Μαρούσι, 23 Φεβρουαρίου 2009

ΑΠΟΦΑΣΗ

(αριθμ.: 52 /2009)

Θέμα: «Σύσταση για τη Διασφάλιση του Απορρήτου των Επικοινωνιών από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών 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 τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών 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 πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών 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 του παρόχου (εξαιρουμένων των ενεργών στοιχείων δικτύου), αποτελούμενο από υλικό (hardware) και λογισμικό (software), το οποίο παρέχει τη δυνατότητα συλλογής, χειρισμού, διαχείρισης, ελέγχου και διαβίβασης δεδομένων προς την Αρμόδια Αρχή για τη διεκπεραίωση αιτημάτων άρσης απορρήτου σε πραγματικό χρόνο. Στο σύστημα άρσης απορρήτου περιλαμβάνεται ο τερματικός εξοπλισμός, ο εξυπηρετητής ηλεκτρονικών αρχείων καταγραφής, ο εξυπηρετητής αντιγράφων ασφαλείας, κλπ.

ενεργό στοιχείο δικτύου ή ενεργός εξοπλισμός δικτύου: εξοπλισμός αποτελούμενος από υλικό (hardware) και λογισμικό (software), ο οποίος εκτελεί λειτουργίες υπηρεσιών ηλεκτρονικών επικοινωνιών. Το σύστημα άρσης απορρήτου διαθέτει κατάλληλες διεπαφές προς/από τον ενεργό εξοπλισμό ώστε να συλλέγει στοιχεία σχετικά με τις άρσεις απορρήτου {ενδεικτικά αναφέρονται ψηφιακά κέντρα μεταγωγής (MSC, GMSC), δρομολογητές (routers), εξυπηρετητές (AAA server, proxies), κλπ}.

εγκαταστάσεις συστήματος άρσης απορρήτου: χώροι ελεγχόμενοι από τον πάροχο, 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 του παρόχου, στο οποίο έχει ανατεθεί η λειτουργία, ο έλεγχος, η χρήση, η ασφάλεια και η διαχείριση του συστήματος άρσης απορρήτου.

3 Μέτρα Ασφάλειας για τη Διασφάλιση του Απορρήτου κατά τη Λειτουργία, Διαχείριση και Χρήση του Συστήματος Άρσης Απορρήτου.

3.1. Μέτρα ως προς το Προσωπικό

1. Ο αριθμός των μελών της ομάδας άρσης απορρήτου είναι ο ελάχιστος απαιτούμενος, προκειμένου να εξασφαλίζεται η ορθή και απρόσκοπτη λειτουργία του συστήματος άρσης απορρήτου.

2. 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 και του ελέγχου λειτουργίας αυτού (audit), και η απονομή των λοιπών ρόλων στα μέλη της ομάδας άρσης απορρήτου. Ο «επικεφαλής ομάδας άρσης απορρήτου» και το προβλεπόμενο στο άρθρο 8 του Π.Δ.47/2005 «εξουσιοδοτημένο πρόσωπο» συνιστάται να είναι το ίδιο πρόσωπο.

(β) «Χειριστής συστήματος άρσης απορρήτου»: πρόσωπο στο οποίο ανατίθεται η τεχνική διεκπεραίωση των αιτημάτων και των υπόλοιπων βασικών λειτουργιών του συστήματος άρσης απορρήτου, όπως η έναρξη (initiation), η τροποποίηση (modification) και ο τερματισμός (termination) εκτέλεσης μίας διάταξης 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.

(δ) «Διαχειριστής εξυπηρετητή ηλεκτρονικών αρχείων καταγραφής»: πρόσωπο στο οποίο ανατίθεται η διαμόρφωση (configuration), συντήρηση (maintenance) και υποστήριξη (support) του εξυπηρετητή ηλεκτρονικών αρχείων καταγραφής και των μέτρων ασφάλειας αυτού.

3. 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.

