ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ
ΤΟΥ ΑΠΟΡΡΗΤΟΥ
ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Βουλή
των
Ελλήνων
Αίθουσα
Γερουσίας

ΑΠΟΡΡΗΤΟ ΕΠΙΚΟΙΝΩΝΙΩΝ:

σύγχρονες προκλήσεις

08.05.2018

ΠΡΑΚΤΙΚΑ ΗΜΕΡΙΔΑΣ
ΑΔΑΕ

ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ
ΤΟΥ ΑΠΟΡΡΗΤΟΥ
ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Βουλή
των
Ελλήνων
Αίθουσα
Γερουσίας

ΑΠΟΡΡΗΤΟ ΕΠΙΚΟΙΝΩΝΙΩΝ:

σύγχρονες προκλήσεις

08.05.2018

ΠΡΑΚΤΙΚΑ ΗΜΕΡΙΔΑΣ

ΑΔΑΕ

Αθήνα 2018

ΑΠΟΡΡΗΤΟ ΕΠΙΚΟΙΝΩΝΙΩΝ: ΣΥΓΧΡΟΝΕΣ ΠΡΟΚΛΗΣΕΙΣ

ΠΡΑΚΤΙΚΑ ΗΜΕΡΙΔΑΣ 8 ΜΑΙΟΥ 2018

ΟΡΓΑΝΩΣΗ ΗΜΕΡΙΔΑΣ: ΑΔΑΕ,

ΑΥΤΟΤΕΛΕΣ ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΣΥΝΕΡΓΑΣΙΩΝ ΚΑΙ ΔΗΜΟΣΙΩΝ ΣΧΕΣΕΩΝ

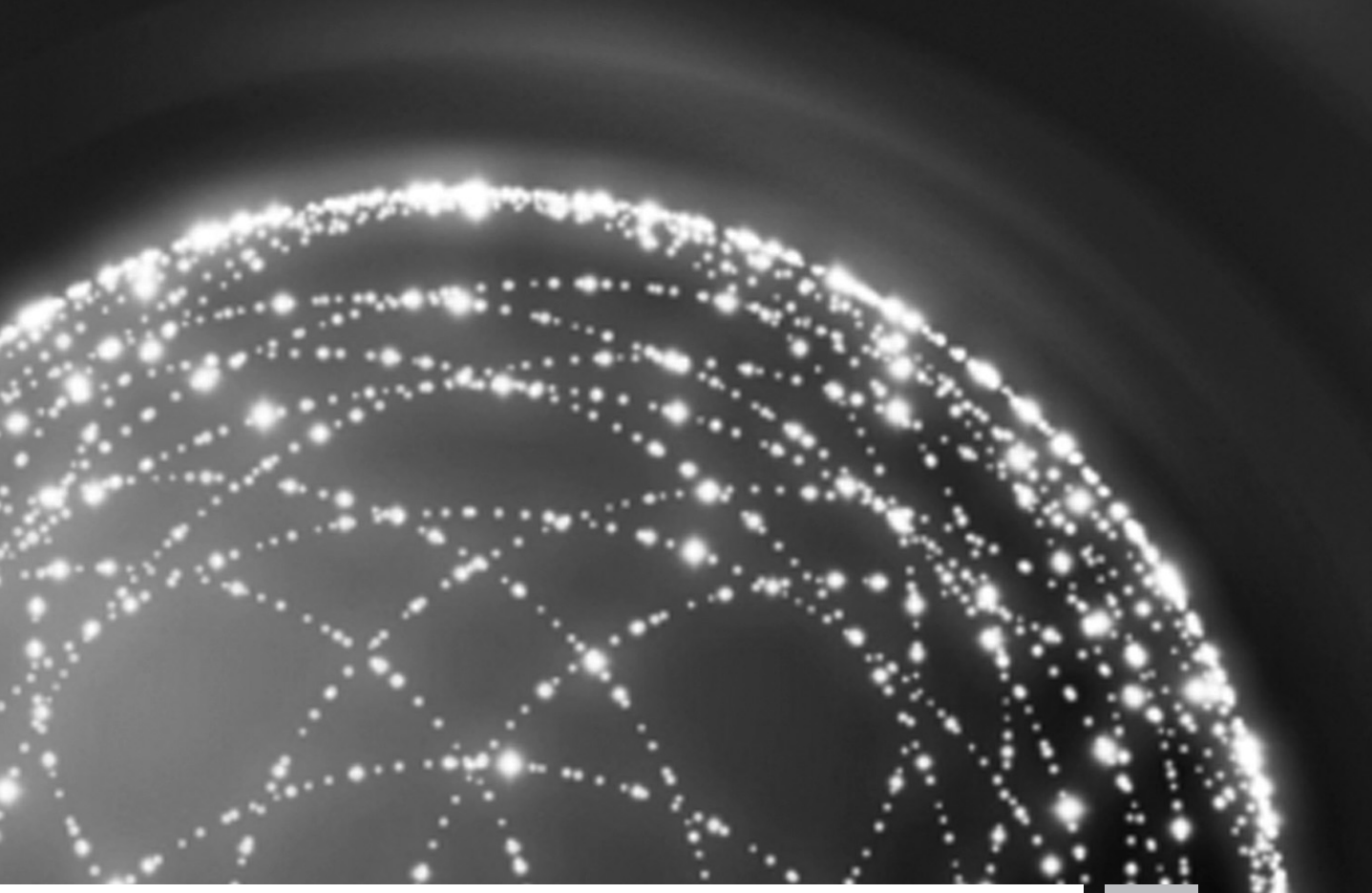
ΕΠΙΜΕΛΕΙΑ ΕΚΔΟΣΗΣ: Αναστασία Λύρα, Προϊσταμένη,
Αυτοτελές Τμήμα Διεθνών Συνεργασιών & Δημοσίων Σχέσεων ΑΔΑΕ,
Ελένη Βαρβαρούση, Δρ. Ειδικό Επιστημονικό Προσωπικό ΑΔΑΕ

ΑΠΟΜΑΓΝΗΤΟΦΩΝΗΣΗ: AELIOS www.aelios.gr

ΣΧΕΔΙΑΣΜΟΣ ΕΝΤΥΠΟΥ: ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ
Άννα Καρακωνσταντή

ΕΚΤΥΠΩΣΗ: ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ **www.et.gr**

ISBN: 978-960-98080-1-9



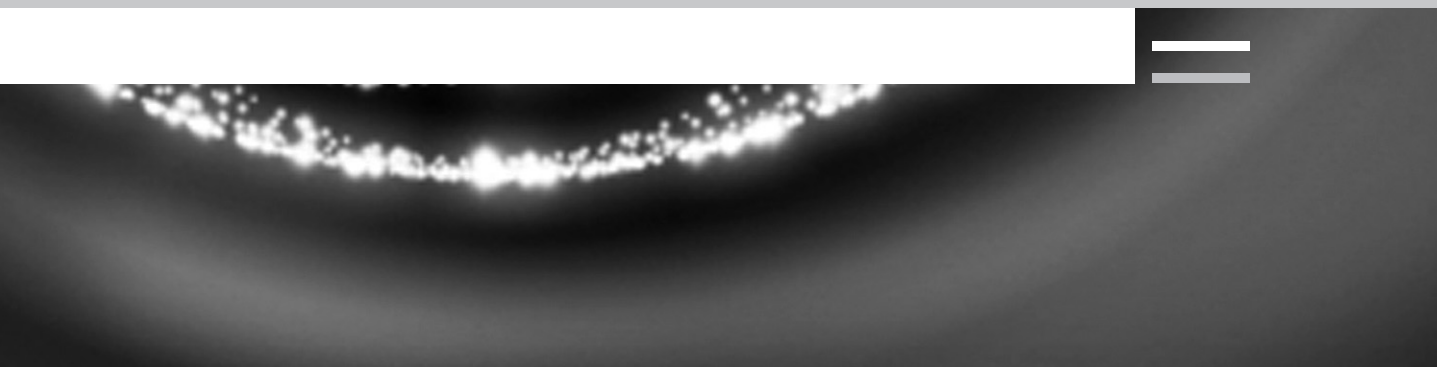
Εισαγωγικό σημείωμα

Η συλλογή αυτή περιλαμβάνει τα πρακτικά της Ημερίδας που διοργάνωσε η **Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών** και φιλοξένησε το Ελληνικό Κοινοβούλιο στις **8 Μαΐου του 2018**. Στην ημερίδα, η οποία διαπραγματεύθηκε σύγχρονες προκλήσεις για το συνταγματικά κατοχυρωμένο δικαίωμα στο απόρρητο των επικοινωνιών, εξέθεσαν τις επιστημονικές τους απόψεις διακεκριμένοι εισηγητές από την ακαδημαϊκή κοινότητα, ανώτατοι δικαστές, εξειδικευμένοι επιστήμονες και στελέχη οργανισμών με στόχο να φωτίσουν νομικά και τεχνικά ζητήματα που θέτουν τα νέα τεχνολογικά δεδομένα για την ιδιωτική ζωή.

Εκ μέρους της Ολομέλειας της Αρχής θα ήθελα να ευχαριστήσω τον Πρόεδρο της Βουλής των Ελλήνων, κ. Νικόλαο Βούτση, ο οποίος απηύθυνε εναρκτήριο χαιρετισμό τιμώντας τα 15 χρόνια από την ίδρυση της ΑΔΑΕ, καθώς και όλους τους εξέχοντες ομιλητές.

Η συλλογή, όπως και η Ημερίδα, περιλαμβάνει δύο ενότητες: στην πρώτη συζητούνται τεχνολογικές εξελίξεις σε σχέση με την ιδιωτικότητα και στη δεύτερη αναλύονται νομικά και κανονιστικά ζητήματα της προστασίας του απορρήτου των επικοινωνιών. Οι παρουσιάσεις των ομιλητών βρίσκονται αναρτημένες στον ιστότοπο της Αρχής, στη διεύθυνση **http://www.adae.gr/enimerosi/epistimoniki-imerida-tis-adae/**

Χρήστος Ζαμπίρας, Πρόεδρος



περιεχόμενα

Καλωσόρισμα και Χαιρετισμοί		σελίδα
Χρήστος Ζαμπίρας	Πρόεδρος της ΑΔΑΕ	12
Νικόλαος Βούτσης	Πρόεδρος της Βουλής των Ελλήνων	13
Σταύρος Κοντονής	Υπουργός Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων	15
Νίκος Παππάς	Υπουργός Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης	16
Κωνσταντίνος Μενουδάκος	Πρόεδρος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Επίτιμος Πρόεδρος του Συμβουλίου της Επικρατείας	18
Κωνσταντίνος Μασσέλος	Καθηγητής, Πρόεδρος της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)	19
Ιωάννης Ταφύλλης	Διευθυντής του Κέντρου Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α)	21
Γεώργιος Παπαπροδρόμου	Ταξίαρχος, Διευθυντής της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος	22
Α΄ Ενότητα: Τεχνολογικές εξελίξεις και απόρρητο των επικοινωνιών		
Συντονισμός: Μιχάλης Σακκάς	Αντιπρόεδρος της ΑΔΑΕ	26
«Η κυβερνοασφάλεια στην Ελλάδα»		
Δρ. Λέανδρος Μαγλαράς	Αναπληρωτής Προϊστάμενος της Διεύθυνσης Κυβερνοασφάλειας, Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης	26
«Το τοπίο των κυβερνοαπειλών: αναγκαιότητα ή πολυτέλεια;»		
Δρ. Λούης Μαρίνος	Ειδικός για θέματα ανάλυσης κυβερνο-απειλών και κινδύνων του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)	31
«Η επίδραση των blockchains στο απόρρητο των τηλεπικοινωνιακών υπηρεσιών»		
Χρήστος Καψάλης	Καθηγητής ΕΜΠ, πρώην Μέλος της Ολομέλειας της ΑΔΑΕ	35
«Ο ρόλος των αρχών για τη διασφάλιση του απορρήτου των επικοινωνιών στον κόσμο της νεφοϋπολογιστικής»		
Χρήστος Καλλονιάτης	Αναπληρωτής Καθηγητής Πανεπιστημίου Αιγαίου, Μέλος της Ολομέλειας της ΑΔΑΕ	38

«Κανονιστικό πλαίσιο για την αντιμετώπιση ευπαθειών δικτύων κινητής τηλεφωνίας»		
Παναγιώτης Τρακάδας	Αναπληρωτής Καθηγητής ΤΕΙ Στερεάς Ελλάδας	49
«Απόρρητο, ακεραιότητα και διαθεσιμότητα στις ηλεκτρονικές επικοινωνίες»		
Ιωάννης Ψαλλίδας	Διευθυντής, Διεύθυνση Διασφάλισης Υποδομών, Απορρήτου Υπηρεσιών και Εφαρμογών Διαδικτύου, ΑΔΑΕ	53
«Ασφάλεια αεροπορικού ταχυδρομείου και μέτρα ανάσχεσης της απειλής»		
Πέτρος Σταμούλης	Επιθεωρητής ασφάλειας, Διεύθυνση Ασφάλειας Πολιτικής Αεροπορίας από Έκνομες Ενέργειες Υπηρεσία Πολιτικής Αεροπορίας	58
«Ασφάλεια ταχυδρομικών αντικειμένων»		
Αριστείδης Μισαηλίδης	Διευθυντής, Διεύθυνση Διασφάλισης Απορρήτου Ταχυδρομικών Υπηρεσιών, ΑΔΑΕ	62
Β΄ Ενότητα: Νομικά και κανονιστικά ζητήματα της προστασίας του απορρήτου των επικοινωνιών		
Συντονισμός: Δρ. Αικατερίνη Παπανικολάου	Δικηγόρος, Μέλος της Ολομέλειας της ΑΔΑΕ	58
«Η συνταγματική προστασία των εξωτερικών στοιχείων της επικοινωνίας»		
Νικόλαος Κ. Μαρκόπουλος	Πάρεδρος Συμβουλίου της Επικρατείας	65
«Η άρση του απορρήτου στο Internet και η αποκάλυψη της διεύθυνσης IP (IP address)»		
Γιώργος Γιαννόπουλος	Επίκουρος Καθηγητής Νομικής Σχολής Πανεπιστημίου Αθηνών	69
«Η πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση 'Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών' και η προστασία του απορρήτου»		
Βασίλειος Κονδύλης	Επίκουρος Καθηγητής Νομικής Σχολής Πανεπιστημίου Αθηνών	44
«Η ποινική προστασία του απορρήτου των επικοινωνιών»		
Γεώργιος Ν. Τριανταφύλλου	Επίκουρος Καθηγητής Νομικής Σχολής Πανεπιστημίου Αθηνών	75
«Non bis in idem»		
Ηλίας Θεοδωράτος	Νομικός Σύμβουλος ΑΔΑΕ, Δικηγόρος, Δρ. Νομικής του Πανεπιστημίου της Σορβόννης	80

πρόγραμμα

Καλωσόρισμα

Χρήστος Ζαμπίρας
Πρόεδρος της ΑΔΑΕ

Χαιρετισμοί

Νικόλαος Βούτσης
Πρόεδρος της Βουλής των Ελλήνων

Σταύρος Κοντονής,
Υπουργός Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων

Νίκος Παππάς
Υπουργός Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης

Κωνσταντίνος Μενουδάκος

Πρόεδρος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,
Επίτιμος Πρόεδρος του Συμβουλίου της Επικρατείας

Κωνσταντίνος Μασσέλος

Καθηγητής, Πρόεδρος της Εθνικής Επιτροπής Τηλεπικοινωνιών
και Ταχυδρομείων (ΕΕΤΤ)

Ιωάννης Ταφύλλης

Διευθυντής του Κέντρου Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α)

Γεώργιος Παπαπροδρόμου

Ταξίαρχος, Διευθυντής της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

Α' ενότητα

ΤΕΧΝΟΛΟΓΙΚΕΣ ΕΞΕΛΙΞΕΙΣ ΚΑΙ ΑΠΟΡΡΗΤΟ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Συντονισμός:
Μιχάλης Σακκάς, Αντιπρόεδρος της ΑΔΑΕ

Δρ. Λέανδρος Μαγλαράς
Αναπληρωτής Προϊστάμενος της Διεύθυνσης Κυβερνοασφάλειας,
Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης
«Η κυβερνοασφάλεια στην Ελλάδα»

Δρ. Λούης Μαρίνος
Ειδικός για θέματα ανάλυσης κυβερνοαπειλών και κινδύνων του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)
«Το τοπίο των κυβερνοαπειλών: αναγκαιότητα ή πολυτέλεια;»

Χρήστος Καψάλης
Καθηγητής ΕΜΠ, πρώην Μέλος της Ολομέλειας της ΑΔΑΕ
«Η επίδραση των blockchains στο απόρρητο των τηλεπικοινωνιακών υπηρεσιών»

Χρήστος Καλλονιάτης
Αναπληρωτής Καθηγητής Πανεπιστημίου Αιγαίου, Μέλος της Ολομέλειας της ΑΔΑΕ
«Ο ρόλος των αρχών για τη διασφάλιση του απορρήτου των επικοινωνιών στον κόσμο της νεφοϋπολογιστικής»

Παναγιώτης Τρακάδας
Αναπληρωτής Καθηγητής ΤΕΙ Στερεάς Ελλάδας

«Κανονιστικό πλαίσιο για την αντιμετώπιση ευπαθειών δικτύων κινητής τηλεφωνίας»

Ιωάννης Ψαλλίδας
Διευθυντής, Διεύθυνση Διασφάλισης Υποδομών,
Απορρήτου Υπηρεσιών και Εφαρμογών Διαδικτύου, ΑΔΑΕ

«Απόρρητο, ακεραιότητα και διαθεσιμότητα στις ηλεκτρονικές επικοινωνίες»

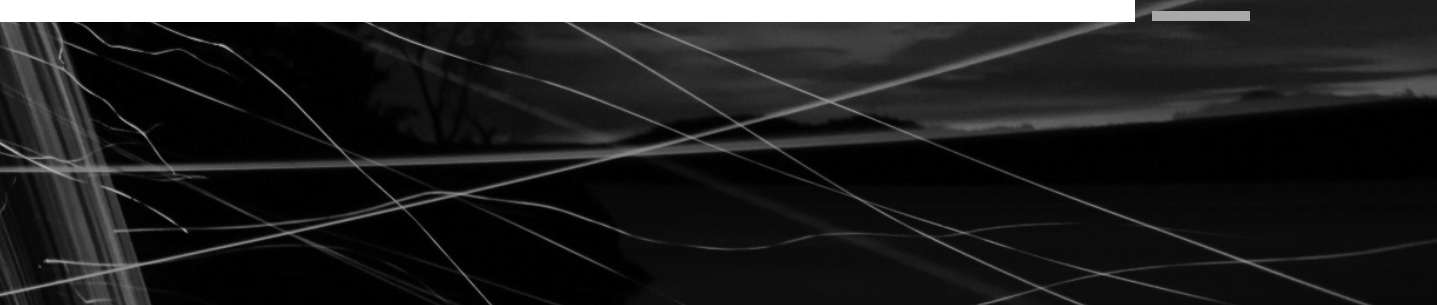
Πέτρος Σταμούλης
Επιθεωρητής ασφάλειας, Διεύθυνση Ασφάλειας Πολιτικής Αεροπορίας από Έκνομες
Ενέργειες Υπηρεσία Πολιτικής Αεροπορίας

«Ασφάλεια αεροπορικού ταχυδρομείου και μέτρα ανάσχεσης της απειλής»

Αριστείδης Μισαηλίδης
Διευθυντής, Διεύθυνση Διασφάλισης Απορρήτου Ταχυδρομικών Υπηρεσιών, ΑΔΑΕ

«Ασφάλεια ταχυδρομικών αντικειμένων»

Ερωτήσεις - Συζήτηση



Β' ενότητα

ΝΟΜΙΚΑ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΑ ΖΗΤΗΜΑΤΑ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Συντονισμός:
Δρ. Αικατερίνη Παπανικολάου, Δικηγόρος, Μέλος της Ολομέλειας της ΑΔΑΕ

Νικόλαος Κ. Μαρκόπουλος
Πάρεδρος Συμβουλίου της Επικρατείας
«Η συνταγματική προστασία των εξωτερικών στοιχείων της επικοινωνίας»

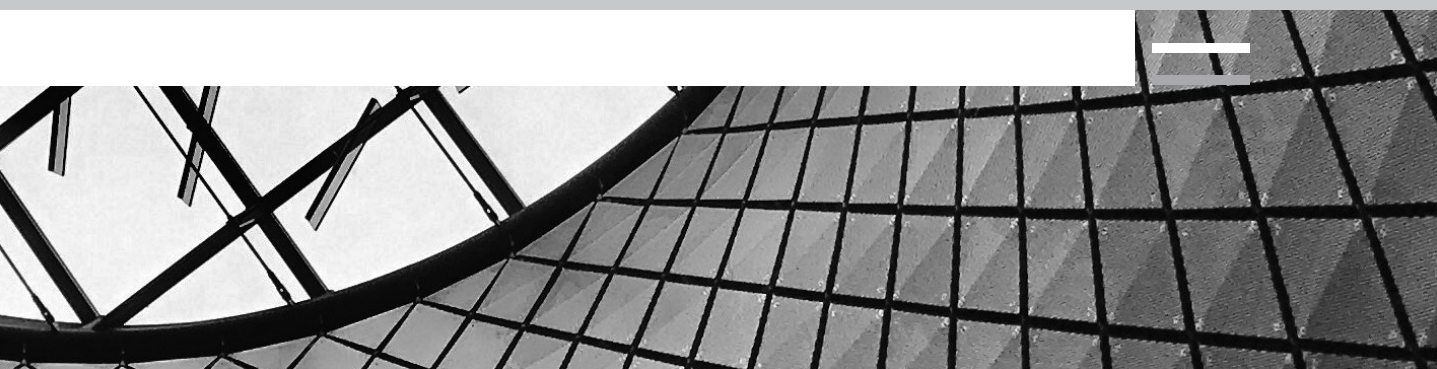
Γιώργος Γιαννόπουλος
Επίκουρος Καθηγητής Νομικής Σχολής Πανεπιστημίου Αθηνών
«Η άρση του απορρήτου στο Internet και η αποκάλυψη της διεύθυνσης IP (IP address)»

Βασίλειος Κονδύλης
Επίκουρος Καθηγητής Νομικής Σχολής Πανεπιστημίου Αθηνών
«Η πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση 'Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών' και η προστασία του απορρήτου»

Γεώργιος Ν. Τριανταφύλλου
Επίκουρος Καθηγητής Νομικής Σχολής Πανεπιστημίου Αθηνών
«Η ποινική προστασία του απορρήτου των επικοινωνιών»

Ηλίας Θεοδωράτος
Νομικός Σύμβουλος ΑΔΑΕ, Δικηγόρος,
Δρ. Νομικής του Πανεπιστημίου της Σορβόννης
«Non bis in idem»

Ερωτήσεις - Συζήτηση



Έναρξη Εργασιών **ΗΜΕΡΙΔΑΣ**

Καλωσόρισμα

ΖΑΜΠΙΡΑΣ Χ.:

Αξιότιμε κύριε Πρόεδρε της Βουλής των Ελλήνων, κυρίες και κύριοι εκπρόσωποι των Κομμάτων της Βουλής, κυρίες και κύριοι Πρόεδροι και Στελέχη των Ανεξάρτητων Αρχών, καλημέρα σας.

Σας καλωσορίζουμε στην ημερίδα που διοργανώνει σήμερα η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, στον χώρο της Βουλής των Ελλήνων, 15 χρόνια από την ίδρυσή της το 2003, σε υλοποίηση του Άρθρου 19 του Συντάγματος.

Οι προσκεκλημένοι ομιλητές, που τους ευχαριστούμε για την αποδοχή της πρόσκλησης, με τον προβληματισμό που θα καταθέσουν είναι βέβαιο ότι θα συμβάλουν στην επίτευξη του στόχου της ημερίδας που είναι:

Πρώτον, η παρουσίαση θεμάτων του απορρήτου και της ασφάλειας των επικοινωνιών υπό το πρίσμα των σύγχρονων τεχνολογικών εξελίξεων καθώς και των νομικών κανονιστικών ζητημάτων που απορρέουν από αυτές.

Δεύτερον, η ανάδειξη του έργου και της συμβολής της Αρχής στην προστασία του απορρήτου και της ασφάλειας των επικοινωνιών καθώς και του ρόλου της στις μελλοντικές εξελίξεις και προκλήσεις λόγω των τεχνολογικών αλλαγών, τόσο στον τηλεπικοινωνιακό όσο και στον ταχυδρομικό τομέα.

Κυρίες και κύριοι, στο στόχαστρο της ΑΔΑΕ είναι διαρκώς η αποτελεσματική αντιμετώπιση των απειλών που η ραγδαία εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών εγκυμονεί για την προστασία του θεμελιώδους δικαιώματος του απορρήτου των επικοινωνιών. Καταβάλλει προς τούτο συνεχείς προσπάθειες για να παρακολουθεί τις εξελίξεις και να επικαιροποιεί τους Κανονισμούς της, ώστε να καθοδηγεί τους παρόχους να λαμβάνουν τα απαραίτητα μέτρα ασφάλειας των επικοινωνιών. Προς την κατεύθυνση αυτή θα συμβάλλει και η υλοποίηση του εγκεκριμένου από την Ολομέλεια 3ετούς σχεδίου δράσης της ΑΔΑΕ, από το 2017 έως το 2019. Με βάση το σχέδιο αυτό, απαιτείται σημαντική ενίσχυση της ΑΔΑΕ -σε προσωπικό, οικονομικούς πόρους και τεχνικά μέσα- προκειμένου να επιτελεί ουσιαστικότερα τον σημαντικό ρόλο της στη σύγχρονη εποχή.

Στο σημείο αυτό είναι απαραίτητο να εξάρω την υψηλή επιστημονική κατάρτιση του προσωπικού της ΑΔΑΕ και την αυταπάρνηση με την οποία επιμένει να μεριμνά για τη διασφάλιση του δικαιώματος του απορρήτου, σε πείσμα τόσο της υποστελέχωσης της Αρχής όσο και των υλικοτεχνικών ελλειμμάτων.

Κυρίες και κύριοι, επιγραμματικά αναφέρω ότι, όσον αφορά τη συζητούμενη πρόταση Κανονισμού της Ευρωπαϊκής Επιτροπής για τον σεβασμό της ιδιωτικής ζωής και της προστασίας δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες, με την υιοθέτηση του Κανονισμού αυτού καταργείται η Οδηγία 2002/58/ΕΚ. Αυτό το σχέδιο Κανονισμού προβλέπει εκσυγχρονισμό και διεύρυνση του πεδίου εφαρμογής της νομοθεσίας για την προστασία του απορρήτου και παράλληλα απαιτεί περαιτέρω ενίσχυση των εποπτικών Αρχών για την εφαρμογή του.

Η εξέλιξη της τεχνολογίας και η χρήση έξυπνων συσκευών απαιτεί, τόσο από τους χρήστες όσο και από τις επιχειρήσεις, την αποτελεσματική διαχείριση των νέων απειλών για την ιδιωτικότητα. Χρειάζεται να διευρυνθεί η ήδη διαμορφωμένη -και με τη συμβολή της ΑΔΑΕ- κουλτούρα ασφάλειας. Παράλληλα, και οι ψηφιακοί χρήστες θα πρέπει να αναζητούν την κατάλληλη ενημέρωση για τους

κινδύνους που ελλοχεύουν για το απόρρητο της επικοινωνίας. Στη διαδικτυακή πύλη της Αρχής, οι πολίτες μπορούν να βρουν πλούσιο ενημερωτικό υλικό σε θέματα ασφάλειας των επικοινωνιών.

Συνεπώς, εν όψει των ανωτέρω τεχνολογικών και νομοθετικών εξελίξεων, η ΑΔΑΕ -με τη μακρόχρονη εμπειρία της- είναι η μόνη αρμόδια Αρχή στην ελληνική έννομη τάξη που είναι σε θέση να διασφαλίσει με τη δράση της την προστασία του απορρήτου των επικοινωνιών. Πιστεύουμε ότι, με τη συμπαράσταση της πολιτείας και τον ζήλο του άξιου προσωπικού της, η ΑΔΑΕ θα ανταποκριθεί στις προκλήσεις των καιρών προστατεύοντας και διασφαλίζοντας για την πολιτεία και τους πολίτες το απόρρητο των επικοινωνιών τους.

Κυρίες και κύριοι, με αυτές τις εισαγωγικές σκέψεις, θα ήθελα να καλέσω στο βήμα τον Πρόεδρο της Βουλής κύριο Νικόλαο Βούτση, να απευθύνει έναν χαιρετισμό στην ημερίδα μας.

Χαιρετισμοί

ΒΟΥΤΣΗΣ Ν.:

Καλημέρα, να είστε καλά.

Θα ήθελα να σας καλωσορίσω στη Βουλή των Ελλήνων και να συγχαρώ την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών για την πρωτοβουλία και τη διοργάνωση της σημερινής ημερίδας.

Την προηγούμενη εβδομάδα είχαμε την ευκαιρία να παρευρεθούμε -κι εγώ αλλά και αρκετοί από εσάς, κύριοι Πρόεδροι- στην επίσης πολύ ενδιαφέρουσα ημερίδα της Ομοσπονδίας Εργαζομένων Ανεξαρτήτων Αρχών, με θέμα συζήτησης «Ανεξάρτητες Αρχές: η εξέλιξη του θεσμού στην ελληνική πραγματικότητα», όπου υπήρξαν πολύ ενδιαφέρουσες τοποθετήσεις για τον ρόλο που καλούνται να παίξουν οι Ανεξάρτητες Αρχές στη σύγχρονη κοινωνία, για την ανάγκη περαιτέρω κατοχύρωσης και θωράκισης της ανεξαρτησίας τους και για την πρόκληση που έχουμε μπροστά μας εν όψει και της επικείμενης συνταγματικής αναθεώρησης.

Στον χαιρετισμό που είχα την τιμή να απευθύνω ως Πρόεδρος της Βουλής αναφέρθηκα, μεταξύ άλλων, στα ανωτέρω -καίρια κατά την άποψή μου- ζητήματα και είχα την ευκαιρία να επισημάνω ότι η παρούσα οκτωκομματική Βουλή κατάφερε να συγκροτήσει -από την πρώτη, κιόλας, σύνοδο- και τις πέντε συνταγματικά κατοχυρωμένες Ανεξάρτητες Αρχές με τα ισχύοντα σήμερα στο Σύνταγμα, σε σχέση με αυξημένες πλειοψηφίες και τα λοιπά.

Η αρχή, μάλιστα, έγινε με τη συγκρότηση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, κατόπιν επιλογής των μελών της από τη Διάσκεψη των Προέδρων της Βουλής με πλειοψηφία 4/5, τον Μάρτιο του 2016. Ακολούθησε η εναρκτήρια πρώτη συνεδρίαση της Αρχής υπό τη νέα σύνθεσή της, στις 23 Μαρτίου του 2016, στην οποία παρευρέθην κι εγώ, θέλοντας έτσι να δώσουμε ένα συμβολικό μήνυμα επανεκκίνησης των Ανεξάρτητων Αρχών μετά από μια μακρά περίοδο απονομιμοποίησής τους μέσω συνεχών παρατάσεων θητειών κ.λπ. Η νέα Ολομέλεια της ΑΔΑΕ έχει παραδώσει την Έκθεση Πεπραγμένων για το έτος 2016, η οποία και θα συζητηθεί στο προσεχές διάστημα στην Επιτροπή Θεσμών και Διαφάνειας της Βουλής. Η βασική αρμοδιότητά της προβλέπεται στο άρθρο 19 του Συντάγματος, το οποίο της αναθέτει να διασφαλίζει το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας. Είναι προφανές ότι σε ένα

ραγδαία εξελισσόμενο περιβάλλον παγκοσμιοποίησης, ή -εάν μου επιτρέπεται η έκφραση- σε έναν νέο «ψηφιακό κόσμο» που γεννιούνται τα παιδιά μας, η ανάγκη προστασίας και θωράκισης θεμελιωδών δικαιωμάτων από σύγχρονες τεχνολογικές απειλές είναι όλο και περισσότερο επιτακτική και επιβεβλημένη.

