ΚΕΦΑΛΑΙΟ 4

Προγραμματισμός δράσης για το 2014

Για το 2014, η ΑΔΑΕ έχει προγραμματίσει να ασχοληθεί με τα ακόλουθα θέματα:

- Έκδοση Κανονισμού για την ασφαλή διαβίβαση των διατηρούμενων δεδομένων, σύμφωνα με το άρθρο 8, παρ. 2 του Ν. 3917/2011.
- Έλεγχος και έγκριση πολιτικών ασφάλειας των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και των ταχυδρομικών επιχειρήσεων, σύμφωνα με τους κανονισμούς της Αρχής. Εκτιμάται ότι μέσα στο 2014 οι υπηρεσίες της Αρχής θα έχουν ολοκληρώσει την επεξεργασία 30 πολιτικών ασφάλειας.
- Διενέργεια όσο το δυνατόν περισσότερων τακτικών και έκτακτων ελέγχων σε παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών, προκειμένου να διαπιστωθεί αν τηρούνται οι όροι που διασφαλίζουν το απόρρητο των επικοινωνιών, καθώς και την ασφάλεια και την ακεραιότητα δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών. Εκτιμάται ότι μέσα στο 2014 οι υπηρεσίες της Αρχής θα διενεργήσουν 26 τακτικούς και 25 έκτακτους ελέγχους.
- Διενέργεια ακροάσεων παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών που μπορεί να κληθούν λόγω ενδεχόμενης παράβασης της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών ή για παροχή πληροφοριών και διευκρίνιση στοιχείων.
- Ενημέρωση φορέων-παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών για θέματα σχετικά με τη λήψη μέτρων διασφάλισης του απορρήτου.
- Εξέταση καταγγελιών που αναφέρονται σε ζητήματα διασφάλισης ή άρσης του απορρήτου των επικοινωνιών. Εκτιμάται ότι μέσα στο 2014 οι υπηρεσίες της Αρχής θα έχουν ολοκληρώσει την επεξεργασία 68 καταγγελιών και 20 ερωτημάτων πολιτών.
- Παρακολούθηση και έλεγχο αν τηρείται η ορθή διαδικασία για την άρση του απορρήτου των επικοινωνιών, σύμφωνα με τα προβλεπόμενα στους Ν. 2225/1994, Ν. 3115/2003 και το ΠΔ 47/2005.
- Επιβολή κυρώσεων σε παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και σε ταχυδρομικές επιχειρήσεις που δεν έχουν συμμορφωθεί με τους κανονισμούς της Αρχής, καθώς και σε άτομα ή φορείς σε περιπτώσεις που διαπιστώνεται ότι δεν τηρείται η νομοθεσία περί απορρήτου των επικοινωνιών.
- Παρακολούθηση και συνεχή ενημέρωση τόσο των αρμόδιων αρχών όσο και των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών για την εγκατάσταση και τη λειτουργία των συστημάτων άρσης του απορρήτου.

- Συνεργασία με τις αρμόδιες αρχές και τις κρατικές υπηρεσίες, καθώς και με αντίστοιχους οργανισμούς άλλων κρατώνμελών της ΕΕ για την αντιμετώπιση προβλημάτων που αφορούν το απόρρητο και την ασφάλεια των επικοινωνιών.
- Συμμετοχή σε ημερίδες, συνέδρια και τεχνικές επιτροπές με αντικείμενο τη διασφάλιση του απορρήτου των επικοινωνιών.
- Υποβολή προτάσεων για νομοθετικές ρυθμίσεις που κρίνονται αναγκαίες για τη λειτουργία της Αρχής και την εκπλήρωση του θεσμικού της ρόλου.
- Εκπαίδευση του προσωπικού με έμφαση σε θέματα σχετικά με τις διαδικασίες και τους τρόπους διενέργειας ελέγχων, καθώς και με τη λειτουργία τηλεπικοινωνιακών συστημάτων.
- Ενημέρωση του κοινού για θέματα που σχετίζονται με την τήρηση του απορρήτου των επικοινωνιών και τη λήψη μέτρων αυτοπροστασίας των χρηστών.
- Σύνταξη και υποβολή σχεδίου προϋπολογισμού της Αρχής για το 2015.