4. Η εξουσιοδότηση και τα δικαιώματα πρόσβασης στο σύστημα άρσης απορρήτου δίνονται στα μέλη της ομάδας άρσης απορρήτου σύμφωνα με το ρόλο που έχει ανατεθεί σε έκαστο εξ αυτών. Ο επικεφαλής ομάδας άρσης απορρήτου και ο διαχειριστής συστήματος άρσης απορρήτου ορίζουν από κοινού τα επίπεδα εξουσιοδότησης και τα δικαιώματα πρόσβασης που αντιστοιχούν σε κάθε ρόλο, και περιοδικά τα ελέγχουν και τα αναθεωρούν.

5. Κάθε μέλος της ομάδας άρσης απορρήτου :

(α) ασκεί τα καθήκοντά του βάσει ρητής και ειδικής εξουσιοδότησης,

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

(γ) είναι κατάλληλα και επαρκώς εκπαιδευμένο για τη διεκπεραίωση του ρόλου του, γνωρίζει τις διαδικασίες που εφαρμόζονται στον πάροχο υπηρεσιών ηλεκτρονικών επικοινωνιών και σχετίζονται με τη διαδικασία άρσης του απορρήτου και τα σχετικά μέτρα ασφάλειας,

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

6. Τα μέλη της ομάδας άρσης απορρήτου, πριν την ανάληψη των καθηκόντων τους, υπογράφουν Συμφωνητικό Αρμοδιοτήτων και Εμπιστευτικότητας, στο οποίο περιέχονται κατ' ελάχιστον τα προβλεπόμενα στην προηγούμενη παράγραφο.

7. Η ταυτότητα των μελών της ομάδας άρσης απορρήτου, πλην του επικεφαλής ομάδας άρσης απορρήτου, καθώς και ο ρόλος τους, αποτελεί εμπιστευτική πληροφορία.

3.2. Φυσική Ασφάλεια

Οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών λαμβάνουν τα κατάλληλα μέτρα για την αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης στις εγκαταστάσεις του συστήματος άρσης απορρήτου. Ειδικότερα:

1. Οι εγκαταστάσεις του συστήματος άρσης απορρήτου είναι καταγεγραμμένες και περιορίζονται στον ελάχιστο δυνατό αριθμό χώρων.

2. Η κατασκευή των χώρων αποκλείει τη μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, οι χώροι προστατεύονται με συστήματα άμεσης ανίχνευσης μη εξουσιοδοτημένης πρόσβασης (όπως συστήματα συναγερμού) καθώς και με σύστημα κλειστού κυκλώματος τηλεόρασης, τηρουμένης της κείμενης νομοθεσίας.

3. Ο πάροχος θέτει σε λειτουργία μηχανισμό ελέγχου της πρόσβασης, προκειμένου αυτή να επιτρέπεται μόνο στα μέλη της ομάδας άρσης του απορρήτου. Η πρόσβαση είναι δυνατή μόνο μετά από την επιτυχή επιβεβαίωση της ταυτότητας του εξουσιοδοτημένου μέλους της ομάδας άρσης απορρήτου.

4. Η πρόσβαση στις εγκαταστάσεις του συστήματος άρσης απορρήτου σε άτομο που δεν ανήκει στην ομάδα άρσης απορρήτου του παρόχου επιτρέπεται μόνο κατόπιν σχετικής άδειας του επικεφαλής της ομάδας άρσης απορρήτου. Στην άδεια πρόσβασης καταγράφονται: α) ο λόγος για τον οποίο παρέχεται άδεια πρόσβασης (π.χ. εργασίες συντήρησης εξοπλισμού, αναβάθμιση του λογισμικού, κ.τλ.), β) το ονοματεπώνυμο του ατόμου στο οποίο δίδεται η άδεια πρόσβασης, γ) η ιδιότητα του ατόμου στο οποίο δίδεται η άδεια πρόσβασης και δ) το χρονικό διάστημα ισχύος της άδειας πρόσβασης. Η παραμονή ατόμου που δεν ανήκει στην

ομάδα άρσης απορρήτου του παρόχου σε εγκαταστάσεις του συστήματος άρσης απορρήτου γίνεται υπό την επίβλεψη μέλους της ομάδας άρσης απορρήτου.

