να υπογράφονται αντίστοιχα συμφωνητικά μεταξύ των τρίτων και του παρόχου διαδικτύου. Ο υπεργολάβος σε καμιά περίπτωση δεν είναι εξουσιοδοτημένος να παραχωρήσει αυτός δικαιώματα χρήσης. Πάντοτε η εκχώρηση δικαιωμάτων γίνεται από τον κύριο του έργου, δηλαδή τον πάροχο διαδικτύου και μόνο.
8. Ο πάροχος διαδικτύου ορίζει συγκεκριμένο φυσικό πρόσωπο που είναι υπεύθυνο για την εποπτεία του υπεργολάβου καθώς και των τυχόν εργολάβων σε ζητήματα διασφάλισης απορρήτου, ο οποίος ονομάζεται Επόπτης Ασφάλειας.
9. Τυχόν παραβίαση των κανόνων από τον υπεργολάβο χρίζει άμεσης καταγγελίας στην ΑΔΑΕ από τον καθορισμένο Επόπτη Ασφάλειας.

ΚΕΦΑΛΑΙΟ IX
ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 19
Γενικά

1. Οι πολιτικές που ορίστηκαν στον κανονισμό αυτό αποτελούν μέρος της γενικότερης Πολιτικής Ασφάλειας του παρόχου διαδικτύου, όπως αυτή ορίστηκε στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».
2. Κατά συνέπεια, η ΑΔΑΕ στα πλαίσια ελέγχου και εποπτείας που καθορίστηκαν στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές», μπορεί ανά πάσα στιγμή να προβεί σε έλεγχο του καθορισμού, επιβολής και σωστής λειτουργίας των πολιτικών που ορίστηκαν στον κανονισμό αυτό.
3. Σχετικά με τις λεπτομερείς διαδικασίες διενέργειας του ελέγχου καθώς και τις προβλεπόμενες διοικητικές κυρώσεις ισχύουν, κατ' αναλογία, τα αναγραφόμενα στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».

Άρθρο 20
Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων

1. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να ζητήσει πλήρη ενημέρωση από τους παρόχους διαδικτύου και από τους παρόχους υπηρεσίας εφαρμογής σχετικά με την τεχνική ή αλγόριθμο κρυπτογράφησης που χρησιμοποιεί στα συστήματα μετάδοσης ή ανά πεδίο εφαρμογής καθώς και το μήκος του κλειδιού.
2. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν όντως εφαρμόζονται οι τεχνικές κρυπτογράφησης όπως δηλώνονται από τους πάροχους διαδικτύου και τους πάροχους υπηρεσίας εφαρμογής.

Άρθρο 21
Πολιτική Προστασίας Κωδικών Ασφάλειας

1. Η ΑΔΑΕ δύναται ανά πάσα στιγμή να διενεργήσει έλεγχο σε οποιονδήποτε φορέα εμπίπτει στη δικαιοδοσία της αναφορικά με την πολιτική κωδικών ασφάλειας.
2. Ο υπό έλεγχο φορέας οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ όλα τα έντυπα στα οποία έχουν καταγραφεί οι πολιτικές κωδικών ασφάλειας καθώς και τυχόν σχετικό συνοδευτικό υλικό, π.χ. έγγραφα με οδηγίες και φόρμες που δίδονται στους χρήστες.

Άρθρο 22
Πολιτική Προστασίας από Ιούς

1. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν όντως ο πάροχος εφαρμόζει Πολιτική Προστασίας από Ιούς, διαθέτει απαραίτητα συστήματα προστασίας από ιούς (ειδικό λογισμικό και ειδικός δικτυακός εξοπλισμός) και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.
2. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Προστασίας από Ιούς, έτσι ώστε να είναι σε πλήρη αντιστοιχία με τις εκάστοτε νέες τεχνολογίες προσβολής και προστασίας των υπολογιστικών συστημάτων από ιούς. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος οφείλει να προσαρμόζει την Πολιτική Προστασίας από Ιούς αναλόγως, εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 23
Πολιτική Ασφάλειας Παρόχου Υπηρεσίας Εφαρμογής

1. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου διαθέτει και εφαρμόζει πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής σύμφωνα με τις αντίστοιχες διατάξεις του παρόντος.
2. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν ο πάροχος υπηρεσίας εφαρμογής εφαρμόζει την πολιτική ασφαλείας παρόχου υπηρεσίας εφαρμογής σύμφωνα με τις αντίστοιχες διατάξεις του παρόντος. Υπενθυμίζεται ότι ο πάροχος διαδικτύου είναι ο τελικός υπεύθυνος για την εφαρμογή και εποπτεία της πολιτικής αυτής από τον πάροχο υπηρεσίας εφαρμογής.
3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής. Μετά από κάθε τέτοιου είδους

τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής και να ενημερώνει τον πάροχο υπηρεσίας εφαρμογής αναλόγως. Τόσο ο πάροχος διαδικτύου, όσο και ο πάροχος υπηρεσίας εφαρμογής οφείλουν να ολοκληρώνουν τις αλλαγές που απαιτούνται εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 24
Αρχές Πιστοποίησης

1. Σκοπός των αρχών πιστοποίησης είναι να επαληθεύουν την αντιστοιχία μιας οντότητας (π.χ. ενός φυσικού προσώπου) με το δημόσιο κλειδί της. Η επαλήθευση γίνεται με την έκδοση των λεγόμενων ψηφιακών πιστοποιητικών.
2. Οι οργανισμοί που μπορούν να δραστηριοποιηθούν στην Ελλάδα ως Αρχές Πιστοποίησης είναι υπό τον έλεγχο της ΑΔΑΕ. Η ΑΔΑΕ θα επιβλέψει ότι η αρχή πιστοποίησης είναι σύμφωνη με την υπάρχουσα νομοθεσία
3. Η ΑΔΑΕ όποτε κρίνει απαραίτητο θα εκδίδει τεχνικούς ή μη κανονισμούς και συστάσεις που αφορούν τη λειτουργία των αρχών πιστοποίησης με κριτήριο την αξιοπιστία και την ασφαλή λειτουργία αυτών.

ΚΕΦΑΛΑΙΟ Χ
ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 25
Μεταβατικές Διατάξεις

1. Όλοι οι πάροχοι διαδικτύου υποχρεούνται:

(α) Να ενημερώσουν ως προς την εφαρμοζόμενη πολιτική ασφάλειας την ΑΔΑΕ εντός έξι (6) μηνών από τη δημοσίευση του παρόντος.

(β) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική ασφάλειας εντός ενός (1) έτους από την έγκρισή της.

ΚΕΦΑΛΑΙΟ ΧΙ
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 26
Έναρξη Ισχύος

Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

Αριθμ. 969/Φ.12

Α Π Ο Φ Α Σ Η

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

Έχοντας υπόψη :

α. το Ν.3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών», ιδίως τα άρθρα 1 παρ. 1, και 6 παρ. 1 (ιβ)

β. το γεγονός ότι από τις διατάξεις αυτής της Απόφασης δεν προκαλείται δαπάνη εις

βάρος του Κρατικού Προϋπολογισμού
Αποφάσισε
Κατά τη συνεδρίασή της την 23η Φεβρουαρίου 2005 την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση του Απορρήτου των Συναλλαγών κατά τη χρήση Αυτόματων Ταμειολογιστικών Μηχανών

ΚΕΦΑΛΑΙΟ Ι
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1
Σκοπός – Πεδίο Εφαρμογής

1. Σκοπός της παρούσας Απόφασης είναι ο καθορισμός ενός ελάχιστου επιπέδου προστασίας του απορρήτου των επικοινωνιών κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών από το κοινό, με τη θέσπιση των υποχρεώσεων των οριζόμενων στην παράγραφο 2 του παρόντος άρθρου φορέων, και την καθιέρωση διαδικασίας ελέγχου των φορέων αυτών από την ΑΔΑΕ σχετικά με τις εν λόγω υποχρεώσεις τους, σύμφωνα με το άρθρο 6 του Ν.3115/2003.
2. Στις διατάξεις της παρούσας Απόφασης εμπίπτουν πιστωτικά ιδρύματα ή άλλοι εξουσιοδοτημένοι φορείς από αυτά, που παρέχουν στο κοινό υπηρεσίες διενέργειας συναλλαγών μέσω αυτόματων ταμειολογιστικών μηχανών με χρήση κωδικού πρόσβασης.
3. Δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας Απόφασης οι ενέργειες που πραγματοποιούνται για την επικοινωνία της αυτόματης ταμειολογιστικής μηχανής με τους διακομιστές και τις υποδομές δικτύωσης του Υπόχρεου Φορέα.

Άρθρο 2
Ορισμοί

Για την εφαρμογή της παρούσας Απόφασης, οι ακόλουθοι όροι έχουν την έννοια που τους αποδίδεται κατωτέρω:

Χρήστης:	ο νόμιμος κάτοχος κάρτας η οποία προορίζεται για χρήση σε αυτόματες ταμειολογιστικές μηχανές
Κωδικός πρόσβασης (PIN):	είναι ο τετραψήφιος (κατά πλειοψηφία) αριθμός πρόσβασης στο λογαριασμό του χρήστη, ο οποίος ζητείται από την αυτόματη ταμειολογιστική μηχανή, ύστερα από την εισαγωγή της κάρτας στη μηχανή, προκειμένου να πραγματοποιηθεί μία συναλλαγή.
Υπόχρεος Φορέας:	κάθε πιστωτικό ίδρυμα ή άλλο φυσικό ή νομικό πρόσωπο, το οποίο, σύμφωνα με την ισχύουσα νομοθεσία, παρέχει στο κοινό υπηρεσίες διενέργειας συναλλαγών μέσω αυτόματων ταμειολογιστικών μηχανών.

Άρθρο 3
Λοιποί Ορισμοί

Άλλοι όροι οι οποίοι χρησιμοποιούνται στο παρόν έχουν την έννοια η οποία τους αποδίδεται στην κείμενη νομοθεσία.

ΚΕΦΑΛΑΙΟ ΙΙ

ΥΠΟΧΡΕΩΣΕΙΣ ΦΟΡΕΩΝ ΠΟΥ ΠΑΡΕΧΟΥΝ ΣΤΟ ΚΟΙΝΟ ΥΠΗΡΕΣΙΕΣ ΔΙΕΝΕΡΓΕΙΑΣ ΣΥΝΑΛΛΑΓΩΝ ΜΕΣΩ ΑΥΤΟΜΑΤΩΝ ΤΑΜΕΙΟΛΟΓΙΣΤΙΚΩΝ ΜΗΧΑΝΩΝ

Άρθρο 4
Ενημέρωση και Προστασία Χρήστη

1. Οι Υπόχρεοι Φορείς μεριμνούν για τη συνεχή, σαφή και έγκυρη ενημέρωση των χρηστών αναφορικά με τους κινδύνους οι οποίοι δύνανται να απειλήσουν το απόρρητο της επικοινωνίας κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών και για τα πλέον πρόσφορα μέτρα για την αποφυγή ή ελαχιστοποίησή τους. Ενδεικτικά και όχι περιοριστικά αναφέρεται η ενημέρωση με ανακοινώσεις αναρτημένες απευθείας πάνω στις αυτόματες ταμειολογιστικές μηχανές (ή στην οθόνη της μηχανής), με ενημερωτικά φυλλάδια, μέσω Διαδικτύου, μέσω του περιοδικού ή ημερήσιου τύπου, και μέσω άλλων μέσων.
2. Οι Υπόχρεοι Φορείς μεριμνούν για την άμεση προστασία των χρηστών κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών, περιορίζοντας στο ελάχιστο τους κινδύνους παρατήρησης και καταγραφής από τρίτους του αριθμού και του κωδικού πρόσβασης της κάρτας.
3. Η πολιτική ενημέρωσης και προστασίας των χρηστών σύμφωνα με το παρόν άρθρο, καθορίζεται από τους Υπόχρεους Φορείς και υποβάλλεται στην ΑΔΑΕ σύμφωνα με τα οριζόμενα στο άρθρο 6 και το Κεφάλαιο ΙΙΙ της παρούσας Απόφασης.

Άρθρο 5
Προστασία, Αναβάθμιση και Κατηγοριοποίηση
Αυτόματων Ταμειολογιστικών Μηχανών

1. Οι Υπόχρεοι Φορείς μεριμνούν για τη φυσική προστασία των αυτόματων ταμειολογιστικών μηχανών από κάθε είδους ενέργεια η οποία ενδέχεται να απειλήσει το απόρρητο της επικοινωνίας κατά τη χρήση αυτών.
2. Οι Υπόχρεοι Φορείς μεριμνούν ώστε το υλικό (hardware) των χρησιμοποιούμενων για την παροχή των υπηρεσιών τους αυτόματων ταμειολογιστικών μηχανών να συμβάλλει στη διασφάλιση του απόρρητου της επικοινωνίας κατά τη χρήση αυτών. Ενδεικτικά και όχι περιοριστικά αναφέρονται οι εξής τρόποι συμβολής του υλικού στη διασφάλιση του απόρρητου της επικοινωνίας κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών:

(α) Το υλικό να εξασφαλίζει τη μη προσαρμοσιμότητα πάνω στη μηχανή ξένων συσκευών. Για την επίτευξη αυτού του στόχου μπορεί να επιλεγούν λύσεις που δεν απαιτούν την εισαγωγή της κάρτας στην αυτόματη ταμειολογιστική μηχανή

(β) Σε περίπτωση κατά την οποία το (α) δεν είναι δυνατόν, το υλικό να δυσκολεύει ή

να αποτρέπει την ανάγνωση της μαγνητικής ή άλλης μορφής πληροφορίας.