Πράγματι, κάνοντας μια αναδρομή στο παρελθόν, πηγαίνοντας όχι πολύ μακριά, στις αρχές του προηγούμενου αιώνα, σοκάρεται κανείς διαπιστώνοντας το εύρος των αλλαγών στα μέσα επικοινωνίας μεταξύ των ανθρώπων: από τις επιστολές μέσω ταχυδρομείου στον τηλέγραφο, από την ενσύρματη σταθερή τηλεφωνία στα κινητά τηλέφωνα, το ηλεκτρονικό ταχυδρομείο, το διαδίκτυο, τα μέσα κοινωνικής δικτύωσης και ούτω καθεξής.

Από την κλασσική κατασκοπεία και τον έλεγχο των επιστολών που διάφορα καθεστώτα προσπάθησαν να επιβάλλουν τον προηγούμενο αιώνα, για να ελέγχουν την επικοινωνία μεταξύ των πολιτών, περάσαμε στις τηλεφωνικές υποκλοπές, στην παρακολούθηση κινητών τηλεφώνων, ηλεκτρονικών ταχυδρομείων, ακόμα και μέσων κοινωνικής δικτύωσης. Οι υποθέσεις Edward Snowden (Wikileaks) και Mark Zuckerberg (Facebook), πρόσφατα, αλλά και η υπόθεση Vodafone με τις υποκλοπές στην Ελλάδα, υπόθεση με την οποία ασχολήθηκε η ΑΔΑΕ, μαρτυρούν τις διαστάσεις του ζητήματος και μας καλούν σε εγρήγορση εν όψει του μέλλοντος.

Ευνόητο είναι ότι δεν θα υπεισέλθω στην ειδικότερη συζήτηση που θα ακολουθήσει, άλλωστε η συμμετοχή τέτοιου κύρους και επιστημονικής κατάρτισης ομιλητών εγγυάται μια πολύπλευρη προσέγγιση των σχετικών ζητημάτων, όμως θα ήθελα πριν κλείσω να κάνω την εξής επισήμανση. Παρ' ότι τα ζητήματα που επιλαμβάνεται η ΑΔΑΕ φαίνονται εκ πρώτης όψεως -και είναι- ζητήματα τεχνικά και πολύπλοκα, αυτό δεν σημαίνει ότι δεν αφορούν τον πολίτη. Γι' αυτό θα ήθελα να προτρέψω την Αρχή να δώσει περισσότερη βαρύτητα στην ενημέρωση και ευαισθητοποίηση επ' αυτών των ζητημάτων και επί των δικαιωμάτων που μπορούν να ασκούν οι πολίτες. Ξέρω ότι ήδη γίνεται αυτό, με τον εντοπισμό και την προστασία που παρέχεται από ενοχλητικές και κακόβουλες κλήσεις ή με τη δυνατότητα άρσης του απορρήτου για τη διακρίβωση εγκλημάτων και ούτω καθεξής.

Κυρίες και κύριοι, πρέπει όλοι -και οι συνάδελφοι βουλευτές, παρόντες-παρούσες, που είναι στις συγκεκριμένες Επιτροπές που διαλαμβάνονται αυτών των θεμάτων- να αντιληφθούμε ότι κάθε τεχνολογική εποχή – επανάσταση, 1η, 2η, 3η, 4η και τα λοιπά, επιφέρει στο πεδίο το νομικό, αλλά κυρίως στο επίπεδο του πολίτη, της καθημερινότητας, της συνείδησής του, των δικαιωμάτων του, έναν νέο ορίζοντα, ένα νέο πεδίο δικαιωμάτων, ταυτόχρονα και εγγυήσεων, έναντι της υπονόμευσης αυτών των δικαιωμάτων ή υποστηρικτικών λογικών ή διασύνδεσής τους με τα προηγούμενα, με τα θεμελιώδη όπως προηγουμένως είπαμε, και ούτω καθεξής.

Είναι προφανές ότι βρισκόμαστε σε μια τέτοια εποχή, και οι Ανεξάρτητες Αρχές -αυτό είναι επιπλέον αυτών των θεμάτων που θίξαμε και την προηγούμενη εβδομάδα- δεν είναι μόνο τα αντίβαρα εν όψει του ότι οι εξουσίες -και η εκτελεστική εξουσία, ενδεχομένως- λειτουργούν με έναν συγκεκριμένο τρόπο και άρα έρχεται μια ισορροπία και με αυτή την έννοια νομιμοποιούνται και ταυτόχρονα θωρακίζουν το δημοκρατικό σύστημα. Έχουν έναν επιπλέον λόγο, κατά τη γνώμη μου, όπως και οι πολύ άξιοι επιστήμονες

-άντρες και γυναίκες- που βλέπω και είχαμε ειδωθεί ξανά στην αρχή αυτής της θητείας της ΑΔΑΕ, καθώς όλοι έχουμε το καθήκον να δούμε αυτό το νέο πεδίο δικαιωμάτων, να το προσδιορίσουμε, να το συζητήσουμε, να το συνειδητοποιήσουμε μέσα στην κοινωνία και να δούμε ποιες είναι οι θεσμικές, νομικές, επιστημονικές, ελεγκτικές και άλλες πρόνοιες με βάση τις οποίες πρέπει να εξυπηρετηθεί, τώρα και στο μέλλον, μέχρι να έρθει και ένα ευρύτερο πεδίο δικαιωμάτων, να υπάρξουν και άλλες ευαισθησίες και λοιπά. Να έχουμε αυτή τη συνείδηση, όχι της στατικότητας ή απλά της μετάβασης, αλλά τη συνείδηση ότι μπαίνουμε κάθε λίγο και λιγάκι -αυτό είναι μερικές δεκαετίες κάθε φορά- σε νέες εποχές και σε νέα δικαιώματα, που η υποστήριξή τους και η ενίσχυσή τους είναι στην καρδιά και του πολιτικού συστήματος και της δημοκρατίας.

Σας ευχαριστώ πολύ.

ΖΑΜΠΙΡΑΣ Χ.:

Ευχαριστούμε πολύ τον Πρόεδρο της Βουλής των Ελλήνων κύριο Νίκο Βούτση.

Ως δεύτερο χαιρετισμό είχαμε καλέσει τον Υπουργό Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων κύριο Κοντονή, ο οποίος μας ενημέρωσε χτες ότι, λόγω ανειλημμένων υποχρεώσεων, αδυνατεί να παραστεί και μας έστειλε τον χαιρετισμό τον οποίο επρόκειτο να απευθύνει, τον οποίο θα διαβάσει ο Αντιπρόεδρος κύριος Σακκάς.

ΣΑΚΚΑΣ Μ.:

(Χαιρετισμός Σ. Κοντονή)

«Αξιότιμοι κυρίες και κύριοι, σας ευχαριστώ ιδιαίτερα για την πρόσκληση να παραστώ στην εκδήλωσή σας. Δυστυχώς, δεν μπορώ να παρευρεθώ ανάμεσά σας.

Θα ήθελα να χαιρετίσω την πολυετή συνεισφορά της Ανεξάρτητης Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων στο πεδίο των ηλεκτρονικών. Σε μια ευνομούμενη κοινωνία, η προστασία της επικοινωνίας αποτελεί κύριο μέλημα. Ο σεβασμός της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα ως γενικότερη έκφανση της ανάπτυξης της προσωπικότητας ανταποκρίνεται σε έναν σκοπό γενικότερου συμφέροντος, δηλαδή στην ελευθερία έκφρασης και επικοινωνίας. Το δικαίωμα αυτό αποτελεί απόλυτα απαραβίαστο έννομο αγαθό αυξημένης συνταγματικής προστασίας κατά τη ρητή πρόβλεψη του άρθρου 19 του Συντάγματος, τυχόν δε παραβίασης αυτού επιφέρουν ποινικές κυρώσεις. Περαιτέρω, στο παράγωγο ενωσιακό Δίκαιο εμφανίζεται ως έκφανση του θεμελιώδους δικαιώματος σεβασμού της ιδιωτικής ζωής όπως κατοχυρώνεται στο άρθρο 7 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Αναγνωρίζοντας τη σπουδαιότητα διαφύλαξης του απορρήτου των επικοινωνιών, ο Έλληνας νομοθέτης επιχειρεί με μια σειρά προβλέψεων να ενισχύει το θεσμικό πλαίσιο προστασίας, παρακολουθώντας παράλληλα τα ευρωπαϊκά δρώμενα και ενσωματώνοντας άμεσα την ευρωπαϊκή νομοθεσία στην εθνική έννομη τάξη, συμβάλλοντας με τον τρόπο αυτόν στον ευρωπαϊκό χώρο ελευθερίας, ασφάλειας και δικαιοσύνης.

Προς την κατεύθυνση αυτή, θα ήθελα να επισημάνω τη συνεργασία μας με το Υπουργείο Ψηφιακής Πολιτικής, για την κατάρτιση του Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, για τον σεβασμό της ιδιωτικής ζωής, την προστασία των δεδομένων

προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της Οδηγίας 2002/58.

Στόχος του υπό διαβούλευση Κανονισμού είναι η προσαρμογή της ευρωπαϊκής έννομης τάξης στις διαρκώς μεταλλασσόμενες τεχνολογικές και οικονομικές εξελίξεις καθώς και η ενίσχυση της εμπιστοσύνης στις ψηφιακές υπηρεσίες και η ασφάλεια των εν λόγω υπηρεσιών. Η μεταρρύθμιση του πλαισίου για την προστασία των δεδομένων επιδιώκει την παροχή υψηλότερου επιπέδου προστασίας της ιδιωτικής ζωής στους χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών και την εφαρμογή ισότιμων όρων ανταγωνισμού για όλους τους παράγοντες της αγοράς. Με την πρόταση αναθεωρείται το μέχρι σήμερα καθεστώς προστασίας της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και διασφαλίζεται η διαφύλαξη των θεμελιωδών δικαιωμάτων και ελευθεριών, το απόρρητο των επικοινωνιών και η προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών. Επιπλέον, ενισχύεται η ελεύθερη κυκλοφορία των δεδομένων, του εξοπλισμού και των υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ένωση. Η Ελλάδα παραμένει στην πρώτη γραμμή των σχετικών εξελίξεων και προσαρμόζεται αρμονικά στις ολοένα αναδυόμενες εξελίξεις.

Εύχομαι κάθε επιτυχία στις εργασίες σας, με την ελπίδα η προστιθέμενη αξία της πρωτοβουλίας να μεταφερθεί στη διατύπωση ώριμων προτάσεων που θα τύχουν εφαρμογής. Προς την κατεύθυνση αυτή, η ηγεσία και οι υπηρεσίες του Υπουργείου Δικαιοσύνης Διαφάνειας και Ανθρωπίνων Δικαιωμάτων παραμένουμε σταθερά πρόθυμοι να συμπράξουμε σε κάθε προσπάθεια με δικαιοκρατικό έρεισμα και θετικό κοινωνικό πρόσημο.

Με εκτίμηση,

Σταύρος Κοντονής
Υπουργός Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων»

ΖΑΜΠΙΡΑΣ Χ.:

Είχε κληθεί για να χαιρετίσει την ημερίδα μας και ο Υπουργός Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης κύριος Παππάς, ο οποίος -αδυνατώντας να παραστεί και αυτός- έστειλε τον χαιρετισμό τον οποίο θα αναγνώσει ο Δρ. Λέανδρος Μαγλαράς, Αναπληρωτής Προϊστάμενος της Διεύθυνσης Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης.

ΜΑΓΛΑΡΑΣ Λ.:

(Χαιρετισμός Ν. Παππά)

«Αξιότιμε κύριε Πρόεδρε της Βουλής, αξιότιμε κύριε Πρόεδρε της ΑΔΑΕ, κυρίες και κύριοι, φίλες και φίλοι, είναι μεγάλη τιμή και χαρά να βρίσκομαι σήμερα εδώ για να απευθύνω εκ μέρους του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης έναν σύντομο χαιρετισμό στην ημερίδα σας, μιας ημερίδας που λαμβάνει χώρα σε μια χρονική περίοδο που η ευαισθητοποίηση σε θέματα ασφάλειας είναι επιβεβλημένη, και το λέμε αυτό γιατί ο Μάιος αναδεικνύεται πανευρωπαϊκά σε μήνα που μπορεί να χαρακτηριστεί τομή σε θέματα ασφάλειας, καθώς εντός του Μαΐου προβλέπεται να μεταφερθεί στο εθνικό Δίκαιο των κρατών-μελών η πρώτη νομοθετική πράξη της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας: η Οδηγία για την ασφάλεια των συστημάτων

δικτύου και πληροφοριών, γνωστή ως Οδηγία NIS, καθώς επίσης να τεθεί σε ισχύ ο Γενικός Κανονισμός Προσωπικών Δεδομένων.

Η νομοθετική θωράκιση είναι ένα πρώτο και αναγκαίο βήμα, αλλά δεν είναι αρκετό. Θα πρέπει να συνδυαστεί και με άλλες πρωτοβουλίες και δράσεις, που θα ενημερώνουν τους πολίτες για τους τρόπους αυτοπροστασίας απέναντι στις κυβερνοεπιθέσεις αλλά και για τα δικαιώματά τους όταν τα δεδομένα τους επεξεργάζονται από τρίτους. Οι δράσεις αυτές θα μεγιστοποιήσουν τα οφέλη, αν πλαισιωθούν από συνεργασίες μεταξύ των αρμόδιων φορέων, με μεταφορά τεχνογνωσίας και ανταλλαγή βέλτιστων πρακτικών· κι εμείς υποστηρίζουμε παρόμοιες δράσεις, όπως είναι η ημερίδα που διοργανώσαμε πριν από 10 μέρες περίπου, με θέμα «Ο ρόλος του OWASP στην προστασία κρίσιμων πληροφοριακών συστημάτων».

Όλες αυτές οι δράσεις πρέπει να είναι συνεκτικές και να μπαίνουν κάτω από την «ομπρέλα» μιας στρατηγικής. Σε αυτή την κατεύθυνση, στις 07/03/2018 εγκρίθηκε η Εθνική Στρατηγική Κυβερνοασφάλειας από τον Υπουργό Ψηφιακής Πολιτικής, που αποτελεί προϊόν μακροχρόνιας μελέτης και συνεργασίας πολλών φορέων που συμμετείχαν στην εντεταλμένη ομάδα εργασίας. Με την έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας ορίζονται οι βασικές αρχές για τη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος -ψηφιακού περιβάλλοντος καλύτερα- στην Ελλάδα, τίθενται στρατηγικοί στόχοι και το πλαίσιο δράσεων μέσω του οποίου αυτοί θα εκπληρωθούν.

Η Εθνική Αρχή Κυβερνοασφάλειας, που συστάθηκε και λειτουργεί στη Γενική Γραμματεία Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, στο πλαίσιο των αρμοδιοτήτων της σχεδιάζει σειρά δράσεων, πρωτίστως για το σύνολο του δημόσιου τομέα αλλά και με στόχο την επέκτασή τους μέσω συνεργασιών και συμπράξεων και στον ιδιωτικό τομέα με γνώμονα το συμφέρον των πολιτών.

Ο τελικός αποδέκτης όλων αυτών των ενεργειών, φυσικά, θα πρέπει να είναι ο πολίτης. Θα πρέπει να χειρίζεται τα ζητήματα ασφάλειας του κινητού και του υπολογιστή του με μεγάλη ευκολία.

Θέλω να κλείσω λέγοντας ότι στη Γενική Γραμματεία Ψηφιακής Πολιτικής δίνουμε ιδιαίτερη σημασία στα θέματα ασφάλειας από τον σχεδιασμό των έργων ΤΠΕ και για τον λόγο αυτό ορίζουμε απαιτήσεις και κανόνες ασφάλειας που αποτελούν αναπόσπαστο μέρος του κάθε έργου ΤΠΕ του Δημοσίου (security by default και privacy by default) και ενσωματώνονται σε αυτά από τη φάση σχεδίασης (security by design) ως απαραίτητη προϋπόθεση των αρχών του ενιαίου σχεδιασμού.

Σας ευχαριστώ πολύ».

ΖΑΜΠΙΡΑΣ Χ.:

Ευχαριστούμε πολύ τον Δρ. Λέανδρο Μαγλαρά που μας μετέφερε τον χαιρετισμό του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης κύριου Παππά.

Με τον χαιρετισμό αυτόν κλείνει η πρώτη ενότητα των χαιρετισμών, που είναι από τον Πρόεδρο της Βουλής και πολιτικά πρόσωπα, όπου μπορούμε -συνοψίζοντας- να πούμε ότι επισημάνθηκε και ο ρόλος της ΑΔΑΕ μέχρι σήμερα στην προάσπιση αυτού του τόσο σημαντικού δικαιώματος, του απορρήτου στις επικοινωνίες και της ασφάλειας των επικοινωνιών, αλλά ταυτόχρονα τονίστηκε

και ο ρόλος που μπορεί να παίξει περαιτέρω και η ΑΔΑΕ στη σύγχρονη εποχή με όλες αυτές τις τεχνολογικές και νομοθετικές εξελίξεις και, κυρίως, όπως τόνισε και ο κύριος Βούτσης, ο ρόλος της Αρχής στη βελτίωση και τη βαρύτητα που πρέπει να δώσει στην ενημέρωση των πολιτών για τα δικαιώματα που έχουν γύρω από το θέμα της ασφάλειας των πολιτών. Νομίζουμε ότι μέχρι σήμερα η Αρχή έχει κάνει βήματα προς αυτή την κατεύθυνση, τα οποία μπορεί συνεχώς να βελτιώνει και να καθοδηγεί.

Θα ήθελα τώρα να καλέσω τον Πρόεδρο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και επίτιμο Πρόεδρο του Συμβουλίου της Επικρατείας κύριο Μενουδάκο για τον δικό του χαιρετισμό προς την Ημερίδα μας.

ΜΕΝΟΥΔΑΚΟΣ Κ.:

Κύριε Πρόεδρε της Βουλής, κύριε Πρόεδρε της ΑΔΑΕ, ευχαριστώ την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών για την πρόσκληση.

Το 2018, τουλάχιστον σε επίπεδο νομοθεσίας, αποτελεί μια χρονιά ορόσημο για την ψηφιακή ασφάλεια, για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, για την ασφάλεια των επικοινωνιών, των πληροφοριών και των δικτύων. Όπως είναι γνωστό, σε λίγες μέρες από σήμερα, στις 25 Μαΐου, αρχίζει να εφαρμόζεται ο Γενικός Κανονισμός Προστασίας Δεδομένων. Προχθές, 6 Μαΐου, έληξε η προθεσμία για την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας 2016/680/ΕΕ, που είναι η αστυνομική και δικαστική Οδηγία για την προστασία έναντι της επεξεργασίας προσωπικών δεδομένων για την πρόληψη και δίωξη των εγκλημάτων και για την εκτέλεση των ποινών. Στο σχέδιο νόμου που έχει καταρτίσει η νομοπαρασκευαστική Επιτροπή για την κατάρτιση νόμου, το οποίο έχει παραδοθεί ήδη στο Υπουργείο, υπάρχουν ορισμένα κεφάλαια με βάση τον ΓΚΠΔ τα οποία αφορούν την ενσωμάτωση αυτής της Οδηγίας, ενσωμάτωση η οποία δεν αργήσει γιατί έχει τεθεί σε διαβούλευση το σχέδιο νόμου, έχει τελειώσει η διαβούλευση και αναμένεται η κατάθεση στη Βουλή. Παράλληλα, το ακούσατε ήδη, καταρτίζεται ο Κανονισμός για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, ένας Κανονισμός που θα αντικαταστήσει μια Οδηγία του 2002. Επιπλέον, προωθείται η κατάρτιση Οδηγίας για τη θέσπιση Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών, που θεωρείται ένα επίσης σημαντικό νομοθέτημα, κρίσιμο στοιχείο της στρατηγικής της ενιαίας ψηφιακής αγοράς, με δεδομένο ότι οι καταναλωτές και -γενικά- οι επιχειρήσεις συναλλάσσονται όλο και περισσότερο μέσω του διαδικτύου.

Με τα τέσσερα αυτά ενωσιακά νομοθετήματα, δύο ψηφισμένα και δύο υπό κατάρτιση, ο Ευρωπαίος νομοθέτης αποβλέπει -κυρίως- σε τρεις στόχους:

Πρώτον, να άρει στον μέγιστο δυνατό βαθμό τους κινδύνους που δημιουργεί για την ιδιωτικότητα η κακή χρήση της συνεχώς εξελισσόμενης τεχνολογίας και να προστατέψει ατομικά δικαιώματα και ελευθερίες που περιλαμβάνονται μεταξύ των πυλώνων του δημοκρατικού κράτους δικαίου και κατοχυρώνονται με θεσμικά νομοθετήματα όπως είναι η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου και ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, βεβαίως και το Σύνταγμά μας.

Δεύτερον, να επιτύχει τη σωστή ισορροπία μεταξύ της διασφάλισης των ατομικών δι-

καιωμάτων και της ανάγκης να ληφθούν τα αναγκαία μέτρα για την ασφάλεια και τη δημόσια τάξη.

Τρίτον, να διαμορφώσει ένα φιλικό περιβάλλον για την ανάπτυξη της εσωτερικής αγοράς, που είναι -όπως ξέρουμε- μια από τις βάσεις του ευρωπαϊκού -ενωσιακού- οικοδομήματος.

Με τα νομοσχέδια αυτά επιχειρείται να ρυθμιστεί με κανόνες δικαίου μία ύλη που έχει κατά βάση τεχνολογικό χαρακτήρα. Για να γίνει αυτό, πρέπει να υπάρξει καλή γνώση της νομοθεσίας, όμως πρέπει να υπάρξει και πλήρης και σε βάθος κατανόηση του υλικού το οποίο ρυθμίζεται. Ορθώς, λοιπόν, η ημερίδα αναπτύσσεται σε δύο ενότητες, σε δύο φάσεις, στις οποίες θα συζητηθούν -αντιστοίχως- θέματα αναφερόμενα στις τεχνολογικές εξελίξεις και θέματα νομικά, πάντα σε συσχέτιση με το απόρρητο των επικοινωνιών.

Από διάφορα επεισόδια, μεγάλα που πήραν και δημοσιότητα ή μικρότερα που όλο και συχνά εμφανίζονται και βλέπουν ή δεν βλέπουν το φως της δημοσιότητας, αποδεικνύεται πόσο αναγκαία είναι η συνεχής αναζήτηση και η εφαρμογή αποτελεσματικών μεθόδων και εργαλείων για την κατοχύρωση της ασφάλειας των πληροφοριών και των επικοινωνιών.

Στο πλαίσιο της νέας ευρωπαϊκής νομοθεσίας και της σημερινής τεχνολογικής, οικονομικής και κοινωνικής πραγματικότητας, η ημερίδα εμφανίζεται άκρως επίκαιρη. Αυτός είναι ένας επιπλέον λόγος για τον οποίο το ενδιαφέρον είναι αυξημένο, εκτός -βεβαίως- από τη σημασία της θεματολογίας και των ομιλητών - εισηγητών οι οποίοι θα αναπτύξουν τα αντίστοιχα θέματα και των οποίων η επιστημονική εγκυρότητα και εμπειρογνωμοσύνη είναι γνωστή και υψηλή.

Εύχομαι καλή επιτυχία στην ημερίδα· το κάνω εκ περισσού γιατί, διαβάζοντας τη θεματολογία και τους εισηγητές, είμαι βέβαιος ότι σήμερα το πρωί και σήμερα το μεσημέρι θα υπάρξει ένας εποικοδομητικός διάλογος που θα φωτίσει πολλές πτυχές των θεμάτων και θα οδηγήσει στη συναγωγή κάποιων χρήσιμων αποτελεσμάτων και συμπερασμάτων.

Ευχαριστώ πολύ.

ΖΑΜΠΙΡΑΣ Χ.:

Ευχαριστούμε τον Πρόεδρο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα κύριο Κωνσταντίνο Μενουδάκο για τον ενδιαφέροντα χαιρετισμό του και θα ήθελα να καλέσω στο βήμα τον Καθηγητή και Πρόεδρο της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων κύριο Κωνσταντίνο Μασσέλο για τον δικό του χαιρετισμό.

ΜΑΣΣΕΛΟΣ Κ.:

Αξιότιμε κύριε Πρόεδρε της Βουλής, αξιότιμε κύριε Πρόεδρε της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, κυρίες και κύριοι, ευχαριστώντας για την πρόσκληση που απευθύνατε προς την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων και εμένα προσωπικά, θα ήθελα να συγχαρώ την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών για την ημερίδα που διοργανώνει με θέμα τις σύγχρονες προκλήσεις στο απόρρητο των επικοινωνιών ως η καθ' ύλην αρμόδια Αρχή που, κατ' επέκταση του Συντάγματος, έχει σκοπό την προστασία του απορρήτου των επικοινωνιών, ηλεκτρονικών και ταχυδρομικών.

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχει αρκετές φορές στο παρελθόν συνεργαστεί με την Αρχή Διασφάλισης

του Απορρήτου των Επικοινωνιών, τόσο σε θέματα που αφορούν το απόρρητο των επικοινωνιών όσο και σε θέματα που αφορούν την ακεραιότητα και διαθεσιμότητα των επικοινωνιών όπως προβλέπεται στο άρθρο 37 του Νόμου 4070/2012.

Στην περίπτωση της διασφάλισης του απορρήτου των επικοινωνιών, όπου έχει παραστεί ανάγκη, η ΕΕΤΤ έχει συνδράμει σε σχετικούς ελέγχους την ΑΔΑΕ, με την παροχή του κατάλληλου προσωπικού και εξειδικευμένου εξοπλισμού για τον έλεγχο ραδιοφάσματος αναφορικά με τον εντοπισμό παράνομου εξοπλισμού κινητής τηλεφωνίας. Όσον αφορά τις ταχυδρομικές υπηρεσίες, οφείλουμε να επισημάνουμε ότι, διαχρονικά, έχει υπάρξει στενή συνεργασία ανάμεσα στην ΕΕΤΤ και την ΑΔΑΕ, σε σημαντικά θεσμικά θέματα όπως η σύνταξη των κανονιστικών κειμένων της κάθε Αρχής ή άλλες ειδικές περιστάσεις όπως τρομοκρατικές ενέργειες μέσω ταχυδρομείου· έχει υπάρξει ουσιαστική σύμπραξη, ώστε το πλαίσιο λειτουργίας κάθε Αρχής όχι μόνο να μην έρχεται σε αντίθεση αλλά να διευκολύνει και να εξυπηρετεί και τους σκοπούς του άλλου, στο πλαίσιο του νόμου και του κοινού στόχου της εύρυθμης λειτουργίας της ταχυδρομικής αγοράς.

Φυσικά, η ΕΕΤΤ φροντίζει και ανταποκρίνεται άμεσα σε αιτήματα ενημέρωσης της ΑΔΑΕ σχετικά με τα επικαιροποιημένα στοιχεία του Μητρώου ταχυδρομικών επιχειρήσεων που τηρεί, όπως νέες εγγραφές και διαγραφές επιχειρήσεων, πληροφορία σημαντική για την αποτελεσματική άσκηση των ιδιαίτερα σημαντικών ρυθμιστικών και ελεγκτικών αρμοδιοτήτων της ΑΔΑΕ.

Στο πλαίσιο της εποπτείας και ελέγχου για την εξασφάλιση της ακεραιότητας και διαθεσιμότητας των ηλεκτρονικών επικοινωνιών, ο Νόμος 4070/2012 προβλέπει ότι οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά την ασφάλεια των δικτύων και υπηρεσιών. Τα παραπάνω μέτρα καθορίζονται από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών με κανονιστικές πράξεις. Στο πλαίσιο εφαρμογής των παραπάνω κανονιστικών πράξεων, η ΕΕΤΤ μπορεί να εκδίδει δεσμευτικές υποδείξεις. Κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που έχει σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών των παρόχων ηλεκτρονικών επικοινωνιών γνωστοποιείται στην ΕΕΤΤ, η οποία με τη σειρά της την κοινοποιεί στην ΑΔΑΕ. Ο έλεγχος ασφάλειας διενεργείται από την ΑΔΑΕ, η οποία θέτει τα σχετικά πορίσματά της στη διάθεση της ΕΕΤΤ. Ειδικότερα σε περιπτώσεις υποβολής καταγγελιών ή περιστατικών ασφάλειας σε μια Αρχή που αφορά αρμοδιότητα της άλλης, γίνεται σχετική προώθηση των υποθέσεων για την περαιτέρω επεξεργασία και έρευνα. Η συγκεκριμένη συνεργασία έχει πραγματοποιηθεί σε αγαστό επίπεδο και με εποικοδομητικά μέσα και έχει αποφέρει άριστα αποτελέσματα.

Σκοπός μας είναι να συνεχίσουμε να υπηρετούμε τους πολίτες και να προσφέρουμε στην κοινωνία με τον ίδιο τρόπο και με τη βέλτιστη συνεργασία μεταξύ των Αρχών μας.

Κλείνοντας, εύχομαι καλή επιτυχία στις εργασίες της ημερίδας και σας ευχαριστώ πολύ.

ΖΑΜΠΙΡΑΣ Χ.:

Ευχαριστούμε πολύ τον Πρόεδρο της ΕΕΤΤ κύριο Κωνσταντίνο Μασσέλο.

Οι δύο τελευταίοι χαιρετισμοί, του κυρίου Μενουδάκου και του κυρίου Μασσέλου, ανέδειξαν ουσιαστικά και τη στενή συνεργασία που υπάρχει μεταξύ της ΑΔΑΕ και των δυο αυτών Ανεξάρτητων Αρχών για κοινού ενδιαφέροντος ζητήματα· πραγματικά, η συνεργασία αυτή είναι πάρα πολύ εποικοδομητική μέχρι στιγμής, φαντάζομαι ότι θα συνεχίσει να είναι έτσι και στο μέλλον.

Θα ήθελα να καλέσω τώρα στο βήμα τον κύριο Ιωάννη Ταφύλλη, Διευθυντή του Κέντρου Μελετών Ασφάλειας, για να απευθύνει τον δικό του χαιρετισμό στην ημερίδα.

ΤΑΦΥΛΛΗΣ Ι.:

Αξιότιμε κύριε Πρόεδρε της Βουλής, αξιότιμε κύριε Πρόεδρε της ΑΔΑΕ, εκλεκτοί προσκεκλημένοι, η βιομηχανική εποχή βασίστηκε σε πολύ μεγάλο βαθμό σε εξορυκτικές τεχνολογίες που παρήγαγαν αξία από την εκμετάλλευση των φυσικών πόρων· και η εποχή μας βασίζεται επίσης σε εξορυκτικές τεχνολογίες, με τη διαφορά ότι οι τεχνολογίες αυτές δεν είναι πλέον αντλίες ή γεωτρύπανα ούτε τα παράγωγά τους χαρακτηρίζονται από φυσικές ιδιότητες, καθώς οι νέες τεχνολογίες που εξελίσσονται διαρκώς είναι υπολογιστές, πομποί, λογισμικό και έξυπνοι αισθητήρες, και ένα σημαντικό παράγωγό τους είναι οι προσωπικές πληροφορίες.

Οι νέες τεχνολογίες συλλογής προσωπικών πληροφοριών μπορούν να διερευνούν σε ολοένα και μεγαλύτερο βάθος και πλάτος, χωρίς να γίνονται αντιληπτές, ξεπερνώντας τα εμπόδια -φυσικά και τεχνητά- που ιστορικά προστάτευαν τα προσωπικά δεδομένα. Σήμερα είναι εύκολο να αποκαλύπτεται το αόρατο, το άγνωστο, το ξεχασμένο, ή το παρακρατημένο. Η τεχνολογική αυτή πίεση μετατοπίζει διαρκώς και τη διαχωριστική γραμμή μεταξύ της δημόσιας και της ιδιωτικής σφαίρας, σε βάρος -δυστυχώς- της τελευταίας. Σε ένα περιβάλλον όπου αυξάνεται διαρκώς ο όγκος των προσωπικών δεδομένων που καταγράφονται, επεξεργάζονται και παρακολουθούνται, πολλά από αυτά που λέμε, κάνουμε, ή ακόμα και αισθανόμαστε, μπορεί να είναι γνωστά και καταγεγραμμένα -με τη θέλησή μας ή όχι- από άλλους που δεν γνωρίζουμε. Ψηφιακά δεδομένα, ανεξάρτητα της μορφής με την οποία καταχωρούνται, ανεξάρτητα τοποθεσίας, οργανισμού, ή και χρονικής περιόδου, μπορούν πλέον εύκολα σήμερα να συγχωνεύονται, να συσχετίζονται και να αναλύονται. Χαρακτηριστικό παράδειγμα των δυνατοτήτων αυτών αλλά και των κινδύνων που διαγράφονται είναι το παράδειγμα επεξεργασίας και εκμετάλλευσης προσωπικών δεδομένων δεκάδων εκατομμυρίων χρηστών από την πλατφόρμα του Facebook για τις ανάγκες της προεκλογικής εκστρατείας στις ΗΠΑ, ένα πολύ σοβαρό ζήτημα που απασχόλησε πρόσφατα την επικαιρότητα.

