Μαρούσι, 23 Φεβρουαρίου 2009

ΑΠΟΦΑΣΗ

(αριθμ.: 53 /2009)

Θέμα: «Σύσταση για τη Διασφάλιση του Απορρήτου των Επικοινωνιών από τις Αρμόδιες Αρχές κατά τη Λειτουργία του Συστήματος Άρσης Απορρήτου σε πραγματικό χρόνο».

Την Τετάρτη, 14 Ιανουαρίου 2009 και ώρα 10.30 π.μ συνήλθε σε συνεδρίαση η Ολομέλεια της Α.Δ.Α.Ε., παρισταμένου του Πρόεδρου κ. Α. Λαμπρινόπουλου, του Αντιπροέδρου κ. Μ. Καρατζά και των τακτικών μελών κ.κ. Σ.Κάτσικα, Χ.Καψάλη, Ι.Βενιέρη, Κ.Μαραβέλα και Σ.Σκοπετέα.

Έχοντας υπόψη το άρθρο 19 του Συντάγματος, το Ν.3115/2003 («Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών», ΦΕΚ Β' 47/27.02.2003) και ιδίως τα άρθρα 1 παρ.1 και 6 παρ.1 περ.ι' του νόμου αυτού, το Π.Δ. 47/05 («Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του», ΦΕΚ Α' 64/10-3-05) και το πρακτικό της συνεδρίασης της Ολομέλειας της Αρχής της 01.10.2008, η Ολομέλεια της Α.Δ.Α.Ε. αποφάσισε την έγκριση της ακόλουθης «Σύστασης για τη Διασφάλιση του Απορρήτου των Επικοινωνιών από τις Αρμόδιες Αρχές κατά τη Λειτουργία του Συστήματος Άρσης Απορρήτου σε πραγματικό χρόνο»:

1 Σκοπός – Πεδίο Εφαρμογής

Σκοπός της παρούσας είναι η καταγραφή των μέτρων που συνιστάται να εφαρμόζουν οι Αρμόδιες Αρχές για τη διασφάλιση του απορρήτου κατά τη λειτουργία, διαχείριση και χρήση του συστήματος άρσης απορρήτου των επικοινωνιών σε πραγματικό χρόνο.

2 Ορισμοί

Για τους σκοπούς της παρούσας, ισχύουν οι ορισμοί του Π.Δ.47/05 «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του» (ΦΕΚ Α' 64/10-3-05).

Επίσης, νοούνται ως:

σύστημα άρσης απορρήτου: το σύνολο του εξοπλισμού της Αρμόδιας Αρχής, συμπεριλαμβανομένου του τερματικού εξοπλισμού, που αποτελείται από υλικό (hardware) και λογισμικό (software) και παρέχει τη δυνατότητα συλλογής, αποθήκευσης, διαχείρισης και ελέγχου των δεδομένων που σχετίζονται με τα αιτήματα άρσης απορρήτου σε πραγματικό χρόνο.

εγκαταστάσεις συστήματος άρσης απορρήτου: χώροι ελεγχόμενοι από την Αρμόδια Αρχή, στους οποίους είναι εγκατεστημένο το σύστημα άρσης απορρήτου ή μέρος αυτού.

τερματικός εξοπλισμός συστήματος άρσης απορρήτου: εξοπλισμός, ο οποίος είναι εγκατεστημένος αποκλειστικά εντός των εγκαταστάσεων του συστήματος άρσης απορρήτου και χρησιμοποιείται για την εκτέλεση λειτουργίας του συστήματος άρσης απορρήτου.

περιστατικό ασφάλειας: κάθε απειλή, επίθεση, αδυναμία ή δυσλειτουργία που εν δυνάμει έχει επιπτώσεις στην ασφάλεια του συστήματος άρσης απορρήτου.

αντίγραφα ασφάλειας: αντίγραφα ηλεκτρονικών αρχείων, τα οποία αποθηκεύονται για την ανάκτηση των πρωτοτύπων αρχείων σε περίπτωση καταστροφής ή αλλοίωσής τους.