(γ) Να υπάρχει δυνατότητα διαπίστωσης παραβίασης στο υλικό, για παράδειγμα με τη χρήση ειδικού αισθητήρα ο οποίος τοποθετείται μέσα στον αναγνώστη καρτών.

(δ) Το υλικό να απενεργοποιείται αμέσως όταν διαπιστώνεται παραβίαση, και να ενεργοποιείται συναγερμός.

(ε) Το υλικό να απενεργοποιείται κατά τις μη συνήθεις ώρες συναλλαγών.

3. Οι Υπόχρεοι Φορείς μεριμνούν ώστε το λογισμικό (software) των χρησιμοποιούμενων για την παροχή των υπηρεσιών τους αυτόματων ταμειολογιστικών μηχανών να αναβαθμίζεται και να συμβάλλει στη διασφάλιση του απόρρητου της επικοινωνίας κατά τη χρήση αυτών καθώς και τη διαπίστωση περιστατικών παραβίασης του απορρήτου. Ενδεικτικά και όχι περιοριστικά αναφέρονται οι εξής τρόποι συμβολής του λογισμικού στη διασφάλιση του απόρρητου της επικοινωνίας κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών:

(α) το λογισμικό να αναλύει μη συνήθεις τρόπους χρησιμοποίησης της κάρτας,

(β) το λογισμικό να αναλύει μη συνήθεις τρόπους χρησιμοποίησης της αυτόματης ταμειολογιστικής μηχανής

4. Οι Υπόχρεοι Φορείς μεριμνούν ώστε να υπάρχει κατηγοριοποίηση των χρησιμοποιούμενων αυτόματων ταμειολογιστικών μηχανών με βάση την πιθανότητα παραβίασης του απορρήτου που γίνεται μέσω αυτών. Η κατηγοριοποίηση αυτή αποτελεί τη βάση για ένα σταδιακό και αποτελεσματικό Προγραμματισμό Επιβολής Μέτρων Προστασίας των αυτόματων ταμειολογιστικών μηχανών, σύμφωνα με τα οριζόμενα στο άρθρο 6 της παρούσας Απόφασης. Ενδεικτικά και όχι περιοριστικά αναφέρονται τα εξής κριτήρια για την εν λόγω κατηγοριοποίηση:

(α) η θέση στην οποία είναι εγκατεστημένη η αυτόματη ταμειολογιστική μηχανή,

(β) τα ιδιαίτερα χαρακτηριστικά της περιοχής στην οποία είναι εγκατεστημένη η αυτόματη ταμειολογιστική μηχανή,

(γ) ο τύπος του χρησιμοποιούμενου υλικού,

(δ) ο τύπος του χρησιμοποιούμενου λογισμικού,

(ε) ο συνήθης όγκος των συναλλαγών,

(στ) η φύλαξη των αυτόματων ταμειολογιστικών μηχανών.

Άρθρο 6
Προγραμματισμός Επιβολής Μέτρων Προστασίας

1. Οι Υπόχρεοι Φορείς λαμβάνουν τα αναφερόμενα στο παρόν Κεφάλαιο μέτρα στο πλαίσιο ενός Προγραμματισμού Επιβολής Μέτρων Προστασίας, τον οποίο καθορίζουν οι ίδιοι, και ο οποίος υπόκειται σε έλεγχο από την ΑΔΑΕ σύμφωνα με τα οριζόμενα στο Κεφάλαιο ΙΙΙ της παρούσας Απόφασης. Κάθε τροποποίηση του Προγραμματισμού Επιβολής Μέτρων Προστασίας γνωστοποιείται άμεσα από τον Υπόχρεο Φορέα στην ΑΔΑΕ. Η ΑΔΑΕ αξιολογεί τα περιεχόμενα στον Προγραμματισμό μέτρα προστασίας και το χρονοδιάγραμμα υλοποίησής των, λαμβάνοντας υπόψη την κείμενη νομοθεσία και τις επεξηγήσεις που θα δίδονται από τον Υπόχρεο Φορέα αναφορικά με τα υιοθετούμενα μέτρα.

.

Άρθρο 7
Γενικές Υποχρεώσεις

1. Οι Υπόχρεοι Φορείς υποχρεούνται:

(α) να παρακολουθούν αδιάκοπα και με συνέπεια την ακεραιότητα τόσο των αυτόματων ταμειολογιστικών μηχανών όσο και των συναλλαγών οι οποίες πραγματοποιούνται μέσω καρτών,

(β) να καταγράφουν τις περιπτώσεις παραβίασης του απορρήτου των συναλλαγών που σχετίζονται με τις μηχανές τους,

(γ) να ενημερώνουν την ΑΔΑΕ σχετικά με τα ως άνω αναφερόμενα γεγονότα,

(δ) σε περίπτωση διαπίστωσης, είτε από τον Υπόχρεο Φορέα, είτε κατόπιν σχετικής υποδείξεως της ΑΔΑΕ, αυξημένης πιθανότητας πραγματοποίησης παραβίασης του απορρήτου της επικοινωνίας σε συγκεκριμένες αυτόματες ταμειολογιστικές μηχανές, ο Υπόχρεος Φορέας οφείλει να ενημερώνει άμεσα τους χρήστες με κάθε πρόσφορο μέσο σχετικά με τους υφιστάμενους κινδύνους και τις συνέπειες αυτών, υποδεικνύοντας μέτρα για την αποτροπή ή αντιμετώπισή τους. Σε κάθε τέτοια περίπτωση οφείλει να ενημερώνει άμεσα την ΑΔΑΕ αναφορικά με τον κίνδυνο που διαπιστώθηκε και τα μέτρα που ελήφθησαν σχετικά.

2. Ο Υπόχρεος Φορέας οφείλει να ορίσει στέλεχος αυτού ως το πρόσωπο επικοινωνίας μεταξύ αυτού και της ΑΔΑΕ.

ΚΕΦΑΛΑΙΟ ΙΙΙ
ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 8
Διαδικασία Ελέγχου από την ΑΔΑΕ

1. Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε φορέα που εμπίπτει στις διατάξεις του παρόντος.

1. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες, σύμφωνα με την ισχύουσα νομοθεσία, υπηρεσίες της ΑΔΑΕ, με βάση τα βήματα που περιγράφονται στο Παράρτημα Α της παρούσας Απόφασης.

3. Κατά τη διάρκεια του ελέγχου, η ομάδα ελέγχου της ΑΔΑΕ καταγράφει αναλυτικά τις ενέργειες στις οποίες προβαίνει, σε ειδικό έντυπο με τίτλο "Έκθεση διενέργειας ελέγχου", αναφορικά με τον Προγραμματισμό Επιβολής Μέτρων Προστασίας των αυτόματων ταμειολογιστικών μηχανών και του απόρρητου των επικοινωνιών κατά τη χρήση αυτών. Τα ελάχιστα απαραίτητα στοιχεία του εν λόγω εντύπου παρατίθενται στο Παράρτημα Β της παρούσας Απόφασης.

4. Η ομάδα ελέγχου κοινοποιεί το πόρισμά της στην Ολομέλεια της ΑΔΑΕ. Η Ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου, λαμβάνοντας υπόψη τον εκάστοτε υποβληθέντα στην ΑΔΑΕ Προγραμματισμό Επιβολής Μέτρων Προστασίας του Υπόχρεου Φορέα , και είτε τα εγκρίνει, είτε προχωρεί, σύμφωνα με τη νόμιμη διαδικασία, στην επιβολή συστάσεων ή κυρώσεων κατά περίπτωση, εφόσον δεν έχουν ληφθεί τα προσήκοντα μέτρα.

5. Οι κυρώσεις της προηγούμενης παραγράφου θα καθοριστούν με μεταγενέστερη απόφαση της ΑΔΑΕ.

Άρθρο 9
Άσκηση Εποπτείας

1. Κάθε Υπόχρεος Φορέας, εντός του πρώτου τριμήνου εκάστου ημερολογιακού έτους, υποβάλλει στην ΑΔΑΕ Ετήσια Έκθεση, η οποία αφορά στο προηγούμενο έτος, με στοιχεία που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών κατά τη χρήση των αυτόματων ταμειολογιστικών μηχανών
2. Το ελάχιστο περιεχόμενο της Ετήσιας Έκθεσης ορίζεται ως εξής:

(α) Περιστατικά που απείλησαν την ασφάλεια του απορρήτου των επικοινωνιών κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών, καθώς και εκτίμηση της ζημίας που υπέστη ο Υπόχρεος Φορέας και οι χρήστες των μηχανών εξαιτίας αυτών των περιστατικών.
(β) Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.
(γ) Ο Προγραμματισμός Επιβολής Μέτρων Προστασίας, όπως ορίζεται στο άρθρο 6 της παρούσας Απόφασης.

3. Η ΑΔΑΕ με Απόφασή της δύναται να μεταβάλλει το ελάχιστο περιεχόμενο της ετήσιας έκθεσης.
4. Η ΑΔΑΕ δύναται να ζητήσει εκτάκτως από τους Υπόχρεους Φορείς οποιεσδήποτε πληροφορίες θεωρεί αναγκαίες στα πλαίσια των αρμοδιοτήτων της για την ασφάλεια του απορρήτου των επικοινωνιών κατά τη χρήση αυτόματων ταμειολογιστικών μηχανών.

ΚΕΦΑΛΑΙΟ IV
ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 10
Μεταβατικές Διατάξεις

1. Όλοι οι Υπόχρεοι Φορείς οφείλουν να συντάξουν και να αποστείλουν στην ΑΔΑΕ έκθεση με το περιεχόμενο της Ετήσιας Έκθεσης εντός έξι (6) μηνών από τη δημοσίευση της παρούσας Απόφασης.

ΚΕΦΑΛΑΙΟ V
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 11
Έναρξη Ισχύος

1. Η παρούσα Απόφαση τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Εφημερίδα της Κυβερνήσεως.

ΠΑΡΑΡΤΗΜΑ Α

Αναλυτική περιγραφή διαδικασίας ελέγχου Υπόχρεου Φορέα

Η διαδικασία ελέγχου Υπόχρεου Φορέα διενεργείται με βάση τα ακόλουθα βήματα:

(α) Η ΑΔΑΕ με απόφασή της ορίζει ομάδα ελέγχου που αποτελείται από τρία (3) τουλάχιστον άτομα με σκοπό τον έλεγχο συγκεκριμένου Υπόχρεου Φορέα. Η ελάχιστη στελέχωση της ομάδας ελέγχου περιλαμβάνει έναν (1)υπεύθυνο της ομάδας, ένα (1) νομικό σύμβουλο και έναν (1) τεχνικό σύμβουλο.

(β) Σε χρόνο που αποφασίζει η ομάδα ελέγχου, επικοινωνεί με τον Υπόχρεο Φορέα και ζητεί να έρθει σε άμεση επικοινωνία με το υπεύθυνο στέλεχος όπως αυτό ορίζεται στην παράγραφο 2 του άρθρου 7 της παρούσας Απόφασης. Τυχόν καθυστέρηση ή κώλυμα που παρουσιάζεται κατά την προσπάθεια επικοινωνίας με το υπεύθυνο στέλεχος καταγράφεται .

(γ) Το υπεύθυνο στέλεχος παραδίδει στην ομάδα ελέγχου πλήρη εικόνα εφαρμογής του Προγραμματισμού Επιβολής Μέτρων Προστασίας καθώς και πιθανής προσαρμογής ή αναθεώρησης αυτού.

(δ) Η ομάδα ελέγχου προβαίνει σε αναλυτική εξέταση όλων των σχετικών εγγράφων και καταγράφονται οι ελλείψεις, ασάφειες, καθυστερήσεις, και προβλήματα που παρατηρούνται. Κατά την διαδικασία αυτή δύναται να ζητηθεί η συνδρομή του Υπόχρεου Φορέα έτσι ώστε να διασαφηνιστούν όποιες ασάφειες παρουσιάζονται στα έγγραφα.

(ε) Κατά τη διάρκεια του ελέγχου ο Υπόχρεος Φορέας δεν έχει τη δυνατότητα να αντικαταστήσει ή να αναθεωρήσει τον Προγραμματισμό του.

(η) Η ομάδα ελέγχου προβαίνει σε αυτοψία των εγκαταστάσεων του Υπόχρεου Φορέα για να διαπιστώσει σε ποιο βαθμό εφαρμόζονται οι διαδικασίες που προβλέπονται από τα προσκομιθέντα έγγραφα. Η αυτοψία δύναται να περιλαμβάνει και επαφή με το προσωπικό του Υπόχρεου Φορέα. Η ομάδα ελέγχου καταγράφει αναλυτικά την εφαρμογή των διαδικασιών καθώς και τις ελλείψεις και τα σφάλματα που διαπιστωθούν.

(ζ) Ο Υπόχρεος Φορέας οφείλει να υποβάλει στην ομάδα ελέγχου οποιοδήποτε στοιχείο θεωρηθεί απαραίτητο από την ομάδα για την επιτυχή ολοκλήρωση του ελέγχου.

(θ) Τυχόν διαπίστωση έλλειψης συνεργασίας από τον Υπόχρεο Φορέα ή/και προσπάθειας παραπλάνησης της ομάδας ελέγχου καταγράφεται .

ΠΑΡΑΡΤΗΜΑ Β

Ελάχιστο περιεχόμενο του εντύπου με τίτλο
"Έκθεση Διενέργειας Ελέγχου "

Το ως άνω έντυπο περιέχει τουλάχιστον τα ακόλουθα στοιχεία:

(α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε ο έλεγχος.

(β) Τα ονοματεπώνυμα και τις ιδιότητες των στελεχών της ΑΔΑΕ τα οποία απαρτίζουν την ομάδα ελέγχου καθώς και την ημερομηνία σύστασής της.