5. Ο πάροχος διατηρεί, καθ' όλη τη διάρκεια ζωής του συστήματος άρσης απορρήτου, ηλεκτρονικό αρχείο καταγραφής α) των προσβάσεων των εξουσιοδοτημένων μελών της ομάδας άρσης του απορρήτου, β) των προσβάσεων των ατόμων που έχουν λάβει σχετική άδεια σύμφωνα με την προηγούμενη παράγραφο και γ) των ανεπιτυχών προσπαθειών πρόσβασης. Για κάθε επιτυχημένη πρόσβαση, το αρχείο περιέχει, κατ' ελάχιστον, την ημερομηνία, την ώρα εισόδου και εξόδου καθώς και το ονοματεπώνυμο του ατόμου που εισήλθε στο χώρο. Για τις ανεπιτυχείς προσβάσεις, το αρχείο περιέχει την ημερομηνία, την ώρα και το ονοματεπώνυμο του ατόμου που προσπάθησε να εισέλθει στο χώρο.

6. Ο πάροχος διατηρεί, καθ' όλη τη διάρκεια ζωής του συστήματος άρσης απορρήτου, σε ηλεκτρονικό αρχείο τα στοιχεία των ατόμων που έχουν δικαίωμα φυσικής πρόσβασης στις εγκαταστάσεις του συστήματος άρσης απορρήτου, την έκταση του δικαιώματος πρόσβασης εκάστου εξ αυτών και ιστορικό των δικαιωμάτων πρόσβασης που έχουν δοθεί από την έναρξη λειτουργίας του συστήματος.

7. Η συλλογή, η αποθήκευση, ο έλεγχος, η διαχείριση και η διατήρηση όλων των δεδομένων που περιέχονται στα ηλεκτρονικά αρχεία, 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, σύμφωνα με τη διαδικασία που έχει οριστεί για το σκοπό αυτό.

3.3. Ασφάλεια Λογικής Πρόσβασης

1. Το σύστημα άρσης απορρήτου έχει προκαθορισμένα και καταγεγραμμένα σημεία λογικής πρόσβασης για κάθε τύπο λειτουργίας (χρήση, διαχείριση, έλεγχο).

2. Η πρόσβαση των μελών της ομάδας άρσης απορρήτου στο σύστημα άρσης απορρήτου πραγματοποιείται με χρήση αντίστοιχου «λογαριασμού» (δηλαδή, ζεύγους ονόματος χρήστη και κωδικού πρόσβασης), ο οποίος δημιουργείται αποκλειστικά για έκαστο μέλος της ομάδας άρσης απορρήτου, και χρήση συσκευής ασφαλούς αυθεντικοποίησης (π.χ. USB token). Τα μέλη της ομάδας άρσης απορρήτου διαφυλάττουν και φροντίζουν για την ορθή χρήση των μέσων πρόσβασης που τους έχουν δοθεί. Το μέσο λογικής πρόσβασης έκαστου μέλους της ομάδας άρσης του απορρήτου προορίζεται για αποκλειστική χρήση από αυτό και δεν επιτρέπεται η χρήση του από άλλο μέλος της ίδιας ομάδας, ακόμα και αν έχουν τον ίδιο ρόλο και δικαιώματα.

3. Ο επικεφαλής ομάδας άρσης απορρήτου διατηρεί ενημερωμένο ιστορικό (κατά προτίμηση σε ηλεκτρονικό αρχείο) το οποίο περιέχει τις πληροφορίες αναφορικά με τους λογαριασμούς πρόσβασης (ονόματα χρήστη, ταυτότητα χρηστών, σχετικές ημερομηνίες δημιουργίας και κατάργησης λογαριασμών κ.ά.) για όλη τη διάρκεια ζωής του συστήματος άρσης απορρήτου. Σχετικά με το αρχείο αυτό ισχύει η απαίτηση της παραγράφου 1 του Κεφαλαίου 3.4 της παρούσας σύστασης.