Οι νέες τεχνολογίες χωρίς το κατάλληλο πλαίσιο μπορούν να δημιουργήσουν πολύ σοβαρά ζητήματα, που είμαι βέβαιος ότι θα απασχολήσουν τη σημερινή ημερίδα, όπως είναι η αδικία, η εισβολή, η απουσία θεσμοθετημένης ενημέρωσης, η παράκαμψη θεσμοθετημένων διαδικασιών, η εξαπάτηση, η χειραγώγηση, τα λάθη, η παρενόχληση, η κατάχρηση ιδιοκτησίας και η μειωμένη αυτονομία. Η προστασία της ιδιωτικότητας, δεδομένου ότι περιλαμβάνει τον έλεγχο προσωπικών πληροφοριών, βρίσκεται στον πυρήνα πολλών από τις κοινωνικές αυτές ανησυχίες που εγείρονται από τις νέες τεχνολογίες της πληροφορίας. Πολιτικές και πρακτικές που έχουν ως βάση τη θεωρία ότι η ιδιωτικότητα είναι ασυμβίβαστη με την πληροφορική

επανάσταση δεν μπορούν και δεν πρέπει να έχουν θέση στις σύγχρονες δημοκρατίες.

Οι τεχνολογίες, όπως επισήμανε και ο κύριος Πρόεδρος της Βουλής, θα πρέπει να πάρουν τον δρόμο τους. Ωστόσο, είναι επιτακτικό να εξελίσσεται παράλληλα και το πλαίσιο διαχείρισής τους σε κοινωνικό, θεσμικό, επιστημονικό, τεχνολογικό, πολιτιστικό αλλά και δεοντολογικό επίπεδο.

Εκπροσωπώντας το Κέντρο Μελετών Ασφάλειας, έναν φορέα ο οποίος εξειδικεύεται στην έρευνα τεχνολογιών που σχετίζονται με την ασφάλεια, επιτρέψτε μου κλείνοντας να κάνω μερικές επισημάνσεις, κύρια τεχνολογικού χαρακτήρα.

Θα ήθελα να εστιάσω στην πολύ στενή σχέση που υπάρχει ανάμεσα στην προστασία του απορρήτου και της ιδιωτικότητας με τα τεχνολογικά προαπαιτούμενα της κυβερνοασφάλειας.

Να εστιάσω, επίσης, στις ιδιαιτερότητες που παρουσιάζει η χώρα μας στον τομέα. Η μέχρι σήμερα ανάπτυξη ψηφιακών υποδομών, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, δεν έλαβε -στον βαθμό που θα έπρεπε υπ' όψιν τις απαιτήσεις της ασφάλειας και η εκ των υστέρων παρέμβαση για τη θωράκισή τους και την προστασία του απορρήτου και της ιδιωτικότητας είναι ένα δύσκολο εγχείρημα, που δεν πρέπει να υποτιμηθεί.

Τα νέα έργα και οι ψηφιακές παρεμβάσεις είναι επιβεβλημένο πλέον να συμπεριλαμβάνουν την ασφάλεια και την προστασία των προσωπικών δεδομένων ως αναπόσπαστο στοιχείο από τη φάση του σχεδιασμού.

Δυστυχώς, υπάρχει ακόμα στη χώρα κατακερματισμός των αρμοδιοτήτων, ένας τομέας τον οποίο οφείλουμε να υπερβούμε. Ένα τεχνολογικό περιβάλλον που εξελίσσεται με πρωτόγνωρους ρυθμούς απαιτεί ταχύτητα προσαρμογής, ταχύτητα αντίδρασης και τη θεσμοθέτηση συνεργειών μεταξύ όλων των εμπλεκόμενων φορέων, κύρια μεταξύ των φορέων άσκησης πολιτικής, των φορέων εσωτερικής ασφάλειας, της ΑΔΑΕ, αλλά και των φορέων παραγωγής γνώσης στον τομέα, όπως είναι τα πανεπιστήμια και τα ερευνητικά κέντρα.

Θα ήθελα να ευχαριστήσω για άλλη μια φορά την ΑΔΑΕ για την πρόσκληση και να ευχηθώ η σημερινή πρωτοβουλία να βρει πολύ σύντομα μιμητές.

Ευχαριστώ πολύ.

ΖΑΜΠΙΡΑΣ Χ.:

Ευχαριστούμε τον κύριο Ταφύλλη για την πολύ ενδιαφέρουσα εισαγωγική του ομιλία, όπου έθιξε όλα τα ζητήματα τεχνολογίας, πληροφορικής, ασφάλειας απορρήτου κ.λπ.

Θα ήθελα να καλέσω τον κύριο Γεώργιο Παπαπροδρόμου, Ταξίαρχο και Διευθυντή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, για τον δικό του χαιρετισμό, λέγοντας ταυτόχρονα ότι η συνεργασία της ΑΔΑΕ με τη Δίωξη Ηλεκτρονικού Εγκλήματος συνεχίζεται εποικοδομητική όπως ήταν μέχρι τώρα.

ΠΑΠΑΠΡΟΔΡΟΜΟΥ Γ.:

Ευχαριστώ, κύριε Πρόεδρε.

Κύριε Πρόεδρε της Βουλής, αξιότιμε κύριε Πρόεδρε, κύριε Αντιπρόεδρε, κύριοι Πρόεδροι των Ανεξάρτητων Αρχών, κυρίες και κύριοι, για εμάς αποτελεί χαρά και τιμή να βρισκόμαστε στην εκδήλωση αυτή και ευχαριστούμε για την πρόσκληση.

Μια διαφωνία θα μου επιτρέψετε, κύριε Πρόεδρε. Μπορεί να γράφεται «Δίωξη Ηλε-

κτρονικού Εγκλήματος», αλλά την αντιλαμβανόμαστε ως «Διεύθυνση Πρόληψης και Δίωξης Εγκλημάτων στον Κυβερνοχώρο», που και επιστημονικά ο όρος αυτός αποδίδει περισσότερο την πραγματικότητα.

Η πρόληψη είναι στρατηγική επιλογή. Δεν είναι τυχαίο ότι κλείνουμε περίπου έναν χρόνο που τέτοιο καιρό είχαμε με το Υπουργείο Παιδείας ένα μνημόνιο συνεργασίας, γιατί πιστεύουμε ότι θα πρέπει να υπάρξει μια δημιουργία κουλτούρας και εμπιστοσύνης, και αυτό πρέπει να ξεκινάει από τη μικρή ηλικία, γι' αυτό και η Υπηρεσία μας έδωσε το παρόν τη χρονιά που πέρασε σε 368 σημεία σε όλη τη χώρα, με πάνω από 30.000 παιδιά και γονείς, γιατί αυτά τα παιδιά αύριο-μεθαύριο θα στελεχώσουν τον δημόσιο και ιδιωτικό τομέα.

Τώρα, να επισημάνω ότι ως Υπηρεσία έχουμε άψογη συνεργασία με όλες τις Ανεξάρτητες Αρχές, και θα ήθελα τις να ευχαριστήσω, γιατί πιστεύουμε στη θεσμική θωράκιση κατ' αρχήν και στην ενίσχυση του πλαισίου αυτού. Αν θα μπορούσαμε με τρεις λέξεις να αποδώσουμε την πραγματικότητα που βιώνουμε, θα έλεγα πως από τη μια έχουμε τις λέξεις "software" και "hardware", που είναι δημιουργήματα του ανθρώπου, αλλά το σημαντικότερο στοιχείο που έχουμε σαν πρόκληση σήμερα είναι το "humanware". Πρέπει να καταλάβουμε ότι ζούμε σε ένα περιβάλλον διεθνών προκλήσεων, όπου κανείς δεν μπορεί να πει σήμερα ότι το στοιχείο της απόλυτης ασφάλειας είναι δεδομένο· θα είναι πάντοτε ζητούμενο! Στην κατεύθυνση αυτή, συνεργαζόμαστε όχι μόνο σε θεσμικό επίπεδο μέσα στη χώρα μας αλλά και έξω, στο ευρωπαϊκό και διεθνές περιβάλλον, και αναφέρομαι στη διεθνή αστυνομική συνεργασία με την Europol και την Interpol, αλλά και την Eurojust και άλλους θεσμούς.

Στο οργανόγραμμα που η Υπηρεσία μας λειτουργεί -ουσιαστικά, πριν τρία χρόνια έχει «κλείσει» ως Διεύθυνση την παρουσία της, καλύπτοντας τον ελλαδικό χώρο με μια υποδιεύθυνση στη Βόρεια Ελλάδα- υπάρχει ειδικό τμήμα στα θέματα των επικοινωνιών. Για εμάς, θέμα-κλειδί είναι το θέμα της ιδιωτικότητας, τόσο στην ατομική της διάσταση, δηλαδή το δικαίωμα του ατόμου να διαχειρίζεται τα δεδομένα που το αφορούν, όσο και στη συλλογική· ακριβώς πριν έναν χρόνο είχαμε την περίπτωση του WannaCry, που χτύπησε το Εθνικό Σύστημα Υγείας της Βρετανίας, κάτι που ανέδειξε τη σημαντικότητα των θεμάτων που εγείρονται και νομίζω ότι έχουμε μπροστά μας πολλά θέματα να δούμε, όμως θεωρούμε ότι η συνεργασία θα είναι η λέξη-κλειδί.

Στο γράφημα που βλέπετε μπροστά σας φαίνεται η διάρθρωση της Υπηρεσίας, με τρία επιχειρησιακά τμήματα και δύο υποστηρικτικά· δίνουμε έμφαση στα υποστηρικτικά τμήματα, που αφορούν τη διαχείριση και την ανταλλαγή των πληροφοριών αλλά και τις καινοτόμες δράσεις και τη στρατηγική. Να πούμε ότι το τρίτο τμήμα χειρίζεται τα θέματα όπου αναφερόμαστε σήμερα, έχοντας άψογη συνεργασία -όπως τονίσατε, κύριε Πρόεδρε- με την ΑΔΑΕ και θέλοντας αυτή τη συνεργασία να την ενισχύσουμε στο μέλλον.

Επίσης, υπάρχει η πρότασή μας και η συνεργασία με τις δικαστικές Αρχές, απ' όπου ζητήσαμε τη θεσμική θωράκιση. Έχουμε ζητήσει να υπάρξει ειδικός δικαστικός λειτουργός, πιστεύουμε και αισιοδοξούμε ότι θα γίνει αυτό, να έχουμε ειδικό εισαγγελικό λειτουργό, εξειδικευμένο, ο οποίος θα αντιμετωπίζει αυτά τα θέματα. Στη χώρα μας έχουμε την πολυτέλεια να έχουμε 63 εισαγγελικές περιφέρειες, έναν μεγάλο κατακερματισμό όπως

καταλαβαίνετε, και υπάρχει ανάγκη εξειδίκευσης. Πρόσφατα, και θέλω να ευχαριστήσουμε την Εισαγγελέα του Αρείου Πάγου, τοποθετήθηκε ανώτατος δικαστικός λειτουργός που εποπτεύει τη Διεύθυνσή μας, κάτι που νομίζω ότι είναι στη θετική κατεύθυνση.

Υπάρχουν συνεργασίες -όπως περιγράφονται στο γράφημα- με τις Αρχές, το CERT και λοιπά, επίσης με τους ISPs, αλλά και με τα εκπαιδευτικά ιδρύματα, με τα οποία -όπως τονίσατε- είναι πάρα πολύ σημαντική η συνεργασία. Υπάρχουν συνεργασίες και με τους φορείς στο εξωτερικό, κι εδώ συμπεριλαμβάνουμε και τον ENISA, ενώ έχουμε ειδικό κέντρο στη Χάγη, το European Cybercrime Centre, στο οποίο συμμετέχουμε. Πάνω κάτω, τα προβλήματα είναι κοινά για όλους μας.

Από τις δράσεις που βλέπετε στη διαφάνεια, να τονίσω ότι πολύ σημαντική είναι η GAAD, και ήμασταν η μοναδική χώρα στον πλανήτη που συμμετείχαμε στην Global Airport Action Day με όλα μας τα αεροδρόμια, που αυτό δείχνει τη στρατηγική μας επιλογή να έχουμε μια ολιστική προσέγγιση στα θέματα ασφάλειας, με ιδιαίτερο στόχο την αντιμετώπιση των απατών στον χώρο των αερομεταφορών. Επίσης σημαντική η καμπάνια "say no!", που αφορά τα παιδιά μας! Να αναφέρουμε και το "no more ransom", καθώς είχαμε φέτος πάρα πολλές περιπτώσεις επιχειρήσεων, δυστυχώς και στη χώρα μας, καθόσον οι μικρομεσαίες επιχειρήσεις δεν επενδύουν στο κομμάτι IT και υπάρχει απουσία πολιτικών ασφάλειας και εκπαίδευσης του προσωπικού, που είναι πολύ σημαντικό κομμάτι.

Εδώ βλέπετε απεικόνιση από τη συνάντηση που είχαμε για το Δίκτυο 24/7. Στο Δίκτυο αυτό μετέχουν 57 + 4 χώρες στον πλανήτη, επομένως είναι σημαντικό να έχουμε Σημείο Επαφής. Θα σταθώ μόνο σε αυτή τη διαφάνεια όπου βλέπετε τον παγκόσμιο πληθυσμό. Θα πρέπει να έχουμε υπ' όψιν μας ότι πάνω από το 50% του πληθυσμού που βλέπετε στη διαφάνεια είμαστε χρήστες, «εδώ» ανήκουμε, «εδώ» είναι η μεγάλη πρόκληση και «εδώ» επιβάλλεται να έχουμε τις συνεργασίες.

Κλείνοντας, θα αναφερθώ στην παρουσία μας στα μέσα κοινωνικής δικτύωσης. Εδώ είναι πολύ σημαντική η πύλη που υπάρχει στο αρχηγείο της Ελληνικής Αστυνομίας, όπου ο πολίτης -είναι μία μορφή e-government- μπορεί να προβεί σε καταγγελία, να παρακολουθήσει την πορεία της καταγγελίας του, γενικά υπηρετείται η διαφάνεια και είναι στη θετική κατεύθυνση. Έχουμε πολύ σημαντική -και πιστοποιημένη, θα έλεγα- παρουσία στα social media. Όπως βλέπετε στη διαφάνεια, το προφίλ μας αυτό είναι στο Facebook, όπου μπορείτε να δείτε στον μικρό κύκλο την πιστοποίηση. Φανταστείτε έναν πολίτη να νομίζει ότι επικοινωνεί με μια δημόσια Υπηρεσία και να είναι fake το προφίλ. Αυτό δεν θεωρείται δεδομένο. Πρόσφατα, επίσης, φτιάξαμε προφίλ και στο Instagram, όπου μετέχουν και τα παιδιά μας, γιατί θέλουμε να φτάσει το μήνυμα εκεί και θεωρούμε ότι θα πρέπει «να παίζουμε στο ίδιο γήπεδο» που παίζει η κοινωνία, πάντα σεβόμενοι τον πολίτη και τα δικαιώματά του.

Εκείνο που θα πω κλείνοντας είναι αυτό που πάντοτε επικαλούμαι από έναν μύθο της αρχαιότητας με τον Ηρακλή. Όταν βρισκόμαστε σε ένα δίστρατο, το τι θα ακολουθήσουμε είναι θέμα επιλογής· δεν φταίνε οι τεχνολογίες, είναι θέμα επιλογής.

Σας ευχαριστώ για την πρόσκληση, καλή επιτυχία στο συνέδριο.

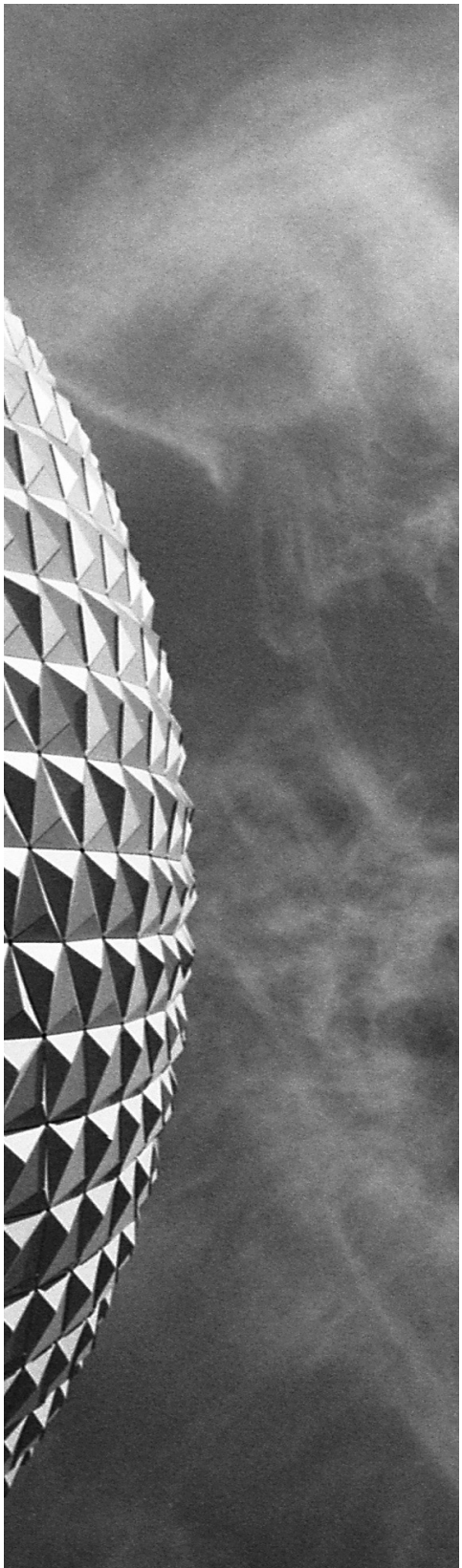
ΖΑΜΠΙΡΑΣ Χ.:

Ευχαριστούμε τον κύριο Παπαπροδρόμου ο οποίος μας ενημέρωσε για το τόσο σημαντικό έργο της Διεύθυνσης που προϊσταται.

Σε αυτό το σημείο κλείνει η ενότητα των χαιρετισμών, για να περάσουμε στην επόμενη, που είναι η ενότητα «Τεχνολογικές εξελίξεις και απόρρητο των επικοινωνιών».

Σε δέκα λεπτά, λοιπόν, ξεκινάμε την επόμενη ενότητα, στην οποία συντονιστής θα είναι ο Αντιπρόεδρος κύριος Σακκάς.

Ευχαριστώ πολύ όλους σας.



Α' ΕΝΟΤΗΤΑ

ΤΕΧΝΟΛΟΓΙΚΕΣ ΕΞΕΛΙΞΕΙΣ ΚΑΙ ΑΠΟΡΡΗΤΟ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΑΚΚΑΣ Μ. – Συντονιστής:

Κυρίες και κύριοι, περνάμε στη δεύτερη ενότητα· επειδή δεν είναι απεριόριστος ο χρόνος, και ο λόγος είναι ότι σε αυτή την αίθουσα -λόγω επισκευών της αίθουσας της Ολομέλειας- γίνονται και επιτροπές και συνέρχεται η κανονική Βουλή, γι' αυτό και κάνουμε αυτό τον περιορισμό.

Για την πρώτη ενότητα, που είναι για τις τεχνολογικές εξελίξεις και το απόρρητο των επικοινωνιών, θα παρακαλούσαμε κατ' αρχάς τον Αναπληρωτή Προϊστάμενο της Διεύθυνσης Κυβερνοασφάλειας στο Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης Δρ. Λέανδρο Μαγλαρά, που έκανε και τον χαιρετισμό εκ μέρους του Υπουργού κυρίου Παππά, να μας μιλήσει με θέμα «Η Κυβερνοασφάλεια στην Ελλάδα».

Παράκληση είναι να τηρούμε τα 12 λεπτά, για να μην ξεφύγουμε από το πρόγραμμα. Τα υπόλοιπα όσα δεν πείτε θα ανεβούν στο site μας και θα τα δει εκεί όποιος ενδιαφέρεται.

Ευχαριστώ.

Κύριε Μαγλαρά, έχετε τον λόγο.

ΜΑΓΛΑΡΑΣ Λ.:

Γεια σας και πάλι.

Ονομάζομαι Λέανδρος Μαγλαράς, είμαι Αναπληρωτής Προϊστάμενος της Διεύθυνσης Κυβερνοασφάλειας στο Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης και σήμερα θα σας μιλήσω σύντομα για την κυβερνοασφάλεια στην Ελλάδα.

Όταν λέμε «κυβερνοασφάλεια», τι ακριβώς εννοούμε; Εννοούμε όλες αυτές τις ενέργειες που χρειάζεται να γίνουν για να διασφαλίσουμε την πληροφορία, είτε αυτή είναι σε φυσική είτε σε ηλεκτρονική μορφή, όλα τα συστήματα και τα δίκτυα που χρησιμοποιούμε για να αποθηκεύσουμε την πληροφορία, να την επεξεργαστούμε, να την διανείμουμε από το ένα σημείο στο άλλο, προστατεύοντας από κακόβουλες ενέργειες, από ατυχήματα, από ιούς, από οτιδήποτε μπορεί να επιφέρει κάποια απώλεια στην πληροφορία ή κάποια αλλαγή στην πληροφορία ως έχει.

Ένα άλλο κομμάτι που απειλεί την κυβερνοασφάλεια, μια άλλη απειλή της κυβερνοασφάλειας είναι να χαθεί η εμπιστοσύνη, δηλαδή να χαθεί η εμπιστοσύνη των πολιτών, των χρηστών ενός συστήματος, κι αυτό μπορεί να οφείλεται στο να έχουν χαθεί κάποια δεδομένα, να έχει «πέσει» το σύστημα, ή σε οτιδήποτε άλλο μπορεί να επιφέρει την απώλεια της εμπιστοσύνης, καθώς επίσης αυτό μπορεί να συνεχιστεί και να έχει σαν αποτέλεσμα να πάψουν να υπάρχουν τηλεπικοινωνίες, ή να μην μπορούν να γίνουν ηλεκτρονικές συναλλαγές, ή -ακόμα χειρότερα- να υπάρχουν επιδράσεις στον τομέα της υγείας και, γενικά, να επηρεαστούν οι κρίσιμες υποδομές μιας χώρας.

Όταν μιλάμε για κρίσιμες υποδομές, εννοούμε όλα αυτά που χρειάζονται για να έχουμε αυτόν τον ευρωπαϊκό -κατά κάποια έννοια τρόπο ζωής, δηλαδή τα δίκτυα της ενέργειας, τη διανομή νερού, τη βιομηχανία, τα δίκτυα μεταφορών, είτε αυτά είναι επίγεια είτε είναι τα αεροπλάνα κ.λπ. Όλα αυτά, λοιπόν, αποτελούν κρίσιμες υποδομές.

Και, φυσικά, δεν μπορεί κανένας να μελετήσει ένα σύστημα σε απομόνωση και να πει «…εγώ ασφαλίζω το δικό μου σύστημα και είμαι εντάξει…», γιατί υπάρχουν πάντα αλληλεξαρτήσεις μεταξύ των διαφόρων δικτύων, με κύριο δίκτυο αυτή τη στιγμή -όπως συζητιέται στην Ευρωπαϊκή Ένωση- να είναι

το δίκτυο της ενέργειας· αν υπάρχει κάποια βλάβη στο δίκτυο της ενέργειας, τότε αυτό θα έχει σαν αποτέλεσμα να επηρεαστούν όλα τα υπόλοιπα δίκτυα, δηλαδή οι διανομές, η τροφοδοσία του νερού, οτιδήποτε άλλο χρησιμοποιούμε.

Επίσης, ένα κράτος δεν μπορεί να πει ότι θα ασφαλίσει τα δικά του δίκτυα και θα είναι καλυμμένο, γιατί υπάρχουν και αλληλεξαρτήσεις μεταξύ των διαφόρων δικτύων των γειτονικών κρατών. Στο πλαίσιο αυτό, η Ευρωπαϊκή Ένωση έχει κάνει μια ειδική ομάδα εργασίας, που λέγεται «Αλληλεξαρτήσεις μεταξύ διαφόρων δικτύων των ευρωπαϊκών κρατών», στην οποία συμμετέχουμε και στην οποία συνδιαμορφώνουμε κάποιες πολιτικές, κάποια μέτρα, κάποιους τρόπους ώστε να διασφαλίσουμε ότι κάποια ζημιά που θα συμβεί σε ένα δίκτυο, σε μια χώρα, δεν θα περάσει ανεμπόδιστα στη γειτονική χώρα. Δυστυχώς, αυτό γίνεται μόνο στο πλαίσιο της Ευρωπαϊκής Ένωσης, δηλαδή μόνο με τα γειτονικά μας κράτη που ανήκουν στην Ευρωπαϊκή Ένωση.

Τώρα, στο κέντρο των κρίσιμων υποδομών υπάρχουν τα βιομηχανικά δίκτυα, τα οποία κάποτε ήταν απομονωμένα και δεν κινδύνευαν, αλλά πλέον έχουν διασυνδεθεί με τα δίκτυα IT και αυτό έχει σαν αποτέλεσμα να έχουν πολλές ευπάθειες και πολλές απειλές.

Οι λόγοι βρίσκονται:

Στην ποικιλία των εκδόσεων και των προϊόντων, καθώς υπάρχουν πολλές διαφορετικές εκδόσεις, και σε hardware και σε software, που έχει ο καθεμία τις δικές της ευπάθειες.

Στη διεύρυνση των δικτύων, καθόσον πλέον μια εταιρία, μια κρίσιμη υποδομή, δεν είναι κεντρικοποιημένη σε ένα κτίριο, αλλά έχει διάφορα δίκτυα που συνεργάζεται, είτε με VPN είτε με μισθωμένες γραμμές, με αποτέλεσμα να ανοίγει το attack service όπως λέγεται, δηλαδή να υπάρχουν περισσότερα σημεία εισόδου για να μπεις στο κεντρικό δίκτυο.

Στη γήρανση του εξοπλισμού.

Στην απλότητα των δεδομένων στα βιομηχανικά δίκτυα, καθώς πολλά δεδομένα μεταφέρονται χωρίς κρυπτογράφηση, σε απλό κείμενο και με σειριακό τρόπο· θα σας δείξω ένα παράδειγμα παρακάτω και είναι πολύ απλό να μπορέσεις να κλέψεις αυτή την πληροφορία, να την αλλάξεις και να επέμβεις πάνω στο δίκτυο, π.χ. στη λειτουργία μιας βιομηχανίας.

Στην επεξεργασία σε πραγματικό χρόνο. Τι σημαίνει αυτό; Δεν έχω τα δεδομένα μου offline, να κάτσω να κάνω data mining, να μαζέψω τα δεδομένα, να βγάλω στατιστικά και να πω ότι αυτό συνέβη ή αυτό θα συμβεί. Εδώ υπάρχει ανταλλαγή πληροφοριών σε πραγματικό χρόνο και αυτό έχει σαν αποτέλεσμα, κατά πρώτον, να μην μπορώ να κάνω ελέγχους εκείνη τη στιγμή. Κάναμε δοκιμαστικά με vulnerability scan σε ένα δίκτυο SCADA και είδαμε ότι κατεβαίνει το επίπεδο της απόδοσης του δικτύου πάρα πολύ, και αυτό δεν είναι επιτρεπτό όταν μιλάς για δίκτυο που ρυθμίζει την ενέργεια ή τις τηλεπικοινωνίες μιας χώρας. Ένα άλλο παράδειγμα, που λένε και πολλοί άλλοι ερευνητές, είναι ότι δεν μπορείς να κάνεις patching τα δίκτυα αυτά σε real time γιατί, όταν πας να το κάνεις, μπορεί να συμβεί ένα γεγονός που δεν το περίμενες -λόγω του patching- και να πέσει μια ολόκληρη περιοχή. Οπότε αυτά είναι θέματα που πρέπει να τα λαμβάνει υπ' όψιν κάθε ένας που χειρίζεται τέτοια δίκτυα.

Στη διασύνδεση με άλλα συστήματα πληροφοριών, όπως είπαμε και πριν.

Στη γενίκευση του εξοπλισμού, όπου πλέον χρησιμοποιούνται παντού IP πρωτόκολλα.

Στο internet of things, όπου όλα πλέον διασυνδέονται· δεν είναι κάτι απομονωμένο και μπορείς να το κοιτάξεις μόνο του και να το λύσεις.

Οι απειλές είναι εσωτερικές και εξωτερικές, κακόβουλες ή μη, μπορεί κατά λάθος να ανοίξω ένα e-mail που λέει «…κάντε κλικ εδώ για να κερδίσετε ένα εκατομμύριο ευρώ» και να περάσει ένας ιός στον υπολογιστή μου, στο δίκτυο, που μετά καταλήγει στα κεντρικά συστήματα της επιχείρησης. Επίσης, κάποιος κακεντρεχής υπάλληλος ο οποίος θέλει να κάνει ζημιά στην εταιρία του, είτε γιατί απολύεται είτε γιατί πρόκειται να απολυθεί είτε γιατί για οποιονδήποτε άλλο λόγο, και υπάρχουν πολλά παραδείγματα καταγεγραμμένα στη βιβλιογραφία. Επιπλέον, εξωτερικές -κερδοσκοπικές ή σκόπιμες- απειλές, κάποιοι χάκερς απλά παίζουν ή κάποιοι χάκερς είναι εντεταλμένοι από κάποια άλλη εταιρία, από κάποιο άλλο κράτος, να κάνουν ζημιά με απώτερο σκοπό ανάλογα από πού έχουν μισθωθεί.

Αν μιλήσουμε για το διαδίκτυο των πραγμάτων, μπορούμε να πούμε ότι υπάρχουν τέσσερεις ξεχωριστοί τομείς που το δημιουργούν, και αυτά είναι η επικοινωνία machine to machine, δηλαδή η επικοινωνία διαφόρων συσκευών μεταξύ τους, το internet of energy που γεννιέται, τα smart meters κ.λπ., το internet of vehicles, δηλαδή τα αυτοκινούμενα οχήματα που έχουν πλέον τη δυνατότητα να επικοινωνούν είτε μέσω DSRC είτε μέσω κινητής τηλεφωνίας, καθώς και το internet of sensors, δηλαδή οι sensors που βάζουμε παντού για να κάνουμε κάποια βελτιστοποίηση σε κάποιον παράγοντα που έχουμε αποφασίσει.

Επίσης, υπάρχει ένα classification των επιθέσεων στο internet of things.

Τώρα, όταν μιλάμε για κυβερνοασφάλεια, δεν μπορεί να ξεχνάμε ότι υπάρχει και κυβερνοτρομοκρατία, όπως θα μας έλεγε και ο κύριος Παπαπροδρόμου ακόμα καλύτερα. Ένας τρόπος για να κάνεις κυβερνοτρομοκρατία είναι να τρομάξεις τον κόσμο. Κάναμε ένα πείραμα κάποια στιγμή, λοιπόν, ανεβάζοντας ένα βίντεο στο Facebook, στο οποίο δείχναμε -από έναν αμερικάνικο Οργανισμό, το DARPA- έναν ιό που έκανε το laptop να εκραγεί. Ευτυχώς, δεν πήγαμε φυλακή, αλλά -κάνοντας ένα ερωτηματολόγιο στο κοινό πριν, και μετά το βίντεο- είδαμε ότι άλλαξε πάρα πολύ ο τρόπος που αντιμετώπιζαν το θέμα της κυβερνοασφάλειας και ο φόβος που είχαν πλέον απέναντι στις κυβερνοεπιθέσεις. Δύο πράγματα διαπιστώσαμε, πόσο εύκολα διαδίδεται μια ψεύτικη είδηση, πόσο γρήγορα διαδόθηκε σε όλο το διαδίκτυο, σε όλο το Facebook, και πώς επηρέασε τον κόσμο κατόπιν. Φυσικά, στο τέλος υπήρχε μια ειδοποίηση ότι όλα αυτά είναι ψεύτικα, είναι στο πλαίσιο ενός πειράματος, ενώ βγάλαμε και κάποιες ανακοινώσεις κατόπιν για να γλυτώσουμε από τις διωκτικές Αρχές· αυτό έγινε στην Αγγλία, οπότε εντάξει.