(γ) Το όνομα του υπό έλεγχο Υπόχρεου Φορέα καθώς και το όνομα του υπευθύνου στελέχους αυτού.

(δ) Το χρόνο ο οποίος απαιτήθηκε έως ότου να αποδοθεί στην ομάδα ελέγχου ο πλήρης Προγραμματισμός Επιβολής Μέτρων Προστασίας του Υπόχρεου Φορέα καθώς και το χρονοδιάγραμμα τήρησής του.

(ε) Την ανάλυση του προγραμματισμού με καταγραφή των ελλείψεων και ασαφειών οι οποίες διαπιστώνονται.

(στ) Το αποτέλεσμα της αυτοψίας για την αποτίμηση της εφαρμογής του προγραμματισμού με καταγραφή των ελλείψεων και ασαφειών που διαπιστώνονται.

(ζ) Την εκτίμηση της ομάδας ελέγχου αναφορικά με τη διάθεση συνεργασίας του

Υπόχρεου Φορέα.
(η) Τις ημερομηνίες έναρξης και περάτωσης του ελέγχου.
(θ) Το τελικό πόρισμα του ελέγχου και την εισήγηση προς την Ολομέλεια της ΑΔΑΕ.

Αριθμ.: 1001/Φ.21
ΑΠΟΦΑΣΗ

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

Έχοντας υπόψη:
α. Το Ν. 3115/27-02-2003, άρθρο 1, παράγρ. 1,
β. Το Ν. 3115/27-02-2003, άρθρο 6, παράγρ.1 (ιβ)
γ. Ότι εκ της Αποφάσεως αυτής δεν προκύπτει δαπάνη για το δημόσιο
δ. Τη σχετική εισήγηση της Υπηρεσίας
Αποφάσισε,
κατά τη συνεδρίασή της την 16η Μαρτίου 2005, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση του Απορρήτου των Ταχυδρομικών Υπηρεσιών.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ – ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός – Πεδίο Εφαρμογής

ι. Σκοπός της παρούσας Απόφασης είναι :
(α) Η θέσπιση των υποχρεώσεων των Ταχυδρομικών Επιχειρήσεων, του προσωπικού που απασχολούν, καθώς και των τρίτων που συνεργάζονται με αυτές δυνάμει οποιασδήποτε έννομης σχέσης για την παροχή των ταχυδρομικών υπηρεσιών, σχετικά με το απόρρητο των ταχυδρομικών υπηρεσιών, όπως αυτό προβλέπεται στο άρθρο 22 του Ν. 2668/98, και τους όρους ασφαλείας που συντελούν στη διασφάλιση αυτού.
(β) Η θέσπιση διαδικασίας ελέγχου των φυσικών ή νομικών προσώπων της παραγράφου ι του παρόντος άρθρου ως προς την τήρηση των ως άνω υποχρεώσεών τους.
2. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλες οι Ταχυδρομικές Επιχειρήσεις.

Άρθρο 2
Ορισμοί
1. Για την εφαρμογή του παρόντος οι όροι που χρησιμοποιούνται στις διατάξεις του έχουν την ακόλουθη έννοια :

α. Ταχυδρομικές υπηρεσίες: Οι βασικές και οι λοιπές ταχυδρομικές υπηρεσίες.
β. Βασικές ταχυδρομικές υπηρεσίες: Οι υπηρεσίες περισυλλογής, διαλογής, μεταφοράς και διανομής των ταχυδρομικών αντικειμένων.
γ. Λοιπές ταχυδρομικές υπηρεσίες: Οι υπηρεσίες, που δεν ανήκουν στις βασικές ταχυδρομικές και έχουν σχέση, κυρίως, με ειδικής επείγουσας διαβίβασης αντικείμενα,

παρακολουθούμενα από ειδικό σύστημα παρακολούθησης και εντοπισμού, με διαφημιστικά αντικείμενα χωρίς διεύθυνση, με την προετοιμασία των ταχυδρομικών αντικειμένων και την ανταλλαγή εγγράφων.

δ. Δημόσιο ταχυδρομικό δίκτυο: Το σύνολο της οργάνωσης και των, κάθε είδους, μέσων και προσώπων που χρησιμοποιεί ο φορέας παροχής της καθολικής υπηρεσίας και επιτρέπουν μεταξύ άλλων:
   - την περισυλλογή των ταχυδρομικών αντικειμένων για τα οποία προβλέπεται υποχρέωση παροχής καθολικής υπηρεσίας από τα σημεία πρόσβασης σε όλη την επικράτεια,
   - τη μεταφορά και διεκπεραίωσή τους από το σημείο πρόσβασης στο ταχυδρομικό δίκτυο ως το κέντρο διανομής,
   - τη διανομή τους στη διεύθυνση που αναγράφεται στο αντικείμενο.

ε. Σημεία πρόσβασης: Οι συγκεκριμένες εγκαταστάσεις, συμπεριλαμβανομένων και των γραμματοκιβωτίων είτε σε δημόσιους χώρους είτε σε χώρους του φορέα παροχής της καθολικής υπηρεσίας, όπου οι χρήστες μπορούν να καταθέτουν ταχυδρομικά αντικείμενα στο δημόσιο ταχυδρομικό δίκτυο.

στ. Ταχυδρομικό αντικείμενο: Αντικείμενο με συγκεκριμένο παραλήπτη, αποστελλόμενο υπό την τελική του μορφή, στην οποία το αναλαμβάνει ο φορέας παροχής της καθολικής υπηρεσίας. Στην κατηγορία αυτή ανήκουν – πέραν των αντικειμένων αλληλογραφίας – βιβλία, κατάλογοι, εφημερίδες, περιοδικά, ταχυδρομικά δέματα μέχρι 20 χιλιόγραμμων που περιέχουν εμπορεύματα – με ή χωρίς εμπορική αξία – καθώς και τα κείμενα που έχουν διαβιβασθεί μέσω της διαδικασίας του ηλεκτρονικού ταχυδρομείου από τη στιγμή που, υπό την τελική τους μορφή, εγκλείονται σε φάκελο προς επίδοση.

ζ. Αντικείμενο αλληλογραφίας: Οποιοδήποτε μέσο επικοινωνίας υπό γραπτή μορφή, που μεταφέρεται και παραδίδεται στη διεύθυνση την οποία έχει αναγράψει ο αποστολέας στο ίδιο το αντικείμενο ή στη συσκευασία του. Τα βιβλία, οι κατάλογοι, οι εφημερίδες και τα περιοδικά δεν θεωρούνται αντικείμενα αλληλογραφίας.

η. Αποστολέας: Κάθε πρόσωπο από το οποίο προέρχονται τα ταχυδρομικά αντικείμενα.

θ. Χρήστης: Κάθε πρόσωπο, στο οποίο ως αποστολέα ή παραλήπτη παρέχεται ταχυδρομική υπηρεσία.

ι. Βασικές απαιτήσεις: Οι λόγοι γενικού συμφέροντος που μπορούν να οδηγήσουν στην επιβολή όρων σχετικών με την παροχή ταχυδρομικών υπηρεσιών χωρίς οικονομικό χαρακτήρα. Οι λόγοι αυτοί είναι : το απόρρητο της αλληλογραφίας, η ασφάλεια της λειτουργίας του δικτύου σε ό,τι αφορά τη μεταφορά επικίνδυνων ουσιών και, σε αιτιολογημένες περιπτώσεις, η προστασία του περιβάλλοντος, η χωροταξία και η προστασία των δεδομένων. Η τελευταία περιλαμβάνει την προστασία των δεδομένων προσωπικού χαρακτήρα, την εμπιστευτικότητα των διαβιβαζόμενων ή αποθηκευόμενων πληροφοριών, καθώς και την προστασία της ιδιωτικής ζωής.

ια. Επιχείρηση: Κάθε φυσικό πρόσωπο και κάθε οργάνωση ή ένωση προσώπων, με ή χωρίς νομική προσωπικότητα, που έχουν κερδοσκοπικό σκοπό. Στην έννοια της επιχείρησης εντάσσεται και κάθε δημόσιος οργανισμός που έχει δική του νομική προσωπικότητα ή εξαρτάται από αρχή που έχει νομική προσωπικότητα.

ιβ. Ταχυδρομική Επιχείρηση: Κάθε επιχείρηση που παρέχει ταχυδρομικές υπηρεσίες.

2. Άλλοι όροι οι οποίοι χρησιμοποιούνται στην παρούσα Απόφαση έχουν την έννοια που τους αποδίδεται στην κείμενη νομοθεσία.

ΚΕΦΑΛΑΙΟ ΙΙ
ΠΟΛΙΤΙΚΗ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΤΑΧΥΔΡΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

Άρθρο 3
Ορισμός – Γενικές Απαιτήσεις

1. Η Πολιτική Διασφάλισης του Απορρήτου των Ταχυδρομικών Υπηρεσιών (ΠΔΑΤΥ) είναι το σύνολο κανόνων που διέπουν τη λειτουργία των Ταχυδρομικών Επιχειρήσεων με σκοπό τη διασφάλιση του απορρήτου των Ταχυδρομικών Υπηρεσιών.
2. Η ΠΔΑΤΥ περιλαμβάνει την Πολιτική Προστασίας του Απορρήτου, την Πολιτική Ασφάλειας και την Πολιτική Διασφάλισης της Εχεμύθειας, οι οποίες αναλύονται στα άρθρα 4, 5 και 7 της παρούσας Απόφασης.
3. Οι Ταχυδρομικές Επιχειρήσεις μεριμνούν για την εκπόνηση και για την εφαρμογή της ΠΔΑΤΥ, σύμφωνα με την κείμενη νομοθεσία και τους όρους και τις κατευθύνσεις της παρούσας Απόφασης.
4. Οι όροι και οι προϋποθέσεις άρσης του απορρήτου, όπως προβλέπονται από την κείμενη νομοθεσία, αποτελούν αναπόσπαστο τμήμα της ΠΔΑΤΥ. Κάθε Ταχυδρομική Επιχείρηση οφείλει να προδιαγράψει με σαφήνεια το μηχανισμό, την εσωτερική διαδικασία και τους υπευθύνους εφαρμογής της άρσης του απορρήτου, και να προβλέψει μέτρα αντιμετώπισης προβλημάτων, τα οποία ενδέχεται να εμφανισθούν κατά την περίοδο της άρσης, καθώς και κατά την αποκατάσταση της προστασίας του απορρήτου μετά την ολοκλήρωση της διαδικασίας άρσης αυτού.
5. Η εφαρμογή της ΠΔΑΤΥ από τις Ταχυδρομικές Επιχειρήσεις προϋποθέτει προσεκτικά επιλεγμένο και άρτια εκπαιδευμένο προσωπικό, σύγχρονο και αποτελεσματικό σύστημα οργάνωσης του ταχυδρομικού δικτύου, μηχανοργάνωση, λήψη μέτρων αποτρεπτικών ενδεχόμενης παραβίασης της εν λόγω πολιτικής και ενημέρωση χρηστών για την επιμέλεια που ενδείκνυται να επιδείξουν κατά την αποστολή ταχυδρομικών αντικειμένων.
6. Η ΠΔΑΤΥ υποβάλλεται στην ΑΔΑΕ σύμφωνα με τα οριζόμενα στο Κεφάλαιο ΙΙΙ της παρούσας Απόφασης, και υπόκειται σε έλεγχο από την ΑΔΑΕ, τόσο ως προς την πληρότητα και αποτελεσματικότητά της, όσο και ως προς τον βαθμό εφαρμογής της.

Άρθρο 4
Πολιτική Προστασίας του Απορρήτου των Ταχυδρομικών Υπηρεσιών

1. Κάθε Ταχυδρομική Επιχείρηση υποχρεούται να διασφαλίζει το απόρρητο των ταχυδρομικών υπηρεσιών, το οποίο είναι απολύτως απαραβίαστο. Για το σκοπό αυτό, μεριμνά για την εκπόνηση και την εφαρμογή Πολιτικής Προστασίας του Απορρήτου των Ταχυδρομικών Υπηρεσιών.
2. Ενδεικτικά, και όχι περιοριστικά, παραβίαση απορρήτου υπάρχει στις ακόλουθες περιπτώσεις:

α. Παράνομη ιδιοποίηση ταχυδρομικού αντικειμένου που διακινείται από ταχυδρομική επιχείρηση.
β. Αποσφράγιση ταχυδρομικών αντικειμένων, εφόσον αυτή πραγματοποιείται κατά παράβαση της κείμενης νομοθεσίας.
γ. Ανάγνωση επιστολής που εμπεριέχεται σε ταχυδρομικό αντικείμενο.
δ. Παροχή πληροφοριών αναφορικά με τα στοιχεία του αποστολέα ή του παραλήπτη, το χρόνο ή το γεγονός της αποστολής ή παραλαβής ενός ταχυδρομικού αντικειμένου, κατά παράβαση της κείμενης νομοθεσίας.

3. Το απόρρητο ισχύει για τα αντικείμενα αλληλογραφίας, αλλά και για κάθε ταχυδρομική επικοινωνία, ανεξαρτήτως του προσωπικού ή του εμπορικού χαρακτήρα της.
4. Τα ταχυδρομικά αντικείμενα (πλην των αντικειμένων αλληλογραφίας) για τα οποία προκύπτει, από τον τρόπο συσκευασίας τους, ότι ο αποστολέας επέλεξε τον απόρρητο χαρακτήρα του περιεχομένου τους, καλύπτονται από τις υποχρεώσεις του απορρήτου και της εχεμύθειας.
5. Στο πλαίσιο της Πολιτικής Προστασίας του Απορρήτου των Ταχυδρομικών Υπηρεσιών, οι Επιχειρήσεις οφείλουν να εντοπίζουν και να εξειδικεύουν τα Ευάλωτα Σημεία του ταχυδρομικού δικτύου, όπως προσδιορίζονται στο άρθρο 6 της παρούσας Απόφασης, καθώς και τους πιθανούς κινδύνους, και να λαμβάνουν μέτρα για την αποφυγή τους ή την αντιμετώπισή τους.