ομάδα άρσης απορρήτου: το προσωπικό της Αρμόδιας Αρχής, στο οποίο έχει ανατεθεί η λειτουργία, ο έλεγχος, η χρήση, η ασφάλεια και η διαχείριση του συστήματος άρσης απορρήτου.

3 Πολιτική Διασφάλισης Απορρήτου κατά τη Λειτουργία, Διαχείριση και Χρήση του Συστήματος Άρσης Απορρήτου

3.1 Ορισμός – Γενικές απαιτήσεις

1. Η Πολιτική Διασφάλισης του Απορρήτου κατά τη λειτουργία, διαχείριση και χρήση του Συστήματος Άρσης Απορρήτου (στο εξής Πολιτική Διασφάλισης του Απορρήτου) είναι το σύνολο των κανόνων και κριτηρίων που διέπουν τη λειτουργία , διαχείριση και χρήση του συστήματος άρσης απορρήτου των Αρμοδίων Αρχών, με σκοπό τη διασφάλιση του απορρήτου κατά τη λειτουργία, διαχείριση και χρήση του συστήματος άρσης απορρήτου. Η Πολιτική Διασφάλισης του Απορρήτου καθορίζει με σαφήνεια τους ρόλους και τις αρμοδιότητες των μελών της ομάδας άρσης απορρήτου και εφαρμόζεται μέσω συγκεκριμένων διαδικασιών και κανόνων. Στην Πολιτική Διασφάλισης του Απορρήτου προβλέπεται η χρήση των απαραίτητων μηχανισμών ασφάλειας, καθώς και η τήρηση, όπου

είναι απαραίτητο, των κατάλληλων αρχείων για την παρακολούθηση όλων των ενεργειών που σχετίζονται με το σύστημα άρσης του απορρήτου.

2. Η Πολιτική Διασφάλισης του Απορρήτου εκπονείται από τις Αρμόδιες Αρχές έχοντας υπόψη την παρούσα σύσταση και αποτελείται, κατ' ελάχιστον, από τις επιμέρους πολιτικές που ορίζονται στα κεφάλαια της παρούσας ενότητας.

3.2 Πολιτική Ασφάλειας Προσωπικού και Πολιτική Αποδεκτής Χρήσης

1. Τα μέλη της ομάδας άρσης απορρήτου έχουν συγκεκριμένους, διακριτούς και σαφώς προσδιορισμένους ρόλους. Συνιστάται να ορίζονται οι παρακάτω διακριτοί ρόλοι:

(α) «Επικεφαλής ομάδας άρσης απορρήτου»: πρόσωπο στο οποίο ανατίθεται συνολικά η ορθή λειτουργία του συστήματος άρσης απορρήτου, συμπεριλαμβανομένου του ελέγχου λειτουργίας αυτού (audit), η εφαρμογή της Πολιτικής Διασφάλισης του Απορρήτου και η απονομή ρόλων στα υπόλοιπα μέλη της ομάδας άρσης απορρήτου. Στο ίδιο πρόσωπο είναι δυνατόν να ανατεθεί και ο ρόλος του ελεγκτή (auditor) της ορθής λειτουργίας του συστήματος άρσης απορρήτου και της εφαρμογής της Πολιτικής Διασφάλισης του Απορρήτου .

(β) «Χειριστής συστήματος άρσης απορρήτου»: πρόσωπο στο οποίο ανατίθεται η τεχνική διεκπεραίωση των αιτημάτων και των υπόλοιπων βασικών λειτουργιών του συστήματος άρσης απορρήτου και συνεπώς δύναται να αποκτά λογική πρόσβαση σε στοιχεία και περιεχόμενο επικοινωνίας στα οποία αναφέρονται οι διατάξεις άρσης απορρήτου.