Ένα άλλο θέμα που έχουμε να πούμε είναι ότι, όπως είπε πριν και ο κύριος Παπαπροδρόμου, η πιο σημαντική πτυχή όσον αφορά την ασφάλεια στον κυβερνοχώρο είναι η ανθρώπινη συμπεριφορά. Ό,τι πολιτικές και να έχουμε, ό,τι διαδικασίες και να έχουμε, ό,τι μέτρα και να έχουμε πάρει, πάντα, αν ο άνθρωπος δεν ακολουθήσει, ο χρήστης, ο διαχειριστής, ο οποιοσδήποτε συναλλάσσεται με το σύστημά μας, θα υπάρχει πρόβλημα.

Στο πλαίσιο αυτό υπάρχουν διάφορα frameworks τα οποία αντιμετωπίζουν αυτή την κατάσταση· εμείς δημιουργήσαμε ένα καινούργιο, το HEART-IS, το οποίο εισάγει τα ανθρώπινα σφάλματα μέσα στα περιστατικά ασφαλείας πληροφοριακών συστημάτων, το δοκιμάσαμε σε κάποια νοσοκομεία στην Αγγλία και πιστεύουμε ότι είναι κάτι το οποίο είχε πάρα πολύ καλά αποτελέσματα, ενώ μπορεί ακόμα και να έρθει στην Ελλάδα κάποια στιγμή και να εφαρμοστεί σε διάφορα ιδρύματα της Ελλάδας.

Θα κλείσω το αρχικό κομμάτι, που είναι λίγο ερευνητικό, με άλλο ένα παράδειγμα, που λέγαμε πριν. Σε ένα δίκτυο που έχουμε ένα PLC και έναν υπολογιστή, «κλέψαμε» τα δεδομένα που ανταλλάσσει το PLC με τον υπολογιστή, φτιάξαμε έναν δικό μας κώδικα, τον ανεβάσαμε σε έναν web server και βάλαμε στον υπολογιστή αυτόν ένα ψεύτικο usb, που ο υπολογιστής αυτός το έβλεπε σαν πληκτρολόγιο με αποτέλεσμα να μη σταματάει το autorun, επομένως σταματήσαμε το autorun. Ωραία, και τι έγινε; Τίποτα. Αν αυτό, όμως, είχε συμβεί μέσα σε ένα μεγάλο βιομηχανικό δίκτυο, μπορεί να είχε συμβεί ακόμα και έκρηξη, μια μεγάλη ζημιά. Εδώ ποιος έφταιγε; Ο άνθρωπος. Οι πολιτικές υπήρχαν, οι διαδικασίες υπήρχαν, αλλά κάποιος πήγε και έβαλε το usb πάνω στον υπολογιστή. Βέβαια, όλο αυτό ήταν ένα πείραμα. Οπότε, φυσικά, χρειάζονται οι διαδικασίες, τα μέτρα, οι νόμοι, όλα τα κείμενα, αλλά χρειάζεται συνέχεια να εκπαιδεύουμε τον κόσμο.

Τώρα, η κυβερνοασφάλεια στην Ευρώπη έχει γίνει κεντρικό σημείο αναφοράς, γιατί μιλάμε για ενιαία ψηφιακή αγορά, για την ψηφιακή ατζέντα, και όλα αυτά δεν μπορούν να γίνουν αν δεν υπάρχει ένα σύστημα να εμπιστεύεσαι για να λειτουργείς επάνω. Το ίδιο και στην Ελλάδα, όπου ο ψηφιακός μετασχηματισμός πρέπει να στηριχτεί σε ένα ασφαλές περιβάλλον, γι' αυτό υπάρχει η Γενική Γραμματεία Ψηφιακής Πολιτικής, στην οποία κάνουμε κεντρικό σχεδιασμό των έργων του Δημοσίου, καθώς επίσης προσπαθούμε να εισάγουμε και την έννοια της ασφάλειας και της ιδιωτικότητας στα νέα έργα ΤΠΕ.

Η κύρια στρατηγική της χώρας είναι α. η ενίσχυση των ψηφιακών δεξιοτήτων, όπως είπα πριν, ώστε να εκπαιδεύσουμε τον κόσμο, τόσο τους δημόσιους υπαλλήλους όσο και τους απλούς πολίτες, β. η προσαρμογή του εθνικού θεσμικού πλαισίου στις νέες τεχνολογικές απαιτήσεις που συνεχώς αλλάζουν, φυσικά και στις ευρωπαϊκές Οδηγίες και τους ευρωπαϊκούς Κανονισμούς που συνεχώς βγαίνουν με σκοπό να θωρακίσουν την Ευρωπαϊκή Ένωση, γ. η επένδυση στην καινοτομία, έρευνα και ανάπτυξη, φυσικά σε σύμπραξη με τα πανεπιστήμιά μας και τα κέντρα ερευνών που έχουμε, καθώς και δ. η συνεργασία σε ευρωπαϊκό και διεθνές επίπεδο συμμετέχουμε και στο Cooperation Group της Ευρωπαϊκής Ένωσης και σε άλλες διεθνείς ομάδες που κοιτούν να κάνουν μέτρα εμπιστοσύνης να βγάλουνε κανόνες και μέτρα προστασίας για τα συστήματα των κρατών.

Οι δράσεις που έχουμε κάνει.

Όπως είπα πριν, επικαιροποιήσαμε την Εθνική Στρατηγική Κυβερνοασφάλειας, που είναι το πρώτο στάδιο, είναι οι κεντρικοί στόχοι, το τι πρέπει να γίνει. Όλα αυτά μετά πρέπει να υλοποιηθούν, σιγά-σιγά να γίνουν ακριβείς δράσεις, σε συνεργασία πάντα με τους συναρμόδιους φορείς.

Προσπαθούμε να κάνουμε αποτύπωση του επιπέδου ασφαλείας των πληροφοριακών συστημάτων των κεντρικών δομών των υπουργείων, έχουμε στείλει ένα ερωτηματολόγιο το οποίο είναι η αρχή και, με βάση αυτή την αποτύπωση και κάποια audits που θα κάνουμε αργότερα, θα μπορέσουμε να κάνουμε συγκεκριμένες δράσεις για να αυξήσουμε την ασφάλεια σε συγκεκριμένα συστήματα.

Υπάρχει εποπτεία και έλεγχος εφαρμογής κανόνων και πολιτικών ασφαλείας στο Δημόσιο και σε κρίσιμες υποδομές.

Είπαμε ότι έχουμε βγάλει μέτρα και απαιτήσεις ασφαλείας και ιδιωτικότητας για όλα τα νέα έργα ΤΠΕ, τα οποία θα συνοδεύουν τα νέα έργα που εγκρίνονται.

Έχουμε κάποιες δράσεις εκπαίδευσης και ενημέρωσης σε θέματα κυβερνοασφάλειας, όπως ένα συνέδριο του ΟΑΣΠ ή με συμμετοχή σε διάφορες ημερίδες. Συμμετέχουμε και σε ενημερώσεις που κάνει ο ENISA, συνδιοργανώνουμε κάποιες ενημερώσεις και άλλα τέτοια αντίστοιχα θέματα.

Είμαστε Εθνική Αρχή Κυβερνοασφάλειας και Ενιαίο Κέντρο Επαφής, σύμφωνα με την Οδηγία NIS, με σκοπό να συντονίσουμε τον δημόσιο τομέα, την Ελλάδα γενικότερα, εσωτερικά, και να ερχόμαστε σε επαφή με τα υπόλοιπα κράτη-μέλη όσον αφορά τη διαχείριση κρίσεων, τη διαχείριση εγκλημάτων και κυβερνοεπιθέσεων.

Έχουμε ολοκληρώσει διαγωνισμό που θα προκηρυχτεί τις επόμενες μέρες για εναρμόνιση του Υπουργείου μας με το GDPR.

Συμμετέχουμε σε ασκήσεις, και του ΝΑΤΟ και του ENISA και της Ευρωπαϊκής Ένωσης, σε θέματα κυβερνοασφάλειας.

Η Εθνική Στρατηγική Κυβερνοασφάλειας, που υπάρχει στη Διαύγεια από τις 07/03, έχει διάφορα σημαντικά σημεία, όπως η αποτύπωση των φορέων, ο ορισμός των κρίσιμων υποδομών, το εθνικό σχέδιο έκτακτης ανάγκης και ούτω καθεξής, τα οποία μπορείτε να τα δείτε και οι ίδιοι αν κοιτάξετε την Εθνική Στρατηγική, η οποία -όπως είπαμε- είναι αποτέλεσμα δουλειάς πάρα πολλών φορέων, για πολύ μεγάλο χρονικό διάστημα, μια πάρα πολύ αξιόλογη δουλειά.

Η οδηγία NIS απαιτεί την εκπροσώπηση στην ομάδα συνεργασίας, το Cooperation Group της Ευρώπης, όπου συμμετέχουμε ήδη και σε πολλές υποομάδες εργασίας, τη θέσπιση εθνικής στρατηγικής, την οποία κάναμε, τον καθορισμό αρμοδιοτήτων, ποια είναι η εθνική Αρχή και ούτω καθεξής, τον καθορισμό κανόνων για τις κυρώσεις που πρέπει να επιβληθούν σε κρίσιμες υποδομές, όταν και εφόσον φταίνε για κάποιο event στον κυβερνοχώρο ή όταν δεν ακολουθούν τις οδηγίες που έχουμε δώσει σαν εθνική Αρχή όσον αφορά το επίπεδο ασφαλείας τους, την κατάρτιση καταλόγου των φορέων εκμετάλλευσης των βασικών υπηρεσιών, κάτι το οποίο ξεκινάμε τώρα, σιγά-σιγά, σε συνεργασία και με τον ENISA, για να δούμε πώς θα καταρτίσουμε αυτόν τον κατάλογο, φυσικά και με άλλους φορείς που θέλουν να συνεργαστούν μαζί μας· με μεγάλη χαρά, θα συνεργαστούμε με όλους.

Λοιπές δράσεις… Συμμετοχή στον ΟΑΣΕ, το Cyber Education Platform, συνεργασία με τον ENISA, διοργάνωση συνεδρίων και ούτω καθεξής.

Αντί επιλόγου, θα σας πω ότι έχουμε μια ιστοσελίδα στην οποία έχουμε βγάλει κάποιες οδηγίες - συμβουλές στους φορείς,

για να εναρμονιστούν με τον GDPR, έχουμε κάποιες δημοσιεύσεις σε περιοδικά, για το NIS Directive, για την ασφάλεια σε κρίσιμες υποδομές κ.λπ., ενώ έχουμε και δύο e-mails, το ένα είναι το NSCA@gsdp.gr, που είναι για εσωτερική επικοινωνία μαζί μας, και το άλλο είναι το SPOC@gsdp.gr, με το οποίο επικοινωνούμε με άλλα κράτη-μέλη όσον αφορά τα θέματα κυβερνοασφάλειας.

Σας ευχαριστώ πολύ.

ΣΑΚΚΑΣ Μ. - Συντονιστής:

Ευχαριστούμε πολύ τον κύριο Μαγλαρά.

Καλούμε στο βήμα τον Δρ. Λούη Μαρίνο, ειδικό για θέματα ανάλυσης κυβερνοαπειλών και κινδύνων του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), ο οποίος θα μας αναπτύξει «Το τοπίο των κυβερνοαπειλών: αναγκαιότητα ή πολυτέλεια;».

Πριν αρχίσει ο κύριος Μαρίνος, επιτρέψτε μου να καλωσορίσω την κυρία Τασία Χριστοδουλοπούλου, η οποία είναι Πρόεδρος της Ειδικής Μόνιμης Επιτροπής Θεσμών και Διαφάνειας της Βουλής, Επιτροπή στην οποία δίνουμε τα πεπραγμένα και μας καλεί να αναφέρουμε διάφορα περιστατικά.

Κύριε Μαρίνο, έχετε το λόγο.

ΜΑΡΙΝΟΣ Λ.:

Σας ευχαριστώ πολύ, κύριε Πρόεδρε, κύριε Αντιπρόεδρε.

Είμαι ενθουσιασμένος να είμαι σήμερα μαζί σας, σας ευχαριστώ πάρα πολύ γι' αυτή την πρόσκληση. Επίσης, χαίρομαι πάρα πολύ που μου δίνεται η δυνατότητα να αντιπροσωπεύσω ένα μικρό κομμάτι των πραγμάτων που γίνονται στον ENISA. Το θέμα είναι «Το τοπίο των κυβερνοαπειλών: …», και ο τίτλος, τώρα που τον βλέπω κι εγώ άλλη μια φορά, διαπιστώνω ότι έχει ρητορικά στοιχεία· φαντάζομαι, δεν περιμένετε να σας πω ότι είναι πολυτέλεια, μάλλον θα σας πω ότι είναι αναγκαιότητα αυτό που θα σας παρουσιάσω.

Στο μικρό χρονοπαράθυρο που έχουμε, θα προσπαθήσω να σας δείξω τα κύρια στοιχεία της παρουσίασής μου και τα υπόλοιπα μπορείτε να τα δείτε ή να έρθετε σε επαφή μαζί μου για να τα συζητήσουμε offline.

Από «αυτό» το γράφημα που βλέπουμε, θα ήθελα να μας μείνει ότι, ακόμα και μεταξύ μας, οι εμπειρογνώμονες ασφαλείας τσακωνόμαστε καμιά φορά για το τι ακριβώς είναι ο κυβερνοχώρος, δεν το ξέρουμε καλά. Ο ορισμός που βλέπετε τώρα είναι περσινός, πέρυσι βγάλαμε πρώτη φορά τι είναι κυβερνοχώρος, και αυτό είναι σημαντικό γιατί μπορούμε, αν αντιληφθούμε το αντικείμενο για το οποίο συζητάμε, να δούμε ποιο από τα εργαλεία που έχουμε, ή τις διάφορες καλές πρακτικές, μπορούν να εφαρμοστούν ή όχι, ή αν χρειαζόμαστε κάτι καινούριο.

Νομίζω ότι είναι πολύ σημαντικό να πούμε ότι ο κυβερνοχώρος όπως τον βλέπετε αποτελείται από πολλούς κόμβους, δισεκατομμύρια κόμβους· ακόμα και «αυτός» είναι ένας κόμβος του διαδικτύου, ή και ο υπολογιστής μου. Θα σας δώσω ένα ενδεικτικό νούμερο. Στον κυβερνοχώρο έχουμε τρομερή δυναμική, αυτό σημαίνει ότι οι κόμβοι αλλάζουν πολύ γρήγορα. Κάποιοι συνάδελφοι που συζητούσαμε την περασμένη εβδομάδα μας είπαν ότι γύρω στα 12 εκατομμύρια IPs -που είναι αυτές οι διευθύνσεις που βλέπουμε εδώ σαν κόμβοι- είναι δυναμικές, έχουν διάρκεια ζωής μερικές ώρες, ή μερι-

κά λεπτά, και δημιουργούνται με κακόβουλο σκοπό. Βλέπετε λοιπόν ότι για τους κακούς υπάρχει τρομερή ευελιξία να αλλάζουν τη «μάσκα» με την οποία παρουσιάζονται!...

Στον κυβερνοχώρο, φυσικά, σε αντίθεση με τον φυσικό χώρο, ναι μεν αναγνωρίζουμε ότι γίνονται εγκληματικές πράξεις και είναι πεδίο μάχης, μόνο που στον φυσικό κόσμο τα στοιχεία είναι συγκεκριμένα κι έχουν μια οριοθέτηση, όμως εδώ -στον κυβερνοχώρο- δεν υπάρχει οριοθέτηση. Θα ήθελα ενδεικτικά να αναφέρω κάτι που το βρήκα αυτές τις μέρες κοιτώντας για την παρουσίασή μου. Συγκεκριμένα, αν κοιτάξουμε να αντλήσουμε εμπειρίες για τον κυβερνοχώρο από διάφορες άλλες περιοχές, όπως -ας πούμε- η αστυνομία ή ο στρατός, βλέπουμε ότι στον στρατό υπάρχει το δόγμα πολέμου 4ης γενιάς, το οποίο αυτή τη στιγμή είναι σε εφαρμογή. Εκεί προβλέπεται ένα θόλωμα των ορίων μεταξύ πολέμου-ειρήνης, μεταξύ πολιτικής, ανάμεσα στο ποιοι είναι μαχόμενοι, ποιοι είναι πολίτες, ποια είναι η θέση της πολιτικής, και σας διαβεβαιώνω ότι ο κυβερνοχώρος είναι ακριβώς το πιο κατάλληλο πεδίο που θα μπορούσε να εξελιχθεί ένας τέτοιος πόλεμος 4ης γενιάς. Αυτό ήδη γίνεται, ανεξάρτητα αν το έχουμε ή όχι αντιληφθεί, αν και είμαι σίγουρος ότι πολλοί από σας το ξέρετε ήδη.

Όσον αφορά το επίπεδο κινδύνου στον κυβερνοχώρο, αυτό που θέλω να σας παρουσιάσω είναι κάτι καινούργιο, μια καινούργια ιδέα που έχουμε στο θέμα της ασφάλειας, όπου λέμε: Μήπως είναι καλό, εκεί που αγοράζουμε firewall, antivirus για κακόβουλο λογισμικό, για τις φορητές συσκευές κ.λπ., να δούμε τι είναι αυτό που μας απειλεί, ώστε ανάλογα να φτιάξουμε τις άμυνές μας; «Εδώ» βλέπετε ότι υπάρχουν κάποιοι κακόβουλοι οι οποίοι σκανάρουν το διαδίκτυο εκατομμύρια φορές την ημέρα και προσπαθούν να αποκτήσουν πρόσβαση σε κόμβους δικτύου οι οποίοι είναι πάρα πολύ ενδιαφέροντες, όπως -για παράδειγμα- το κινητό κάποιας προσωπικότητας, κάποιου προέδρου, κάποιου αντιπροέδρου και λοιπά.

Γιατί γίνεται αυτό; Είναι γιατί έχουμε αλλαγές -ο κύριος Μαγλαράς το είπε προηγουμένως- στην αρχιτεκτονική, και εκεί που παλιά πηγαίναμε σε πιο κεντρικά οργανωμένες πληροφορικές υποδομές, τώρα έχουμε αρχίσει και αποκεντρώνουμε τις συσκευές μας, μέχρι που έχουμε και το διαδίκτυο των πραγμάτων, όπου έχουμε δισεκατομμύρια συσκευές, οι οποίες είναι κόμβοι σε αυτό το δίκτυο που σας έδειξα στην αρχή. Είναι προφανές ότι κάποιοι που θέλουν να μας επιτεθούν θα κοιτάξουν να βρουν αυτές τις μικροσυσκευές, που δεν τις έχουμε προστατεύσει και τόσο καλά, και θα τις χρησιμοποιήσουν σαν εφαλτήριο για να μπουν στις υποδομές μας.

Εδώ, λοιπόν, έρχεται μια καινούργια κατεύθυνση, μια καινούργια ιδέα στο χώρο της κυβερνοασφάλειας: όπως το cloud computing ήταν καινούργιο σχήμα marketing αλλά λίγο ή πολύ όλα αυτά που εμπεριείχε προϋπήρχαν, έτσι και το θέμα ανάλυσης κυβερνοαπειλών βασίζεται σε υπάρχοντα κομμάτια πληροφορίας, που απλά έχουμε σκεφτεί ότι υπάρχει ένας νέος τρόπος να τα οργανώσουμε, με αποτέλεσμα να αντιληφθούμε πιο καλά ποιος μας επιτίθεται. Με αυτήν την καινούργια περιοχή αναζητούμε απαντήσεις στις ερωτήσεις: ποιος μας επιτίθεται, με ποια πρόθεση, ποια είναι τα εργαλεία επίθεσης, ποια είναι τα ασθενή σημεία που οι επιτιθέμενοι ψάχνουν, ποιες είναι οι στρατηγικές για να εκτελεστεί μια επίθεση, ο τελικός σκοπός

και τα λοιπά - βλέπετε τα αναφερθέντα σημεία σε «αυτή» τη διαφάνεια.

Ένα πάρα πολύ σημαντικό σημείο είναι το επίπεδο ικανοτήτων του επιτιθέμενου, δηλαδή είναι αλλιώς να σας επιτίθεται το παιδί του γείτονα στο router που έχετε σπίτι σας και αλλιώς μια μυστική υπηρεσία ενός κράτους το οποίο πιθανά να επενδύει και δισεκατομμύρια στο θέμα των κυβερνοεπιθέσεων.

Εμείς, από τον ENISA, αναγνωρίζοντας ότι το πρώτο κομμάτι είναι πολύ σημαντικό, και συγκεκριμένα τα εργαλεία επιθέσεων, κάνουμε κάθε χρόνο μια ανάλυση, να δούμε ποια είναι τα πιο δημοφιλή εργαλεία κυβερνοεπιθέσεων που υπάρχουν.

Βλέπετε ένα πρώτο βήμα στη δημιουργία της πληροφορίας κυβερνοαπειλών - αυτό το λέμε threat intelligence, δηλαδή πληροφορία επιθέσεων.

Η πυραμίδα που βλέπετε στη διαφάνεια αποτελεί ένα οικοσύστημα το οποίο θέλει να δείξει ότι στην κορυφή έχουμε κάποιες αναλυτικές ικανότητες, δηλαδή αναλύουμε τι γίνεται, ενώ βρισκόμαστε σε στενή συνεργασία με ένα security operation center αλλά και με την ηγεσία, ώστε να προσπαθήσουμε στις διάφορες πλευρές αυτής της πυραμίδας να αναπτύξουμε τακτική πληροφορία όσον αφορά τις επιθέσεις που γίνονται, στρατηγική πληροφορία, αλλά να έχουμε και μια επίβλεψη μέσα από τις διάφορες υπηρεσίες.

Τι σημαίνει, θα μου πείτε, αυτό για την Ελλάδα; Για την Ελλάδα σημαίνει ότι χρειαζόμαστε κάτι σαν μια υπηρεσία πληροφοριών κυβερνοαπειλών, η οποία να παίρνει διάφορα δεδομένα από αυτούς που λειτουργούν την ασφάλεια και, σε στενή συνεργασία με κάποια ηγεσία, π.χ. στρατηγική κυβερνοασφάλειας, να ορίζει τρόπους άμυνας για κάθε τύπο χρήστη που θα μπορούσε να τους υλοποιήσει άμεσα. Αυτό το έχουν αναγνωρίσει στη βιομηχανία και βλέπουμε ότι μεγάλες εταιρίες (Symantec, Kaspersky κ.λπ.) μας δίνουν υπηρεσίες που βασίζονται πάνω στο τοπίο των κυβερνοαπειλών, επί καθημερινής βάσεως, κάτι το οποίο μας επιτρέπει -για παράδειγμα ρυθμίζουμε τα firewall ή τις διάφορες άλλες αμυντικές υποδομές που έχουμε ανάλογα με το πεδίο των κυβερνοαπειλών, κάτι πάρα πολύ σημαντικό, γιατί αυτό που καταφέρνουμε με την πληροφορία των κυβερνοαπειλών είναι να επιτύχουμε την ευελιξία των μέτρων προστασίας. Είμαι σίγουρος ότι γνωρίζετε τη μακροχρόνια διάσταση μιας ανάλυσης κινδύνων ή μιας θεσμοθέτησης ενός θέματος ασφάλειας. Όμως, τη στιγμή που έχουμε 12 εκατομμύρια κακόβουλες ιστοσελίδες ημερησίως, σημαίνει ότι πρέπει να προσαρμόσουμε την ταχύτητα αντίδρασής μας στα «αναγκαία για την εποχή επίπεδα», που είναι -ουσιαστικά- ισάξια της τεράστιας ταχύτητας με την οποία δεχόμαστε τις επιθέσεις.

Στον ENISA, εδώ και 6-7 χρόνια, ασχολούμαστε με αυτό το θέμα και δίνουμε κάποιες πληροφορίες για τεχνικές στην ανάλυση κυβερνοαπειλών. Αναλύουμε τις 15 βασικές κυβερνοαπειλές κάθε χρόνο, αναλύουμε τις μεθόδους επιθέσεων, έχουμε ένα 15νθημερο δελτίο επίκαιρων απειλών και, τώρα τελευταία, έχουμε και ένα online εργαλείο με το οποίο, ουσιαστικά, προσπαθούμε να μεταδώσουμε αυτή την πληροφορία με απλό τρόπο.

Θα ήθελα να σας πω κάτι που ίσως σας ενδιαφέρει: από το 2018 αναπτύσσουμε και εκπαιδευτικά προγράμματα σε αυτόν τον τομέα. Στο φετινό summer school, τον Σεπτέμβριο, στην Κρήτη, που διοργανώνει ο ENISA σε συνεργασία με το ITE, υπάρχουν hands-on trainings, και ένα από αυτά θα είναι στο θέμα

ανάλυσης κυβερνοαπειλών. Όσοι από εσάς ενδιαφέρεστε, θα μπορούσατε να έρθετε ή να στείλετε κάποιον να το παρακολουθήσει.

Θα ήθελα να σας δώσω μερικές στατιστικές, για να έχετε μια καλύτερη εντύπωση για το τι συζητάμε. Από τα καταγεγραμμένα περιστατικά που έχουμε, 75% περίπου αφορούν το κυβερνοέγκλημα, ενώ το υπόλοιπο 25% είναι δράση μυστικών υπηρεσιών και κυβερνοπόλεμος. Βλέπουμε ότι είναι ένα σημαντικό κομμάτι το οποίο έχει να κάνει με τον κυβερνοπόλεμο, αλλά το περισσότερο είναι κυβερνοέγκλημα. Πιστεύουμε ότι μόλις το 25-50% των συμβάντων δηλώνονται ή γίνονται γνωστά, οπότε καταλαβαίνετε ότι, ουσιαστικά, αυτό είναι η «μύτη του παγόβουνου». Μόλις διάβαζα χτες ότι στην Αυστρία, για παράδειγμα, πέρυσι, είχαν 25.000 καταγεγραμμένες κυβερνοεπιθέσεις την ημέρα σε όλο το κράτος, οπότε καταλαβαίνετε ότι το πραγματικό νούμερο θα είναι πολύ μεγαλύτερο.

Θα ήθελα να σας πω, επίσης, τις σπουδαιότερες αναδυόμενες κυβερνοαπειλές τις οποίες βλέπουμε και διάφορα γεγονότα που μας ανησυχούν.

Το ένα είναι η διαφορά ταχυτήτων μεταξύ επιθέσεων και άμυνας, όπως είπα και προηγουμένως, καθώς ακόμη διαρκεί πάρα πολύ μέχρι να αμυνθούμε για επιθέσεις τις οποίες δεχόμαστε με έναν τρομερό ρυθμό. Αυτό θα μπορούσε κανείς να το μεταφράσει και σε μια αποτυχία της αγοράς της κυβερνοασφάλειας γιατί, ενώ επενδύουμε, δεν έχουμε καταφέρει ακόμα να μειώσουμε το πεδίο των απειλών, άρα πρέπει να δουλέψουμε πολύ ακόμα σε αυτό το κομμάτι.

Θα περάσω το δεύτερο, την εμπορικοποίηση των vulnerabilities που λέμε, και θα πάω σε ένα πολύ σημαντικό κομμάτι…

Θα ήθελα επίσης να πω ότι αυτή τη στιγμή μας απασχολεί πολύ το ότι βλέπουμε απειλές στις δημοκρατίες. Γνωρίζετε πάρα πολύ καλά ότι μυστικές υπηρεσίες αποκτούν εμπιστευτικά δεδομένα, που τα χρησιμοποιούν μετά για να επηρεάσουν τις εκλογές, κάτι το οποίο απασχολεί πολύ αυτή τη στιγμή και το Ευρωπαϊκό Κοινοβούλιο, ενόψει των εκλογών που έχουμε του χρόνου.

Τελειώνοντας, θα ήθελα να σας πω ότι η ανάλυση των κυβερνοαπειλών είναι ένας πολύ σημαντικός παράγοντας στο θέμα της κυβερνοασφάλειας. Είναι ένα σημαντικό γραναζάκι στο θέμα της επιτάχυνσης της ανάλυσης κινδύνων αλλά και της αξιοποίησης στοιχείων από το security management και το incident management. Είναι καινοτόμος περιοχή, επομένως θα πρέπει οι άνθρωποι που είναι στην έρευνα να δώσουν έμφαση σε αυτήν.

Γι' αυτούς που θα κοιτάξουν τα slides μου σε κάποια άλλη στιγμή, σας παραθέτω και κάποιους χρήσιμους συνδέσμους, οι οποίοι θα σας βοηθήσουν να εμβαθύνετε πιο πολύ σε αυτά που σας είπα.

Σας ευχαριστώ πάρα πολύ.

ΣΑΚΚΑΣ Μ. - Συντονιστής:

Ευχαριστούμε πάρα πολύ τον κύριο Μαρίνο και, βεβαίως, θα πυκνώσουμε τη συνεργασία με τον ENISA· θυμίζω σε όσους δεν ξέρουν ότι ο ENISA, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών, εδρεύει στη χώρα μας - όπως σε διάφορες άλλες χώρες εδρεύουν άλλοι Οργανισμοί.

Και τώρα καλώ στο βήμα τον Καθηγητή του ΕΜΠ κύριο Χρήστο Καψάλη, πρώην μέλος της Ολομέλειας της ΑΔΑΕ, να μας αναπτύξει το θέμα «Η επίδραση των blockchains στο απόρρητο των τηλεπικοινωνιακών υπηρεσιών».

ΚΑΨΑΛΗΣ Χ.:

Κύριε Πρόεδρε, κύριε Αντιπρόεδρε, αξιότιμοι κυρίες και κύριοι, στην παρουσίαση που θα σας κάνω -την πολύ σύντομη- θα ήθελα να αναφερθώ σε ένα ειδικότερο θέμα που αφορά την επίδραση της τεχνολογίας "blockchains" στο απόρρητο των τηλεπικοινωνιακών υπηρεσιών.

Σύμφωνα με την Gartner, έχουμε 10 αναδυόμενες -όπου πέφτει το βάρος- νέες τεχνολογίες για το 2018. Σε αυτή τη διαφάνεια μπορεί να δει κανείς τρεις περιοχές σε ό,τι αφορά τον κόσμο μας, για τον οποίο ξέρουμε ότι είναι ψηφιακός, ξέρουμε ότι υπάρχει ευφυΐα, και όλα αυτά συνδέονται με ένα δίκτυο προκειμένου να συνδεθεί ο αληθινός και φυσικός κόσμος με τον ψηφιακό κόσμο.

Ένα χαρακτηριστικό παράδειγμα. Μιλώντας για ευφυή αυτοκίνητα, φανταστείτε στην εθνική οδό τα προπορευόμενα από το δικό μας αυτοκίνητα να στήνουν ένα ad hoc δίκτυο όπου κάθε αυτοκίνητο είναι ένας κόμβος αυτού του μικρού δικτύου, ή του μεγαλύτερου, και μπορεί το προπορευόμενο όχημα που διαπιστώνει ένα ατύχημα ή κάποιον κίνδυνο μπροστά να ειδοποιεί όλα τα αυτοκίνητα που έπονται προκειμένου να επιβραδύνουν ή οτιδήποτε άλλο, και μάλιστα μερικές φορές η επιβράδυνση να γίνεται διαφανώς από τον οδηγό, δηλαδή ο οδηγός να μην το επιδιώκει, αλλά η μέγιστή του ταχύτητα να γίνεται 50 χλμ. λόγω ακριβώς του συμβάντος.

Αυτός είναι ο κόσμος ο οποίος έρχεται και ο οποίος αναδύεται και ο οποίος μαζί με τα καλά του -που, προφανώς, στο παράδειγμα που σας είπα, το καλό είναι η αποφυγή των ατυχημάτων- έχει και τα κακά του. Τα στοιχεία επικοινωνίας, για παράδειγμα το στίγμα του κάθε χρήστη αυτού του δικτύου, βγαίνουν και εκτίθενται σε ένα δίκτυο. Εφόσον εκτίθενται σε ένα δίκτυο, αυτά τα στοιχεία επικοινωνίας μπορεί να υποκλαπούν ή μπορεί να τροποποιηθούν, ή μπορεί να δημιουργηθούν άλλα πράγματα.