Άρθρο 5
Πολιτική Ασφάλειας των Ταχυδρομικών Υπηρεσιών

1. Προϋπόθεση για τη διασφάλιση του απορρήτου των ταχυδρομικών υπηρεσιών είναι η λήψη επαρκών μέτρων ασφαλείας κατά την παροχή των υπηρεσιών αυτών. Για το σκοπό αυτό, κάθε Ταχυδρομική Επιχείρηση μεριμνά για την εκπόνηση και την εφαρμογή Πολιτικής Ασφάλειας των Ταχυδρομικών Υπηρεσιών.
2. Η ασφάλεια κατά την παροχή ταχυδρομικών υπηρεσιών συνίσταται στην εξασφάλιση συνθηκών αποτρεπτικών της οποιασδήποτε παραβίασης, απώλειας, παράνομης ιδιοποίησης, αλλοίωσης του περιεχομένου του ταχυδρομικού αντικειμένου, καθώς και στην αποφυγή μεταφοράς επικίνδυνων αντικειμένων ή απαγορευμένων ουσιών.
3. Οι Ταχυδρομικές Επιχειρήσεις οφείλουν να τηρούν τους κανονισμούς της Παγκόσμιας Ταχυδρομικής Ένωσης (Π.Τ.Ε) σε ό,τι αφορά τη μεταφορά επικίνδυνων ταχυδρομικών αντικειμένων και απαγορευμένων ουσιών.
4. Η Πολιτική Ασφάλειας των Ταχυδρομικών Υπηρεσιών δεν θα πρέπει να παρεμποδίζει την εύκολη πρόσβαση των χρηστών σε σταθερά σημεία του ταχυδρομικού δικτύου, τη συχνή συλλογή και διανομή των ταχυδρομικών αντικειμένων και την ομαλή λειτουργία των ταχυδρομικών υπηρεσιών.
5. Σε περίπτωση διαπίστωσης έκτακτου και ιδιαίτερα σοβαρού κινδύνου που απειλεί τη δημόσια υγεία ή ασφάλεια, οι Ταχυδρομικές Επιχειρήσεις δύνανται να λαμβάνουν έκτακτα μέτρα ασφαλείας, τα οποία γνωστοποιούνται στην ΑΔΑΕ. Τα μέτρα αυτά περιλαμβάνουν:

α) Προσκόμιση ανοικτών των αντικειμένων πάχους άνω των 6,35mm.

β) Έλεγχο ταυτότητας του αποστολέα ή του κομιστή, και αναγραφή των στοιχείων τους στο στέλεχος της απόδειξης παραλαβής του αντικειμένου στις περιπτώσεις συστημένων και γενικά αντικειμένων που παραδίδονται στα χέρια του παραλήπτη.

γ) Άρνηση παραλαβής και διαχείρισης αντικειμένων τα οποία δεν φέρουν ονοματεπώνυμο αποστολέα.

Άρθρο 6
Ευάλωτα Σημεία

1. Οι Ταχυδρομικές επιχειρήσεις διαπιστώνουν τα σημεία της διαδικασίας διαχείρισης των ταχυδρομικών αντικειμένων, τα οποία χρήζουν ιδιαίτερης προστασίας και ενίσχυσης αναφορικά με τη διαφύλαξη του απορρήτου και της ασφάλειας των ταχυδρομικών υπηρεσιών, και λαμβάνουν τα αντίστοιχα μέτρα. Τα ευάλωτα σημεία εντοπίζονται κυρίως:

α. Στα σημεία κατάθεσης των αντικειμένων, και ειδικότερα, στα κατά τόπους γραφεία των Ταχυδρομικών Επιχειρήσεων και στα υπαίθρια γραμματοκιβώτια ή γραμματοθυρίδες.
Ως προς τα εξουσιοδοτημένα κατά τόπους γραφεία παραλαβής ταχυδρομικών αντικειμένων, οι Ταχυδρομικές Επιχειρήσεις οφείλουν να τα στελεχώνουν με προσωπικό ιδιαίτερα ενημερωμένο και ευαισθητοποιημένο σε θέματα απορρήτου, ικανό να ανταποκριθεί στις απαιτήσεις και στους όρους τήρησης της ΠΔΑΤΥ.
Ως προς τα υπαίθρια γραμματοκιβώτια, οι Ταχυδρομικές Επιχειρήσεις οφείλουν να μεριμνούν ώστε η κατασκευή τους να εξασφαλίζει αφενός τη στεγανότητα και την ανθεκτικότητά τους στις καιρικές συνθήκες, και αφετέρου το απαραβίαστο από οποιονδήποτε τρίτο που αποπειράται να αφαιρέσει ή καταστρέψει τα ταχυδρομικά αντικείμενα.

β. Στα σημεία εναπόθεσης των ταχυδρομικών αντικειμένων στους χώρους των Ταχυδρομικών Επιχειρήσεων για περαιτέρω διαχείριση (διαλογή, μεταφορά, διανομή). Στα σημεία αυτά οι Ταχυδρομικές Επιχειρήσεις οφείλουν να δίνουν προτεραιότητα στην οργάνωση και στην εκπαίδευση του προσωπικού τους, στην εφαρμογή ευέλικτου σχεδιασμού διαχείρισης των ταχυδρομικών αντικειμένων, και στην τήρηση βασικών μέτρων ασφαλείας ως προς τη διαχείριση των ταχυδρομικών αντικειμένων, απαγορεύοντας την πρόσβαση στους χώρους αυτούς σε οποιοδήποτε ξένο πρόσωπο ή αναρμόδιο υπάλληλο.

γ. Στη μεταφορά προς και από τα Κέντρα Διαχείρισης (Διαλογής). Τα οχήματα των Ταχυδρομικών Επιχειρήσεων, τα οποία μεταφέρουν ταχυδρομικά αντικείμενα πρέπει να είναι κλειστά και ασφαλισμένα, ώστε να αποτρέπονται πράξεις παραβίασης του απορρήτου.

δ. Στα σημεία επίδοσης των ταχυδρομικών αντικειμένων, στην περίπτωση που αυτά δεν επιδίδονται στα χέρια του παραλήπτη, δηλαδή δεν είναι συστημένα ή αντικείμενα ταχυμεταφορών. Οι επιστολές θα πρέπει να ρίπτονται σε γραμματοκιβώ-

τια, εάν αυτά υπάρχουν. Σε περίπτωση μη ύπαρξης γραμματοκιβωτίων, το προσωπικό των Ταχυδρομικών Επιχειρήσεων οφείλει να εναποθέτει το αντικείμενο σε μέρος ασφαλές, ορατό για την εύρεσή του από τον παραλήπτη, επιδεικνύοντας κάθε φορά την προσήκουσα, για την διασφάλιση του απορρήτου και τη μη απώλεια του αντικειμένου, επιμέλεια.

ε. Στο περιεχόμενο των ταχυδρομικών αντικειμένων και στη διασφάλιση του απορρήτου του περιεχομένου, σε συνδυασμό με την αναγκαιότητα ελέγχου των αντικειμένων για λόγους προστασίας της δημόσιας ασφάλειας. Οι Ταχυδρομικές Επιχειρήσεις οφείλουν να τηρούν την αρχή της αναλογικότητας κατά τη λήψη μέτρων για την αποτροπή μεταφοράς αντικειμένων επικίνδυνων για τη δημόσια υγεία και ασφάλεια, ή απαγορευμένων ουσιών, ώστε οι διενεργούμενοι έλεγχοι να μην είναι δυσανάλογα επαχθείς για το απόρρητο σε σχέση με το επιδιωκόμενο αποτέλεσμα.

Άρθρο 7
Πολιτική Διασφάλισης της Εχεμύθειας

1. Οι Ταχυδρομικές Επιχειρήσεις διασφαλίζουν την επαγγελματική εχεμύθεια σε σχέση με την διαχείριση των ταχυδρομικών αντικειμένων ή τη συναλλαγή με τους χρήστες. Για το σκοπό αυτό, κάθε Ταχυδρομική Επιχείρηση μεριμνά για την εκπόνηση και την εφαρμογή Πολιτικής Διασφάλισης της Εχεμύθειας κατά την παροχή των Ταχυδρομικών Υπηρεσιών.
2. Οι υπάλληλοι των Ταχυδρομικών Επιχειρήσεων και τα λοιπά πρόσωπα που συνεργάζονται με αυτές δυνάμει οποιασδήποτε έννομης σχέσης για την παροχή ταχυδρομικών υπηρεσιών, οφείλουν να μην ανακοινώνουν σε τρίτους πληροφορίες σχετικά με :
   α. Το περιεχόμενο και τον τρόπο αποστολής των ταχυδρομικών αντικειμένων
   β. Τα στοιχεία αποστολέα και παραλήπτη των ταχυδρομικών αντικειμένων
   γ. Τα στοιχεία (όνομα, δ/νση) προσώπων που πραγματοποίησαν συναλλαγή με Ταχυδρομικές Επιχειρήσεις
   δ. Το γεγονός της αποστολής ή της παραλαβής ενός ταχυδρομικού αντικειμένου
   ε. Τον τρόπο αποστολής (απλή ή συστημένη επιστολή)
   στ. Τις ταχυδρομικές σχέσεις προσώπων ή επιχειρήσεων
   ζ. Το όνομα του αποστολέα, για τα συστημένα αντικείμενα τα οποία, όταν παραδίδονται στις Ταχυδρομικές Επιχειρήσεις, δεν φέρουν το όνομα του αποστολέα. Σε σχέση με την υποχρέωση αυτή ως τρίτος θεωρείται και ο παραλήπτης του αντικειμένου.
3. Η εχεμύθεια παραβιάζεται και όταν η ανακοίνωση των ανωτέρω πληροφοριών γίνεται όχι μόνο σε τρίτα πρόσωπα, αλλά και σε προσωπικό της ταχυδρομικής επιχείρησης που δεν έχει την ευθύνη της διαχείρισης των συγκεκριμένων αντικειμένων.
4. Οι Ταχυδρομικές Επιχειρήσεις υποχρεούνται να περιλαμβάνουν ρητό όρο αναφορικά με τη διασφάλιση του απορρήτου και της επαγγελματικής εχεμύθειας στις συμβάσεις με τους υπαλλήλους τους ή με άλλα πρόσωπα με τα οποία συνεργάζονται για την παροχή ταχυδρομικών υπηρεσιών.

Άρθρο 8
Δείκτης Διασφάλισης Απορρήτου και Δείκτης Ασφάλειας Ταχυδρομικών Αντικειμένων

1. Οι Ταχυδρομικές Επιχειρήσεις υποχρεούνται, στο πλαίσιο της ΠΔΑΤΥ, να προσδιορίζουν τις διαδικασίες διαχείρισης των παραπόνων των χρηστών αναφορικά με την απώλεια ή παραβίαση των ταχυδρομικών αντικειμένων που διαχειρίζονται, και να ανακοινώνουν, εντός του πρώτου τριμήνου εκάστου ημερολογιακού έτους, τους αναφερόμενους στην παράγραφο 2 του παρόντος άρθρου δείκτες, για κάθε είδους ταχυδρομικά αντικείμενα που διαχειρίζονται.
2. Οι Ταχυδρομικές Επιχειρήσεις υποχρεούνται να ανακοινώνουν τους παρακάτω δείκτες, όπου Διν είναι ο Δείκτης Διασφάλισης του Απορρήτου και της Εχεμύθειας και Δ2ν είναι ο Δείκτης Ασφάλειας Ταχυδρομικών Αντικειμένων :

$$\text{Διν} = \frac{\text{Αριθμός περιπτώσεων παραβίασης απορρήτου και εχεμύθειας}}{\text{Σύνολο διαχειριζομένων αντικειμένων}}$$

$$\text{Δ2ν} = \frac{\text{Αριθμός απολεσθέντων αντικειμένων}}{\text{Σύνολο διαχειριζομένων αντικειμένων}}$$

ΚΕΦΑΛΑΙΟ ΙΙΙ
ΥΠΟΧΡΕΩΣΕΙΣ ΤΑΧΥΔΡΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ, ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 9
Υποχρεώσεις Ταχυδρομικών Επιχειρήσεων αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Ταχυδρομικών Υπηρεσιών

ι. Οι Ταχυδρομικές Επιχειρήσεις υποχρεούνται :
α. Να εκπονήσουν και να εφαρμόσουν την ΠΔΑΤΥ.
β. Να ενημερώνουν την ΑΔΑΕ σχετικά με την εφαρμοζόμενη ΠΔΑΤΥ. Η ΑΔΑΕ εγκρίνει την εφαρμοζόμενη ΠΔΑΤΥ, διατυπώνοντας παρατηρήσεις και επιφέροντας μεταβολές σε αυτή, όπου το κρίνει απαραίτητο
γ. Να ενημερώνουν την ΑΔΑΕ για οποιαδήποτε τροποποίηση του περιεχομένου της εφαρμοζόμενης ΠΔΑΤΥ.
2. Κάθε Ταχυδρομική Επιχείρηση ορίζει κατάλληλα καταρτισμένο στέλεχός της, που θα φέρει τον τίτλο του Υπευθύνου Ασφαλείας, ως το πρόσωπο επικοινωνίας μεταξύ αυτής και της ΑΔΑΕ.
3. Κάθε Ταχυδρομική Επιχείρηση οφείλει να προβαίνει σε τακτικές επισκοπήσεις και αναθεωρήσεις της ΠΔΑΤΥ, είτε αυτόβουλα, είτε ύστερα από σχετική εντολή της ΑΔΑΕ.
4. Σε περίπτωση που διαπιστωθεί, είτε από τις Ταχυδρομικές Επιχειρήσεις, είτε κατόπιν σχετικής υποδείξεως της ΑΔΑΕ, έκτακτος και ιδιαίτερα σοβαρός κίνδυνος παραβίασης της ΠΔΑΤΥ, οι Ταχυδρομικές Επιχειρήσεις οφείλουν να ενημερώσουν άμεσα

και με κάθε πρόσφορο μέσο τους χρήστες αναφορικά με τον εν λόγω κίνδυνο, προτείνοντας μέτρα προστασίας.