(γ) «Διαχειριστής συστήματος άρσης απορρήτου»: πρόσωπο στο οποίο ανατίθεται η διαμόρφωση (configuration), συντήρηση (maintenance) και υποστήριξη (support) του συστήματος άρσης απορρήτου και των μέτρων ασφάλειας αυτού. Ο Διαχειριστής συστήματος άρσης απορρήτου δεν έχει πρόσβαση σε στοιχεία και περιεχόμενο επικοινωνίας στα οποία αναφέρονται οι διατάξεις άρσης απορρήτου.

2. Ο καθορισμός των δικαιωμάτων πρόσβασης των μελών της ομάδας άρσης απορρήτου στο σύστημα άρσης του απορρήτου βασίζεται στις ακόλουθες αρχές:

(α) αναγκαιότητα γνώσης ('need-to-know principle'): κάθε μέλος της ομάδας άρσης απορρήτου έχει δικαίωμα πρόσβασης μόνο σε πληροφορίες που είναι απαραίτητες για την εκτέλεση ενεργειών που προβλέπονται από το ρόλο του,

(β) ελάχιστα δικαιώματα ('least privilege principle'): κάθε μέλος της ομάδας άρσης απορρήτου έχει δικαίωμα πρόσβασης μόνο στα συστήματα στα οποία είναι απαραίτητο να έχει πρόσβαση για την εκτέλεση ενεργειών που προβλέπονται για το ρόλο του, και

(γ) διαχωρισμός ρόλων και επιπέδων εξουσιοδότησης ('segregation of duties and authorization level'): κανένα μέλος της ομάδας άρσης απορρήτου δεν κατέχει περισσότερους από έναν ρόλους ή επίπεδα εξουσιοδότησης.

3. Κάθε μέλος της ομάδας άρσης απορρήτου :

(α) τηρεί ως εμπιστευτική κάθε πληροφορία που σχετίζεται με το ρόλο του, τη συνολική λειτουργία της άρσης απορρήτου, καθώς και οποιαδήποτε πληροφορία ή στοιχείο υποπίπτει στην αντίληψή του ή την κατοχή του, ως αποτέλεσμα της φύσης της εργασίας του,

(β) είναι κατάλληλα και επαρκώς εκπαιδευμένο για τη διεκπεραίωση του ρόλου του, γνωρίζει τις διαδικασίες που εφαρμόζονται και σχετίζονται με τη διαδικασία άρσης του απορρήτου και τα σχετικά μέτρα ασφάλειας,

(γ) είναι ενημερωμένο ως προς τις νομικές, τεχνικές και άλλες υποχρεώσεις και ευθύνες που απορρέουν από το ρόλο του.

3.3 Πολιτική Φυσικής Ασφάλειας

1. Η Αρμόδια Αρχή διαθέτει και εφαρμόζει την Πολιτική Φυσικής Ασφάλειας στους χώρους εγκατάστασης και λειτουργίας του συστήματος άρσης απορρήτου.

2. Η Πολιτική Φυσικής Ασφάλειας καθορίζει τα κατάλληλα μέτρα για την αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης στις εγκαταστάσεις του συστήματος άρσης απορρήτου, καθώς και τους μηχανισμούς ελεγχόμενης εισόδου, ώστε να διασφαλίζεται ότι η είσοδος επιτρέπεται μόνο στα εξουσιοδοτημένα άτομα .

3. Οι εγκαταστάσεις του συστήματος άρσης απορρήτου βρίσκονται σε διακριτούς χώρους, που προορίζονται αποκλειστικά για τη λειτουργία, διαχείριση και χρήση του συστήματος άρσης απορρήτου.

3.4 Πολιτική Λογικής Πρόσβασης

1. Το σύστημα άρσης απορρήτου έχει προκαθορισμένα σημεία λογικής πρόσβασης για κάθε τύπο λειτουργίας (χρήση, διαχείριση, έλεγχο), τα οποία είναι καταγεγραμμένα στην Πολιτική Λογικής Πρόσβασης.