4. Συνιστάται να ορίζεται ο μέγιστος αριθμός ανεπιτυχών προσπαθειών λογικής πρόσβασης στο σύστημα άρσης του απορρήτου, πέραν του οποίου εκκινεί η διαδικασία χειρισμού περιστατικών ασφάλειας, σύμφωνα με το Κεφάλαιο 3.6 της παρούσας σύστασης.

5. Κάθε επιτυχής ή ανεπιτυχής προσπάθεια λογικής πρόσβασης στο σύστημα άρσης απορρήτου καταγράφεται (logged) σε *ηλεκτρονικό αρχείο καταγραφής πρόσβασης*. Το αρχείο αυτό περιλαμβάνει κατ' ελάχιστο: (α) όνομα χρήστη, (β) ημερομηνία και ώρα προσπάθειας πρόσβασης, (γ) σημείο λογικής πρόσβασης, και (δ) ένδειξη επιτυχούς ή ανεπιτυχούς πρόσβασης. Για το εν λόγω αρχείο ισχύουν τα προβλεπόμενα στο Κεφάλαιο 3.4 της παρούσας σύστασης. Ο επικεφαλής της ομάδας άρσης απορρήτου ελέγχει περιοδικά το περιεχόμενο του εν λόγω αρχείου, σύμφωνα με το Κεφάλαιο 3.7 της παρούσας σύστασης.

6. Μετά από κάθε επιτυχή πρόσβαση στο σύστημα άρσης απορρήτου, ενεργοποιείται αυτόματα η καταγραφή των ενεργειών στο σύστημα άρσης απορρήτου σε *ηλεκτρονικό αρχείο καταγραφής εντολών*. Οι εντολές και ενέργειες που καταγράφονται σχετίζονται με τις διάφορες εφαρμογές χρήσης, διαχείρισης, και ελέγχου του συστήματος άρσης απορρήτου, αλλά και του λειτουργικού συστήματος. Για το εν λόγω αρχείο ισχύουν τα προβλεπόμενα στο Κεφάλαιο 3.4 της παρούσας σύστασης. Ο επικεφαλής ομάδας άρσης απορρήτου ελέγχει περιοδικά το περιεχόμενο του εν λόγω αρχείου, σύμφωνα με το Κεφάλαιο 3.7 της παρούσας σύστασης.

7. Προ της πρόσβασης στο σύστημα άρσης απορρήτου, στην οθόνη του χρησιμοποιούμενου τερματικού εξοπλισμού του συστήματος άρσης απορρήτου εμφανίζεται προειδοποιητικό μήνυμα που ενημερώνει τον χρήστη ότι η πρόσβαση επιτρέπεται μόνο στα εξουσιοδοτημένα προς τούτο μέλη της ομάδας άρσης του απορρήτου, σύμφωνα με τους όρους του σχετικού Συμφωνητικού Αρμοδιοτήτων και Εμπιστευτικότητας και ότι οι ενέργειες όλων των χρηστών του συστήματος άρσης απορρήτου καταγράφονται και ελέγχονται. Η πρόσβαση επιτρέπεται μόνο εφόσον ο χρήστης αποδεχθεί το μήνυμα.

8. Ο τερματικός εξοπλισμός του συστήματος άρσης απορρήτου, ο οποίος επιτρέπει την πρόσβαση στο σύστημα άρσης απορρήτου, διασυνδέεται μόνο με το σύστημα άρσης απορρήτου και όχι με άλλα συστήματα ή δίκτυα (π.χ. το Διαδίκτυο), κάθε δε περίπτωση διασύνδεσης επιτυγχάνεται μέσα από δικτυακή υποδομή του παρόχου, αποκλειστικής χρήσης.