Άρθρο 10
Διαδικασία Ελέγχου από την ΑΔΑΕ – Κυρώσεις

1. Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε Ταχυδρομική Επιχείρηση που εμπίπτει στις διατάξεις της παρούσας Απόφασης.
2. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες, σύμφωνα με την ισχύουσα νομοθεσία, υπηρεσίες της ΑΔΑΕ, με βάση τα βήματα που περιγράφονται στο Παράρτημα Α' της παρούσας Απόφασης.
3. Κατά τη διάρκεια του ελέγχου, η Ομάδα Ελέγχου καταγράφει αναλυτικά τις ενέργειες σε ειδικό έντυπο με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Ταχυδρομική Επιχείρηση». Τα ελάχιστα απαραίτητα στοιχεία του εν λόγω εντύπου παρατίθενται στο Παράρτημα Β' της παρούσας Απόφασης.
4. Η Ομάδα Ελέγχου κοινοποιεί το πόρισμά της στην Ολομέλεια της ΑΔΑΕ. Η Ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου, λαμβάνοντας υπόψη την υποβληθείσα από την Ταχυδρομική Επιχείρηση ΠΔΑΤΥ, και είτε εγκρίνει τα μέτρα που εφαρμόζει η ελεγχόμενη Ταχυδρομική Επιχείρηση, είτε προχωρεί, σύμφωνα με τη νόμιμη διαδικασία, στην επιβολή συστάσεων ή κυρώσεων, εφόσον δεν έχουν ληφθεί τα προσήκοντα μέτρα.

Άρθρο 11
Άσκηση Εποπτείας

1. Οι Ταχυδρομικές Επιχειρήσεις εντός του πρώτου τριμήνου εκάστου ημερολογιακού έτους υποβάλλουν στην ΑΔΑΕ Ετήσια Έκθεση με στοιχεία που αφορούν στην διασφάλιση του απορρήτου των Ταχυδρομικών Υπηρεσιών.
2. Το ελάχιστο περιεχόμενο της Ετήσιας Έκθεσης ορίζεται ως εξής:

α) Πλήρης φάκελος ΠΔΑΤΥ, όπως ορίζεται στο Κεφάλαιο ΙΙ της παρούσας Απόφασης.

β) Περιστατικά που απείλησαν τη διασφάλιση του απορρήτου των Ταχυδρομικών Υπηρεσιών, καθώς και εκτίμηση της ζημίας που υπέστη η Ταχυδρομική Επιχείρηση και οι χρήστες εξαιτίας αυτών των περιστατικών.

γ) Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.

3. Η ΑΔΑΕ με Απόφασή της δύναται να μεταβάλλει το ελάχιστο περιεχόμενο της Ετήσιας Έκθεσης.
4. Η ΑΔΑΕ δύναται να ζητήσει εκτάκτως από τις Ταχυδρομικές Επιχειρήσεις οποιεσδήποτε πληροφορίες θεωρεί αναγκαίες στο πλαίσιο των αρμοδιοτήτων της για τη διασφάλιση του απορρήτου των Ταχυδρομικών Υπηρεσιών.

ΚΕΦΑΛΑΙΟ IV
ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 12
Μεταβατικές Διατάξεις

1. Όλες οι Ταχυδρομικές Επιχειρήσεις οφείλουν να συντάξουν και να αποστείλουν στην ΑΔΑΕ έκθεση με το περιεχόμενο της Ετήσιας Έκθεσης, όπως αυτή ορίζεται στο άρθρο ιι της παρούσας Απόφασης, εντός τριών (3) μηνών από τη δημοσίευση της παρούσας Απόφασης.
2. Ταχυδρομικές Επιχειρήσεις, που έχουν συσταθεί σε χρόνο μεταγενέστερο του χρόνου έναρξης ισχύος της παρούσας, υποχρεούνται να καταθέσουν στην ΑΔΑΕ την ΠΔΑΤΥ, εντός τριμήνου από της εκδόσεως της αδείας λειτουργίας τους.

ΚΕΦΑΛΑΙΟ V
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 13
Έναρξη Ισχύος

Η παρούσα Απόφαση τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Εφημερίδα της Κυβερνήσεως.

ΠΑΡΑΡΤΗΜΑ Α
Περιγραφή Διαδικασίας Ελέγχου Ταχυδρομικών Επιχειρήσεων

Η διαδικασία ελέγχου των Ταχυδρομικών Επιχειρήσεων διενεργείται με βάση τα ακόλουθα βήματα:

(α) Η ΑΔΑΕ με Απόφασή της ορίζει Ομάδα Ελέγχου που αποτελείται από τρία (3) τουλάχιστον άτομα με σκοπό τον έλεγχο συγκεκριμένης Ταχυδρομικής Επιχείρησης. Η ελάχιστη στελέχωση της ομάδας ελέγχου περιλαμβάνει έναν υπεύθυνο της ομάδας, ένα νομικό σύμβουλο και έναν τεχνικό σύμβουλο.

(β) Σε χρόνο που αποφασίζει η Ομάδα Ελέγχου, επικοινωνεί με την Ταχυδρομική Επιχείρηση και ζητεί να έρθει σε άμεση επικοινωνία με τον Υπεύθυνο Ασφάλειας όπως αυτός ορίζεται στο Άρθρο 9 της παρούσας Απόφασης. Τυχόν καθυστέρηση ή κώλυμα που παρουσιάζεται κατά την προσπάθεια επικοινωνίας με τον Υπεύθυνο Ασφάλειας καταγράφεται.

(γ) Ο Υπεύθυνος Ασφάλειας παραδίδει στην Ομάδα Ελέγχου πλήρη φάκελο της ΠΔΑΤΥ.

(δ) Η Ομάδα Ελέγχου προβαίνει σε αναλυτική εξέταση όλων των σχετικών εγγράφων του φακέλου και καταγράφονται οι ελλείψεις, ασάφειες, καθυστερήσεις και προβλήματα που διαπιστώνονται. Κατά την διαδικασία αυτή δύναται να ζητηθεί η παροχή διευκρινίσεων από την Ταχυδρομική Επιχείρηση αναφορικά με την ΠΔΑΤΥ.

(ε) Κατά την διάρκεια του ελέγχου οι Ταχυδρομικές Επιχειρήσεις δεν δύνανται να μεταβάλλουν την εφαρμοζόμενη ΠΔΑΤΥ.

(στ) Η Ομάδα Ελέγχου προβαίνει σε αυτοψία των εγκαταστάσεων των Ταχυδρομικών Επιχειρήσεων προκειμένου να διαπιστώσει σε ποιο βαθμό εφαρμόζονται οι διαδικασίες που προβλέπονται στην ΠΔΑΤΥ. Στο πλαίσιο της αυτοψίας, η Ομάδα

Ελέγχου δύναται να έρθει σε επαφή με το προσωπικό των Ταχυδρομικών Επιχειρήσεων. Η Ομάδα Ελέγχου καταγράφει αναλυτικά τις ελλείψεις και τα σφάλματα που ενδεχομένως διαπιστώνονται.

(ζ) Οι Ταχυδρομικές Επιχειρήσεις υποχρεούνται να υποβάλουν στην Ομάδα Ελέγχου οποιοδήποτε στοιχείο θεωρηθεί απαραίτητο για την επιτυχή ολοκλήρωση του ελέγχου.
(η) Τυχόν διαπίστωση έλλειψης συνεργασίας από την Ταχυδρομική Επιχείρηση ή/και προσπάθειας παραπλάνησης της Ομάδας Ελέγχου καταγράφεται.

ΠΑΡΑΡΤΗΜΑ Β
Ελάχιστο περιεχόμενο του εντύπου με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Ταχυδρομική Επιχείρηση»

Το ως άνω έντυπο περιέχει τουλάχιστον τα ακόλουθα στοιχεία:
(α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε ο έλεγχος.
(β) Τα ονοματεπώνυμα και τις ιδιότητες των στελεχών της ΑΔΑΕ που απαρτίζουν την **Ομάδα Ελέγχου καθώς και την ημερομηνία σύστασής της.**
(γ) Την επωνυμία της υπό έλεγχο Ταχυδρομικής Επιχείρησης, καθώς και το όνομα του Υπευθύνου Ασφάλειας.
(δ) Το χρόνο που απαιτήθηκε έως ότου να παραδοθεί στην Ομάδα Ελέγχου πλήρης η ΠΔΑΤΥ.
(ε) Ημερολόγιο ενεργειών, ερωτηματολόγιο της Ομάδας Ελέγχου και καταγραφή της ανταπόκρισης της υπό έλεγχο Ταχυδρομικής Επιχείρησης.
(στ) Το αποτέλεσμα της αυτοψίας για την αποτίμηση της εφαρμογής της ΠΔΑΤΥ, με καταγραφή των ελλείψεων και ασαφειών που ενδεχομένως διαπιστώνονται.
(ζ) Ημερομηνία έναρξης και περάτωσης του ελέγχου.
(η) Τελικό πόρισμα του ελέγχου και εισήγηση προς την Ολομέλεια της ΑΔΑΕ.

ΠΑΡΑΡΤΗΜΑ Β

ΕΚΘΕΣΗ ΠΕΠΡΑΓΜΕΝΩΝ
ΕΤΟΥΣ 2005

ΠΑΡΑΡΤΗΜΑ Β

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ΄ΑΡΙΘ. 47

Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του.

Ο ΠΡΟΕΔΡΟΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

΄Εχοντας υπόψη:

1. Τις διατάξεις του άρθρου 19 παρ.1 του Συντάγματος.
2. Τις διατάξεις του άρθρου 9 του Ν. 3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» (Α΄- 47).
3. Τις διατάξεις του Ν. 2225/1994 « Για την προστασία της ελευθερίας και ανταπόκρισης και επικοινωνίας και άλλες διατάξεις», (Α΄-121) όπως ισχύουν.
4. Τις διατάξεις του άρθρου 29Α του Ν. 1558/1985 «Κυβέρνηση και Κυβερνητικά όργανα» (Α΄ - 137), όπως προστέθηκε με το άρθρο 27 του Ν. 2081/1992 (Α΄- 154) και αντικαταστάθηκε με την παρ. 2α του άρθρου 1 του Ν. 2469/1997 (Α΄- 38).
5. Τις διατάξεις της υπ΄ αριθμ. 14650/ΔΙΟΕ85/17.3.2004 απόφασης του Πρωθυπουργού και του Υπουργού Οικονομίας και Οικονομικών «Καθορισμός αρμοδιοτήτων των Υφυπουργών Οικονομίας και Οικονομικών» (Β΄- 519).
6. Την υπ΄ αριθμ. ΕΠ 03\5.5.2004 γνώμη της «Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών».
7. Το γεγονός ότι από την εφαρμογή του παρόντος διατάγματος προκαλείται ενδεχόμενη δαπάνη, το ύψος της οποίας δεν είναι δυνατό να υπολογισθεί, καθόσον τούτο εξαρτάται από πραγματικά γεγονότα όπως η τυχόν απαιτούμενη μίσθωση κυκλωμάτων για την άρση του απορρήτου των τηλεπικοινωνιών καθώς και η τυχόν απαιτούμενη από την αρμόδια αρχή ειδική επεξεργασία ή ανάλυση των στοιχείων επικοινωνίας.

Η ανωτέρω ενδεχόμενη δαπάνη θα καλύπτεται από πιστώσεις του προϋπολογισμού των Υπουργείων Δικαιοσύνης, Εθνικής Άμυνας, και Δημόσιας Τάξης, κατά περίπτωση.

8. Την υπ΄ αριθμ. 28/2005 γνωμοδότηση του Συμβουλίου της Επικρατείας, μετά από πρόταση των Υπουργών Δημόσιας Τάξης, Δικαιοσύνης, Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης και Μεταφορών και Επικοινωνιών και του Υφυπουργού Οικονομίας και Οικονομικών, αποφασίζουμε:

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1
Γενικά.

Για την άρση του απορρήτου των επικοινωνιών και την καταγραφή σε ενιαίο κείμενο των όρων και της διαδικασίας αυτής καθώς και των τεχνικών και οργανωτικών μεθόδων με τις οποίες μπορεί αυτή να πραγματοποιηθεί και να διασφαλισθούν τα αποτελέσματά της, έτσι ώστε να μη θίγεται η ιδιωτική ζωή και η προσωπικότητα του πολίτη, παρά μόνο στο μέτρο και για όσο χρονικό διάστημα είναι απολύτως αναγκαίο, χάριν της προστασίας της εθνικής ασφάλειας, της διακρίβωσης των εγκλημάτων που προβλέπονται στο άρθρο 4 του Ν. 2225/1994 (Α΄-121), όπως αντικαταστάθηκε με το άρθρο 12 του Ν. 3115/2003 (Α΄- 47) και των εν γένει ατομικών δικαιωμάτων και ελευθεριών, εφαρμόζονται οι διαδικασίες που προβλέπονται από τις διατάξεις του παρόντος.

Άρθρο 2
Ορισμοί.