2. Η λογική πρόσβαση στο σύστημα άρσης απορρήτου γίνεται με τρόπο ώστε να αναγνωρίζεται η ταυτότητα των μελών της ομάδας άρσης απορρήτου που αποκτούν πρόσβαση στο σύστημα με σκοπό την χρήση, τη διαχείριση και τον έλεγχο του συστήματος άρσης απορρήτου. Η χρήση του ίδιου μέσου πρόσβασης (π.χ. όνομα χρήστη και κωδικού πρόσβασης) από περισσότερους χρήστες δεν επιτρέπεται.

3. Η Πολιτική Λογικής Πρόσβασης καθορίζει κατ'ελάχιστον, και με τρόπο λεπτομερή και σαφή, τις ακόλουθες διαδικασίες:

(α) Διαδικασία διαχείρισης (προσθήκης/διαγραφής/τροποποίησης) χρηστών στο σύστημα άρσης απορρήτου. Η διαδικασία περιλαμβάνει την εξουσιοδότηση των χρηστών ανάλογα με το ρόλο που τους έχει ανατεθεί. Η διαδικασία προβλέπει τη διατήρηση των στοιχείων των χρηστών που έχουν ή είχαν πρόσβαση στο σύστημα για όλη τη διάρκεια ζωής του συστήματος.

(β) Διαδικασία ελέγχου της διαδικασίας διαχείρισης χρηστών. Ο επικεφαλής ομάδας άρσης απορρήτου σε συνεργασία με τον διαχειριστή συστήματος άρσης απορρήτου πραγματοποιούν περιοδικά έλεγχο με σκοπό την επαλήθευση της ορθής εφαρμογής της διαδικασίας διαχείρισης χρηστών.

4. Κάθε επιτυχής ή ανεπιτυχής προσπάθεια πρόσβασης στο σύστημα άρσης απορρήτου καταγράφεται (logged) σε ηλεκτρονικό αρχείο καταγραφής πρόσβασης, το οποίο διατηρείται καθ' όλη τη διάρκεια ζωής του συστήματος άρσης απορρήτου και περιλαμβάνει κατ' ελάχιστον τα ακόλουθα : (α) όνομα χρήστη, (β) ημερομηνία και ώρα πρόσβασης, (γ) σημείο λογικής πρόσβασης, και (δ) ένδειξη επιτυχούς ή ανεπιτυχούς πρόσβασης. Η Πολιτική Διασφάλισης του Απορρήτου περιγράφει τα κατάλληλα μέτρα για την εξασφάλιση της εμπιστευτικότητας και ακεραιότητας του ηλεκτρονικού αρχείου καταγραφής πρόσβασης.

5. Μετά από κάθε επιτυχή πρόσβαση στο σύστημα άρσης απορρήτου, ενεργοποιείται αυτόματα η καταγραφή των ενεργειών των μελών της ομάδας άρσης απορρήτου σε ηλεκτρονικό αρχείο καταγραφής εντολών, το οποίο διατηρείται καθ' όλη τη διάρκεια ζωής του συστήματος άρσης απορρήτου. Οι εντολές και ενέργειες που καταγράφονται σχετίζονται με τις διάφορες εφαρμογές χρήσης, διαχείρισης και ελέγχου του συστήματος άρσης απορρήτου, αλλά και του λειτουργικού συστήματος. Η Πολιτική Διασφάλισης του Απορρήτου περιγράφει τα κατάλληλα μέτρα για την εξασφάλιση της εμπιστευτικότητας και της ακεραιότητας του ηλεκτρονικού αρχείου καταγραφής εντολών.

3.5 Πολιτική Ασφάλειας Ηλεκτρονικών Αρχείων Καταγραφής (logfiles)

1. Η συλλογή, η αποθήκευση, ο έλεγχος, η διαχείριση και η διατήρηση όλων των απαραίτητων δεδομένων των ηλεκτρονικών αρχείων καταγραφής εντολών και προσβάσεων πραγματοποιείται με τέτοιο τρόπο ώστε να εξασφαλίζεται η αυθεντικότητα, η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητά τους καθ'όλη τη διάρκεια ζωής του συστήματος άρσης απορρήτου, ακολουθώντας τη διαδικασία που έχει οριστεί για το σκοπό αυτό.