9. Το μέλος της ομάδας άρσης απορρήτου που έχει πρόσβαση στο σύστημα άρσης του απορρήτου, τερματίζει την χρησιμοποιούμενη εφαρμογή προ της απομάκρυνσής του από τον τερματικό εξοπλισμό του συστήματος άρσης απορρήτου. Ο τερματικός εξοπλισμός του συστήματος άρσης απορρήτου θα πρέπει να τερματίζει αυτόματα την χρησιμοποιούμενη εφαρμογή στην περίπτωση που μείνει ανενεργός για περισσότερο από ένα προκαθορισμένο χρονικό όριο.

3.4. Ασφάλεια Ηλεκτρονικών Αρχείων Καταγραφής εντολών και λογικών προσβάσεων (logfiles)

1. Η συλλογή, η αποθήκευση, ο έλεγχος, η διαχείριση και η διατήρηση όλων των δεδομένων που περιέχονται στα ηλεκτρονικά αρχεία 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, σύμφωνα με τη διαδικασία που έχει οριστεί για το σκοπό αυτό.

2. Τα ηλεκτρονικά αρχεία καταγραφής εντολών και προσβάσεων αποθηκεύονται σε έναν εξυπηρετητή ηλεκτρονικών αρχείων καταγραφής (log server), που χρησιμοποιείται αποκλειστικά για τον σκοπό αυτό.

3. Η καταγραφή εντολών και προσβάσεων στα ηλεκτρονικά αρχεία είναι: α) πλήρης, σύμφωνα με τα προβλεπόμενα στην παρούσα σύσταση, β) συνεχής, γ) πραγματοποιείται σε πραγματικό χρόνο με μικρές αποκλίσεις και δ) πραγματοποιείται ούτως ώστε να μην υπάρχουν διακοπές στη λειτουργία του συστήματος άρσης απορρήτου.

4. Η δυνατότητα του συστήματος άρσης απορρήτου (συμπεριλαμβανόμενου του λειτουργικού συστήματος) για την απενεργοποίηση του ηλεκτρονικού αρχείου καταγραφής εντολών και προσβάσεων στο σύστημα άρσης του απορρήτου χρησιμοποιείται μόνο σε περιπτώσεις που είναι 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.

5. Τα ηλεκτρονικά αρχεία καταγραφής εντολών και προσβάσεων στο σύστημα άρσης του απορρήτου κρυπτογραφούνται κατά τρόπο ώστε να διασφαλίζεται η εμπιστευτικότητά τους. Ο αλγόριθμος κρυπτογράφησης που θα επιλεγεί πρέπει να είναι ευρέως αποδεκτός και προτυποποιημένος. Το μήκος των κλειδιών κρυπτογράφησης πρέπει να παρέχει επαρκή ασφάλεια από όλες τις γνωστές απειλές. Η διαχείριση των κλειδιών κρυπτογράφησης κατά τη δημιουργία, χρήση, αποθήκευση και καταστροφή αυτών πρέπει να πραγματοποιείται με ασφάλεια, σύμφωνα με τα διεθνή πρότυπα.

6. Για τη διασφάλιση της ακεραιότητας των δεδομένων που περιέχουν τα ηλεκτρονικά αρχεία καταγραφής εντολών και προσβάσεων στο σύστημα άρσης του απορρήτου, αφού κρυπτογραφηθούν σύμφωνα με την προηγούμενη παράγραφο, υπογράφονται με τη χρήση κοινά αποδεκτών μεθόδων ηλεκτρονικών υπογραφών και τα αποτελέσματα της επιβεβαίωσης καταγράφονται σε ένα μέσο WORM (Write Once, Read Many).

7. Για λόγους διαθεσιμότητας των ηλεκτρονικών αρχείων καταγραφής εντολών και προσβάσεων στο σύστημα άρσης του απορρήτου, ο πάροχος διατηρεί αντίγραφα ασφάλειας σε έναν εξυπηρετητή αντιγράφων ασφαλείας (backup server).