Για την εφαρμογή του παρόντος οι ακόλουθοι όροι έχουν την εξής έννοια:

1. **«Αρμόδια αρχή» :**
   Η Δικαστική ή άλλη πολιτική, στρατιωτική ή αστυνομική δημόσια αρχή, η οποία δικαιούται να υποβάλει αίτηση για άρση του απορρήτου και να λάβει τα στοιχεία της επικοινωνίας.
2. **«Δικαστική αρχή»:**
   Η Αρχή που έχει αρμοδιότητα να εκδώσει διάταξη για άρση του απορρήτου.
3. **«Διάταξη»:**
   Η απόφαση για άρση του απορρήτου που εκδίδεται από την δικαστική αρχή.
4. **«Πάροχος υπηρεσιών επικοινωνιών»:**
   Η Επιχείρηση, η οποία παρέχει υπηρεσίες επικοινωνιών διαθέσιμες στο κοινό.
5. **«Πάροχος δικτύου επικοινωνιών»:**
   Η Επιχείρηση, η οποία εγκαθιστά, λειτουργεί, ελέγχει ή διαθέτει δίκτυο που παρέχει υπηρεσίες επικοινωνιών.
6. **«Συνδρομητής»:**
   Κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με πάροχο υπηρεσιών επικοινωνιών ή πάροχο δικτύου επικοινωνιών για την παροχή τέτοιων υπηρεσιών.
7. **«Χρήστης»:**
   Κάθε φυσικό ή νομικό πρόσωπο που χρησιμοποιεί ή ζητεί να χρησιμοποιήσει υπηρεσίες επικοινωνιών.
8. **«Φορητότητα αριθμού κλήσης»:**
   Η δυνατότητα των χρηστών να διατηρούν τον ή τους αριθμούς κλήσης τους όταν αλλάζουν πάροχο υπηρεσίας επικοινωνιών, τοποθεσία ή τύπο υπηρεσίας.
9. **«Υπηρεσία προστιθέμενης αξίας»:**
   Κάθε μη τηλεπικοινωνιακή Υπηρεσία, η οποία παρέχεται ή υποστηρίζεται από δίκτυα τηλεπικοινωνιών .

10. **«Εξουσιοδοτημένο πρόσωπο»:**
Υπάλληλος δημόσιας υπηρεσίας ή παρόχου υπηρεσιών επικοινωνιών, το οποίο εκτελεί εμπιστευτική αποστολή στη διαδικασία της άρσης του απορρήτου των επικοινωνιών.
11. **«Επισύνδεση»:**
Η παράλληλη σύνδεση τρίτου σε δίκτυο επικοινωνιών κατά τρόπο ώστε να παρακολουθεί διεξαγόμενη επικοινωνία και να λαμβάνει το περιεχόμενο και τα στοιχεία αυτής σε πραγματικό χρόνο.
12. **«Διεπιλογή»:**
Η απευθείας επιλογή καλούμενου εσωτερικού αριθμού Συνδρομητικού Κέντρου (PABX) από τον καλούντα.
13. **«Περιαγωγή»**
Παρεχόμενη υπηρεσία που εξασφαλίζει σε συνδρομητές να χρησιμοποιούν δίκτυο άλλο από εκείνο του οποίου είναι συνδρομητές.
14. **«Εκτροπή κλήσης»**
Αυτόματη μεταβίβαση εισερχόμενης κλήσης σε άλλον αριθμό κλήσης του ιδίου ή άλλου παρόχου με εντολή του συνδρομητή.
15. **«Πάροχος υπηρεσιών πιστοποίησης»:**
Φυσικό ή νομικό πρόσωπο ή άλλος φορέας που είναι αρμόδιος σύμφωνα με το νόμο να εκδίδει πιστοποιητικά ή να παρέχει άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές.
16. **«Ονοματοδότης»:**
Σειρά αλφαριθμητικών χαρακτήρων προς ένδειξη της ταυτότητας τηλετυπικού συνδρομητή που μεταδίδεται αυτόματα στην τηλετυπική επικοινωνία.

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ
ΕΙΔΗ ΚΑΙ ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

Άρθρο 3
Είδη επικοινωνίας.

1. Η άρση του απορρήτου δεν αφορά την δια ζώσης επικοινωνία, αλλά κάθε είδους επικοινωνία, η οποία διεξάγεται μέσω δικτύου επικοινωνίας ή παρόχου υπηρεσιών επικοινωνιών και την οποία χρησιμοποιεί ο συνδρομητής ή χρήστης κατά του οποίου λαμβάνεται το μέτρο της άρσης.
2. Τα είδη και οι μορφές επικοινωνίας, που υπόκεινται στην άρση του απορρήτου, είναι ιδίως τα ακόλουθα:
   - **α. Επιστολογραφία, ήτοι επιστολές, δέματα, ταχυμεταφορές στοιχείων, τηλεγραφήματα, επιταγές κ.λπ.**
   - **β. Τηλετυπική επικοινωνία (συνδρομητική).**
   - **γ. Τηλεφωνική επικοινωνία, ήτοι σταθερή και κινητή τηλεφωνία.**
   - **δ. Επικοινωνία δεδομένων μέσω δικτύων δεδομένων, μισθωμένων κυκλωμάτων κ.α.**
   - **ε. Επικοινωνίες μέσω διαδικτύου (Internet).**
   - **στ. Ασυρματική επικοινωνία, ήτοι σταθερή ασύρματη πρόσβαση, επικοινωνία κλειστών ομάδων χρηστών κ.α.**
   - **ζ. Δορυφορική επικοινωνία, ήτοι επικοινωνία μέσω δορυφορικής σύνδεσης τελικού**

χρήστη (π.χ. VSAT).

η. Επικοινωνία κάθε μορφής μέσω μισθωμένων κυκλωμάτων.

θ. Υπηρεσίες προστιθέμενης αξίας, που υπερτίθενται επί των προηγούμενων μορφών επικοινωνίας, αποτελούν ιδίως:

I. Ο Αυτόματος τηλεφωνητής
II. Τα Τηλεομοιοτυπήματα (FAX)
III. Τα Γραπτά μηνύματα (SMS / MMS)
IV. Οι Υπηρεσίες πληροφοριών
V. Το Ηλεκτρονικό Ταχυδρομείο
VI. Η πρόσβαση σε ιστοσελίδες
VII. Η πρόσβαση σε βάσεις δεδομένων
VIII. Οι Ηλεκτρονικές συναλλαγές
IX. Οι Τηλεδιασκέψεις
X. Οι Πληροφορίες καταλόγου
XI. Οι Υπηρεσίες έκτακτης ανάγκης

1. Οι συνδυασμένες μορφές επικοινωνίας που περιλαμβάνουν περισσότερες της μιας από τις παραπάνω επικοινωνίες, όπως είναι π.χ. η πρόσβαση σε δίκτυα δεδομένων ή σε δίκτυα Internet από το Επιλεγόμενο Δημόσιο Τηλεφωνικό Δίκτυο (PSTN). Ειδικότερα στις υπηρεσίες προστιθέμενης αξίας είναι δυνατόν να διαφοροποιείται ο πάροχος υπηρεσιών διαδικτύου (πρόσβαση στο διαδίκτυο) από τον πάροχο της συγκεκριμένης υπηρεσίας.

Άρθρο 4
Στοιχεία επικοινωνίας.

1. Τα συγκεκριμένα στοιχεία επικοινωνίας, στα οποία είναι δυνατόν να αναφέρεται μία διάταξη άρσης του απορρήτου εξαρτώνται από το είδος της επικοινωνίας και εξειδικεύονται κατά περίπτωση ως εξής:

α. Επιστολογραφία:
- αα. Πάροχος υπηρεσίας
- ββ. Αποστολέας
- γγ. Αποδέκτης
- δδ. Περιεχόμενο

β. Τηλετυπική επικοινωνία:
- αα. Φυσικό ή νομικό πρόσωπο συνδρομητή ή χρήστη
- ββ. Καλών και καλούμενος αριθμός και ονοματοδότης
- γγ. Χρόνος και διάρκεια κλήσης
- δδ. Χρέωση
- εε. Περιεχόμενο τηλετυπήματος

γ. Τηλεφωνική επικοινωνία:

Επί συγκεκριμένου φυσικού ή νομικού προσώπου, που είναι συνδρομητής ή χρήστης παρόχου υπηρεσιών σταθερής ή κινητής τηλεφωνίας, είναι δυνατόν να ζητηθούν τα ακόλουθα συγκεκριμένα στοιχεία εισερχόμενων και απερχόμενων κλήσεων.

αα. Καλών και καλούμενος αριθμός κλήσης και στις αναπάντητες κλήσεις.
ββ. Καλών και καλούμενος συνδρομητής και πελάτης και στις αναπάντητες κλήσεις.
γγ. Ὡρα έναρξης και ώρα λήξης της επικοινωνίας.
δδ. Γεωγραφικός εντοπισμός καλούντος και καλούμενου (στις κινητές επικοινωνίες) είτε ομιλούν, είτε πρόκειται για SMS, είτε είναι σε θέση stand- by , είτε πραγματοποιούν αναπάντητη κλήση.
εε. Περιεχόμενο επικοινωνίας (φωνή, εικόνα κ.λπ)
στστ. Στοιχεία ταυτότητας τερματικής συσκευής (IMEI, IMSI, TMSI)
ζζ. Οι αλφαριθμητικοί χαρακτήρες που εισάγει ο χρήστης για την πραγματοποίηση της σύνδεσης ή για την ενεργοποίηση ειδικών υπηρεσιών ή λειτουργιών.
ηη. Η σηματοδότηση της ετοιμότητας για την πρόσβαση (προειδοποιητικό σήμα επικοινωνίας).
θθ. Πραγματικός προορισμός και ενδιάμεσοι αριθμοί κλήσεως, σε περίπτωση εκτροπής της κλήσης.

δ. Επικοινωνία δεδομένων :

Η επικοινωνία δεδομένων (data) πραγματοποιείται με τους ακόλουθους τρόπους:

αα. Μέσω μισθωμένων κυκλωμάτων
ββ. Μέσω ειδικών δικτύων υπολογιστών (μεταγωγής πακέτων):
- με αφιερωμένες συνδρομητικές γραμμές,
- με πρόσβαση από το Επιλεγόμενο Δημόσιο Τηλεφωνικό Δίκτυο (PSTN)

γγ. Μέσω του Διαδικτύου (Internet)

Στις παραπάνω περιπτώσεις είναι δυνατή η παροχή όλων των ενδιαφερόντων στοιχείων, ιδίως του καλούντος και καλούμενου χρήστη, του χρόνου και διάρκειας επικοινωνίας, και των μεταβιβαζόμενων στοιχείων .

ε. Επικοινωνίες μέσω διαδικτύου (Internet)

αα. Η πρόσβαση των χρηστών στο διαδίκτυο πραγματοποιείται με τους ακόλουθους τρόπους:
- Με μισθωμένο ψηφιακό κύκλωμα (μόνιμη σύνδεση)
- Μέσω του Επιλεγόμενου Δημόσιου Τηλεφωνικού Δικτύου (σύνδεση αναλογική, ISDN, DSL), καθώς και των δικτύων κινητής τηλεφωνίας.
- Με σταθερή ασύρματη πρόσβαση (ΣΑΠ).

ββ. Ο πάροχος υπηρεσιών διαδικτύου, ο οποίος διαθέτει εγκαταστάσεις διαδικτύου (ISP, Internet Service Provider), υποχρεούται να διαθέτει τα πλήρη στοιχεία ταυτότητας των χρηστών- πελατών του (ονοματεπώνυμο, διεύθυνση, ιστοσελίδα) καθώς και τον τρόπο πρόσβασής τους. Κάθε πρόσβαση του χρήστη στο διαδίκτυο καταγράφεται στις εγκαταστάσεις του ISP στο επίπεδο του δικτύου (πακέτα IP). Με τη διάταξη μπορεί να επιτραπεί η εξέταση του περιεχομένου των πακέτων προκειμένου να αποκαλυφθούν χρήσιμες πληροφορίες αναφορικά με τις ενέργειες του χρήστη στο διαδίκτυο, όπως:

- επισκεπτόμενες διευθύνσεις
- χρησιμοποιούμενες υπηρεσίες (e-mail, συναλλαγές κ.λπ.)
- περιήγηση σε ιστοσελίδες και βάσεις πληροφοριών
- ανταλλαγή δεδομένων /αρχείων μέσω της υπηρεσίας FTP
- τηλεφωνική επικοινωνία μέσω διαδικτύου (VoIP).

στ. Ασυρματική επικοινωνία

αα. Σταθερή ασύρματη πρόσβαση (ΣΑΠ)

Τα δίκτυα ΣΑΠ μπορούν να παρέχουν όλες τις υπηρεσίες επικοινωνίας που παρέχονται από τα τηλεπικοινωνιακά δίκτυα, ήτοι τηλεφωνία, υπηρεσίες ISDN, πρόσβαση σε δίκτυα δεδομένων και Internet, μισθωμένα κυκλώματα, υπηρεσίες προστιθέμενης αξίας κ.λπ.

Για την εξασφάλιση των στοιχείων επικοινωνίας, που αφορούν τις ανωτέρω παρεχόμενες υπηρεσίες, μπορεί να επιτραπεί η πρόσβαση στους σταθμούς βάσης των δικτύων ΣΑΠ με την συγκατάθεση και συνεργασία των παρόχων υπηρεσιών ΣΑΠ.

ββ. Τοπικά ασυρματικά δίκτυα

Τα τοπικά ασυρματικά δίκτυα 802.11 και Bluetooth λειτουργούν στη ζώνη συχνοτήτων 2,4 GHz και εξυπηρετούν περιορισμένες γεωγραφικές περιοχές παρέχοντας κυρίως υπηρεσίες τηλεφωνίας, δεδομένων και Internet.