Θα μπορούσαμε να λέμε πάρα πολλά παραδείγματα, μάλιστα μερικά είναι και αστεία, όπως το ευφυές ψυγείο που θα παραγγέλλει γάλα για εμάς, το οποίο είναι πολύ κοντά στην πραγματοποίηση παρ' ότι φαίνεται σαν επιστημονική φαντασία, αλλά για φανταστείτε τώρα να υπάρξει μια παραβίαση και να υποκλαπεί το ψυγείο μου που θα έχει παραγγείλει γάλα -επειδή «σώθηκε» το γάλα και το διαπίστωσε μέσω ενός δικτύου από σένσορες- για να μου έρθει στο σπίτι. Τι θα γίνει αν δέκα διαφορετικά σουπερμάρκετ έρθουν να γεμίσουν γάλα το σπίτι;

Αυτά είναι τα αστεία της ιστορίας, όμως από τη στιγμή που εκθέτεις δεδομένα επικοινωνίας μέσα στο δίκτυο, γενικότερα σε οποιοδήποτε δίκτυο, αυτό σημαίνει ότι πρέπει να υπάρχει μια ανάγκη προστασίας. Αυτή η προστασία δεν είναι πάντοτε εφικτό να γίνεται μέσα από κάποιον πάροχο ή κάποια Ανεξάρτητη Αρχή. Πρέπει να ψάξουμε, λοιπόν, να βρούμε και τεχνολογίες, και τουλάχιστον η Gartner αναφέρεται σε κάποια από αυτές, ώστε να μπορεί να γίνει αυτόματα, μιας και, πλέον, η επικοινωνία σε δισεκατομμύρια συσκευές μεταξύ τους -φυσικά πρόσωπα, ψηφιακούς δίδυμους και ούτω καθεξής- αυξάνεται και γίνεται σχεδόν άπειρη.

Από όλη αυτή την ιστορία, έχω επιλέξει να συζητήσω για το "blockchain", το οποίο είναι παρεξηγημένο. Όλοι στο πίσω μέρος του μυαλού μας έχουμε το bitcoin, δεν είναι όμως μόνο αυτό, καθώς αυτή τη στιγμή πάρα πολλές εταιρίες και μεγάλοι οργανισμοί ασχολούνται με την τεχνολογία η οποία είναι αναδυόμενη.

Ας έρθουμε να δούμε τώρα το blockchain, να το εντάξουμε μέσα στο θέμα του απορρήτου και στο θέμα των παρόχων. Σήμερα, οι πάροχοι τηλεπικοινωνιακών υπηρεσιών αντιμετωπίζουν διάφορες προκλήσεις, για μερικές από τις οποίες υπάρχουν ειδικότεροι εμού να μιλήσουν, αλλά -εν πάση περιπτώσει- βλέπει κανείς ότι κάποτε ξεκινήσαμε με έναν διαχωρισμό παροχής δικτύου και υπηρεσιών. Κλασσική περίπτωση η τηλεόραση, όπου παλιότερα κάθε κανάλι είχε το δικό του δίκτυο, τώρα υπάρχει ένας πάροχος δικτύου και πολλοί πάροχοι περιεχομένου, ενώ το βλέπουμε αυτό να γίνεται και στις τηλεπικοινωνιακές υπηρεσίες, οι οποίες φορτώνουν τα δίκτυά τους με πληθώρα υπηρεσιών προστιθέμενης αξίας. Μάλιστα, λόγω της μείωσης του κόστους, υπάρχει πια η δυνατότητα το περιεχόμενο να γίνεται και on demand, όπως βλέπουμε σήμερα. Αλλά ακόμα και σε αυτή την περίπτωση, από τη στιγμή που εγώ ζητάω να δω μια ταινία σπίτι μου on demand, θα πρέπει με κάποιον τρόπο αυτή η επιθυμία μου, που είναι και αυτό ένα στοιχείο επικοινωνίας, να προστατεύεται.

Ερχόμαστε στην αναγκαιότητα ελέγχου, λοιπόν, την οποία ξέρουμε πάρα πολύ καλά, καθώς χρόνια τώρα η ΑΔΑΕ ασχολείται με καταγγελίες πολιτών, με τακτικούς ή έκτακτους ελέγχους, περιοδικούς ελέγχους και λοιπά, αλλά και οι ίδιες οι εταιρίες κάνουν πολλούς εσωτερικούς ελέγχους στην προσπάθειά τους να διατηρήσουν τα αποτελέσματα.

Εδώ μπαίνει ένα άλλο πολύ σημαντικό ζήτημα. Υπάρχουν σχέσεις εμπιστοσύνης μεταξύ των παρόχων, των πελατών, των συνεργατών και των Αρχών; Η απάντηση είναι, ναι, θέλουμε να υπάρχουν. Για να πάμε σε ένα παράλληλο ζήτημα και να το δούμε πριν 8 χρόνια, στην αρχή της κρίσης, η σχέση εμπιστοσύνης υπήρχε μεταξύ πολιτών και τραπεζών; Μήπως διαταράχτηκε αυτή, τουλάχιστον στην Ελλάδα που είχαμε πολύ σημαντικό παράδειγμα, αλλά και σε άλλες χώρες; Επομένως υπάρχει μια κρίση εμπιστοσύνης για την ανάγκη έμπιστου τρίτου μέρους το οποίο θα εγγυάται το απόρρητο των επικοινωνιών.

Ας έρθουμε τώρα να δούμε -να εισάγουμε τι ιστορία είναι αυτή με το blockchain.

Γενικώς, όταν έχουμε μια φυσική αλληλεπίδραση μεταξύ δυο ανθρώπων στον φυσικό κόσμο, ένας χρήστης θέλει -εδώ το παράδειγμα είναι δανεισμένο από το bitcoin- να δώσει κάποια χρήματα, ή να κάνει κάποια συναλλαγή, ή να δώσει ένα αγαθό, σε έναν άλλο χρήστη. Στον φυσικό κόσμο αυτό γίνεται με το φυσικό χρήμα, πηγαίνει και εγχειρίζει ο ένας στον άλλο τα χρήματα, ή το αγαθό, και τελειώνει η ιστορία. Στο παράδειγμά μας, από τη στιγμή που ο Bob πήρε από την Αλίκη τα χρήματα, τελείωσε εκεί η συναλλαγή.

Εάν πάμε στον ψηφιακό κόσμο, όμως, θα πρέπει να γίνει μια ψηφιακή συναλλαγή. Θα μου πεις, τα στέλνει ηλεκτρονικά. Ναι, αλλά αυτό σημαίνει ότι χρειάζεται μια ανάγκη επιβεβαίωσης, αλλιώς μπορεί να γίνουν τέτοιες συναλλαγές που να μην επιβεβαιώνονται. Η ανάγκη επιβεβαίωσης μπορεί να αναπαραχθεί και, επομένως, να μην είναι ασφαλής. Σε αυτή την περίπτωση, τι κάνουμε; Μπαίνει ένας ενδιάμεσος, το τρίτο μέρος, που κρατάει ένα λογιστικό βιβλίο. Δηλαδή, στο transaction που κάνω με την πιστωτική μου κάρτα για να πληρώσω κάποιο αγαθό σε ένα κατάστημα, ο εγγυητής στη μέση είναι το λογιστικό βιβλίο που κρατάει η τράπεζα και ξέρει ότι εγώ πλήρωσα 10 ευρώ, και τα 10 ευρώ πήγαν στον προμηθευτή μου με το αντίστοιχο αγαθό, άρα εκεί υπάρχει έμπιστο μέρος.

Μπορεί να παρακαμφθεί το έμπιστο μέρος; Η απάντηση έρχεται από το blockchain και είναι η εξής: Σε οποιαδήποτε ψηφιακή αλληλεπίδραση μεταξύ δύο χρηστών, εάν αυτό το λογιστικό βιβλίο, αντί να το κρατάει ένα έμπιστο μέρος, κρατιέται μέσα στον ιστό και γίνεται συναλλαγή -κρυπτογραφημένη, βέβαια- από πάρα πολλούς χρήστες, τότε σε αυτή την περίπτωση έχουμε την εγγύηση του 51% των χρηστών ότι αυτή η συναλλαγή είναι έγκυρη. Αυτή, αν θέλετε, με πολύ απλά λόγια, είναι και η κεντρική φιλοσοφία του blockchain.

Ποια είναι τα καινοτόμα χαρακτηριστικά της τεχνολογίας blockchain; Δεν υπάρχει ανάγκη για πιστοποίηση τρίτου μέρους, οι εμπλεκόμενοι δεν εμπιστεύονται -κατ' ανάγκη- ο ένας τον άλλο, οι εγγραφές είναι ελέγξιμες και μη αναστρέψιμες, οι συναλλαγές είναι κρυπτογραφημένες, και έτσι αυτά όλα μαζί μπορούν να οδηγήσουν σε ευφυή συμβόλαια μεταξύ χρηστών.

Να δούμε τώρα ποιες είναι οι δυνητικές περιοχές χρήσης αυτής της τεχνολογίας -της τεχνικής, της μεθόδου- στον τηλεπικοινωνιακό τομέα. Εδώ κάποιος μπορεί να διαπιστώσει ότι θα μπορούσε να εισαχθεί, βεβαίως με πλεονεκτήματα αλλά και με μειονεκτήματα, και θα αναφερθούμε στη συνέχεια, στη διαχείριση του δικτύου, στη διαχείριση της εταιρίας, στη διαχείριση συνεργατών, στη διαχείριση πελατών και ούτω καθεξής.

Ποιες μπορεί να είναι οι πιθανές εφαρμογές χρήσης του blockchain; Για παράδειγμα, ο έλεγχος πρόσβασης σε αρχεία κλήσεων. Ένα τεράστιο θέμα που έχουν οι πάροχοι είναι ότι κάθε φορά έχουν ανάγκη να κρατούν κάποιο log file έτσι ώστε να πιστοποιούν στην Αρχή που κάνει τον έλεγχο ότι η πρόσβαση κλήσεων σε αρχεία δεν έχει γίνει από κακόβουλο χρήση ή από τρίτο μέρος, ή δεν έχει ξεφύγει ένα αρχείο. Επίσης πιθανές εφαρμογές, οι βάσεις φορητότητας αριθμού, οι αιτήσεις άρσης -πολύ σημαντικό θέμα- απορρήτου, οι χρεώσεις περιαγωγής, όπου πάντα υπάρχει ένα τρίτο μέρος για να μπορούν να γίνουν καθώς περιηγείται ένας χρήστης μεταξύ δύο ή περισσότερων παρόχων και ούτω καθεξής, τα συμβόλαια των παρόχων κ.α.

Οι τομείς χρήσης του blockchain είναι πολύ ευρείς - ενδεικτικά αναφέρω το spectrum sharing, δηλαδή τη διαχείριση φάσματος, καθώς επίσης το 5G, μέσα στο οποίο πλέον η πρόσβαση από κάθε χρήστη θα γίνεται σε διαφορετικά δίκτυα επικοινωνίας και ούτω καθεξής.

Αν θέλει κανείς να δει με περισσότερη εμβάθυνση ένα παράδειγμα της περιαγωγής, θα μπορούσε να πραγματοποιείται ένα blockchain μεταξύ παρόχων, όπου θα υπάρχουν ειδικοί κόμβοι των παρόχων οι οποίοι θα κάνουν επαλήθευση των transactions και θα δρουν ως miners, θα υπάρχουν ευφυή συμβόλαια μεταξύ του home location register και του visitor location register, κάθε φορά που ο χρήστης ενεργοποιεί ένα γεγονός στον VLR ενημερώνεται ο αντίστοιχος HLR, ταυτοχρόνως θα κάνει και τη χρέωση. Τα πλεονεκτήματα, προφανώς, είναι η μείωση του κόστους γιατί δεν απαιτείται τρίτο μέρος το οποίο θα κάνει το clearing μεταξύ των παρόχων, η ελάττωση περιπτώσεων απατηλής ενεργοποίησης γεγονότων περιαγωγής και, βεβαίως, οι αμοιβαία επαληθεύσιμες συναλλαγές μεταξύ παρόχων,

Άλλο παράδειγμα θα μπορούσε να είναι η εφαρμογή του blockchain για έλεγχο σε αρχεία ενεργειών.

Κι αν έρθει κανείς, πια, να καταλήξει και να δει αν υπάρχουν πλεονεκτήματα της χρήσης αυτής της τεχνικής της τεχνολογίας, θα βρει

τη βελτίωση του συντονισμού μεταξύ συνεργατών, την απαλλαγή από ύπαρξη έμπιστου τρίτου μέρους, που αυτό είναι πολύ σημαντικό μέρος και θα διευκολύνει πάρα πολύ τις ανταλλαγές ηλεκτρονικών συναλλαγών, το ότι οι προσβάσεις και οι ενέργειες μπορούν να είναι άμεσα ελέγξιμες χωρίς να υπάρχουν αμφισβητήσεις, το ότι υπάρχουν αδιάβλητοι και μη αναστρέψιμοι όροι συμβολαίων, την εισαγωγή νέων επιχειρηματικών μοντέλων και, φυσικά, τη διαθεσιμότητα και την ακεραιότητα των δεδομένων που θα προστατεύονται με αυτόν τον τρόπο.

Από την άλλη μεριά -και κλείνω, κύριε Πρόεδρε- έχουμε τεχνολογικές προκλήσεις, ανοιχτά θέματα και προβλήματα. Ο ρυθμός εκτέλεσης ή αποθήκευσης συναλλαγών είναι ένα ερώτημα διότι, από τη στιγμή που έχω αποθήκευση σε πολλά εκατομμύρια χρήστες, αυτό σημαίνει πιθανές καθυστερήσεις στον ρυθμό εκτέλεσης ή αποθήκευσης συναλλαγών. Η επεκτασιμότητα είναι ένα θέμα. Η αποθήκευση πλήρους αντιγράφου σε κάθε κόμβο σημαίνει τεράστιες ανάγκες σε αποθηκευτικό χώρο. Η κατανάλωση ενέργειας διότι, για να σπάσει ένα blockchain, μπορεί να απαιτείται τεράστιο ποσό ενέργειας σε υπολογιστικό χρόνο, άρα και η κατανάλωση ενέργειας από τους υπολογιστές είναι ένα ζήτημα. Επίσης, η συμβατότητα με ισχύοντα πρότυπα δεδομένων και, βέβαια, η απουσία ρυθμιστικού πλαισίου ως προς την εισαγωγή ή όχι τέτοιου είδους τεχνολογιών.

Βεβαίως, το μέλλον θα δείξει εάν τέτοιου είδους ιδέες και διαδικασίες θα βοηθήσουν πάρα πολύ στη δυνατότητα επίλυσης πολλών άλλων προβλημάτων.

Ευχαριστώ πολύ.

ΣΑΚΚΑΣ Μ. - Συντονιστής:

Ευχαριστούμε τον Καθηγητή κύριο Καψάλη.

Καλούμε στο βήμα τον κύριο Χρήστο Καλλονιάτη, Αναπληρωτή Καθηγητή του Πανεπιστημίου Αιγαίου και μέλος της Ολομέλειας της ΑΔΑΕ, ο οποίος θα μας αναπτύξει το θέμα «Ο ρόλος των Αρχών για τη διασφάλιση του απορρήτου των επικοινωνιών στον κόσμο της νεφοϋπολογιστικής».

Κύριε Καθηγητά.

ΚΑΛΛΟΝΙΑΤΗΣ Χ.:

Ευχαριστώ, κύριε Πρόεδρε.

Αξιότιμε κύριε Πρόεδρε, κύριε Αντιπρόεδρε, αξιότιμα μέλη των Ανεξαρτήτων Αρχών, αγαπητές και αγαπητοί συνάδελφοι, κυρίες και κύριοι, όταν πριν 7 χρόνια ξεκινούσαμε ερευνητικά στις αίθουσες του πανεπιστημίου να συζητάμε για υπηρεσίες νεφοϋπολογιστικής και ζητήματα ασφάλειας, δεν θα αναλογιζόμουν ποτέ ότι θα ερχόμασταν 7 χρόνια μετά στην αίθουσα της Γερουσίας της Βουλής να συζητάμε για ακόμα ένα τόσο επίκαιρο θέμα το οποίο, έχοντας την τύχη να υπηρετώ τα τελευταία δύο χρόνια ως μέλος της Ολομέλειας της ΑΔΑΕ, να το βλέπουμε στην πράξη σε όλες τις εκφάνσεις του και να μας οδηγεί σήμερα εδώ, να κάνουμε μια μικρή, στενή τοποθέτηση πάνω στα θέματα της νεφοϋπολογιστικής, cloud computing πιο δημοφιλές στα ελληνικά, και στα ζητήματα ασφάλειας που συναντάμε στη συνεργασία με τους παρόχους. Βέβαια, το σημαντικότερο που θα συζητήσουμε σήμερα είναι οι προκλήσεις που αυτό δημιουργεί και στις ίδιες τις διαδικασίες της ΑΔΑΕ, κυρίως ως προς τους παρόχους.

Είναι σαφές ότι ολοένα και περισσότερος αριθμός χρηστών κινείται προς την ψηφιακή εποχή και υιοθετεί υπηρεσίες, είτε αυτές είναι γνωστές ότι ανήκουν στον χώρο της νεφοϋπολογιστικής είτε όχι. Είμαι σίγουρος ότι αν κάναμε και ένα γκάλοπ εδώ μεταξύ μας, θα βλέπαμε ότι οι περισσότεροι χρησιμοποιούμε υπηρεσίες νεφοϋπολογιστικής, απλά πολλοί από εσάς μπορεί να μην ξέρετε ότι το κάνετε.

Το ίδιο πράγμα συμβαίνει και με τους παρόχους τηλεπικοινωνιακών υπηρεσιών. Οι πάροχοι, από τη μεριά τους, είναι προφανές ότι θα κινηθούν προς αυτή την κατεύθυνση, εκμεταλλευόμενοι τα πλεονεκτήματα που παρέχει αυτή η νέα εποχή της νεφοϋπολογιστικής, γιατί κερδίζουν σε απλούστευση των εσωτερικών τους διαδικασιών, αναβαθμίζουν τις υπηρεσίες τους, κάτι που είναι αρκετά καλό και γι' αυτούς αλλά και για τους πελάτες τους, γιατί τους προσφέρει καλύτερη διαφήμιση, τους αυξάνει τη φήμη, άρα το να χρησιμοποιούμε καινοτόμες υπηρεσίες δεν κάνει μόνο καλό στο εσωτερικό μας αλλά και στο εξωτερικό μας, άρα είναι αναμενόμενο να βλέπουμε τους παρόχους να κινούνται προς αυτή την κατεύθυνση.

Αυτό προκαλεί και κάποια άλλα ζητήματα, όμως, όπως η αύξηση του αριθμού των πληροφοριών που καλούνται οι πάροχοι να διαχειριστούν, ερχόμενοι από μια εποχή που όλα ήταν in house, όλα ήταν στις δικές τους εγκαταστάσεις. Η αύξηση αυτή των πληροφοριών, αναπόφευκτα, θα οδηγήσει και στην υιοθέτηση υπηρεσιών νεφοϋπολογιστικής, υπηρεσίες οι οποίες ναι μεν μπορούν να καλυφθούν εκ των έσω, αλλά βλέπουμε ότι πολλές φορές θα χρειαστεί να χρησιμοποιηθούν και εξωτερικές υπηρεσίες και εξωτερικοί -τρίτοι- πάροχοι, προφανώς γιατί οι πηγές μας δεν είναι άπειρες.

Η θετική εισβολή της νεφοϋπολογιστικής στη ζωή μας είναι γεγονός. Βέβαια, το οξύμωρο «θετική εισβολή» ερμηνεύεται ως ότι πολλοί υιοθετούμε αυτές τις υπηρεσίες γιατί μας αρέσουν, μας δίνουν πλεονεκτήματα στην καθημερινή μας ζωή, αυτό είναι το θετικό, όμως είναι εισβολή γιατί πολλές φορές -θέλοντας ή μη- αναγκαζόμαστε να τις χρησιμοποιήσουμε.

Η νεφοϋπολογιστική -τεχνικά να σας πω μόνο- χωρίζεται σε τρία βασικά επίπεδα. Οι πάροχοι υπηρεσιών νεφοϋπολογιστικής μας παρέχουν τρεις βασικές υπηρεσίες: α. έτοιμο λογισμικό, για παράδειγμα υπηρεσίες ηλεκτρονικού ταχυδρομείου, που άπτεται και των αρμοδιοτήτων της ΑΔΑΕ, β. υπολογιστικούς πόρους (πλατφόρμες), ή γ. απλά αποθηκευτικό χώρο ώστε να αποθηκεύουμε δεδομένα. Το πλεονέκτημα όλων αυτών είναι ότι δεν χρειάζεται εμείς να δαπανήσουμε χρήματα, ούτε για να αγοράσουμε εξοπλισμό ούτε για να συντηρήσουμε εξοπλισμό. Είναι αναμενόμενο, λοιπόν, ο πάροχος να προχωρά σε συμφωνίες με τέτοιες εταιρίες, μόνο και μόνο για να εκμεταλλευτεί υπολογιστικούς πόρους, λογισμικό, πλατφόρμες, για όσο χρόνο χρειαστεί -αυτό είναι το μεγαλύτερο πλεονέκτημα- κι ανάλογα με την απαίτηση που έχει την εκάστοτε στιγμή. Μετά, προφανώς, θα τα αποδεσμεύσει. Άρα το κόστος του ρυθμίζεται πολύ πιο εύκολα.

Βέβαια, πλείστα είναι τα πλεονεκτήματα των παρόχων από τη χρήση των υπηρεσιών νεφοϋπολογιστικής: εξυπηρέτηση ανάλογα με τις ανάγκες τους, ευρεία πρόσβαση, διάθεση υπολογιστικών πόρων, ελαστικότητα, μετρήσιμη παροχή υπηρεσιών και πολλά άλλα. Βλέπουμε λοιπόν ότι η ίδια η φύση των υπηρεσιών νεφοϋπολογιστικής είναι τέτοια που θεωρούμε ότι όλοι οι πάροχοι και όλες οι

εταιρίες θα κινηθούν προς αυτή την κατεύθυνση, αν δεν το έχουν κάνει ήδη, διότι είναι μονόδρομος.

Αυτό το σχήμα -όπως θα δείτε- με το πράσινο και το πορτοκαλί χρώμα δείχνει απλά τα τρία επίπεδα παροχής υπηρεσιών νεφοϋπολογιστικής. Το μόνο πράγμα που θέλω να δείτε είναι ότι η αριστερή στήλη, που είναι όλο πράσινο, δείχνει τι έχει ο πάροχος στη δικαιοδοσία του όταν χρησιμοποιεί δικές του εγκαταστάσεις για να χτίσει επάνω τις υπηρεσίες του και τι συμβαίνει όταν χρησιμοποιούμε υπηρεσίες νεφοϋπολογιστικής. Στη δεύτερη στήλη, που φέρει ως τίτλο "Infrastructure", θα δείτε ότι μόνο τα πράσινα κομμάτια είναι αυτά που μπορούμε εμείς που αγοράζουμε την υπηρεσία να επέμβουμε, ενώ σε όλα τα υπόλοιπα είναι στο χέρι του τρίτου παρόχου, αυτού που μας δίνει την υπηρεσία. Σε συνέχεια, στη στήλη που φέρει ως τίτλο "Platform", θα δείτε ότι έχουμε σε πολύ πιο λίγα σημεία πρόσβαση εμείς ως πελάτες που παίρνουμε υπηρεσίες νεφοϋπολογιστικής και τα περισσότερα ανήκουν στον πάροχο. Τέλος, σε υπηρεσίες που ανήκουν στην τελευταία κατηγορία, το "Software (as a service)", π.χ. το e-mail, θα δείτε πολύ απλά ότι εμείς δεν έχουμε καμία δικαιοδοσία, σε κανένα κομμάτι της υποδομής, διότι όλα ανήκουν στον πάροχο που μας παρέχει την υπηρεσία.

Γιατί επιμένουμε σε αυτό… Όταν συζητάμε για cloud computing και όταν οι χρήστες μας συζητάνε για could computing, προφανώς, στο μυαλό μας έχουμε μια πολύ ωραία ιδέα, ένα ωραίο συννεφάκι, μιας και από εκεί προέρχεται η ιδέα του cloud, όπου εμείς έχουμε τη συσκευή μας, το laptop μας, το κινητό μας, και χρησιμοποιούμε κάπου κάποιες υπηρεσίες. Καλώς, όταν αυτό δεν θίγει ζητήματα ιδιωτικότητας ή απορρήτου, ή οτιδήποτε άλλο. Ποια όμως είναι η πραγματικότητα πίσω στον πάροχο; Ποια είναι η πραγματικότητα μιας εταιρίας η οποία υιοθετεί υπηρεσίες νεφοϋπολογιστικής για να δώσει τηλεπικοινωνιακές υπηρεσίες στους πολίτες; Δεν είναι αυτός ο ωραίος κόσμος που βλέπετε με μπλε και άσπρο, αλλά είναι μια ολίγον τι πολύπλοκη δομή, η οποία συνδέει διάφορους τύπους υποδομών. Διότι, όπως σας είπα, για να μπορέσουμε να προσφέρουμε ευέλικτες -και γρήγορα- υπηρεσίες, θα πρέπει από πίσω να υπάρχει μια υποδομή που να υποστηρίζει αυτή την αλλαγή. Άρα δεν υπάρχει ένα δίκτυο από πίσω όπως το έχουμε όλοι στο μυαλό μας, που απλά προσθέτουμε πάνω υπηρεσίες και τις δίνουμε στον πολίτη. Αν αύριο, λοιπόν, ο πάροχος που μας παρέχει τηλεπικοινωνίες και υπηρεσίες δει ότι υπάρχει μια μεγάλη ζήτηση, αυτομάτως θα πάει να υιοθετήσει υπηρεσίες από τρίτους, οι οποίοι τρίτοι -με τη σειρά τους- θα δανειστούν υπηρεσίες πάλι από άλλους για να μπορέσουν να εξυπηρετήσουν τον πάροχο και ούτω καθεξής. Όπως καταλαβαίνετε, ο έλεγχος φεύγει λίγο από το κτίριο, τον υπολογιστή ή τις εγκαταστάσεις που έχουμε μάθει μέχρι τώρα.

Ενδεικτικές απειλές… Οι συνάδελφοι που ασχολείστε στον χώρο της πληροφορικής, και ειδικότερα της ασφάλειας, θα δείτε ότι πολλές από αυτές τις απειλές υπάρχουν και στα παραδοσιακά περιβάλλοντα και αφορούν κακόβουλους εσωτερικούς παράγοντες, διαρροή ή υποκλοπή δεδομένων επικοινωνίας, απόκτηση μη εξουσιοδοτημένης πρόσβασης σε λογαριασμό ή υπηρεσία, συμμόρφωση, τοποθεσία εναπόθεσης των δεδομένων, ανεπαρκή διαχωρισμό δεδομένων. Στις ενδεικτικές αυτές απειλές που σας διάβασα προσθέστε ότι σε όλα αυτά δεν μπορού-

με να ξέρουμε πού είναι ο τρίτος πάροχος, πού είναι οι εξυπηρετητές του, πού είναι τα δεδομένα μας. Αυτό είναι και το κλειδί της αλλαγής όταν χρησιμοποιούμε υπηρεσίες νεφοϋπολογιστικής. Δεν γνωρίζουμε πού είναι όλα αυτά. Μπορεί οι ίδιες απειλές να συμβαίνουν και σε έναν πάροχο που έχει τις εγκαταστάσεις του στο διπλανό κτίριο, όπου πάλι μπορεί κάποιος να δει τα δεδομένα μας, πάλι θέλουμε να δούμε αν αποθηκεύονται με ασφάλεια, ενώ φανταστείτε τώρα όλα αυτά να συμβαίνουν σε μια τρίτη χώρα η οποία δεν έχει καν την υποχρέωση εναρμόνισης με την ελληνική νομοθεσία, που αυτή είναι και η μεγαλύτερη πρόκληση.

Να ευχαριστήσω τους συναδέλφους, τα στελέχη της ΑΔΑΕ που με βοήθησαν να καταγράψουμε κάποια περιστατικά όσον αφορά ζητήματα που έχουν έρθει ήδη στην Ολομέλεια προς επίλυση. Θα σας διαβάσω 4 ενδεικτικά περιστατικά για να σας δείξω πώς αλλάζει το τοπίο και πώς η ΑΔΑΕ θα πρέπει να εναρμονιστεί στις νέες εξελίξεις.

Πρόσφατα είχαμε καταγγελία για παραβίαση του απορρήτου της επικοινωνίας σε εταιρία που εδρεύει στην Αθήνα με γραφεία και εγκαταστάσεις σε άλλη ευρωπαϊκή χώρα, που τα γραφεία και οι εγκαταστάσεις στην άλλη ευρωπαϊκή χώρα νοίκιασαν υπηρεσίες που ανήκαν σε τρίτη χώρα, εκτός Ευρώπης.

Καταγγελία για παραβίαση του απορρήτου της επικοινωνίας σε μεγάλης εμβέλειας παρόχους σε ό,τι αφορά τους οποίους, αφού κινούνται πλέον ευρωπαϊκά, είναι λογικό τα κέντρα δεδομένων τους να είναι κατανεμημένα σε όλη την Ευρώπη· και θα είμαστε τυχεροί αν είναι σε όλη την Ευρώπη μόνο - για ποιον λόγο τα δεδομένα να μένουν στην Ελλάδα μόνο όταν η θυγατρική μου βρίσκεται και στην Αγγλία;

Καταγγελία για παραβίαση του απορρήτου της επικοινωνίας σε παρόχους που μέρος των τηλεπικοινωνιακών τους συστημάτων -που τα χρησιμοποιούν όμως για να παρέχουν υπηρεσία στους πολίτες- βρίσκονται σε άλλο πάροχο στο εξωτερικό· όχι στον ίδιο πάροχο που έχει γραφεία στο εξωτερικό.

Τέλος, καταγγελία για παραβίαση του απορρήτου της επικοινωνίας σε εταιρίες παροχής υπηρεσιών σχεδιασμού ιστοσελίδων. Δεν είναι μόνο οι τηλεπικοινωνιακοί πάροχοι. Το μεγαλύτερο κομμάτι που -κατά τη γνώμη μου- θα «ταλαιπωρήσει» τους ελεγκτικούς μηχανισμούς της ΑΔΑΕ θα είναι οι πάροχοι που θα δίνουν σωρηδόν υπηρεσίες ιστοσελίδων, που μέσα στις ιστοσελίδες θα παρέχουν και υπηρεσίες όπως ηλεκτρονικού ταχυδρομείου. Ακριβώς επειδή θα είναι μικρές εταιρίες και δεν θα θέλουν να δαπανήσουν πολλά χρήματα ή δεν θα έχουν την ικανότητα να δαπανήσουν πολλά χρήματα, θα υιοθετούν υπηρεσίες νεφοϋπολογιστικής όπου είναι φτηνότερα – και το «…όπου είναι φτηνότερα» δεν σημαίνει εντός Ελλάδος, σημαίνει οπουδήποτε στον κόσμο.

Αυτές οι 4 καταγγελίες γεννούν -κατά τη γνώμη μου- και τις προκλήσεις που θα έχουμε να αντιμετωπίσουμε σε λίγα χρόνια στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών· τις αντιμετωπίζουμε από σήμερα, αλλά θα αυξηθούν και θα πολλαπλασιαστούν σε λίγα χρόνια.

Ποια ήταν η δυσκολία που καταγράψαμε διενεργώντας τους ελέγχους γι' αυτά τα περιστατικά;

Μεγάλη δυσκολία στη λήψη στοιχείων· το αντιλαμβάνεστε.

Ποιος είναι ο έλεγχος συμμόρφωσης των εταιριών που ανήκουν σε τρίτες χώρες σε

σχέση με την ελληνική νομοθεσία στην οποία υπάγεται η εταιρία που ελέγχεται.

Διεξαγωγή ελέγχων με φυσική παρουσία· πάρα πολύ δύσκολο, ενώ είναι απαραίτητο.