Τεχνολογικές Προκλήσεις και Μέθοδοι Αντιμετώπισης

Οι εξελίξεις που συντελούνται τα τελευταία χρόνια στις τεχνολογίες πληροφορικής και τηλεπικοινωνιών είναι ραγδαίες και δημιουργούν, μεταξύ άλλων, νέες προκλήσεις για την ασφάλεια το απόρρητο και την προστασία της ιδιωτικής ζωής.

Τεράστιος όγκος δεδομένων, τα οποία συλλέγονται υπό τη μορφή αναζητήσεων (search queries), ηλεκτρονικού ταχυδρομείου, σημάτων ομιλίας, φωτογραφιών και video καταγράφονται από έξυπνα τηλέφωνα (smart phones), υπολογιστές tablet ή από ειδικές συσκευές (γυαλιά, ρολόι, κα) χάρις σε λειτουργικά συστήματα όπως το Android και το IOS, συνδυάζονται σε εφαρμογές όπως οι χάρτες και διαβιβάζονται μέσω κοινωνικών δικτύων. Η ανάλυση των μαζικών αυτών δεδομένων (big data) είναι πλέον εφικτή με τη χρήση αλγόριθμων αναγνώρισης, μηχανικής μάθησης και προβλεπτικής νοημοσύνης.

Εξάλλου, το διαδίκτυο των πραγμάτων (internet of things) δημιουργεί ένα σύνθετο περιβάλλον, στο οποίο λογισμικό, αισθητήρες και ασύρματη συνδεσιμότητα επιτρέπουν σε ηλεκτρονικές διατάξεις να επικοινωνούν με τον ιδιοκτήτη τους και μεταξύ τους. Σημαντικές τεχνολογικές πλατφόρμες (ευφυής κατοικία, αυτοοδηγούμενα οχήματα, ηλεκτρονικό πορτοφόλι με βιομετρικά στοιχεία κα) και ρομποτικές εφαρμογές, που αξιοποιούν την υπολογιστική του νέφους (cloud computing), πρόκειται να εισαχθούν μαζικά στις καταναλωτικές αγορές τα επόμενα χρόνια.

Οι εξελίξεις επηρεάζουν τη δομή και τον τρόπο διάθεσης των υπηρεσιών ηλεκτρο-

νικών επικοινωνιών και, όπως είναι ευνόητο, δημιουργούν νέα δεδομένα και σε ό, τι αφορά την ασφάλεια και την προστασία του απορρήτου της επικοινωνίας. Στο χώρο της Ευρωπαϊκής Ένωσης (ΕΕ), σε αρκετές περιπτώσεις, η διάθεση τέτοιων υπηρεσιών πραγματοποιείται σε ένα κράτος-μέλος, ενώ τμήμα των λειτουργικών μερών του δικτύου τους είναι εγκατεστημένο και λειτουργεί σε άλλο κράτος-μέλος (ή ακόμη και σε χώρες εκτός ΕΕ), με αποτέλεσμα να δυσχεραίνεται ο έλεγχος από τις αρμόδιες αρχές. Σε τέτοιες περιπτώσεις είναι αναγκαία η εναρμόνιση του κανονιστικού πλαισίου με τα νέα δεδομένα με στόχο την αποτελεσματική συνεργασία μεταξύ των κρατών-μελών και την κατάλληλη προσαρμογή των διαδικασιών ώστε να επιτευχθεί ευελιξία σε θέματα όπως οι έλεγχοι και η επιτήρηση από τις αρμόδιες αρχές. Η ΑΔΑΕ παρακολουθεί τις εξελίξεις τόσο σε τεχνολογικό όσο και σε ρυθμιστικό/κανονιστικό επίπεδο και θα συνεχίσει να θέτει τα παραπάνω ζητήματα στα αρμόδια όργανα της ΕΕ με σκοπό να γίνουν οι απαραίτητες τροποποιήσεις στους Κανονισμούς και τις Οδηγίες που έχουν εκδοθεί για τη διασφάλιση του απορρήτου των επικοινωνιών.