8. Η αποθήκευση μαγνητικών ή άλλων μέσων που περιέχουν ηλεκτρονικά αρχεία καταγραφής εντολών και προσβάσεων στο σύστημα άρσης του απορρήτου ή αρχεία

αποτελεσμάτων επιβεβαίωσης ηλεκτρονικής υπογραφής, πραγματοποιείται σε χώρο που εξασφαλίζει το ίδιο ή υψηλότερο επίπεδο ασφάλειας σε σχέση με τις υπόλοιπες εγκαταστάσεις του συστήματος άρσης απορρήτου.

9. Σε περίπτωση δυσλειτουργίας του εξυπηρετητή ηλεκτρονικών αρχείων καταγραφής ή του εξυπηρετητή αντιγράφων ασφαλείας, ο πάροχος εφαρμόζει τα προβλεπόμενα στο κεφάλαιο 3.6 της παρούσας σύστασης.

3.5. Ασφάλεια κατά την Ανάπτυξη, Συντήρηση και Υποστήριξη του Συστήματος Άρσης Απορρήτου

1. Οι εργασίες ανάπτυξης, συντήρησης και υποστήριξης του συστήματος άρσης απορρήτου πραγματοποιούνται στις εγκαταστάσεις του συστήματος άρσης απορρήτου από μέλη της ομάδας άρσης απορρήτου ή από ειδικά προς τούτο εξουσιοδοτημένα πρόσωπα, που ανήκουν στο προσωπικό του προμηθευτή/κατασκευαστή του συστήματος άρσης απορρήτου, υπό την επίβλεψη μέλους της ομάδας άρσης απορρήτου. Ο επικεφαλής ομάδας άρσης απορρήτου παρέχει ειδική έγγραφη εξουσιοδότηση για όλες τις σχετικές εργασίες.

2. Ο διαχειριστής συστήματος άρσης απορρήτου διατηρεί κατάλογο, σε μορφή ηλεκτρονικού αρχείου, στον οποίο καταγράφεται ο εξοπλισμός του συστήματος άρσης απορρήτου (υλικό, λογισμικό και τρέχουσα έκδοση αυτών). Επιπρόσθετα, στο αρχείο αυτό καταγράφονται όλες οι μεταβολές που λαμβάνουν χώρα στο υλικό και λογισμικό του συστήματος άρσης απορρήτου και των ενεργών στοιχείων δικτύου αναφορικά με λειτουργίες άρσης απορρήτου, οι λόγοι μεταβολής και το εμπλεκόμενο προσωπικό. Σχετικά με το αρχείο αυτό ισχύουν τα προβλεπόμενα στην παράγραφο 1 του Κεφαλαίου 3.4 της παρούσας. Ο επικεφαλής της ομάδας άρσης απορρήτου ελέγχει περιοδικά το περιεχόμενο του εν λόγω αρχείου, σύμφωνα με το Κεφάλαιο 3.7. της παρούσας.

3. Το λογισμικό του συστήματος άρσης απορρήτου, συμπεριλαμβανόμενων των προγραμμάτων αναβάθμισης (updates, patches, κτλ), συνοδεύεται από τα κατάλληλα μέσα και μηχανισμούς για τη διασφάλιση της αυθεντικότητας και ακεραιότητάς του από τον προμηθευτή/κατασκευαστή. Ενδεικτικά αναφέρεται η ηλεκτρονική υπογραφή. Ο διαχειριστής συστήματος άρσης απορρήτου χρησιμοποιεί τα μέσα και τους μηχανισμούς αυτούς ώστε να ελέγχει την αυθεντικότητα και ακεραιότητα του λογισμικού.

4. Κατά τη διαδικασία απεγκατάστασης ή απενεργοποίησης εξοπλισμού ή λογισμικού που σχετίζεται με το σύστημα άρσης απορρήτου, ο πάροχος 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).

5. Τα προβλεπόμενα στο παρόν κεφάλαιο ισχύουν και σχετικά με την ανάπτυξη, συντήρηση και υποστήριξη των ενεργών στοιχείων δικτύου του παρόχου, αναφορικά με λειτουργίες άρσης απορρήτου.