Κατανόηση της αρχιτεκτονικής των δικτύων στο εξωτερικό. Πώς μπορούμε να κατανοήσουμε εμείς ένα σύστημα το δίκτυο του οποίου θα πάμε να ελέγξουμε από απόσταση; Την πολυπλοκότητά του, τα Hotspot σημεία που πρέπει να δούμε;… Δύσκολο. Πολλές φορές έτυχε τα στελέχη μας να παίρνουν ως πληροφορίες υποσύνολο των πληροφοριών από αυτές που ζητούσαν, χωρίς να μπορούμε να κάνουμε κάτι για να πάρουμε το σύνολο των πληροφοριών, γιατί ήταν σε άλλη χώρα, σε άλλο καθεστώς, επομένως ακόμα και ο έλεγχος που κάναμε εξ αποστάσεως ήταν δύσκολος.

Υψηλή πολυπλοκότητα ανάλογα με το πλήθος των συνεργαζόμενων εταιριών. Αν μία εταιρία νοικιάζει υπηρεσίες από άλλη εταιρία, που παίρνει -με τη σειρά της- από τρίτη εταιρία τις υπηρεσίες νεφοϋπολογιστικής που χρησιμοποιεί και τα λοιπά και τα λοιπά, φανταστείτε πόσο δύσκολο είναι να μπορέσουμε να συγκεντρώσουμε τα στοιχεία που χρειαζόμαστε για να καταλήξουμε σε ένα πόρισμα· όχι για να βρούμε λύση, αλλά για να βρούμε τι έφταιξε.

Απαίτηση ύπαρξης στελεχών με εξειδικευμένες γνώσεις· φάνηκε από τους ελέγχους, τα στελέχη μας είναι ικανά, γνωρίζουν για νέες τεχνολογίες, αλλά οι προκλήσεις που μας φέρνει το νέο τοπίο είναι πολύ μεγάλες.

Ποια είναι η επόμενη μέρα;

Κατ' αρχάς, θα πρέπει να βρούμε έναν τρόπο ώστε οι εταιρίες των οποίων εγκρίνουμε τις πολιτικές ασφάλειας στην Ελλάδα να υιοθετούν αυτά που ψηφίζουμε, τους κανονισμούς και τη νομοθεσία που έχουμε στην Ελλάδα και στο εξωτερικό, αλλιώς το παιχνίδι των θυγατρικών εταιριών δεν θα σταματήσει ποτέ και ο έλεγχος ο δικός μας δεν θα γίνεται ποτέ σωστά.

Δυνατότητα απομακρυσμένης πρόσβασης των ελληνικών παρόχων στα δεδομένα των θυγατρικών τους. Αν πάμε να κάνουμε έναν έλεγχο σε μια εταιρία που βρίσκεται στην Ελλάδα, να μπορεί η εταιρία αυτή να έχει πρόσβαση και στα δεδομένα των θυγατρικών της εταιριών· κι όχι να απευθυνόμαστε στις θυγατρικές εταιρίες, οι οποίες αρνούνται να μας δώσουν τα δεδομένα που χρειαζόμαστε.

Μεγαλύτερη ευελιξία των Αρχών, προφανώς, κατά την εκπόνηση των ελέγχων.

Εκπαίδευση των στελεχών των Αρχών στις νέες τεχνολογικές προκλήσεις και απειλές. Είναι πολύ σημαντικό και κάνουμε ήδη προσπάθειες -εδώ και δύο χρόνια το γνωρίζω εγώ, αλλά είμαι σίγουρος ότι ο κύριος Πρόεδρος θα μου πει ότι το έχουν κάνει και πολύ παλιότερα- να βρούμε και να κάνουμε εξειδικευμένες καταρτίσεις, προγράμματα κατάρτισης στα στελέχη μας, γιατί θα πρέπει να είναι μπροστά στις τεχνολογικές εξελίξεις και όχι ουραγοί.

Συνεργασία με τις Ανεξάρτητες Αρχές των άλλων κρατών για συμβολή στην πραγματοποίηση από κοινού ελέγχων. Πλέον, από τη στιγμή που οι τεχνολογικές προκλήσεις είναι τέτοιες που όλη η Ευρώπη δεν έχει σύνορα, τεχνολογικά δεν μπορούμε να περιορίσουμε μια υπηρεσία στην Ελλάδα ή σε μια άλλη χώρα, πρέπει και οι ελεγκτικοί μηχανισμοί να διευρυνθούν με τέτοιον τρόπο που και οι Ανεξάρτητες Αρχές να έχουν αντίστοιχα πρωτόκολλα συνεργασίας και να μπορούμε ανά πάσα στιγμή να επέμβουμε σε οποιαδήποτε χώρα. Μόνο έτσι θα μπορέσουμε να κάνουμε αποτελεσματικούς ελέγχους, βέβαια, στις προκλήσεις που έρχονται.

Προφανώς, αν μπορούσαμε να κάνουμε και μια προσωπική πρόταση για φόρουμ κοινών συνεδριάσεων των Ανεξαρτήτων Αρχών που ασχολούνται με ζητήματα απορρήτου, θα ήταν ακόμα καλύτερο για μεταφορά τεχνογνωσίας στα ίδια μας τα στελέχη αλλά και για αντιμετωπίσεις αντίστοιχων περιστατικών που έχουν συμβεί σε άλλες χώρες.

Η φύση των υπηρεσιών έχει αλλάξει, αυτό είναι γνωστό και δεδομένο.

Οι πάροχοι δεν περιμένουμε μόνο υιοθέτηση τέτοιων τεχνολογιών από μεγάλους παρόχους. Θεωρώ ότι μεγαλύτερο πρόβλημα θα έχουμε σε λίγα χρόνια από τους μικρούς παρόχους, που θα τρέξουν να υιοθετήσουν τέτοιες υπηρεσίες γιατί δεν θα έχουν την οικονομική δυνατότητα να κάνουν κάτι άλλο. Άρα το παιχνίδι, το άνοιγμα των εταιριών προς αυτή την κατεύθυνση, θα είναι μεγάλο.

Ο τρόπος διεξαγωγής που κι εμείς κάνουμε τους ελέγχους θα πρέπει να αλλάξει. Τα περιστατικά, πια, δεν είναι τα ίδια· κι αν κάποιος μας πει ότι θα προχωρήσουμε σε ψηφιακές γραμμές, άρα θα λυθεί το θέμα των περιστατικών που ήδη γνωρίζουμε, προφανώς και θα λυθεί, αλλά θα ανοίξουν άλλα τόσα με την υιοθέτηση των νέων τεχνολογιών που έρχονται, επομένως το πλήθος των ελέγχων δεν θα μειωθεί, απλά θα αλλάξει πεδίο, θα τροποποιηθεί προς μια άλλη κατεύθυνση, όπου θα απαιτηθεί άριστη τεχνογνωσία από τα στελέχη για να μπορέσουμε να είμαστε μπροστά στις όποιες εξελίξεις.

Η διασφάλιση του απορρήτου στη νέα ψηφιακή εποχή αποτελεί συνθήκη sine qua non.

Κι όχι μόνο αυτό, αλλά η e-privacy Οδηγία κάνει ξεκάθαρο ότι, όταν μιλάμε για ιδιωτικότητα, δεν μπορούμε να μιλήσουμε μόνο για την προστασία των προσωπικών δεδομένων per se, αλλά και για το απόρρητο της επικοινωνίας που αφορούν τα δεδομένα αυτά.

Εδώ είναι και ο σημαντικός ρόλος της ΑΔΑΕ, γιατί το απόρρητο της επικοινωνίας θα πρέπει να συνεχίσει να διαφυλάσσεται από την ΑΔΑΕ, θα πρέπει να γίνει η ανάλογη ενίσχυση του ανθρώπινου δυναμικού, όπως είπε πολύ σωστά και ο κύριος Πρόεδρος, όχι γιατί έχει γίνει σύνηθες να το λέμε, αλλά γιατί -όπως σας έδειξα προηγουμένως- οι ανάγκες είναι τέτοιες που κλιμάκιά μας θα πρέπει να βρίσκονται παντού ανά πάσα στιγμή, να προλαμβάνουν και να φέρουν εις πέρας ελέγχους που θα έχουν μεγάλη απαίτηση σε πόρους, και οικονομικούς αλλά -προπάντων- και υψηλούς σε ζητήματα τεχνογνωσίας, γι' αυτό και η κατάρτιση είναι ένα απαραίτητο χαρακτηριστικό το οποίο πρέπει να το δούμε άμεσα ως Αρχή, για να μπορέσουμε να ξεπεράσουμε τις όποιες προκλήσεις.

Σας ευχαριστώ πολύ.

ΣΑΚΚΑΣ Μ. - Συντονιστής:

Ευχαριστούμε πολύ τον Καθηγητή κύριο Καλλονιάτη.

Στο σημείο αυτό θα μου επιτρέψετε να παρεισφρήσει στην πρώτη ενότητα ο Καθηγητής κύριος Κονδύλης, παρ' ότι ήταν στη δεύτερη, κι ελπίζω να μην έχει πάρα πολύ νομική σχολαστικότητα, για να συνταυτίζεται με την ενότητα αυτή, καθώς λόγω ανειλημμένων υποχρεώσεων είπαμε να κάνει τώρα τη δική του παρουσίαση.

Ο κύριος Κονδύλης, Επίκουρος Καθηγητής της Νομικής Σχολής του Πανεπιστημίου Αθηνών, θα μας αναπτύξει το θέμα «Η πρόταση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση Ευρω-

παϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών και η προστασία του απορρήτου».

ΚΟΝΔΥΛΗΣ Β.:

Κύριε Πρόεδρε, κατ' αρχάς, επιτρέψτε μου να ευχαριστήσω την ΑΔΑΕ για τη μεγάλη τιμή που μου κάνει να είμαι σήμερα εδώ, σε αυτή την ημερίδα, να παρουσιάσω αυτό το θέμα της σημασίας της προσεχούς έκδοσης υιοθέτησης πρότασης της Επιτροπής για τη θέσπιση ενός Κώδικα Ηλεκτρονικών Επικοινωνιών.

Η πρόταση αυτή της Επιτροπής δημοσιεύτηκε τον Οκτώβρη του 2016. Έκτοτε έχουν γίνει πάρα πολλές συνεδρίες, αλλά δεν έχουν καταλήξει στην υιοθέτηση ενός κειμένου. Επίκειται πάλι η συζήτησή της, από ό,τι μαθαίνω τον επόμενο μήνα, με προοπτική να υιοθετηθεί κάποια στιγμή, επομένως θα τεθεί το ζήτημα της συμμόρφωσης της Ελλάδος προς τη νέα Οδηγία, συνεπώς αντικείμενο αυτής της παρουσίασης θα είναι η προστασία του απορρήτου και η πρόταση της Ευρωπαϊκής Επιτροπής για τη θέσπιση Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών.

Από τη στιγμή που δημοσιοποιήθηκε -12/10/2016- η πρόταση της Ευρωπαϊκής Επιτροπής, τίθενται τα εξής ζητήματα: Αν η προστασία του απορρήτου αποτελεί αντικείμενο της εν λόγω Οδηγίας, της σκοπούμενης να υιοθετηθεί Οδηγίας, αν το τιθέμενο προστατευτικό πλαίσιο θεσπίζει διατάξεις για τον φορέα που διασφαλίζει το απόρρητο και ποιες είναι οι ασφαλιστικές δικλείδες στο σχέδιο του κειμένου της πρότασης της Επιτροπής που σκοπούν άμεσα ή έμμεσα στην προστασία του απορρήτου.

Διευκρινίζεται ότι, όπως αναφέρθηκε ήδη από προηγούμενους εισηγητές, το απόρρητο είναι μέρος άλλης νομοθετικής πρωτοβουλίας, του Κανονισμού e-privacy, αναθεωρημένο σχέδιο του οποίου δημοσιεύτηκε τον Μάρτιο του 2018, κατά τη διάρκεια της βουλγαρικής Προεδρίας του Συμβουλίου της ΕΕ. Ο Κανονισμός αυτός αποτελεί ουσιώδες τμήμα της μεταρρύθμισης του νομοθετικού πλαισίου της ΕΕ για την προστασία των δεδομένων, σε συνδυασμό -μεταξύ άλλων- με τον Γενικό Κανονισμό για την προστασία των δεδομένων που δημοσιεύτηκε στις 04/05/2016 και η ισχύς του αρχίζει στις 25/05/2018, φέτος.

Στο πρώτο μέρος θα δούμε την προστασία του απορρήτου, κατά πόσο και γιατί συνδέεται με το αντικείμενο του σχεδίου της Οδηγίας. Κατ' αρχάς, από την τελευταία αναθεώρηση του κανονιστικού πλαισίου για τις ηλεκτρονικές επικοινωνίες, που έλαβε χώρα το 2009, ο εν λόγω τομέας των ηλεκτρονικών επικοινωνιών έχει εξελιχθεί σημαντικά και ο ρόλος του ως καταλύτη για την ηλεκτρονική οικονομία έχει ενισχυθεί, ζητήματα στα οποία αναφέρθηκαν οι προηγούμενοι εισηγητές. Συνεπώς ορισμένες παρατηρήσεις επί των μετά του 2009 εξελίξεων όπως παρατίθενται ιδίως στην αιτιολογική έκθεση του σχεδίου της πρότασης της Επιτροπής καταδεικνύουν άμεσα ότι οι διατάξεις του σχεδίου αυτού θα αφορούν τον τομέα της προστασίας του απορρήτου, είτε άμεσα, στο μέτρο που γίνεται αναφορά σε όρους όπως το απόρρητο των δικτύων, είτε έμμεσα, για πολλούς άλλους λόγους, π.χ. το γεγονός ότι οι καταναλωτές και οι επιχειρήσεις βασίζονται όλο και περισσότερο σε υπηρεσίες πρόσβασης σε δεδομένα και στο διαδίκτυο αντί των τηλεφωνικών και των άλλων παραδοσιακών υπηρεσιών επικοινωνιών.

Η εξέλιξη αυτή έχει οδηγήσει μέχρι πρότινος φορείς της αγοράς σε καινοφανούς μορφής ανταγωνισμό με παραδοσιακούς φορείς εκ-

μετάλλευσης τηλεπικοινωνιών όπως είναι οι λεγόμενοι πάροχοι επιφυών υπηρεσιών, και γνωρίζουμε όλοι π.χ. το Skype, το Viber, το WhatsApp κ.λπ.

Η εξέλιξη αυτή έχει επίσης αυξήσει τη ζήτηση για υψηλής ποιότητας σταθερή και ασύρματη συνδεσιμότητα δεδομένων με την αύξηση του αριθμού και της δημοτικότητας των υπηρεσιών επί γραμμικού περιεχομένου, στα οποία αναφέρθηκαν ήδη οι συνάδελφοι. Παραδείγματα τέτοιων υπηρεσιών είναι οι υπηρεσίες του υπολογιστικού νέφους, που προαναφέρθηκαν, του διαδικτύου των πραγμάτων, των επικοινωνιών μηχανής προς μηχανή.

Τα δίκτυα ηλεκτρονικών επικοινωνιών επίσης έχουν εξελιχθεί. Στις βασικές αλλαγές συγκαταλέγονται, παραδείγματος χάριν, η εν εξελίξει μετάβαση σε ένα ενιαίο δικτυακό -αποκλειστικά βασισμένο στο πρωτόκολλο διαδικτύου- περιβάλλον, οι δυνατότητες που προσφέρουν νέες και ενισχυμένες βασικές υποδομές δικτύων, οι οποίες υποστηρίζουν τη σχεδόν απεριόριστη χωρητικότητα μετάδοσης των δικτύων οπτικών ινών, η σύγκλιση σταθερών και κινητών δικτύων, η ανάπτυξη καινοτόμων τεχνικών προσεγγίσεων διαχείρισης του δικτύου και της εικονικοποίησης της λειτουργίας του δικτύου. Οι ενδεικτικά παρατιθέμενες αλλαγές - προκλήσεις στη χρήση και λειτουργία του δικτύου ηλεκτρονικών επικοινωνιών έχουν μια σειρά από αποτελέσματα.

Πολύ συνοπτικά, καθιστούν αναγκαία την επαναξιολόγηση των ισχυόντων κανόνων του 2002 όπως τροποποιήθηκαν το 2009, επομένως αυτές οι αλλαγές πρέπει να λαμβάνονται υπ' όψιν κατά την αναθεώρηση του κανονιστικού πλαισίου και συνδέονται τόσο με την προστασία του απορρήτου όσο και με την προστασία προσωπικών δεδομένων. Η αναθεώρηση αυτή εξετάζεται κατ' ανάγκην υπό το πρίσμα της στρατηγικής για την ψηφιακή ενιαία αγορά της Ευρώπης όπως εκτίθεται σε σχετική ανακοίνωση της Επιτροπής του 2015. Κατά την Επιτροπή, μια ψηφιακή ενιαία αγορά θα έδινε τη δυνατότητα στους καταναλωτές και τις επιχειρήσεις να επωφεληθούν πλήρως από τις ευκαιρίες που προσφέρουν το διαδίκτυο και οι ψηφιακές τεχνολογίες.

Τέλος, στο πλαίσιο αυτών των εισαγωγικών παρατηρήσεων, είναι αναγκαίο να κάνω μια σειρά από περαιτέρω διευκρινήσεις. Η πρόταση της Επιτροπής συνάδει με τις υφιστάμενες υποχρεώσεις βάσει του διεθνούς Δικαίου συμπεριλαμβανομένης της γενικής συμφωνίας για τις συναλλαγές στον τομέα των υπηρεσιών. Βασίζεται στο άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, που αποσκοπεί στη δημιουργία της εσωτερικής αγοράς ηλεκτρονικών επικοινωνιών, διότι αποσκοπεί στη δημιουργία αυτής της αγοράς και στην εξασφάλιση της λειτουργίας της. Είναι σύμφωνη με την αρχή της αναλογικότητας. Συνίσταται στην οριζόντια αναδιατύπωση των 4 υφισταμένων Οδηγιών του 2002 όπως τροποποιήθηκαν το 2009. Επισημαίνεται ποιες είναι αυτές οι Οδηγίες, και συγκεκριμένα: η Οδηγία για την πρόσβαση, η Οδηγία για την αδειοδότηση, η Οδηγία - Πλαίσιο και η Οδηγία για την καθολική υπηρεσία όπως τροποποιήθηκε με σχετικό Κανονισμό το 2015.

Η πρόταση της Επιτροπής προβλέπει την κατάργηση των 4 Οδηγιών και την ενσωμάτωσή τους σε ενιαία Οδηγία. Η Επιτροπή ενήργησε στο πλαίσιο σεβασμού της αρχής της επικουρικότητας λαμβάνοντας υπ' όψιν της τον νέο στόχο της πανταχού παρούσας συνδεσιμό-

τητας χωρίς περιορισμούς, ούτε τεχνικούς ούτε οικονομικούς, την εναρμόνιση των αρμοδιοτήτων των εθνικών ρυθμιστικών Αρχώνν την αποφυγή αλληλοεπικαλύψεων αρμοδιοτήτων, την εναρμόνιση των ζητημάτων που σχετίζονται με το ραδιοφάσμα και των αναθεωρημένων κανόνων για τις υπηρεσίες των ηλεκτρονικών επικοινωνιών.

Σχετικά με την κατανομή αρμοδιοτήτων, δύο ζητήματα μπορεί να ανακύψουν. Υπάρχουν αλληλοεπικαλύψεις αρμοδιοτήτων ή δεν υπάρχει σαφής οριοθέτηση αυτών. Αυτό, πρακτικά, μπορεί να έχει ως συνέπεια συγκεκριμένες αρμοδιότητες να μην ασκούνται -εν τέλει- από καμία Αρχή. Επίσης, θεωρητικά, μπορεί να υπάρχουν αρμοδιότητες που -τελικά- να μην ανατεθούν από τον νομοθέτη σε καμιά Ανεξάρτητη Αρχή. Κατ' αυτόν τον τρόπο, βεβαίως, η αρμοδιότητα μπορεί να ανατεθεί σε κάποιο Υπουργείο· στο μέτρο που το εν λόγω ζήτημα αφορά τις αρμοδιότητες των εθνικών ρυθμιστικών Αρχών, μας ενδιαφέρει στο πλαίσιο της παρούσας εισήγησης.

Τώρα, η εναρμόνιση των καθηκόντων των εθνικών ρυθμιστικών Αρχών σύμφωνα με το νέο πλαίσιο δεν θα πρέπει να οδηγήσει, κατ' αρχάς, σε μείωση της πολιτικής ανεξαρτησίας τους, αλλά -αντιθέτως- σε επέκταση της προστασίας έναντι της καθοδήγησης σε εντελώς νέους τομείς αρμοδιότητας.

Στο δεύτερο μέρος επιτρέψτε μου συνοπτικά να αναφερθώ στο σχέδιο του Ευρωπαϊκού Κώδικα και τον φορέα ασκήσεως των αρμοδιοτήτων που προβλέπει.

Πρώτα από όλα, κάποιες γενικές παρατηρήσεις. Ο Ευρωπαϊκός Κώδικας θα θεσπιστεί -επιτρέψτε μου- με Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Αυτό σημαίνει ότι κάθε κράτος-μέλος θα πρέπει να διασφαλίσει ότι εντός της προθεσμίας που τάσσει η Οδηγία θα επιτύχει τη μεταφορά των διατάξεών της στην εθνική έννομη τάξη ορίζοντας με σαφήνεια τις Αρχές που θα ασκούν τις αρμοδιότητες που προβλέπει.

Γενικότερα, ανάλογα με τη συνταγματική του έννομη τάξη, προς συμμόρφωση με την Οδηγία, κάθε κράτος-μέλος μπορεί είτε να συστήσει ενιαία κανονιστική Αρχή είτε να αναθέσει τις αρμοδιότητες -για παράδειγμα, τις σχετικές με την ασφάλεια των δικτύων- σε περισσότερες εθνικές κανονιστικές Αρχές, π.χ. διαχωρίζοντας τη διαθεσιμότητα από την ακεραιότητα των δικτύων και το απόρρητο των δεδομένων που αφορούν τις επικοινωνίες, είτε να αναθέσει τις σχετικές αρμοδιότητες σε μονοπρόσωπο ή συλλογικό Όργανο.

Περαιτέρω, λόγω της αρχής της θεσμικής αυτονομίας των κρατών-μελών, τον Ευρωπαίο νομοθέτη δεν ενδιαφέρει ποιο εθνικό κρατικό Όργανο θα συστήσει μια ή περισσότερες ανεξάρτητες Αρχές των οποίων τη δημιουργία επιτάσσει, αλλά αν το Όργανο που θα συσταθεί πληροί τα κριτήρια που χαρακτηρίζουν την ανεξαρτησία του, δηλαδή θεσμική ανεξαρτησία, προσωπική και λειτουργική ανεξαρτησία των μελών, καθώς και οργανωτική ανεξαρτησία, δηλαδή διοικητική και οικονομική αυτοτέλεια του συνιστώμενου φορέα. Το αρμόδιο Όργανο προς σύσταση θεσμού μπορεί να είναι είτε ο συνταγματικός νομοθέτης είτε ο κοινός νομοθέτης. Παραδείγματος χάριν, στην Ελλάδα, αρμόδια ρυθμιστική Αρχή του τομέα των ηλεκτρονικών επικοινωνιών είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, αλλά -κατά συνταγματική επιταγή- σε θέματα απορρήτου αποκλειστικά αρμόδια είναι η ΑΔΑΕ, που έχουμε την τιμή σήμερα να μας φιλοξενεί, ενώ σε θέματα προσωπικών δεδομένων η

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Την πολυαρχία αυτή δεν θίγει η πρόταση της Επιτροπής.

Όσον αφορά την ισχύουσα νομοθεσία σε θέματα ασφάλειας δικτύων ηλεκτρονικών επικοινωνιών, ήδη αναφέρθηκε σε αυτά τα ζητήματα ο Πρόεδρος της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων, ο Καθηγητής κύριος Μασσέλος. Πρόκειται για ένα χαρακτηριστικό παράδειγμα επιτρεπτής κατανομής αρμοδιοτήτων μεταξύ περισσοτέρων Ανεξαρτήτων Αρχών, της ΑΔΑΕ και της ΕΕΤΤ εν προκειμένω. Ένα τέτοιο χαρακτηριστικό παράδειγμα αποτελεί το ζήτημα της κατανομής αρμοδιοτήτων σε ζητήματα ασφάλειας δικτύων, την οποία απαιτεί η νομοθεσία της Ευρωπαϊκής Ένωσης, ζητήματα τα οποία ρυθμίζει το άρθρο 37 του νόμου 4070/2012. Κατά το άρθρο αυτό, οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών λαμβάνουν όλα τα κατάλληλα μέτρα για την εξασφάλιση της ακεραιότητας των δικτύων τους, έτσι ώστε να διασφαλίζεται η συνέχεια της παροχής των υπηρεσιών που διανέμονται μέσω των δικτύων αυτών. Σε σχετικό Κανονισμό της ΑΔΑΕ, που εκδόθηκε μετά το 2013, επομένως μετά την έναρξη ισχύος του νόμου 4070/2012, ορίζεται τι είναι ακεραιότητα δικτύων, η κατάσταση κατά την οποία ένα δίκτυο διατηρεί τη λειτουργικότητα για την οποία έχει σχεδιαστεί και τι αποτελεί περιστατικό ασφαλείας, ένα γεγονός που επηρεάζει την ακεραιότητα του δικτύου. Επομένως τίθεται μια χρονική διάσταση σχετικά με την ασυνέχεια στην προσφορά των υπηρεσιών, που μας ενδιαφέρει για να δούμε τι σημαίνει ακεραιότητα.

Η πρόταση της Επιτροπής ασχολείται με το θέμα της ασφάλειας των δικτύων, δίδεται ο ορισμός της ασφάλειας δικτύων και αναλύονται τα στοιχεία που τη συνθέτουν. Συγκεκριμένα, στους ορισμούς που περιέχονται στο υπό στοιχείο 22, η ασφάλεια δικτύων ορίζεται ως ικανότητα να ανθίστανται τα δίκτυα -σε δεδομένο βαθμό αξιοπιστίας- σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα και το απόρρητο των δεδομένων, επομένως έχουμε 4 στοιχεία στα οποία αναλύεται -κατά το σχέδιο Οδηγίας- το σχέδιο του Κώδικα, η ασφάλεια των δικτύων.

Αν εξαιρέσουμε χωριστά τα εν λόγω στοιχεία του ορισμού της ασφάλειας δικτύων και υπηρεσιών, ο εθνικός νομοθέτης -μεταφέροντας τις σχετικές διατάξεις· ας υποθέσουμε ότι θα παραμείνουν κατ' αυτόν τον τρόπο οι διατάξεις αυτές όπως έχουν στο σχέδιο- οφείλει να αποσαφηνίσει ποια αρμοδιότητα ανήκει σε ποια Αρχή.

Λόγου χάριν, η διαθεσιμότητα είναι κάτι το οποίο αφορά και την ΕΕΤΤ, διότι την ελέγχει. Πώς την ελέγχει; Παραδείγματος χάριν, η διαθεσιμότητα δικτύου και η ραδιοκάλυψη εντός ορισμένου χρονικού διαστήματος ενός δικτύου παροχής κινητών υπηρεσιών είναι μετρώμενος από την ΕΕΤΤ δείκτης ποιότητας των δικτύων κινητών επικοινωνιών, που οφείλει να μετρά.

Η αυθεντικότητα, ένα άλλο παράδειγμα, θα πρέπει να τύχει ειδικής μέριμνας, αποσαφηνίζοντας αν το πεδίο εφαρμογής της έννοιας αυτής συμπίπτει με την έννοια της αξιοπιστίας του δικτύου.

Όσον αφορά την ακεραιότητα, όπως είπαμε, υφίστανται κανονιστικά κείμενα που αναφέρονται στην ακεραιότητα δικτύων, σε συνδυασμό με τη διαθεσιμότητα των υπηρεσιών που εκδόθηκαν από την ΑΔΑΕ και την ΕΕΤΤ με διαφορετικά νομικά ερείσματα.

Περισσότερο σαφή είναι τα πράγματα, νομίζω, σχετικά με την αρμοδιότητα που αφορά το απόρρητο των δεδομένων, που αποθηκεύονται, μεταδίδονται, υποβάλλονται σε επεξεργασία, ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω δικτύων και υπηρεσιών, και εδώ έχουμε νομοθετικά κείμενα τα οποία ασχολούνται με το θέμα ήδη σήμερα, έχοντας μεταφέρει σχετικές κοινοτικές Οδηγίες.

Εν πάση περιπτώσει, τα θέματα αυτά θα πρέπει να επανεξεταστούν στο πλαίσιο του νέου σχεδίου Κανονισμού για το e-privacy. Επισημαίνεται πως η λήψη μέτρων για την ασφάλεια και -ιδίως- η διασφάλιση του απορρήτου αποτελούν όρο της γενικής αδείας του παρόχου ή της πράξης εκχώρησης δικαιωμάτων χρήσης σπανίων πόρων.

Εν πάση περιπτώσει, η πρόταση της Επιτροπής περιέχει μια «λυδία λίθο». Πρόκειται για την ανάγκη προστασίας των θεμελιωδών δικαιωμάτων που διασφαλίζει ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ, που έχει το ίδιο νομικό κύρος με τις συνθήκες.

Κάποια συμπεράσματα, λοιπόν. Ο ορισμός της ασφαλείας καθιστά αναγκαία την περαιτέρω αποσαφήνιση των αρμοδιοτήτων μεταξύ των συναρμοδίων Αρχών, της ΑΔΑΕ και της ΕΕΤΤ. Ο νομοθέτης δεν κωλύεται να αναθέσει τις αρμοδιότητες αυτές σε περισσότερες Αρχές, αρκεί να διασφαλίζεται το χρήσιμο αποτέλεσμα των διατάξεων της Οδηγίας, δηλαδή να εφαρμόζονται οι σχετικές διατάξεις, όπως επιχειρείται σήμερα, βέβαια, με την αγαστή συνεργασία των δυο Αρχών, της ΑΔΑΕ και της ΕΕΤΤ. Η αποσαφήνιση της ισχύουσας κατάστασης πρέπει να ξεκινήσει και από τους χρησιμοποιούμενους όρους. Παραδείγματος χάριν, πρέπει να προβληματίσει αν συνιστά στοιχείο καλής νομοθέτησης, η ΑΔΑΕ να εκδίδει Κανονισμούς και η ΕΕΤΤ δεσμευτικές υποδείξεις στο πλαίσιο εφαρμογής των κανονιστικών πράξεων που εκδίδει η ΑΔΑΕ όπως προβλέπει το άρθρο 37 του νόμου 4070/2012.

Ευχαριστώ για την προσοχής σας.

ΣΑΚΚΑΣ Μ. - Συντονιστής:

Ευχαριστούμε πολύ τον κύριο Κονδύλη.

Καλούμε στο βήμα τον κύριο Παναγιώτη Τρακάδα, Αναπληρωτή Καθηγητή του ΤΕΙ Στερεάς Ελλάδας, να μας αναπτύξει το θέμα «Το κανονιστικό πλαίσιο για την αντιμετώπιση ευπαθειών των δικτύων κινητής τηλεφωνίας».

Κύριε Καθηγητά.

ΤΡΑΚΑΔΑΣ Π.:

Σας ευχαριστώ πολύ.

Αξιότιμε κύριε Πρόεδρε, κύριε Αντιπρόεδρε, αξιότιμες κυρίες και κύριοι, στα επόμενα 10-15 λεπτά θα κάνουμε δύο τεχνολογικά βήματα πίσω, πίσω από τα blockchains, πίσω από το cloud computing, για να δούμε προβλήματα και ευπάθειες που υπάρχουν σε πρωτόκολλα επικοινωνίας που είναι εδώ· δεν θα έρθουν, δεν θα τα συναντήσουμε στο μέλλον, είναι στο παρόν και τα αντιμετωπίζουμε τώρα.

Θα σας παρουσιάσουμε μια μελέτη που κάναμε και με άλλους συναδέλφους μέσα από την ΑΔΑΕ, ήδη το όνομα του κυρίου Μανιάτη είναι στη διαφάνεια, αλλά έχουν βοηθήσει και άλλοι, όπως η κυρία Φλώρα Τσαγκαράκη από τη Νομική Υπηρεσία. Ο στόχος ήταν να καταγράψουμε τις ευπάθειες του πρωτοκόλλου σηματοδοσίας SS7, επίσης τη δέσμη

μέτρων που ήδη έπαιρναν οι πάροχοι και να καταλήξουμε με ένα κείμενο σύστασης, το οποίο θα μας άνοιγε διαύλους επικοινωνίας και θα μας επέτρεπε χρόνο με τον χρόνο να βελτιώνουμε όλο και περισσότερο τα μέτρα ασφάλειας που πρέπει να λαμβάνουν οι πάροχοι, βοηθώντας μας έτσι στην εποπτεία και στον έλεγχο των διαδικασιών.