Η λήψη και καταγραφή των άνω στοιχείων επικοινωνίας μπορεί να επιτραπεί με την πρόσβαση στους σταθμούς βάσης WiFi των δικτύων αυτών, με την συνεργασία των παρόχων.

γγ. Συστήματα επικοινωνίας κλειστών ομάδων χρηστών

Τα εν λόγω δίκτυα είναι ιδιωτικά και η πρόσβαση για τη λήψη στοιχείων επικοινωνίας σε αυτά γίνεται αναγκαίως με τη συνεργασία των ιδιοκτητών τους, οι οποίοι και υποχρεούνται προς τούτο.

ζ. Δορυφορική επικοινωνία :

αα. Συστήματα VSAT

Τα συστήματα VSAT παρέχουν στον τελικό χρήστη, ο οποίος διαθέτει κατάλληλο τερματικό VSAT συνδεόμενο με τον επίγειο δορυφορικό σταθμό βάσης (HUB) του συστήματος, όλες τις τηλεπικοινωνιακές υπηρεσίες.

Εφόσον ο σταθμός HUB βρίσκεται εντός της χώρας, μπορεί να επιτραπεί η λήψη των προσωπικών στοιχείων του χρήστη και των δεδομένων επικοινωνίας με τη συνεργασία του παρόχου της υπηρεσίας VSAT.

ββ. Δορυφορικά συστήματα επικοινωνίας πλοίων

Τα συστήματα αυτά παρέχουν τη δυνατότητα στα πλοία, με τη χρήση κατάλληλων τερματικών, να εξασφαλίζουν μέσω δορυφορικών συνδέσεων πρόσβαση στα λοιπά δημόσια τηλεπικοινωνιακά δίκτυα, μέσω των οποίων μπορούν να λαμβάνονται στοιχεία.

η. Μισθωμένα κυκλώματα:

Τα απαιτούμενα στοιχεία εξαρτώνται από το είδος του μισθωμένου κυκλώματος (αναλογικό, ψηφιακό, δορυφορικό) και τη συγκεκριμένη μορφή επικοινωνίας για την οποία χρησιμοποιούνται (π.χ. τηλεφωνική επικοινωνία, μετάδοση δεδομένων, σύνδεση Internet κ.λπ.), σύμφωνα με τα αναφερόμενα στις προηγούμενες παραγράφους.

θ. Υπηρεσίες προστιθέμενης αξίας:

Τα απαιτούμενα στοιχεία εξαρτώνται από την συγκεκριμένη υπηρεσία, καθώς και από το είδος επικοινωνίας η οποία την εξυπηρετεί. Συγκεκριμένα για τις υπηρεσίες που αναφέρονται παραπάνω (άρθρο 3 παρ. 2) σημειώνονται τα ακόλουθα:

αα Αυτόματος τηλεφωνητής

Τα μεταδιδόμενα φωνητικά μηνύματα καταγράφονται με τον ίδιο τρόπο που καταγράφεται η συνομιλία (περιπτ. γ).

ββ. Τηλεομοιοτυπήματα (FAX)

Η αποτύπωση των σχετικών στοιχείων γίνεται με τη χρήση συσκευής FAX.

γγ. Γραπτά μηνύματα (SMS /MMS)

Καταγραφή και αποθήκευση στα αρχεία του παρόχου υπηρεσιών γίνεται εφόσον ζητηθεί.

δδ. Υπηρεσίες πληροφοριών

Καταγραφή κάθε πρόσβασης γίνεται στα αρχεία του παρόχου.

εε. Ηλεκτρονικό Ταχυδρομείο

Καταγράφονται στα αρχεία του παρόχου τα ακόλουθα στοιχεία:

- Ηλεκτρονική διεύθυνση
- Παραλήπτες των εξερχομένων μηνυμάτων (ηλεκτρονική διεύθυνση)
- Αποστολείς των εισερχομένων μηνυμάτων (ηλεκτρονική διεύθυνση)
- Το περιεχόμενο των ηλεκτρονικών μηνυμάτων.

στστ. Πρόσβαση σε ιστοσελίδες

Καταγράφονται στα αρχεία του παρόχου τα ακόλουθα στοιχεία:

- Ιστοσελίδες που επισκέπτεται ο χρήστης
- Σε περίπτωση που ο χρήστης διαθέτει εξυπηρετητή ιστοσελίδων (Web Server), μπορεί να αποκαλυφθεί το περιεχόμενο των ιστοσελίδων και τα στοιχεία των συναλλαγών που γίνονται μέσω του εξυπηρετητή.

ζζ. Πρόσβαση σε Βάσεις Δεδομένων

Καταγράφονται στα αρχεία του παρόχου τα ακόλουθα στοιχεία:

- Βάσεις δεδομένων που επισκέπτεται ο χρήστης
- Περιεχόμενο των βάσεων δεδομένων.

ηη. Ηλεκτρονικές συναλλαγές

(τραπεζικές e-banking), κρατικές (e-gov), εμπορικές (e-commerce).

Τα στοιχεία που μπορούν να αποκαλυφθούν είναι:

- Είδος συναλλαγών
- Στοιχεία συναλλασσόμενων προσώπων
- Χρόνος συναλλαγής
- Αριθμοί πιστωτικών καρτών
- Αριθμοί τραπεζικών λογαριασμών, καταθέσεις/αναλήψεις
- Οφειλές προς τρίτους
- Περιουσιακά στοιχεία

θθ. Τηλεδιασκέψεις:

- Σε περίπτωση τηλεφωνικής τηλεδιάσκεψης ισχύει ό,τι στις τηλεφωνικές επικοινωνίες (περιπτ. γ).
- Σε περίπτωση τηλεδιάσκεψης με μετάδοση εικόνας (video) απαιτείται ειδικός εξοπλισμός.
- Σε περίπτωση υπηρεσίας chat room στο διαδίκτυο, καταγραφή των στοιχείων από τον πάροχο υπηρεσιών διαδικτύου είναι δυνατή εφόσον ζητηθεί.
- Σε περίπτωση τηλεδιάσκεψης πολλαπλών προσώπων δύνανται να καταγραφούν οι αριθμοί κλήσης των συμμετεχόντων, καθώς και το περιεχόμενο της επικοινωνίας.

ιι. Πληροφορίες καταλόγου:

Σε περίπτωση που παρέχονται τηλεφωνικώς τα στοιχεία είναι δυνατόν να ζητηθούν σύμφωνα με την περίπτωση γ της παρούσας παραγράφου. Σε περίπτωση παροχής μέσω διαδικτύου τα στοιχεία είναι δυνατόν να ζητηθούν σύμφωνα με την περίπτωση ε της παρούσας παραγράφου. Σε περίπτωση έντυπης καταχώρησης ή σε δισκέτα αναζήτησης, τα στοιχεία είναι δυνατόν να ζητηθούν στις ανωτέρω πηγές.

ιαια. Υπηρεσίες έκτακτης ανάγκης

Καταγραφή των στοιχείων γίνεται από τον πάροχο υπηρεσίας.

2. Όλα τα ανωτέρω στοιχεία εφόσον τηρούνται οι νόμιμες προϋποθέσεις είναι δυνατόν να ζητούνται από τους παρόχους υπηρεσιών προστιθέμενης αξίας ή από τους παρόχους υπηρεσιών δικτύου ή και από αμφοτέρους.
3. Η παράθεση των στοιχείων επικοινωνίας της παραγράφου ι είναι ενδεικτική. Η διάταξη άρσης απορρήτου δεν αποκλείεται να αναφέρεται και σε άλλα στοιχεία κατά είδος επικοινωνίας, κάθε φορά που η εξέλιξη της επιστήμης και της τεχνολογίας επιφέρει διεύρυνση του καταλόγου των στοιχείων αυτών.

Άρθρο 5
Ειδικές περιπτώσεις.

1. **Αριθμοί κλήσης εκτός δημοσίων καταλόγων.**
   Η αρμόδια αρχή μπορεί να λαμβάνει γνώση απευθυνόμενη σε εξουσιοδοτημένα πρόσωπα ή υπηρεσίες του παρόχου υπηρεσίας.
2. **Φορητότητα αριθμών κλήσης.**
   Σε περίπτωση που συνδρομητής έχει χρησιμοποιήσει την ευχέρεια της φορητότητας του αριθμού κλήσης, η αρμόδια αρχή απευθύνεται στον αρμόδιο φορέα που διαθέτει τη βάση δεδομένων στην οποία καταχωρούνται όλοι οι αριθμοί κλήσης, για να λαμβάνει από αυτόν τις απαραίτητες πληροφορίες. Πρόσθετα στοιχεία μπορεί να ζητηθούν από τους παρόχους υπηρεσίας.
3. **Εκτροπή κλήσης**
   Σε περίπτωση χρησιμοποίησης από συνδρομητή της υπηρεσίας εκτροπής εισερχόμενων κλήσεων:
   α) εφόσον η εκτροπή γίνεται σε αριθμό κλήσεως του ίδιου παρόχου υπηρεσίας, ο πάροχος προβαίνει άμεσα και με βάση τη διάταξη που του έχει επιδοθεί στην πραγματοποίηση επισύνδεσης και στον αριθμό κλήσης της εκτροπής, ενημερώνοντας επί αυτού την αρμόδια αρχή,
   β) εφόσον η εκτροπή παραπέμπει στον αριθμό κλήσης άλλου παρόχου υπηρεσίας, ο πάροχος στον οποίο έχει επιδοθεί η διάταξη ενημερώνει σχετικώς άμεσα την αρμόδια αρχή, η οποία μπορεί να εκδώσει νέα διάταξη για τον άλλο πάροχο.
4. **Περιαγωγή (roaming)**
   Σε περίπτωση που ένας συνδρομητής δικτύου κινητής τηλεφωνίας βρίσκεται εκτός της χώρας και πραγματοποιεί ή δέχεται κλήσεις από χρήστες επίσης εκτός χώρας, η καταγραφή του περιεχομένου της επικοινωνίας (φωνή, μηνύματα) είναι δυνατή μόνο με συνεργασία με τους παρόχους υπηρεσιών των αντίστοιχων χωρών μέσω διαδικασίας δικαστικής συνδρομής ή με άλλο πρόσφορο τρόπο. Καταγράφονται όμως οπωσδήποτε στις περιπτώσεις αυτές οι καλούμενοι και οι καλούντες αριθμοί κλήσης και ο χρόνος.
5. **Συνδρομητικά Κέντρα (PABX) και Ιδιωτικά Δίκτυα**
   α. Σε περίπτωση που ενδιαφέρει το σύνολο της επικοινωνίας που διεξάγεται μέσω του PABX κάποιου φορέα – πελάτη, ισχύουν όσα προβλέπονται στο άρθρο 4 παράγραφος ι περιπτ. γ΄.
   β. Σε περίπτωση που η αρμόδια αρχή ενδιαφέρεται για συγκεκριμένο πρόσωπο και

συγκεκριμένη/ες εσωτερική/ές τηλεφωνική/ές σύνδεση/εις, γίνεται από τον πάροχο καταγραφή των στοιχείων του συνόλου των επικοινωνιών του PABX, πλην του περιεχομένου, και ανάλυσής τους εκ των υστέρων.

γ. Η καταγραφή και λήψη στοιχείων επικοινωνίας εφόσον είναι αναγκαία γίνεται με την συνεργασία των ιδιοκτητών του PABX ή / και του Ιδιωτικού Δικτύου η οποία εξασφαλίζεται με μέριμνα της αρμόδιας αρχής.

6. Τηλεκάρτες ή κάρτες ανανέωσης χρόνου ομιλίας.

Σε περίπτωση χρήσης των ανωτέρω καρτών σε δίκτυα σταθερής ή κινητής τηλεφωνίας και στο διαδίκτυο, η εκτέλεση της διάταξης πραγματοποιείται είτε με εξατομίκευση των άνω καρτών εφόσον προβλέπεται αυτή, είτε με ανάλυση των επικοινωνιών που διεξάγονται από κοινόχρηστες παροχές (στο PSTN), και από PC και τηλεφωνικές συνδέσεις στο Internet.

7. Ειδικές περιπτώσεις στις υπηρεσίες διαδικτύου:

α) Εφόσον από την ίδια σύνδεση, μέσω τοπικών δικτύων LAN ή μέσω VPN, εξυπηρετούνται περισσότεροι χρήστες, όπως προσωπικό εταιρειών, υπηρεσιών και ιδρυμάτων, ο εντοπισμός κάθε χρήστη γίνεται με ανάλυση των διεξαγομένων επικοινωνιών σε συνεργασία με τον πάροχο του δικτύου.

β) Σε περίπτωση εξυπηρέτησης χρήστη από πάροχο υπηρεσίας Internet εξωτερικού (e-mail, ιστοσελίδες κ.λ.π.) η εκτέλεση της διάταξης συντελείται με παρακολούθηση πακέτων IP και σχετική ανάλυσή τους.

γ) Κρυπτογράφηση με δημόσιο/ιδιωτικό κλειδί .