Ένα δεύτερο σημείο που αποτελεί πρόκληση είναι η αντιμετώπιση περιστατικών ασφάλειας, η οποία απαιτεί τη συνεργασία αρμόδιων υπηρεσιών από δύο ή περισσότερα κράτη-μέλη. Για παράδειγμα, έχουν καταγραφεί περιστατικά ασφάλειας, τα οποία εκδηλώνονται στο κράτος-μέλος όπου διατίθεται η αντίστοιχη υπηρεσία επικοινωνιών, ενώ τα συστήματα που παρέχουν τη συγκεκριμένη υπηρεσία, τα οποία επίσης επηρεάζονται από τα περιστατικά ασφάλειας, είναι εγκατεστημένα στην επικράτεια άλλου κράτους-μέλους. Αυτό σημαίνει ότι όχι μόνο είναι απαραίτητο ένα κοινό πλαίσιο μέτρων ασφάλειας μεταξύ των κρατών-μελών που θα υλοποιείται βάσει συγκεκριμένων δομών και διαδικασιών, αλλά χρειάζεται επίσης να θεσπιστούν κανόνες για τη διακρατική συνεργασία των εμπλεκομένων αρμοδίων αρχών των κρατών-μελών για την αποτελεσματική αντιμετώπιση περιστατικών ασφάλειας.

Η ΑΔΑΕ θα συνεχίσει τη συνεργασία, παρακολούθηση και συμμετοχή σε ευρωπαϊκά fora και ομάδες εργασίας. Τέτοιες ομάδες είναι η Ομάδα Εργασίας που οργανώνει ο Ευρωπαϊκός Οργανισμός ENISA για το Άρθρο 13α της Οδηγίας 2009/140/ΕΚ [7] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την Ασφάλεια και Ακεραιότητα Δικτύων και Υπηρεσιών, η Ομάδα Εργασίας για το Άρθρο 4 του Κανονισμού ΕΚ/611/2013 της Επιτροπής [8] για τα εφαρμοστέα μέτρα κοινοποίησης

[7] *http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:02009L0140-20091219&rid=1*
[8] *http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013R0611&rid=6*

παραβιάσεων δεδομένων επικοινωνίας και προσωπικών δεδομένων που οργανώνει η Γενική Διεύθυνση της Ευρωπαϊκής Επιτροπής για την ασφάλεια Δικτύων Επικοινωνιών (DG Connect) και η Ομάδα Εργασίας για την Ασφάλεια Δικτύων και Πληροφοριών (Informal Working Group on Network and Information Security) του Διεθνούς Δικτύου Εθνικών Ρυθμιστικών Αρχών IRG (Independent Regulators Group) που στοχεύει στην ανταλλαγή απόψεων μεταξύ των κρατών-μελών.

Από τις απόψεις που διατυπώνονται στις παραπάνω Ομάδες Εργασίας διαφαίνονται οι ακόλουθες τάσεις και προοπτικές για το μέλλον:

Σε ευρωπαϊκό επίπεδο φαίνεται να συνειδητοποιείται η ανάγκη διαχείρισης της ασφάλειας με συλλογικό και ενιαίο τρόπο από όλα τα κράτη-μέλη. Πράγματι, τα τελευταία χρόνια, η ευρωπαϊκή νομοθεσία αναφορικά με ζητήματα ασφάλειας δικτύων επικοινωνίας, υπηρεσιών επικοινωνίας, διατηρούμενων και διακινούμενων δεδομένων επικοινωνίας, ενισχύεται και διευρύνεται συνεχώς προκειμένου να καλύψει το σύνολο των απαιτήσεων στους παραπάνω τομείς. Επιγραμματικά αναφέρεται το άρθρο 13α της Οδηγίας 2002/21/ΕΚ, και το Άρθρο 4 της Οδηγίας 2002/58/ΕΚ, όπως τροποποιήθηκαν από την οδηγία 2009/140/ΕΚ και 2009/136/ΕΚ αντίστοιχα, ο Κανονισμός ΕΚ/611/2013 κυρίως για αναφορές περιστατικών ασφάλειας και το Άρθρο 15 της πρότασης της Ευρωπαϊκής Επιτροπής για την ηλεκτρονική ταυτοποίηση και υπηρεσίες εμπιστοσύνης. [9]