Για την ΑΔΑΕ δεν θα πω τίποτα, είμαι βέβαιος ότι όσοι παρευρίσκεστε εδώ γνωρίζετε με τι ακριβώς ασχολείται η ΑΔΑΕ. Θα σας πω μόνο ότι στο πέρασμα των ετών που η ΑΔΑΕ δραστηριοποιείται έχουν βγει για τις ηλεκτρονικές επικοινωνίες δύο Κανονισμοί, ο πρώτος το 2011 ως απόρροια του ιδρυτικού της νόμου, ο δεύτερος το 2013 καθόσον προέκυψε από την ενσωμάτωση ευρωπαϊκών Οδηγιών στο εθνικό Δίκαιο. Και, βέβαια, κάποιος μπορεί να πει «Ωραία, και δεν φτάνει αυτό το κανονιστικό πλαίσιο για να καλύψει τις ευπάθειες του πρωτοκόλλου SS7;». Σε γενικές γραμμές, ναι. Σε ειδικές γραμμές, όμως, όχι.

Τι στάθηκε σαν αφορμή για να ξεκινήσουμε αυτή τη μελέτη και την έρευνα για τις ευπάθειες του πρωτοκόλλου SS7; Διάφορα δημοσιεύματα, που ήρθαν κατά το τέλος του 2014, και στις ΗΠΑ και στην Ευρώπη, συνεχίστηκαν μέχρι και τα μέσα του 2015, με ένα από τα χαρακτηριστικά παραδείγματα να είναι συνέδριο που έγινε στη Γερμανία, το 2014, όπου ερευνητές εκεί έδειξαν τρόπους που κάποιος κακόβουλος χρήστης θα μπορούσε να εκμεταλλευτεί ευπάθειες του πρωτοκόλλου επικοινωνίας SS7 για να εκτελέσει κακόβουλες ενέργειες μέσα στα δίκτυα παρόχων.

Τι είναι, όμως, το SS7; Χωρίς να κάνουμε update αυτή τη στιγμή, το SS7 είναι μια στοίβα πρωτοκόλλων· τέλος πάντων, είναι ένα πρωτόκολλο σηματοδοσίας που επιτρέπει στους παρόχους να παρέχουν υπηρεσίες. Σχεδιάστηκε για την επικοινωνία παρόχων σταθερών υπηρεσιών κατά τις δεκαετίες του ΄70 και του ΄80, αναθεωρήθηκε στην δεκαετία του ΄90, όταν προσπάθησαν να του δώσουν και κάποιον μανδύα ασφάλειας, μέτρων ασφάλειας, κατόπιν ήρθε η κινητή τηλεφωνία, οι πρώτες γενιές της, το 2G και το 3G, που -ακόμα και για λόγους compatibility- υιοθέτησαν αυτή την τεχνολογία μαζί με τα προβλήματά της.

Και ποια είναι αυτά τα προβλήματα; Γιατί δεν υπήρχαν τότε και παρουσιάζονται τώρα; Γιατί, όπως είπαν και οι προηγούμενοι ομιλητές, έχει αλλάξει τελείως όλο το τοπίο στις τηλεπικοινωνίες. Παλιά υπήρχαν πάροχοι σταθερής τηλεφωνίας με πολύ περιορισμένο εύρος υπηρεσιών (τηλέφωνο, φαξ και κάποιες ακόμα υπηρεσίες), ήξεραν ότι διασυνδέονταν πάροχος με πάροχο, με έμπιστα μέρη, όμως αυτό έχει αλλάξει. Από την τελευταία δημοσίευση του GSM Association φαίνεται ότι υπάρχουν παγκοσμίως περισσότερες από 5 δισεκατομμύρια συνδέσεις κινητής τηλεφωνίας. Υπάρχουν, πια, περί τους 2000 πάροχους παγκοσμίως, σε πάνω από 200 χώρες. Φανταστείτε αυτό το πλέγμα συνδέσεων για ανταλλαγή πληροφοριών μεταξύ των παρόχων. Και δεν είναι μόνο αυτό, έχουν αλλάξει και οι υπηρεσίες. Πλέον, έχοντας πάρει τη θέση σου, το στίγμα σου, το δίκτυο μπορεί να σου πει ποιο είναι το καλύτερο εστιατόριο στη γειτονιά που μένεις. Τέλος πάντων, υπάρχει πλήθος υπηρεσιών, άρα έχει αλλάξει το πεδίο.

Συνεχίζουμε, όμως, στα δίκτυα 2ης και 3ης γενιάς, να χρησιμοποιούμε το SS7 μαζί με τα προβλήματά του, σε ένα πρωτόκολλο επικοινωνίας που δεν είχε σχεδιαστεί με γνώμονα την ασφάλεια. Πρέπει να πω εδώ ότι στις τε-

λευταίες γενιές, στη 4G και στην επερχόμενη 5ης γενιάς τεχνολογία κινητής τηλεφωνίας, το πρωτόκολλο αυτό έχει εγκαταλειφτεί και ήδη υπάρχουν περισσότερο ασφαλή πρωτόκολλα όπως το DIAMETER που φαίνεται στην παρουσίαση.

Να ένα πολύ υψηλού επιπέδου σχήμα για το πώς ανταλλάσσεται η πληροφορία μεταξύ δύο δικτύων παρόχων με σκοπό την εξυπηρέτηση των συνδρομητών τους. Δεν θα μπω σε ιδιαίτερη λεπτομέρεια, θα σας πω μόνο ότι θα μπορούσαμε να χωρίσουμε αυτές τις εντολές στο πρωτόκολλο σηματοδοσίας SS7 -τις χωρίζει, δηλαδή, και το GSM Association- σε τρεις κατηγορίες. Η πρώτη κατηγορία εντολών είναι εντολές για να εξυπηρετηθεί η σύνδεση χρηστών που ανήκουν στο ίδιο δίκτυο, τις οποίες είναι και αρκετά εύκολο κάποιος να τις φιλτράρει και να καταλάβει πότε πρόκειται για κακόβουλο μήνυμα και πότε όχι. Η δεύτερη κατηγορία είναι μηνύματα που έρχονται στο δίκτυό μας επειδή εξυπηρετούμε συνδρομητές που έχουν έρθει από άλλες χώρες· φανταστείτε έναν τουρίστα που έρχεται και εξυπηρετείται από κάποιον πάροχο που δραστηριοποιείται στην Ελλάδα. Η τρίτη κατηγορία είναι ακριβώς το αντίθετο, δηλαδή πληροφορίες που μας ζητούν τα έξω δίκτυα για να εξυπηρετήσουν συνδρομητές μας που βρίσκονται στη χώρα τους, π.χ. έναν Έλληνα τουρίστα σε μια άλλη χώρα. Αυτές είναι γενικώς οι τρεις κατηγορίες εντολών, με αυξημένο κίνδυνο όσο πηγαίνουμε από τη μία κατηγορία στην άλλη.

Όπως σας είπα, το SS7 είναι μια στοίβα από πρωτόκολλα. Εμείς εδώ θα αναφερθούμε πιο πολύ στα δύο επάνω της διαφάνειας, στο MAP και στο CAP, για να δούμε τις απειλές, τις κατηγορίες των απειλών που μπορεί να προκύψουν από το πρωτόκολλο σηματοδοσίας SS7. Οι δύο επάνω είναι οι σημαντικότερες, και αφορούν, η πρώτη την αποκάλυψη πληροφοριών δικτύου, ήτοι μηνύματα που θα πουν στον κακόβουλο πού βρίσκεται το ένα ή το άλλο στοιχείο του δικτύου της εταιρίας, ή τι απαντάει το δίκτυο της εταιρίας σε συγκεκριμένα SS7 ερωτήματα, η δεύτερη την αποκάλυψη πληροφοριών των ιδίων των χρηστών, το να μπορεί -για παράδειγμα- ο κακόβουλος να ανακτήσει τον IMSI, τον μοναδικό αριθμό της σύνδεσης κινητής τηλεφωνίας, ή τη θέση, την τοποθεσία που βρίσκεται ο χρήστης. Γιατί είναι σημαντικές αυτές οι δύο κατηγορίες απειλών; Γιατί εάν αυτές είναι επιτυχείς, έχοντας συλλέξει αυτά τα στοιχεία, πληροφορίες της διαμόρφωσης του δικτύου και των συνδρομητών, μπορούν πια μετά να πάνε στις υπόλοιπες κατηγορίες, όπως είναι η υποκλοπή κλήσεων και SMS, όπως είναι η άρνηση υπηρεσίας, δηλαδή να μην μπορεί το κινητό να συνδεθεί στο δίκτυο κινητής τηλεφωνίας, όπως είναι η απάτη, πιο πολύ θέματα χρέωσης, να μπορούν να στείλουν SMS χωρίς να χρεωθούν, να μειώσουν ή να αυξήσουν τις μονάδες, καθώς επίσης όπως είναι η ανεπιθύμητη αλληλογραφία, δηλαδή το να σταλούν πολλά SMS χωρίς χρέωση, πιο πολύ με στόχο να καταφέρουν να κάνουν άρνηση υπηρεσίας.

Η διαφάνεια που βλέπετε έρχεται από μια έκθεση που δημοσίευσε ο ENISA το 2018, ακριβώς με αυτό το αντικείμενο, όπου 39 πάροχοι που δραστηριοποιούνται στην Ευρώπη απάντησαν στα ερωτήματα του ENISA, και αυτό που πρέπει να συγκρατήσει κανείς είναι ότι αυτό που οι ίδιοι οι πάροχοι θεωρούν ως τη μεγαλύτερη απειλή για το δίκτυό τους -από τις 6 κατηγορίες απειλών που αναφέραμε πριν- είναι το SMS spam, γιατί είναι πολύ πιο εύκολο να πραγματοποιηθεί μια τέτοια επίθεση, ενώ η κατηγορία επιθέσεων

που θεωρούν ότι μπορούν να την αντιμετωπίσουν -με ποσοστό 2,5% μόνο θεωρούν ότι είναι σημαντική- είναι το να μπορέσει κάποιος κακόβουλος να υποκλέψει κλήσεις. Και, βέβαια, όλες οι υπόλοιπες κατηγορίες είναι μια διαβάθμιση.

Η επόμενη διαφάνεια είναι τα αποτελέσματα μιας εταιρίας στις Ηνωμένες Πολιτείες Αμερικής η οποία, κατά τα έτη 2015-2016-2017, έκανε penetration testing σε παρόχους στο εξωτερικό, βέβαια εν γνώσει τους, προσπαθώντας να επιτύχει επιθέσεις που θα αποκάλυπταν στοιχεία του δικτύου ή των συνδρομητών. Τα αποτελέσματα αυτά φαίνονται σε αυτή τη διαφάνεια, δείχνουν μια σαφή μείωση του ποσοστού των επιτυχών επιθέσεων, και μάλιστα αυτό είναι πρόδηλο στις δυο τελευταίες κατηγορίες, όπου έχει μειωθεί πάρα πολύ το ποσοστό επιτυχών επιθέσεων, και ως προς την ανάκτηση πληροφοριών συνδρομητών και ως προς την ανάκτηση πληροφοριών της διαμόρφωσης του δικτύου των παρόχων, κάτι που δείχνει μια επαγρύπνηση από τους παρόχους.

Δεν θα μπω σε περισσότερες λεπτομέρειες, όμως φαίνεται ότι, γενικώς, σε παγκόσμιο επίπεδο και ακριβώς επειδή το πρωτόκολλο σηματοδοσίας SS7 έχει αρκετά χρόνια που χρησιμοποιείται, είναι γνωστές οι απειλές και είναι γνωστός και ο τρόπος που μπορούν να αντιμετωπιστούν. Θα έλεγα ότι σε αρκετές περιπτώσεις οι απειλές προκύπτουν από λάθος διαμόρφωση των ίδιων των παρόχων, δηλαδή κάνουν λάθος στη διαμόρφωση των δικτύων τους.

Τι περισσότερο μπορούν να κάνουν; Ποια στοιχεία θεωρεί η ΑΔΑΕ ότι -κι αυτά γράψαμε και στη σύστασή μας που εκδόθηκε το 2017- μπορούν να κάνουν οι πάροχοι ως προς την αντιμετώπιση των ευπαθειών;

Το πρώτο και το σημαντικότερο είναι να παρακολουθούν την κίνηση σε πραγματικό χρόνο. Να φιλτράρουν τα μηνύματα, όχι τόσο αυτά που διακινούνται εντός τους, για την εξυπηρέτηση των συνδρομητών μέσα στο ίδιο το δίκτυό τους, όσο εκείνα που τους έρχονται από ξένα δίκτυα, γιατί κάποια από αυτά μπορεί να μην έρχονται ζητώντας πληροφορίες από το δίκτυο του παρόχου για να εξυπηρετήσουν έναν συνδρομητή του, αλλά να είναι κακόβουλα. Υπάρχουν εργαλεία για να βοηθήσουν τους παρόχους; Ναι, υπάρχουν, και είναι αυτά τα SS7 firewalls, που μπορούν να βοηθήσουν αποτελεσματικά στην αποτροπή τέτοιων επιθέσεων και απειλών.

Μπορούν, επίσης, να διατηρούν τα αρχεία καταγραφής. Εδώ, βέβαια, υπάρχει ένα ζήτημα με το κόστος της διατήρησης, γιατί ο όγκος τους είναι μεγάλος, αλλά σίγουρα ένα trade-off μπορεί να βρεθεί.

Αφού τα κρατάνε, μπορούν και να τα αναλύουν. Η ανάλυση δεν γίνεται σε πραγματικό χρόνο· μπορεί να γίνει κάθε βράδυ, μπορεί να γίνει μια φορά την εβδομάδα, όπου ακόμα και εκεί οι πιο έξυπνες μέθοδοι στατιστικής ανάλυσης μπορούν να αναδείξουν προβλήματα μέσα στο δίκτυο.

Υπάρχουν και ειδικά μέτρα προστασίας, τα οποία είναι αρκετά τεχνικά και ίσως δεν είναι η κατάλληλη στιγμή για να υπεισέλθουμε σε λεπτομέρειες. Τι κάνουν οι πάροχοι; Τι από όλα αυτά εφαρμόζουν; Σε ποσοστό, 9 στους 10 παρόχους για την πρώτη κατηγορία και 7 στους 10 παρόχους για τη δεύτερη κατηγορία έχουν μηχανισμούς φιλτραρίσματος των μηνυμάτων και έχουν υλοποιήσει αυτές τις τεχνικές SMS home routing, δηλαδή να μη δίνουν πληροφορία του δικτύου τους σε ξένα δίκτυα. Η κατηγορία που έρχεται τελευταία

είναι οι ευφυείς μέθοδοι ανάλυσης των log αρχείων, που μόνο το 12-13% των παρόχων τα υλοποιούν.

Είναι μόνοι τους οι πάροχοι σε αυτόν τον αγώνα κατά των απειλών από τις ευπάθειες του πρωτοκόλλου SS7; Όχι. Υπάρχουν οδηγίες από την Ένωσή τους, από το GSM Association. Βέβαια, δεν είναι ανοιχτές για το κοινό, αλλά έχουν εκδοθεί. Κάποιος πάροχος θα μπορούσε να πάρει μια γενική ιδέα, να εφαρμόσει και να φτάσει ένα επίπεδο ασφάλειας.

Τι άλλο χρειάζεται; Σίγουρα χρειάζεται συνεργασία μεταξύ των παρόχων. Αν κάτι συμβεί σε κάποιον, πρέπει να ενημερώνει τους υπολοίπους, και αυτό υπάρχει.

Θέλω να σταθώ σε κάτι μόνο, και αυτή είναι η τελευταία μου διαφάνεια, ούτως ή άλλως.

Ήρθαμε σε επαφή με πάρα πολλούς Οργανισμούς. Συνεργαζόμαστε με τον ENISA τα τελευταία χρόνια, συνεργαστήκαμε πάρα πολύ στενά με τις ρυθμιστικές Αρχές των σκανδιναβικών χωρών, που είχαν ακριβώς τα ίδια προβλήματα και καθόντουσαν και σκέφτονταν πώς θα μπορούσαν να λύσουν θέματα ασφάλειας του SS7 κατά τα έτη 2015 και 2016. Τελικά, περί τα μέσα του 2017, καταλήξαμε να εκδώσουμε την Τεχνική Σύσταση για την Αντιμετώπιση Ευπαθειών Δικτύων Κινητής Τηλεφωνίας. Δεν θα τη βρείτε, δεν είναι δημόσιο κείμενο, όμως οι πάροχοι το ξέρουν ήδη, εφαρμόζουν κάποια μέτρα, ενώ μέσα στο επόμενο χρονικό διάστημα η ΑΔΑΕ σκοπεύει να ασκήσει και τον εποπτικό της ρόλο και, χρόνο με το χρόνο, σε συνεργασία με τους παρόχους, να αυξάνεται όλο και περισσότερο το επίπεδο ασφάλειας έναντι των απειλών από το σύστημα SS7.

Σας ευχαριστώ πολύ.

ΣΑΚΚΑΣ Μ. - Συντονιστής:

Ευχαριστούμε τον κύριο Τρακάδα.

Καλούμε τον τελευταίο ομιλητή της πρώτης ενότητας, τον κύριο Ιωάννη Ψαλλίδα, Διευθυντή στη Δ/νση Διασφάλισης Υποδομών, Απορρήτου Υπηρεσιών και Εφαρμογών Διαδικτύου της ΑΔΑΕ, να μας αναπτύξει το θέμα: «Απόρρητο, ακεραιότητα και διαθεσιμότητα στις ηλεκτρονικές επικοινωνίες».

Κύριε Ψαλλίδα.

ΨΑΛΛΙΔΑΣ Ι.:

Ευχαριστώ πολύ, κύριε Αντιπρόεδρε.

Καλώς ήλθατε στην ημερίδα της ΑΔΑΕ.

Αυτό που θα κάνω εγώ είναι να σας δείξω μερικά πράγματα, όχι τόσο σε τεχνολογικό βάθος όσο να σας δείξω το «δάσος», για το τι κάνει η ΑΔΑΕ, ποια είναι η αποστολή της, ποιο είναι το κανονιστικό πλαίσιο μέσα στο οποίο κινείται προκειμένου να εξασκήσει την εποπτική και ελεγκτική της αρμοδιότητα, τι έχει κάνει τα τελευταία χρόνια και ποιες είναι οι προκλήσεις που έχει να αντιμετωπίσει στο άμεσο μέλλον.

Η αποστολή της -από το όνομά της μπορείτε να το καταλάβετε- έχει να κάνει με τη διασφάλιση απορρήτου των ηλεκτρονικών επικοινωνιών, όμως μερικοί από εσάς ίσως να μη γνωρίζετε ότι, με βάση τον Νόμο 4070/2012, είναι υπεύθυνη να βγάζει Κανονισμούς και να ελέγχει ό,τι αφορά την ασφάλεια και την ακεραιότητα δικτύων και υπηρεσιών, όπως αναφέρθηκε σε προηγούμενες ομιλίες.

Το κανονιστικό πλαίσιο μέσα στο οποίο κινείται προκειμένου να εξασκήσει αυτές τις

αρμοδιότητές της, φυσικά, καθορίζεται από το Σύνταγμα, από τους Νόμους, αλλά και τους Κανονισμούς που εκδίδει, και οι οποίοι υποχρεώνουν τους παρόχους να υιοθετούν κατάλληλα οργανωτικά, διαδικαστικά και τεχνικά μέτρα. Για το απόρρητο των ηλεκτρονικών επικοινωνιών υπάρχει ένας Κανονισμός γνωστός ως απόφαση 165/2011 και για την ασφάλεια και ακεραιότητα δικτύων και υπηρεσιών -των ηλεκτρονικών επικοινωνιών πάντα- έχει βγάλει έναν Κανονισμό γνωστό ως απόφαση 205/2013, ενώ πέρυσι έβγαλε άλλη μια απόφαση, συμπληρωματική στον 205/2013, που στην ουσία θα βοηθήσει -και αυτό είναι μια πρόκληση και για εμάς- να αντλούμε στοιχεία σε συνεργασία με τους παρόχους, προκειμένου να βγάζουμε διάφορα συμπεράσματα όσον αφορά το επίπεδο της «υγείας» των δικτύων των παρόχων ώστε να προσφέρουν αδιάλειπτα δίκτυα και υπηρεσίες.

Η εποπτεία και ο έλεγχος, βασικά, εξασκούνται από ένα βασικό εργαλείο, των ελέγχων. Κάνουμε προληπτικούς ελέγχους, γνωστούς ως τακτικούς, προκειμένου να δούμε το επίπεδο εφαρμοσιμότητας των Κανονισμών από τους παρόχους, και κατασταλτικούς ελέγχους με την έννοια ότι, αφού μας υποβάλλουν καταγγελίες πολίτες ή διάφοροι οργανισμοί, ή μας γνωστοποιούνται από τους παρόχους διάφορα περιστατικά ασφάλειας τα οποία μπορεί να επηρεάσουν είτε το απόρρητο των ηλεκτρονικών επικοινωνιών είτε την ασφάλεια και την ακεραιότητα των δικτύων και των υπηρεσιών, πάμε να κάνουμε ελέγχους στα συστήματα, στα αρχεία που παράγονται από τη λειτουργία των συστημάτων, προκειμένου να διαπιστώσουμε τι ακριβώς έχει συμβεί σε αυτές τις περιπτώσεις. Φυσικά, απαντάμε σε ερωτήματα πολιτών και ερωτήματα φορέων, σε θέματα που έχουν να κάνουν με τις δύο αρμοδιότητές μας, ενώ ελέγχουμε και πολιτικές ασφάλειας, οι οποίες -στην ουσία- είναι κάποια κείμενα στα οποία οι πάροχοι δεσμεύονται ότι θα διασφαλίσουν το απόρρητο των ηλεκτρονικών επικοινωνιών, λαμβάνοντας υπ' όψιν και τον Κανονισμό, παίρνοντας και τα κατάλληλα μέτρα για να το κάνουν αυτό.

Τώρα, να δούμε τι έχουμε κάνει τα τελευταία χρόνια. Στο Μητρώο της ΕΕΤΤ υπάρχουν 550 εγγεγραμμένοι πάροχοι, από τους οποίους 95 έχουν καταθέσει πολιτική ασφάλειας και 85 είναι υπό διερεύνηση υποχρέωσης υποβολής πολιτικής ασφάλειας, δηλαδή εν δυνάμει έχουμε να ελέγξουμε 180 παρόχους. Από το γράφημα μπορείτε να δείτε ότι από το 2012 και μετά ο ρυθμός υποβολής των πολιτικών ασφάλειας έχει μειωθεί και έχει φτάσει σε ένα σημείο «ωρίμανσης», με την έννοια ότι κάθε χρόνο παίρνουμε γύρω στις 15 με 16 καινούργιες πολιτικές ασφάλειας. Για τους υπόλοιπους παρόχους, οι περισσότεροι από αυτούς έχουν δηλώσει ότι δεν εξασκούν εν τοις πράγμασι τηλεπικοινωνιακές υπηρεσίες, οπότε δεν ασχολούμαστε μαζί τους, αλλά έχουν την υποχρέωση -αν ασχοληθούν- να μας το γνωστοποιήσουν.

Όσον αφορά τους τακτικούς ελέγχους, που -όπως είπα και πριν- χρησιμοποιούνται για να διαπιστώσουμε την εφαρμοσιμότητα του Κανονισμού 165/2013, μπορούμε να δούμε τι έχουμε κάνει τα τελευταία χρόνια. Μέσα σε αυτή την 5ετία έχουμε πάει δύο φορές στους πέντε μεγαλύτερους παρόχους της Ελλάδας, οι οποίοι αντιπροσωπεύουν πάνω από το 95% του μεριδίου αγοράς των ηλεκτρονικών επικοινωνιών. Αυτό που θέλουμε να κάνουμε, όμως, είναι να αυξήσουμε αυτούς τους τακτικούς ελέγχους και στην περιφέρεια, γιατί είναι καλό να γίνει και αυτό.

Σε «αυτό» το γράφημα μπορείτε να δείτε τις καταγγελίες που μας έχουν υποβληθεί τα τελευταία 10 χρόνια, τις οποίες -όλες- έχουμε επεξεργαστεί.

Σε αυτή τη διαφάνεια μπορείτε να δείτε τον αριθμό των περιστατικών ασφάλειας που μας έχουν γνωστοποιηθεί από τους παρόχους, περιστατικά τα οποία έχουμε ερευνήσει και έχουμε καταλήξει σε συμπεράσματα.

Επίσης, βλέπετε τον αριθμό των έκτακτων ελέγχων, ειδικού σκοπού όπως τους λέμε. Στην ουσία, είναι δύο ομάδες ελέγχων, που η μία έχει να κάνει με το ότι από προηγούμενους ελέγχους έχουμε διαπιστώσει κάποια πράγματα που μας έχουν απασχολήσει και πάμε και κάνουμε ειδικούς συγκεκριμένους ελέγχους σε συγκεκριμένα συστήματα των παρόχων προκειμένου να βγάλουμε κάποια συγκεκριμένα συμπεράσματα, από τα οποία μπορεί να καταλήξουμε στο να βγάλουμε τεχνικές συστάσεις που τις δίνουμε στους παρόχους, ενώ η άλλη κατηγορία των ελέγχων έχει να κάνει με τους ελέγχους που κάνουμε σε Αρχές όπως είναι η ΕΥΠ, η ΔιΔΑΠ και η ΔΑΕΕΒ, Υπηρεσίες της Ελληνικής Αστυνομίας με συστήματα νόμιμης συνακρόασης καθώς επίσης συστήματα εντοπισμού συσκευών κινητής τηλεφωνίας.

Ως προς το κυρωτικό της έργο, σε αυτή τη διαφάνεια -την οποία μπορείτε να την κατεβάσετε από το site μας- μπορείτε να δείτε τι κυρώσεις έχει εκδώσει κατά καιρούς η ΑΔΑΕ· με μπλε είναι ο αριθμός των Αποφάσεων που κατέληξαν σε χρηματικό πρόστιμο -ως κύρωση- σε παρόχους, με βυσσινί φαίνονται οι στήλες που είναι το άθροισμα των προστίμων που έχει επιβάλει η ΑΔΑΕ σε παρόχους και με πράσινο είναι ο αριθμός των αποφάσεων της ΑΔΑΕ που έχουν καταλήξει σε συστάσεις. Υπάρχει ένα κενό για το 2011 και το 2012, αλλά αυτό το κενό δικαιολογείται, με την έννοια ότι το Συμβούλιο της Επικρατείας ακύρωσε την πρώτη Απόφαση της ΑΔΑΕ για το γνωστό περιστατικό υποκλοπών που εκδηλώθηκε το 2004-2005 και γνωστοποιήθηκε το 2006, για τυπικούς λόγους, με το σκεπτικό ότι η Αρχή έπρεπε να κάνει ανοιχτές/δημόσιες συνεδριάσεις, αλλά το 2012 αυτό λύθηκε με νόμο, ο οποίος επηρέασε όλες τις Ανεξάρτητες Αρχές, οπότε και ξεκίνησε πάλι το κυρωτικό της έργο.

Μέχρι τώρα σας μίλησα για το τι έχουμε κάνει για το απόρρητο των ηλεκτρονικών επικοινωνιών, θα σας μιλήσω και για το τι έχουμε κάνει σχετικά με την εποπτεία και τον έλεγχο για την ακεραιότητα και τη διαθεσιμότητα. Το 2012 βγήκε ο Νόμος 4070, ο οποίος ρύθμιζε εκ νέου την αγορά των ηλεκτρονικών επικοινωνιών. Το άρθρο 37, όμως, όρισε ότι η ΑΔΑΕ θα έπρεπε να βγάζει Κανονισμούς και να κάνει ελέγχους προκειμένου να διαπιστώνεται το επίπεδο της ακεραιότητας και της διαθεσιμότητας των δικτύων και υπηρεσιών των παρόχων. Είναι κάτι το οποίο κάνουμε, σε συνεργασία και με την ΕΕΤΤ. Το 2013 προχωρήσαμε με έκδοση Κανονισμού, γνωστή ως Απόφαση 205/2013, το 2014 κάναμε ελέγχους στους 10 μεγαλύτερους παρόχους της Ελλάδας προκειμένου να διαπιστώσουμε ότι έχουν κάνει κάτι σχετικά με την εφαρμογή αυτού του Κανονισμού, και τα συμπεράσματα ήταν πολύ θετικά, ενώ τα επόμενα τρία χρόνια είχαμε τρία περιστατικά ασφάλειας τα οποία μας γνωστοποιήθηκαν, αλλά -όπως θα σας εξηγήσω και αργότερα- θεωρήσαμε ότι ένα χρήσιμο εργαλείο, το οποίο θα μπορούσαμε να χρησιμοποιήσουμε προκειμένου να δούμε ποια είναι η κατάσταση των δικτύων και των υπηρεσιών όσον αφορά τη διαθεσιμότητά τους προς το κοινό που εξυπηρετούν, και σε συνεργασία με τους παρόχους, θα ήταν

να κρατούν στοιχεία που έχουν να κάνουν με περιστατικά ασφάλειας, τα οποία θα μας τα δίνουν σε δομημένη μορφή και, αφού τα επεξεργαστούμε, θα μπορούμε να καταλήγουμε σε κάποια ωφέλιμα συμπεράσματα.

Άλλες εργασίες που κάνουμε σαν ΑΔΑΕ είναι ότι εκδίδουμε Τεχνικές Συστάσεις, όπως ακούσατε και από τον προηγούμενο εισηγητή, ειδικότερα για μία Σύσταση που είχε να κάνει με τις υπηρεσίες κινητής τηλεφωνίας. Συμμετέχουμε σε συναντήσεις με ευρωπαϊκές και εθνικές ομάδες εργασίες για θέματα που άπτονται των αρμοδιοτήτων μας· όπως είπε και προηγούμενος εισηγητής, είχαμε συμμετάσχει και εμείς στην ομάδα εργασίας για την Εθνική Στρατηγική Κυβερνοασφάλειας. Συμμετέχουμε όποτε μας ζητηθεί σε έρευνες της Αστυνομίας που έχουν να κάνουν με το απόρρητο της επικοινωνίας. Συμμετέχουμε κι εμείς σε ασκήσεις κυβερνοάμυνας, για παράδειγμα στον «Πανόπτη» του ΓΕΕΘΑ. Επίσης, συνεργαζόμαστε με τις άλλες Ανεξάρτητες Αρχές, όπως την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθώς και με Υπουργεία όποτε αυτό μας ζητηθεί.

Ποιες είναι οι προκλήσεις; Να μπορούμε όσο το δυνατόν καλύτερα να αντιμετωπίζουμε παράνομα φορητά μέσα παρακολούθησης κινητής τηλεφωνίας. Ένα πρώτο βήμα, ουσιαστικό, ήταν η τεχνική Οδηγία που εκδώσαμε πέρυσι και που σας ανέλυσε ειδικότερα ο κύριος Τρακάδας. Θέλουμε να δούμε να πετυχαίνει αυτή η καινούργια Απόφαση, η 99/2017, που έχει να κάνει με τη συνεργασία με τους παρόχους, οι οποίοι θα μας δίνουν τα στοιχεία για περιστατικά ασφάλειας που επηρεάζουν τη διαθεσιμότητα των δικτύων και των υπηρεσιών τους, ώστε εμείς να μπορούμε να κάνουμε μια επεξεργασία και να καταλήγουμε σε έγκαιρα και έγκυρα συμπεράσματα. Αναμένουμε με πολύ αγωνία τον νέο ευρωπαϊκό Κανονισμό e-privacy, γιατί -όπως ανέλυσε και ο κύριος Καλλονιάτης πριν- ένα από τα μεγαλύτερα προβλήματα που έχουμε αυτή τη στιγμή είναι να κάνουμε ελέγχους σε παρόχους που βρίσκονται στο εξωτερικό. Για παράδειγμα, αν έρθει κάποιος από εσάς και μας πει ότι υποψιάζεται ότι υποκλέπτεται το email που διατηρεί στη Google ή στη Yahoo, τότε εκεί δεν θα μπορέσουμε να σας βοηθήσουμε. Από ό,τι βλέπουμε μέσα από τον e-privacy, τουλάχιστον το draft, και σε συνεργασία με τον GDPR Κανονισμό που ισχύει, φαίνεται ότι θα δημιουργηθεί μια πλατφόρμα συνεργασίας Ανεξάρτητων Αρχών προκειμένου να αντιμετωπίζονται τέτοιου είδους αιτήματα, οπότε όταν ψηφιστεί ο Κανονισμός e-privacy, τέλος πάντων, θα ανανεώσουμε και τον Κανονισμό μας που έχει να κάνει με το απόρρητο της επικοινωνίας, που είναι ο 165/2011.