2. Η δυνατότητα του συστήματος άρσης απορρήτου (συμπεριλαμβανομένου του λειτουργικού συστήματος) για την απενεργοποίηση του ηλεκτρονικού αρχείου καταγραφής χρησιμοποιείται μόνο σε περιπτώσεις που κρίνεται απολύτως απαραίτητο και υπό την προϋπόθεση ότι: α) η αιτία απενεργοποίησης καταγράφεται β) έχει εξασφαλιστεί η έγγραφη εξουσιοδότηση του επικεφαλής της ομάδας άρσης απορρήτου και γ) καταγράφεται το όνομα χρήστη, η ημερομηνία και η ώρα της απενεργοποίησης.

3. Σε περίπτωση που η συλλογή, η αποθήκευση, ο έλεγχος, η διαχείριση και η διατήρηση των δεδομένων των ηλεκτρονικών αρχείων καταγραφής εντολών και προσβάσεων εμφανίζει λειτουργικά προβλήματα, εφαρμόζονται τα προβλεπόμενα στο Κεφάλαιο 3.7 της παρούσας.

3.6 Πολιτική Ασφάλειας κατά την Ανάπτυξη, Συντήρηση και Υποστήριξη του Συστήματος Άρσης Απορρήτου.

1. Η Πολιτική Ασφάλειας κατά την Ανάπτυξη, Συντήρηση και Υποστήριξη του Συστήματος Άρσης Απορρήτου εξασφαλίζει ότι οι εργασίες ανάπτυξης, συντήρησης και υποστήριξης στον υπάρχοντα εξοπλισμό καθώς και η εισαγωγή καινούριου εξοπλισμού γίνεται κατά τέτοιο τρόπο ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών και να μην παραβιάζεται η Πολιτική Διασφάλισης του Απορρήτου.

2. Η Πολιτική Ασφάλειας κατά την Ανάπτυξη, Συντήρηση και Υποστήριξη του Συστήματος Άρσης Απορρήτου περιλαμβάνει, κατ'ελάχιστον, διαδικασίες οι οποίες αφορούν: (α) τη δοκιμή και την εγκατάσταση νέου εξοπλισμού, (β) την καταγραφή των αλλαγών που πραγματοποιούνται σε υπάρχοντα εξοπλισμό, (γ) τη διαχείριση και τη διαμόρφωση του εξοπλισμού, και (δ) την εξουσιοδότηση και τον έλεγχο τρίτων (π.χ. εξωτερικών συνεργατών, προμηθευτών) που ενδεχομένως εμπλέκονται στις εργασίες ανάπτυξης, συντήρησης και υποστήριξης του συστήματος άρσης απορρήτου.

3. Κατά τη διαδικασία απεγκατάστασης ή απενεργοποίησης εξοπλισμού ή λογισμικού που σχετίζεται με το σύστημα άρσης απορρήτου, η Αρμόδια Αρχή λαμβάνει τα κατάλληλα μέτρα ώστε να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση στην πληροφορία που έχει εγγραφεί στον εν λόγω εξοπλισμό ή λογισμικό (π.χ. σε μνήμες, δίσκους, βάσεις δεδομένων, κτλ).

3.7 Διαδικασία Χειρισμού Περιστατικών Ασφάλειας

1. Για τον χειρισμό των περιστατικών ασφάλειας ακολουθείται η σχετική διαδικασία που διαμορφώνει η κάθε Αρμόδια Αρχή**.**

2. Ως ομάδα άμεσου χειρισμού των περιστατικών που σχετίζονται με το σύστημα άρσης απορρήτου ορίζεται η ομάδα άρσης απορρήτου. Τα περιστατικά ασφάλειας που αφορούν το σύστημα άρσης απορρήτου αξιολογούνται ως κρίσιμα, καταγράφονται σε ειδική έκθεση και αναφέρονται στον επικεφαλής της ομάδας άρσης απορρήτου.