Σε περίπτωση κρυπτογραφημένου περιεχομένου, που βασίζεται στις αρχές του δημόσιου κλειδιού, η αρμόδια αρχή επιτρέπεται να έχει πρόσβαση στο ιδιωτικό (ή δημόσιο κατά περίπτωση) κλειδί του παραλήπτη (ή αποστολέα) ώστε να μπορεί να αποκτά πρόσβαση στο περιεχόμενο. Σε αυτή την περίπτωση οι Πάροχοι Υπηρεσιών Πιστοποίησης (Certification Authorities), υποχρεούνται α συνεργάζονται με την αρμόδια αρχή για την εξασφάλιση του εν λόγω κλειδιού.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ
ΕΞΟΠΛΙΣΜΟΣ-ΜΕΣΑ-ΜΕΘΟΔΟΣ-ΥΠΟΧΡΕΩΣΕΙΣ ΠΑΡΟΧΩΝ

Άρθρο 6
Εξοπλισμός

1. Σε περίπτωση που το τηλεπικοινωνιακό σύστημα ενός παρόχου διαθέτει τον κατάλληλο εξοπλισμό και το λογισμικό που απαιτείται για την άρση του απορρήτου, ο πάροχος υποχρεούται να τα ενεργοποιεί, όταν του ζητείται από την αρμόδια αρχή η εκτέλεση μίας διάταξης, εντός τριών (3) ωρών από τη γνωστοποίηση της διάταξης ανεξαρτήτως του χρόνου επίδοσης της διάταξης στον πάροχο και σε επείγουσες περιπτώσεις, οι οποίες ειδικά θα επισημαίνονται, εντός του αμέσως δυνατού χρόνου,
2. Σε περίπτωση που το τηλεπικοινωνιακό σύστημα ενός παρόχου δεν διαθέτει τον αναγκαίο εξοπλισμό και λογισμικό για την άρση του απορρήτου και την παροχή στις αρμόδιες αρχές των στοιχείων επικοινωνίας, όπως αυτά καθορίζονται κατά περίπτωση στο άρθρο 4 του παρόντος, ο πάροχος, αφού γνωστοποιήσει αυτό εγγράφως στην ΑΔΑΕ,

υποχρεούται να προμηθευτεί, εγκαταστήσει και θέσει σε λειτουργία στο σύστημά του τον προς τούτο απαιτούμενο εξοπλισμό ή και λογισμικό εντός προθεσμίας εννέα (9) μηνών από τη δημοσίευση του παρόντος και να ενημερώσει σχετικώς εγγράφως την ΑΔΑΕ.

Σε περίπτωση μελλοντικών εγκαταστάσεων νέων συστημάτων ή υπηρεσιών ή αναβάθμισης/τροποποίησης υφισταμένων συστημάτων / υπηρεσιών, οι πάροχοι υποχρεούνται να μεριμνούν για τον εφοδιασμό τους με τον απαιτούμενο εξοπλισμό ή / και λογισμικό για άρση του απόρρητου σύμφωνα με τις διατάξεις του παρόντος.

3. Τα τυχόν απαιτούμενα μισθωμένα κυκλώματα για την άρση του απορρήτου εξασφαλίζονται με μέριμνα της αρμόδιας αρχής, την οποία βαρύνει και το σχετικό κόστος το οποίο βασίζεται στα ισχύοντα τιμολόγια των παρόχων.

Άρθρο 7.
Μέσα και μέθοδοι.

1. Η διάταξη που επιβάλλει την άρση του απορρήτου προσδιορίζει τις συγκεκριμένες μορφές και τα στοιχεία επικοινωνίας στα οποία αναφέρεται η άρση και εξατομικεύει τα στοιχεία αυτά και δη την ταυτότητα του συνδρομητή ή χρήστη, τους αριθμούς κλήσεις, τα στοιχεία μισθωμένων γραμμών και τους κωδικούς πρόσβασης σε δίκτυα δεδομένων ή στο διαδίκτυο, εφαρμοζομένων κατά τα λοιπά των διατάξεων των άρθρων 5 του Ν.2225/1994 και 12 του Ν. 3115 /2003.
2. Η εκτέλεση μιας διάταξης για άρση απορρήτου, μετά την αποστολή της από την αρμόδια αρχή στον πάροχο υπηρεσίας, πραγματοποιείται με την συνεργασία του παρόχου και της αρμόδιας αρχής, η οποία έχει και την ευθύνη.

Συγκεκριμένα:

α. Τα στοιχεία της επικοινωνίας , τα οποία καταγράφονται στα αρχεία του παρόχου (καλών, καλούμενος, χρόνος, εντοπισμός κ.λ.π), γνωστοποιούνται από αυτόν εγγράφως στην αρμόδια αρχή, σύμφωνα και με τα αναφερόμενα στο άρθρο 4.

β. Σε περίπτωση που ζητείται καταγραφή του περιεχομένου της επικοινωνίας για συγκεκριμένο διάστημα, αυτή πραγματοποιείται στις εγκαταστάσεις της αρμόδιας αρχής με επισύνδεση μέσω μισθωμένου κυκλώματος ή με άλλο κατάλληλο τρόπο με ταυτόχρονη διαβίβαση του περιεχομένου και των στοιχείων επικοινωνίας στην αρμόδια αυτή Αρχή.

γ. Σε περίπτωση που τα στοιχεία της επικοινωνίας δεν μπορούν να παραδοθούν αμέσως στην αρμόδια αρχή, αποθηκεύονται πλην του περιεχομένου, με μέριμνα του παρόχου έως ότου καταστεί δυνατή η παράδοσή τους και για διάστημα όχι μεγαλύτερο των επτά (7) ημερών.

δ. Ο Πάροχος υποχρεούται να μεριμνά ώστε να παρέχεται δυνατότητα πολλαπλής και ταυτόχρονης διάθεσης στα στοιχεία επικοινωνίας από περισσότερες της μιας αρμόδιας αρχής.

3. Η εκτέλεση της διάταξης από τον πάροχο και η διαβίβασης των στοιχείων στην αρμόδια αρχή γίνεται με τρόπο που θα εξασφαλίζεται αξιοπιστία, εγκυρότητα, ακρίβεια, ταχύτητα και ασφάλεια. Στην διαδικασία εκτέλεσης εμπλέκεται ο ελάχιστος αναγκαίος αριθμός εξουσιοδοτημένων προσώπων.
4. Τα χρησιμοποιούμενα μέσα για την εκτέλεση μιας διάταξης διατίθενται από τον πάροχο

υπηρεσίας τον οποίον βαρύνει και το σχετικό κόστος.

5. Σε περίπτωση που για την εκτέλεση μιας συγκεκριμένης διάταξης απαιτείται ειδική διαδικασία ή ειδικός εξοπλισμός ή πρόσθετα στοιχεία, ο πάροχος υποχρεούται να ενημερώσει για αυτά αμέσως την αρμόδια αρχή με την οποία και συνεργάζεται για την αντιμετώπιση των σχετικών προβλημάτων.
6. Σε περίπτωση που μια συγκεκριμένη διάταξη δεν είναι δυνατό να εφαρμοστεί για τεχνικούς ή άλλους λόγους, ο πάροχος υπηρεσίας υποχρεούται να ενημερώσει αμέσως περί αυτού την αρμόδια αρχή και την ΑΔΑΕ με σχετικό έγγραφο στο οποίο θα πρέπει να αιτιολογείται πλήρως η αδυναμία αυτή.
7. Σε περίπτωση που τα διατιθέμενα ή συγκεντρούμενα στοιχεία από τον πάροχο κατά την εκτέλεση μιας διάταξης απαιτείται να υποβληθούν σε ειδική επεξεργασία ή ανάλυση, η εργασία αυτή πραγματοποιείται κατά περίπτωση από την αρμόδια αρχή ή από τον πάροχο εφόσον ζητήσει αυτό η αρμόδια αρχή. Η επιλογή της λύσης θα γίνεται, ανάλογα με την ιδιαιτερότητα της κάθε συγκεκριμένης περίπτωσης, μετά από συνεννόηση των εξουσιοδοτημένων προσώπων του παρόχου και της αρμόδιας αρχής. Εφόσον η επεξεργασία γίνεται από τον πάροχο και συνεπάγεται κόστος αυτό θα καταβάλλεται από το Δημόσιο με μέριμνα της αρμόδιας αρχής.
8. Στην περίπτωση επιστολής ή δέματος η εκτέλεση μιας διάταξης πραγματοποιείται με την συγκρότηση τριμελούς επιτροπής αποτελούμενης από ένα εισαγγελικό λειτουργό οριζόμενο από την αντίστοιχη υπηρεσία, ένα ανακριτικό υπάλληλο που ορίζεται από τον προϊστάμενο της αρμόδιας αρχής και ένα εξουσιοδοτημένο υπάλληλο του παρόχου υπηρεσίας.

Η σύγκληση επιτροπής γίνεται κατά περίπτωση με μέριμνα του παρόχου ευθύς ως του κοινοποιείται η διάταξη και για την αποσφράγιση και τα τυχόν ευρήματα συντάσσεται σχετικό πρακτικό.

Άρθρο 8
Υποχρεώσεις των παρόχων υπηρεσιών και δικτύων

1. Οι πάροχοι υπηρεσιών και δικτύων επικοινωνίας υποχρεούνται να ανταποκρίνονται αμέσως σε κάθε αίτημα για άρση του απορρήτου της επικοινωνίας που τους κοινοποιείται από τις αρμόδιες αρχές σύμφωνα με τα προβλεπόμενα στο παρόν.
2. Οι πάροχοι οφείλουν να ενημερώνουν και να συνεργάζονται με τις αρμόδιες αρχές για την παροχή τεχνικών πληροφοριών που αφορούν τη διασύνδεση της αρμόδιας αρχής με τον πάροχο ώστε να πραγματοποιείται η απρόσκοπτη και ακριβής εκτέλεση κάθε σχετικής διάταξης που τους κοινοποιείται.
3. Οι πάροχοι υποχρεούνται να λαμβάνουν όλα τα αναγκαία μέτρα για τη διασφάλιση του απορρήτου κατά την εκτέλεση των διατάξεων άρσης απορρήτου που τους κοινοποιούνται.
4. Σε περίπτωση που για την εκτέλεση μιας διάταξης άρσης απορρήτου, που κοινοποιείται σε ένα πάροχο υπηρεσίας, απαιτείται και η συνεργασία ή συμμετοχή άλλου ή άλλων παρόχων υπηρεσιών ή δικτύων, ο πάροχος υποχρεούται να ενημερώνει την αρμόδια αρχή και την ΑΔΑΕ και στη συνέχεια να ενεργεί σύμφωνα με τις σχετικές υποδείξεις τους.
5. Ο πάροχος υπηρεσίας ή δικτύου οφείλει να ενημερώνει την αρμόδια αρχή και την ΑΔΑΕ για οποιοδήποτε έκτακτο περιστατικό ή πρόβλημα που τυχόν εμφανίζεται κατά τη διάρ-

κεια της εκτέλεσης μιας διάταξης που του έχει αποσταλεί.

6. Οι πάροχοι υπηρεσιών υποχρεούνται να γνωστοποιούν στην αρμόδια αρχή τους αριθμούς κλήσης που είναι εκτός καταλόγων. Εφόσον αυτοί τους ζητηθούν και να συνδράμουν αυτοί με κάθε τρόπο στις περιπτώσεις των παραγράφουν 2,3 και 4 του άρθρου 5 του παρόντος, σύμφωνα με τα αναφερόμενα στις παραγράφους αυτές.
7. Σε περίπτωση που ένας πάροχος υπηρεσίας χρησιμοποιεί μεθόδους κωδικοποίησης, συμπίεσης ή κρυπτογράφησης, υποχρεούται κατά την εκτέλεση μιας διάταξης να παραδίδει ή διαβιβάζει τα ζητούμενα στοιχεία σε αποκωδικοποιημένη μορφή.
8. Οι πάροχοι υπηρεσιών οφείλουν να επιλέγουν ως «εξουσιοδοτημένο πρόσωπο» υπάλληλο που παρέχει πλήρη εγγύηση όχι μόνο από πλευράς τεχνικών γνώσεων αλλά και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Δεν ορίζεται ως εξουσιοδοτημένο πρόσωπο όποιος έχει καταδικαστεί για οποιοδήποτε κακούργημα η πλημμέλημα σε ποινή φυλάκισης τουλάχιστον 3 μηνών ή εκκρεμεί σε βάρος του ποινική δίωξη για κακούργημα ή για αδίκημα σχετιζόμενο με τη διασφάλιση του απορρήτου των επικοινωνιών και των δεδομένων προσωπικού χαρακτήρα. Τα στοιχεία των προσώπων αυτών γνωστοποιούνται στην Α.Δ.Α.Ε. εντός μηνός από τη δημοσίευση του παρόντος στην Εφημερίδα της Κυβερνήσεως.

Επίσης στην ίδια Αρχή γνωστοποιείται και κάθε αλλαγή που επέρχεται ως προς τα πρόσωπα αυτά.

9. Οι πάροχοι υποχρεούνται:
   α. Να παρέχουν στις αρμόδιες αρχές μία ή περισσότερες διεπαφές από τις οποίες ζητούμενα στοιχεία επικοινωνίας θα μπορούν να διαβιβαστούν στις εγκαταστάσεις παρακολούθησης.
   β. Να διαβιβάζουν στις αρμόδιες αρχές το περιεχόμενο της επικοινωνίας και τα στοιχεία της κατά το χρόνο πού αυτή διεξάγεται καθ' όλο το εικοσιτετράωρο.
   γ. Να παρέχουν πληροφορίες ή και βοήθεια στις αρμόδιες αρχές προκειμένου αυτές να βεβαιωθούν ότι τα στοιχεία επικοινωνίας που φτάνουν στην διεπαφή διασύνδεσης είναι αυτά πού συνδέονται με το στόχο.
   δ. Να διατηρούν την αξιοπιστία του συστήματος διασύνδεσης σε τουλάχιστον εφάμιλλο επίπεδο αξιοπιστίας με αυτό τον παρεχομένων υπηρεσιών στο συνδρομητή ή χρήστη.

Άρθρο 9
Έναρξη ισχύος.

Η ισχύς του παρόντος αρχίζει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως. Στον Υπουργό Δημόσιας Τάξης αναθέτουμε τη δημοσίευση και εκτέλεση του παρόντος Διατάγματος.