3. 6. Χειρισμός Περιστατικών Ασφάλειας

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

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.

3.7. Εσωτερικός Έλεγχος 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 και η σχετική διαδικασία (μεθοδολογία, περιοδικότητα, αναφορά αποτελεσμάτων) των ελέγχων καθορίζονται από κοινού με τους διαχειριστές συστημάτων άρσης απορρήτου.

2. Ο εσωτερικός έλεγχος πραγματοποιείται κατ' ελάχιστον κάθε τετράμηνο, ενώ τα αποτελέσματα του ελέγχου καταγράφονται σε ειδική αναφορά (Αναφορά Εσωτερικού Ελέγχου).

3. Ειδικά σε σχέση με την ορθή χρήση του συστήματος άρσης απορρήτου, ο επικεφαλής της ομάδας άρσης απορρήτου ελέγχει τις ενέργειες τεχνικής διεκπεραίωσης των αιτημάτων άρσης απορρήτου που έχουν πραγματοποιηθεί από τους χειριστές συστήματος άρσης απορρήτου ευθύς αμέσως από την πραγματοποίησή τους. Σε περίπτωση που διαπιστωθεί κάποια ασυνέπεια (ενδεικτικά: λανθασμένη εισαγωγή αριθμού ή/και ημερομηνιών, εισαγωγή αριθμών που δεν περιέχονται σε διάταξη άρσης απορρήτου) εκκινεί άμεσα η Διαδικασία χειρισμού περιστατικών ασφάλειας, σύμφωνα με το Κεφάλαιο 3.6 της παρούσας.

3.8. Γενικές απαιτήσεις διασύνδεσης του συστήματος άρσης απορρήτου

1. Ο πάροχος λαμβάνει όλα τα απαραίτητα μέτρα ώστε κάθε πληροφορία σχετική με τη λειτουργία του συστήματος άρσης απορρήτου, η οποία αποθηκεύεται στα ενεργά στοιχεία του δικτύου ή διαβιβάζεται μέσω αυτών στο σύστημα άρσης απορρήτου, να είναι ορατή και προσβάσιμη μόνο από τα εξουσιοδοτημένα προς τούτο πρόσωπα. Εάν αυτό δεν είναι τεχνικά εφικτό, η αιτία καταγράφεται και ο πάροχος περιορίζει την πρόσβαση στον ελάχιστο δυνατό αριθμό ατόμων, των οποίων η πρόσβαση καταγράφεται, και τα αρχεία καταγραφής των αντίστοιχων ενεργειών αποθηκεύονται σύμφωνα με τα προβλεπόμενα στο κεφάλαιο 3.4 της παρούσας. Τα αρχεία αυτά υπόκεινται στους περιοδικούς εσωτερικούς ελέγχους που περιγράφονται στο κεφάλαιο 3.7 της παρούσας.

2. Η διαβίβαση των στοιχείων και του περιεχομένου της επικοινωνίας στις Αρμόδιες Αρχές πραγματοποιείται μόνο μέσω ασφαλών καναλιών, τα οποία ικανοποιούν τις βασικές απαιτήσεις ασφάλειας: εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity) και

αυθεντικοποίηση (authentication). Ειδικότερα, για την εξασφάλιση της εμπιστευτικότητας 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 παρέχει επαρκή ασφάλεια από τις γνωστές απειλές. Για την εξασφάλιση της ακεραιότητας χρησιμοποιούνται κοινά αποδεκτοί αλγόριθμοι δημιουργίας ψηφιακών υπογραφών. Για την εξασφάλιση της αμοιβαίας αυθεντικοποίησης (authentication) της ταυτότητας αποστολέα (Παρόχου) και παραλήπτη (Αρμόδιας Αρχής) χρησιμοποιούνται τεχνικές ασύμμετρης κρυπτογράφησης με ευρέως αποδεκτούς και προτυποποιημένους αλγορίθμους.

Ο Πρόεδρος

Ανδρέας Λαμπρινόπουλος