3.8 Πολιτική Εσωτερικού Ελέγχου Διασφάλισης Απορρήτου κατά τη χρήση του Συστήματος Άρσης του Απορρήτου

1. Ο επικεφαλής της ομάδας άρσης απορρήτου πραγματοποιεί εσωτερικούς περιοδικούς ελέγχους σχετικούς με τη διασφάλιση του απορρήτου κατά τη λειτουργία του συστήματος άρσης του απορρήτου. Οι εσωτερικοί έλεγχοι αναφέρονται ρητά στην Πολιτική Διασφάλισης του Απορρήτου, ενώ η σχετική διαδικασία (μεθοδολογία, περιοδικότητα, αναφορά αποτελεσμάτων) των ελέγχων καθορίζεται από κοινού με τον διαχειριστή συστημάτων άρσης απορρήτου.

2. Οι εσωτερικοί έλεγχοι πραγματοποιούνται κατ' ελάχιστον σε ετήσια βάση, ενώ τα αποτελέσματα των ελέγχων καταγράφονται σε ειδική αναφορά (Αναφορά Εσωτερικού Ελέγχου).

3.9 Πολιτική Ασφάλειας Εσωτερικού Δικτύου Συστήματος Άρσης Απορρήτου

1. Η Πολιτική Ασφάλειας Εσωτερικού Δικτύου Συστήματος Άρσης Απορρήτου περιγράφει αναλυτικά τα μέτρα ασφάλειας που εφαρμόζει η Αρμόδια Αρχή για την προστασία του εσωτερικού δικτύου του συστήματος άρσης απορρήτου και την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε αυτό.

2. Το εσωτερικό δίκτυο του συστήματος άρσης απορρήτου αποτελεί διακριτό υποδίκτυο (διακριτή ζώνη) του εσωτερικού δικτύου της Αρμόδιας Αρχής και δεν επικοινωνεί με οποιονδήποτε τρόπο με άλλα υποδίκτυα (ζώνες) ή με το Διαδίκτυο. Επιτρέπεται μόνο η διασύνδεσή του με το δίκτυο των παρόχων για τη διαβίβαση των στοιχείων και του περιεχομένου επικοινωνίας, στο πλαίσιο εκτέλεσης των διατάξεων άρσης απορρήτου, σύμφωνα με την κείμενη νομοθεσία.

3. Σε φυσικό επίπεδο, το εσωτερικό δίκτυο του συστήματος άρσης απορρήτου είναι δυνατόν να εκτείνεται σε περισσότερα του ενός απομακρυσμένα σημεία. Στην περίπτωση αυτή, η διασύνδεση επιτυγχάνεται μέσα από δικτυακή υποδομή, με τη χρήση ισχυρών μεθόδων κρυπτογράφησης.

3.10 Πολιτική Ασφάλειας των αποθηκευμένων στοιχείων και περιεχομένου επικοινωνίας

1. Το περιεχόμενο και τα στοιχεία επικοινωνίας που διαβιβάζονται από τους παρόχους στις Αρμόδιες Αρχές, αποθηκεύονται με ασφάλεια στα συστήματα των Αρχών. Προς τούτο, χρησιμοποιούνται τεχνικές κρυπτογράφησης με ευρέως αποδεκτούς και προτυποποιημένους αλγορίθμους. Η διαχείριση των κλειδιών κρυπτογράφησης κατά τη δημιουργία, χρήση, αποθήκευση και καταστροφή αυτών γίνεται με ασφάλεια, ενώ το μήκος των κλειδιών πρέπει να παρέχει επαρκή ασφάλεια από τις γνωστές απειλές.

Ο Πρόεδρος

Ανδρέας Λαμπρινόπουλος