Από τα παραπάνω προκύπτει ότι το ζήτημα της ασφάλειας στις ηλεκτρονικές επικοινωνίες είναι πολύπλοκο και η ανάγκη διαχείρισής του με ενιαίο τρόπο από όλα τα κράτη-μέλη αποτελεί απαραίτητη προϋπόθεση για τη σωστή αντιμετώπισή του. Παράλληλα, κάθε κράτος-μέλος διατηρεί τη δυνατότητα να νομοθετεί και να θεσπίζει ειδικότερα μέτρα ασφάλειας ανάλογα με τις εθνικές ανάγκες. Αλλά και για τις ειδικότερες αυτές απαιτήσεις γίνονται προσπάθειες συντονισμού και κοινής δράσης. Έτσι, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια (ENISA) πρόσφατα κοινοποίησε έγγραφο με τίτλο «Security Framework for Article 4 and 13a – Proposal for one security framework for Article 4 and 13a» [10] που αφορά στη νέα πρόταση για τη δημιουργία ενός γενικού πλαισίου ασφάλειας όπου θα χρησιμοποιούνται κοινά ειδικά μέτρα και κοινοί κανόνες αναφορικά με την ασφάλεια και ακεραιότητα δικτύων και υπηρεσιών καθώς και τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών από όλα τα κράτη-μέλη.

[9] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF*
Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. COM(2012)0238 - 04/06/2012 Legislative proposal 2012/0146 (COD)

[10] *www.enisa.europa.eu/*

Όλες οι παραπάνω προσπάθειες αποδεικνύουν ότι έχει κατανοηθεί από όλους πως η διασφάλιση ενός ικανοποιητικού επιπέδου ασφάλειας απαιτεί συλλογική αντιμετώπιση του ζητήματος με συνεισφορά από όλα τα κράτη-μέλη. Για παράδειγμα, μία αδυναμία ασφάλειας ή ακόμα και ένα περιστατικό ασφάλειας, που διαπιστώνεται σε ένα κράτος-μέλος καθώς και ο τρόπος αντιμετώπισής τους, αποτελεί χρήσιμη πληροφορία για τα υπόλοιπα κράτη-μέλη προκειμένου να (υπάρξει η κατάλληλη μέριμνα και) να ληφθούν τα απαραίτητα μέτρα, ώστε σε περίπτωση εκδήλωσης ανάλογου περιστατικού να αντιμετωπιστεί αυτό ελαχιστοποιώντας τις επιπτώσεις.

Γενικότερα σε ό,τι αφορά το μέλλον, φαίνεται ότι στο χώρο της ΕΕ επιδιώκεται η καθιέρωση μιας ολοκληρωμένης πλατφόρμας επικοινωνίας μεταξύ των κρατών-μελών για την ανταλλαγή απόψεων και πληροφοριών για ζητήματα ασφάλειας. Κάτι τέτοιο όμως δεν απαιτεί μόνο την οργάνωση της επικοινωνίας σε επίπεδο Υπηρεσιών μεταξύ των κρατών-μελών, αλλά και την κατηγοριοποίηση, οργάνωση και διάθεση της πληροφορίας βάσει κοινών προτύπων.

Η ΑΔΑΕ, έχοντας διαπιστώσει από νωρίς την ανάγκη επικοινωνίας και ανταλλαγής απόψεων με άλλους φορείς και κράτη-μέλη αναφορικά με ζητήματα ασφάλειας και προστασίας του απορρήτου, συμμετέχει, στο βαθμό που της επιτρέπουν οι διαθέσιμοι πόροι (ειδικευμένο προσωπικό και οικονομικά μέσα), στους Ευρωπαϊκούς θεσμούς και επιδιώκει να συμβάλλει ώστε να διαμορφωθούν κατά το δυνατόν, οι κατάλληλες δομές για την αποτελεσματικότερη αντιμετώπιση των σχετικών προβλημάτων.