Ένα από τα θέματα τα οποία έχουμε ζητήσει από την ελληνική πολιτεία τα τελευταία χρόνια είναι να υπάρχει και επέκταση στις αρμοδιότητες της ΑΔΑΕ, και ειδικότερα θα αναφερθώ στα εσωτερικά δίκτυα. Αυτή τη στιγμή μπορούμε να κάνουμε ελέγχους μόνο σε παρόχους, δηλαδή δεν μας δίνει την εξουσιοδότηση ο νόμος να πάμε να κάνουμε έλεγχο σε εσωτερικά δίκτυα, εταιρών, οργανισμών και ούτω καθεξής.

Λοιπόν, μια μεγάλη πρόκληση αποτελεί και η ραγδαία εξέλιξη της τεχνολογίας, για την οποία ο μόνος τρόπος αντιμετώπισης είναι η επένδυση συγκεκριμένα σε εξειδικευμένες αλλά ακριβές επενδύσεις σε εκπαιδεύσεις και υλικοτεχνικό εξοπλισμό προκειμένου να μη μείνουμε πίσω.

Όπως ανέφερα και πριν, από το 2012 η ΑΔΑΕ ανέλαβε την αρμοδιότητα έκδοσης κανονιστικών πράξεων και ελέγχων εφαρμογής τους όπου αφορά την ακεραιότητα και διαθεσιμότητα των δικτύων και υπηρεσιών. Ο νομοθέτης, όμως, δεν προέβλεψε αντίστοιχα την ανάλογη στελέχωση. Έχουν ακολουθηθεί όλες οι προβλεπόμενες διαδικασίες μετάταξης, αλλά -δυστυχώς- υπάρχουν πρακτικά προβλήματα ολοκλήρωσης. Παραδείγματος χάριν, άτομα που έχουν επιλεγεί μέσα από αυτή τη διαδικασία δεν αποδεσμεύονται από τις υφιστάμενες Υπηρεσίες τους. Σε «αυτόν» τον πίνακα μπορείτε να δείτε και το στελεχιακό δυναμικό, μπορείτε να δείτε ότι το 2008 ήμασταν 14 τεχνικοί συν 4 δικηγόροι που μας υποστηρίζουν στο ελεγκτικό μας έργο, ενώ τώρα, το 2018, έχουμε απομείνει 9. Με άλλα λόγια, προκειμένου να εξασφαλιστεί ότι η ποιότητα των αποτελεσμάτων ελέγχου καταγγελιών και περιστατικών ασφάλειας παραμένει υψηλή, γιατί είναι αυτή τη στιγμή υψηλή, οι χρόνοι ανταπόκρισης παραμένουν οι εύλογοι, το κανονιστικό έργο της ΑΔΑΕ παραμένει υψηλού επιπέδου, να μην μείνουμε πίσω στις τεχνολογικές εξελίξεις, με απώτερο σκοπό να διαφυλάσσεται το απόρρητο των επικοινωνιών και να εξασφαλίζεται σε ικανοποιητικά επίπεδα η διαθεσιμότητα των δικτύων και των υπηρεσιών, και όλα αυτά στο πλαίσιο ενός εκπονημένου στρατηγικού σχεδίου της ΑΔΑΕ με στοχοθεσία 3ετίας, είναι απαραίτητο να επιταχυνθούν οποιεσδήποτε διαδικασίες πρόσληψης νέου στελεχιακού δυναμικού, είτε μέσω μετατάξεων είτε μέσω νέων προσλήψεων, και να ανταποκριθεί η Πολιτεία σε αιτήματα αύξησης προϋπολογισμού της ΑΔΑΕ προκειμένου να γίνουν οι απαραίτητες επενδύσεις σε γνώση και σε εξοπλισμό.

Σας ευχαριστώ πολύ.

ΣΑΚΚΑΣ Μ. - Συντονιστής:

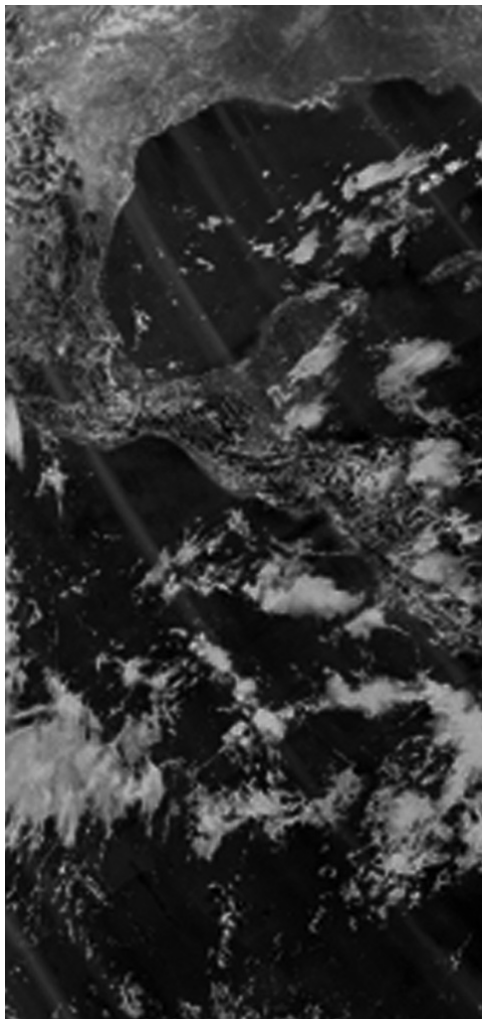
Ευχαριστούμε τον κύριο Ψαλλίδα.

Έχει τελειώσει η πρώτη ενότητα. Βέβαια, προβλέπει ερωτήσεις και συζήτηση, οπότε αν υπάρχουν μια-δυο επιτακτικές ερωτήσεις μπορούν να απαντηθούν. Υπάρχει ερώτηση; Όχι, από ό,τι βλέπω.

Να ευχαριστήσουμε ιδιαίτερα και τον κύριο Μασσέλο και τον κύριο Παπαπροδρόμου που παρακολούθησαν μέχρι τέλους την πρώτη ενότητα. Λοιπόν, 10 λεπτά διάλειμμα και επανερχόμαστε για τη δεύτερη ενότητα.

Σας ευχαριστώ πολύ.

Λήξη Α΄ Ενότητας



Β' **ΕΝΟΤΗΤΑ**

ΝΟΜΙΚΑ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΑ ΖΗΤΗΜΑΤΑ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Συντονίστρια:
Δρ. Αικατερίνη Παπανικολάου

Δικηγόρος, Μέλος της Ολομέλειας της ΑΔΑΕ

ΠΑΠΑΝΙΚΟΛΑΟΥ ΑΙ. - Συντονίστρια:

Σας ευχαριστώ πολύ.

Με τη σειρά μου, σας καλωσορίζω στην ημερίδα της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών, στο πολλά υποσχόμενο δεύτερο μέρος της σημερινής συνεδρίας. Στο πλαίσιο της δεύτερης αυτής θεματικής ενότητας, θα επιχειρήσουμε να προσεγγίσουμε νομικά και κανονιστικά ζητήματα που απασχολούν το ζήτημα της προστασίας του απορρήτου των επικοινωνιών, με μια πολύ μικρή εμβαλωματική παρέμβαση στην αρχή, δύο ομιλητών, των οποίων η συμμετοχή είχε αρχικά προγραμματιστεί για την προηγούμενη συνεδρία,. Αυτό ωστόσο, δεν κατέστη δυνατό λόγω κωλύματος του καθηγητή, κυρίου Κονδύλη, ο οποίος χρειάστηκε να προταχθεί και να περιληφθεί, όπως ήδη διαπιστώσατε, στους ομιλητές της πρώτης ενότητας. Συνεπώς, ξεκινάμε με τον κύριο Σταμούλη, Επιθεωρητή ασφάλειας στη «Δ/νση Ασφάλειας Πολιτικής Αεροπορίας από Έκνομες Ενέργειες».

Το ενδιαφέρον θέμα που ευθύς αμέσως, θα πραγματευθεί ο κος Σταμούλης αφορά την ασφάλεια των ταχυδρομικών αποστολών ως ειδικότερη έκφανση της ασφάλειας του αεροπορικού ταχυδρομείου.

Παρακαλώ, σας ακούμε, κύριε Σταμούλη.

ΣΤΑΜΟΥΛΗΣ Π.:

Ευχαριστώ πολύ.

Αξιότιμε Πρόεδρε της ΑΔΑΕ, κύριε Αντιπρόεδρε, κύρια Πρόεδρε της συνελεύσεως, θα ήθελα να σας ευχαριστήσω από πλευράς Υπηρεσίας Πολιτικής Αεροπορίας για την πρόσκληση στην τόσο πολύ ενδιαφέρουσα ημερίδα.

Όπως γνωρίζουν οι «παροικούντες την Ιερουσαλήμ», με την ΑΔΑΕ και με την ΕΕΤΤ, η ΥΠΑ, και μάλιστα η Διεύθυνση Ασφάλειας από Έκνομες Ενέργειες, προσφύεται όσον αφορά μια όχι και τόσο άυλη απειλή, αλλά μια υπαρκτή απειλή, χειροπιαστή, η οποία δεν απειλεί το απόρρητο των επικοινωνιών, αλλά απειλεί τη ζωή των επιβατών! Όπως όλοι θα έχετε καταλάβει, η έγνοια της Διεύθυνσης την οποία υπηρετώ είναι η ασφάλεια των αεροπορικών μεταφορών, και συγκεκριμένα, για να έρθουμε στο προκείμενο και να δούμε ποια είναι η σχέση μας με την ΑΔΑΕ, η ασφάλεια μεταφοράς του αεροπορικού φορτίου και ταχυδρομείου. Άρα, όταν μιλάμε για μέτρα ανάσχεσης της απειλής, κι εδώ θα κάνουμε μια παράκαμψη από αυτά που ακούσαμε μέχρι τώρα, για εμάς η απειλή προέρχεται από τις βόμβες, που με χρονική συχνότητα κάποιων ετών μας ταλαιπωρούν στο ίδιο μοτίβο και με τα ίδια -ευτυχώς μέχρι στιγμής- αναίμακτα σχετικά αποτελέσματα.

Αρχικώς, θα πρέπει να πούμε ορισμένα λόγια για το τι θεωρούμε εμείς φορτίο και ταχυδρομείο. Θα δείτε ότι αυτό προέρχεται από μια νομοθεσία, η οποία πηγάζει τόσο από τον Διεθνή Οργανισμό Πολιτικής Αεροπορίας όσο και από την Ευρωπαϊκή Ένωση, η οποία, προκειμένου να τονίσει το θέμα της ασφάλειας των αεροπορικών μεταφορών και -αν θέλετε- γραφειοκρατικά, έχει ειδικό τμήμα στην Ευρωπαϊκή Επιτροπή το οποίο ασχολείται και με την παραγωγή νομοθεσίας και με την αξιολόγηση απειλών και με τον έλεγχο των κρατών-μελών της ΕΕ, για το αν τα κάνουμε όλα σωστά και όπως πρέπει.

Άρα έχουμε δύο οργανισμούς, έναν διεθνή και έναν υπερεθνικό, τον Διεθνή Οργανισμό Πολιτικής Αεροπορίας και την Ευρωπαϊκή Ένωση δια της Ευρωπαϊκής Επιτροπής, με ένα αρκετά πυκνό πλέγμα κανόνων, υποχρεώσεων και δεσμεύσεων προκειμένου οι αεροπορικές μεταφορές να εκτελούνται με την απαιτούμενη ασφάλεια· και μιλώντας από πλευράς της Διεύθυνσης στην οποία ανήκω, δεν μιλάμε για αμέλεια, αλλά για ασφάλεια από δόλιες έκνομες ενέργειες – βόμβες, για να το φέρουμε στο προκείμενο.

Για εμάς, βάσει της δικής μας νομοθεσίας, φορτίο και ταχυδρομείο είναι το ίδιο πράγμα. Τις ίδιες απειλές μπορεί να έχει μια κάρτα που την ανοίγετε και παίζει το «τροπάρι» του Βαλεντίνου, τις ίδιες απειλές μπορεί να έχει και ένα πολύ μεγάλο κοντέινερ το οποίο να περιέχει μια βόμβα. Άρα εμείς πρέπει σαν Υπηρεσία, καθ' ύλην αρμόδια για τον τομέα αυτό, να διασφαλίσουμε με άλλες συναρμόδιες Υπηρεσίες ότι δεν υπάρχει ταχυδρομείο το οποίο φορτώνεται σε αεροσκάφος πριν να έχει υποστεί έλεγχο ασφαλείας

Να πάμε τώρα στην επόμενη καρτέλα, όπου βλέπετε τη νομοθεσία η οποία διέπει την ΥΠΑ και τη Διεύθυνση Ασφάλειας. Έχουμε έναν Εθνικό Κανονισμό Ασφάλειας και δυο Τεχνικές Οδηγίες. Ο Εθνικός Κανονισμός Ασφάλειας, που είναι υπουργική Απόφαση, και η 1η Τεχνική Οδηγία, που είναι απόφαση του διοικητή της Υπηρεσίας Πολιτικής Αεροπορίας, είναι διαθέσιμες -όπως βλέπετε- σε ΦΕΚ, γιατί πρέπει ο πολίτης να γνωρίζει πού θα παρανομήσει και τι μέτρα πρέπει να πάρουν οι φορείς που είναι αρμόδιοι για την αεροπορική ασφάλεια· εννοώ τους παρόχους, όχι τις εποπτικές Αρχές, αλλά και τις εποπτικές Αρχές εν προκειμένω. Η 2η Τεχνική Οδηγία είναι αυτό που λένε οι Αμερικανοί ή οι Άγγλοι "…for your eyes only", δηλαδή είναι -πάλι σε «τρέχοντα ελληνικά»- on a need-to-know basis, δηλαδή παρέχει πληροφορίες σε 12 κεφάλαια αεροπορικής ασφάλειας, εκ των οποίων το αεροπορικό φορτίο - ταχυδρομείο είναι ένα, στο πώς θα διαχειριστούν συγκεκριμένα οι φορείς που είναι επιφορτισμένοι με το έργο αυτό τις απειλές· και δεν θέλουμε αυτό να πάει σε λάθος χέρια, γι' αυτό και η νομοθεσία αυτή είναι περιορισμένης διαδοσιμότητας. Επίσης, έχουμε ένα εθνικό εκπαιδευτικό πρόγραμμα αεροπορικής ασφάλειας.

Όλα αυτά που σας λέω προκύπτουν από υποχρεώσεις αντίστοιχων κοινοτικών Κανονισμών. Οι κοινοτικοί Κανονισμοί επιβάλλουν αυτά, οι κοινοτικοί Κανονισμοί αλλάζουν, επομένως σε αυτό το πλαίσιο αλλάζουμε κι εμείς τα νομοθετήματά μας.

Τώρα, ο σκοπός του ελέγχου ασφαλείας, τον οποίο οι φορείς που εποπτεύουμε είναι υποχρεωμένοι να ασκούν, είναι ο εντοπισμός τυχόν απαγορευμένων αντικειμένων, που στη δικιά μας γλώσσα τα απαγορευμένα αντικείμενα είναι τα εργαλεία με τα οποία ένας κακόβουλος θα διαπράξει την έκνομη ενέργεια. Ανάλογα με το πού θα πάει ο κακόβουλος - του οποίου η πρόσβαση αρχικά θα πρέπει να αποτραπεί, γιατί αν δεν έχει πρόσβαση δεν θα πράξει την κακόβουλη ενέργεια, ό,τι και αν έχει μαζί του. Ανάλογα, λοιπόν, με τον τομέα που θα πάει, επιβάτης ή χειραποσκευές, θα πάει αντίστοιχα το απαγορευμένο αντικείμενο· και βλέπετε ότι ταλαιπωρείστε με τα υγρά, τα ψαλιδάκια, τα μαχαιράκια και λοιπά. Εδώ, στον δικό μου τομέα, «ταλαιπωρούνται» οι άνθρωποι που μπλέκουν με τις βόμβες. Για εμάς, απαγορευμένα αντικείμενα στο φορτίο - ταχυδρομείο, που μπορεί να επιφέρουν μεγίστη ζημιά και τραγικά αποτε-

λέσματα, είναι αυτά που ονομάζει η ορολογία της αστυνομίας «αυτοσχέδιους εκρηκτικούς ή εμπρηστικούς μηχανισμούς».

Γι' αυτό, λοιπόν, έχουμε ένα δίκτυο πιστοποιημένων φορέων τους οποίους ελέγχει η Υπηρεσία, από λεπτομέρεια σε λεπτομέρεια, τι εγκαταστάσεις έχουν, τι εξοπλισμό έχουν, ποιον αφήνουν -σας τα λέω γρήγορα και παραστατικά- να μπει μέσα, πώς κλειδώνουν, πώς ξεκλειδώνουν, πώς ελέγχουν το φορτίο, πώς το μεταφέρουν στα αεροσκάφη. Αυτού του είδους οι φορείς λέγονται εγκεκριμένα μεταφορικά γραφεία, μερικά από αυτά είναι «κολλημένα» πάνω στο αεροδρόμιο, άλλα είναι εκτός αεροδρομίου. Αυτό που είναι σημαντικό είναι το φορτίο - ταχυδρομείο να έχει υποστεί πριν τη φόρτωση στο αεροσκάφος έλεγχο ασφαλείας, δηλαδή να έχει περάσει από αυτούς τους φορείς οι οποίοι είναι εγκεκριμένοι από την ΥΠΑ και να έχει υποβληθεί σε μια από τις μεθόδους που αναφέρει η καρτέλα, οι οποίες είναι εγκεκριμένες τόσο από την Ευρωπαϊκή Επιτροπή όσο και -σε αντίστοιχο επίπεδο, λίγο πολύ- υπερατλαντικά, με συγκεκριμένο modus operandi, ως προς το πώς θα χρησιμοποιήσουν αυτά τα πράγματα άνθρωποι οι οποίοι είναι πιστοποιημένοι από τις Υπηρεσίες της Ελληνικής Αστυνομίας, αργότερα και από τη Σχολή Πολιτικής Αεροπορίας, ως προς τον τρόπο με τον οποίο θα χειριστούν τον εξοπλισμό και θα διεξαγάγουν αυτόν τον έλεγχο. Άρα έχουμε ένα δίκτυο, μια αλυσίδα από αυτά τα εγκεκριμένα μεταφορικά γραφεία, που έχουν εξοπλισμό και πιστοποιημένους ελεγκτές -έτσι λέγονται στη γλώσσα μας- ασφαλείας, οι οποίοι συνήθως ανήκουν σε ΙΕΠΥΑ, άλλος ένας όρος, δηλαδή σε εταιρία παροχής υπηρεσιών ασφάλειας.

Ανάλογα με τη φύση -που, κατά το δυνατόν, πρέπει να είναι εγνωσμένη στον φορέα από πριν, και αυτό γίνεται με τις αεροπορικές φορτωτικές, αλλά είναι δύσκολο στον τομέα των couriers- του φορτίου – ταχυδρομείου, πρέπει να εφαρμόσουν μία από τις επτά μεθόδους ανίχνευσης των βομβών -οι οποίες παρατίθενται εδώ, να μην σας ταλαιπωρώ- με συγκεκριμένες προδιαγραφές από την Ευρωπαϊκή Διάσκεψη Πολιτικής Αεροπορίας· δεν είναι το όποιο ακτινοσκοπικό, δεν είναι ο όποιος σκύλος, δεν είναι ο όποιος τομογράφος, αλλά συγκεκριμένος εξοπλισμός.

Τώρα, ο εξοπλισμός είναι το ένα κομμάτι, ο ανθρώπινος παράγοντας -πολύ σημαντικός- είναι το άλλο. Η αποτροπή από το να βρεθεί κάποιος στην κατάλληλη θέση να φορτώσει ένα απαγορευμένο αντικείμενο μέσα στο φορτίο, ή να το έχει βάλει στο ταχυδρομείο, είναι ένα άλλο κομμάτι. Όλα αυτά, έως εδώ, λίγο πολύ τα ελέγχουμε, αλλά το πρώτο και τελευταίο -όπως θα καταλάβατε- όριο αμύνης για την αποτροπή της τρομοκρατικής ενέργειας είναι αυτό που σας προανέφερα, ο θεσμός του εγκεκριμένου μεταφορικού γραφείου, είτε στο αεροδρόμιο είτε έξω από αυτό, όπου μετά μεταφέρεται το ελεγμένο φορτίο - ταχυδρομείο με ασφάλεια στα αεροσκάφη. Αυτό επειδή πολλές φορές αναρωτιέται κανείς «…πώς πέρασε;…». Ναι, είναι πάρα πολύ πιθανόν να περάσει. Τίποτα δεν είναι 100% foolproof. Αυτό το οποίο συζητάμε, το ερώτημα και η παρουσία μας εδώ, αφορά το πώς δεν θα διευκολύνουμε κάποιον να το κάνει με άνεση. Μέχρι στιγμής, απ' ό,τι ξέρετε, και το 2010 και πρόσφατα, οι τρομοκράτες το έκαναν με άνεση. Εκμεταλλευόμενοι ένα δίκτυο το οποίο δεν ζητάει ούτε το όνομα του αποστολέα ούτε το περιεχόμενο, τίποτα μα τίποτα απολύτως, έφτασαν στο σημείο να στείλουν στις

ευρωπαϊκές πρωτεύουσες -και τότε και τώρα- αυτά τα «τρομοδέματα» όπως τα λένε οι εφημερίδες.

Με βάση το ισχύον νομοθετικό πλαίσιο, αν και θα μπορούσε να ισχυριστεί κανείς ότι ενδεχομένως θα πρέπει σε κάποια σημεία να ξαναδούμε ορισμένα θέματα, είχαμε προτείνει ως Υπηρεσία το 2010, ξαναπροτείνουμε και τώρα, και φυσικά αυτά που λέμε είναι ενδεικτικά, κάποια μέτρα ούτως ώστε να μπορέσει να μπει ένα φίλτρο σε πρώιμο στάδιο, και αναφέρομαι στην τρωτότητα των εταιρών courier, εκεί που ο καθένας μπορεί να δώσει οτιδήποτε -θα μου πείτε, μπορεί να ρίξει και σε ένα κουτί των ΕΛΤΑ οτιδήποτε· ναι, συμφωνώ, έτσι είναι η πραγματικότητα σήμερα- και να φτάσει με την απόλυτη βεβαιότητα και ασφάλεια στον προορισμό του. Αυτό, λοιπόν, είναι εκείνο που πρέπει να μας προβληματίσει μέσα στο υπάρχον νομοθετικό πλαίσιο.

Ενδεικτικά θα αναφέρουμε ορισμένα πράγματα, τα οποία ανάγονται σε λεπτομέρειες. Με βάση τη νομοθεσία, κάθε φορέας που ασχολείται με το αεροπορικό φορτίο - ταχυδρομείο είναι υποχρεωμένος να έχει ένα λεγόμενο «πρόγραμμα ασφάλειας», να έχει έναν υπεύθυνο ασφάλειας, το προσωπικό να έχει υποστεί 5ετία ως προς τον έλεγχο ιστορικού, να έχει υποστεί εκπαίδευση πριν μπει μέσα στους χώρους που για εμάς είναι απαραβίαστοι διαφορετικά. Εδώ, λοιπόν, είναι μια σειρά από προτάσεις που είχαμε κάνει και επανερχόμεθα σε αυτές. Βέβαια, δεν είναι γραμμένες στις «πλάκες του Μωυσή», όμως η φιλοσοφία είναι που μετράει, και η φιλοσοφία είναι ότι κάτι παραπάνω χρειαζόμαστε από την τρέχουσα εμπειρία. Βλέπετε ότι θα θέλαμε να δούμε στις εταιρίες courier ορισμό υπευθύνου ασφαλείας με τη σύνταξη διαδικασιών ασφαλείας, τη διενέργεια ελέγχων στο ιστορικό του προσωπικού, την ενημέρωση του προσωπικού σε θέματα ασφάλειας, ιδιαίτερα για αποφυγή παραλαβής και διακίνησης απαγορευμένων αντικειμένων, σύμφωνα με τον ΕΚΑΠΑ. Επίσης, και εδώ αρχίζουν τα δύσκολα, την παραλαβή φορτίου και ταχυδρομείου από χώρο -γραφείο ή οτιδήποτε άλλο- κατόπιν επίδειξης και καταγραφής των στοιχείων του αποστολέα με ταυτοποίηση μέσω αστυνομικού δελτίου ταυτότητας ή άλλου αποδεκτού εγγράφου, καθώς και την αποδοχή -ει δυνατόν- ανοικτού κατά την παραλαβή δέματος με δήλωση του περιεχομένου. Αυτά θα μπορούσαν κατ' αρχάς να θεσμοθετηθούν για το αεροπορικό φορτίο – ταχυδρομείο, όπου και είδαμε να πραγματώνεται η απειλή, αλλά θα μπορούσαν κάλλιστα να επεκταθούν και αλλού. Επειδή όμως ο τομέας -εν γένει- των αερομεταφορών είναι πιο ευάλωτος στις τρομοκρατικές ενέργειες, γι' αυτό κι εμείς έχουμε αυτή την ιδιάζουσα νομοθεσία, σε επίπεδο Ευρωπαϊκής Ένωσης αλλά και διεθνώς.

Τέλος, μια από αυτές τις άλλες υποδείξεις είναι η σήμανση με ειδικό κωδικό -αποδεκτό και αναγνωρίσιμο από τους εμπλεκόμενους φορείς που θα διεξάγουν τον έλεγχο- των δεμάτων που δεν έχουν τα παραπάνω.

Σας ευχαριστώ για τον χρόνο σας.

ΠΑΠΑΝΙΚΟΛΑΟΥ Αι. - Συντονίστρια:

Εμείς σας ευχαριστούμε ιδιαίτερα. Είμαι σίγουρη ότι όλοι όσοι βρισκόμαστε στην αίθουσα σας ακούσαμε με μεγάλο ενδιαφέρον, δεδομένου ότι το θέμα σας αφορά την ασφάλεια των αεροδιαδρομών και ειδικότερα, την ασφάλεια ενός εκάστου των μετακινούμενων δι' αυτών. Εξαιρετικά και δυστυχώς, διαχρο-

νικά επίκαιρο θέμα, είναι αλήθεια. Αυτό που αντιλαμβάνεται κανείς είναι ότι, τελικώς, ζητούμενο παραμένει πάντα η στάθμιση μεταξύ ασφάλειας και διασφάλισης του απορρήτου.

Σας ευχαριστούμε πάρα πολύ.

Επόμενος ομιλητής είναι ο κύριος Μισαηλίδης, Διευθυντής στη Δ/νση Διασφάλισης Απορρήτου Ταχυδρομικών Υπηρεσιών στην Αρχή μας και στέλεχος, με διεθνή εμπειρία στον τομέα των επικοινωνιών. Από τη θέση που κατέχει, ο κος Μισαηλίδης έχει εισφέρει πολλά και σημαντικά στην τεχνογνωσία της ΑΔΑΕ ως προς την ανάπτυξη του έργου της Αρχής στην αγορά ταχυδρομικών υπηρεσιών. Τον καλώ λοιπόν στο βήμα και τον παρακαλώ να μοιραστεί μαζί μας τους προβληματισμούς του για ζητήματα ασφάλειας των διακινούμενων ταχυδρομικών αντικειμένων, σε συνέχεια των επισημάνσεων και παρατηρήσεων του κυρίου Σταμούλη.

Παρακαλώ, κύριε Μισαηλίδη.

ΜΙΣΑΗΛΙΔΗΣ Α.:

Καλησπέρα σας, κύριε Πρόεδρε, κύριε Αντιπρόεδρε, κυρία Παπανικολάου, αξιότιμοι κύριοι και κυρίες.

Τα είπε τόσο καλά ο κύριος Σταμούλης που δεν έχω πολλά να σας πω· αυτά που θα σας πω είναι συνέχεια σχεδόν όσων είπε ο κύριος Σταμούλης.

Στην ΑΔΑΕ, η Δ/νση Ταχυδρομικών Υπηρεσιών είναι μια Διεύθυνση που έχει δυο τμήματα, που το ένα ασχολείται με τα ταχυδρομεία και το άλλο με τις ταχυμεταφορές. Σε αυτή τη Διεύθυνση δεν κάνουμε τίποτε άλλο παρά να είμαστε οι θεματοφύλακες του άρθρου 19 του Συντάγματος, το οποίο πολύ απλά, μα πάρα πολύ απλά, λέει ότι η επικοινωνία και η ανταπόκριση είναι απόλυτα απαραβίαστες· υπάρχει ειδικός νόμος όταν χρειαστεί να αρθεί το απόρρητο, σε συγκεκριμένες περιπτώσεις εκτάκτου κινδύνου, όπως πόλεμος κ.λπ.

Τι θα πούμε τώρα;… Αφού τα είπαμε όλα αυτά, ας πούμε δύο πράγματα για το τι κάνουμε εμείς, για το τι κυρίως κάνουν οι ταχυμεταφορείς και τα ταχυδρομεία, τι εννοούμε μέτρα και τι εννοούμε αλληλεπίδραση μέτρων και απορρήτου, καθώς και τι είναι αυτή η περίφημη αρχή της αναλογικότητας· είμαι σίγουρος ότι κάποιος από τους προλαλήσαντες αναφέρθηκε σε αυτήν, νομίζω ο κύριος Κονδύλης.

Προτού πάω στο κύριο έργο, να σας πω δυο πράγματα για την αγορά. Η αγορά έχει ως εξής… Σύμφωνα με μια καταμέτρηση που κάναμε το 2016, οι εταιρίες ανά την επικράτεια ήταν γύρω στις 400. Όπως με πληροφόρησαν οι συνάδελφοι που συνεργάζονται μαζί μου, σήμερα έχουμε φτάσει γύρω στις 540 συν-πλην. Ένας λόγος είναι το ηλεκτρονικό εμπόριο, αλλά δεν είναι ο μόνος λόγος. Περίπου 100 εταιρίες από αυτές βρίσκονται στη Βόρεια Ελλάδα, ο κύριος όγκος των εταιριών είναι στη Στερεά Ελλάδα και στη Θεσσαλία, ενώ η Πελοπόννησος με το Ιόνιο και η Κρήτη με το Αιγαίο έχουν και αυτές ορισμένες ταχυδρομικές εταιρίες.

Ποιο είναι το έργο -συνοπτικά και πολύ γρήγορα, καθώς τα είπε και ο κύριος Ψαλλίδας πριν από εμένα- που εμείς κάνουμε στην Αρχή. Υποχρεώνουμε τις ταχυδρομικές επιχειρήσεις να μας δίνουν μία πολιτική για το πώς διασφαλίζουν το απόρρητο όταν μετακινούν ένα δέμα από τον αποστολέα έως τον παραλήπτη. Ως ΑΔΑΕ ελέγχουμε τις πολιτικές αυτές και είτε τις εγκρίνουμε είτε όχι, ή κάνουμε προτάσεις. Διεξάγουμε ελέγχους, έκτακτους όταν γίνεται καταγγελία ή τακτι-

κούς. Καλούμε σε ακρόαση τις διοικήσεις των εταιριών ή τους νόμιμους εκπροσώπους των διοικήσεων αυτών για να μας βοηθήσουν στο έργο μας. Συμμετέχουμε στην Άρση του Απορρήτου, την 3μελή Επιτροπή όπως αναφέρεται στον νόμο 2225/1994 (άρθρα 3, 4 και 5) και στο Προεδρικό Διάταγμα 47 (άρθρα 7 και 8) - τα ξέρετε αυτά, δεν είναι ανάγκη να πούμε άλλα πράγματα.

Ποιο είναι, λοιπόν, το κύριο έργο των παρόχων; Ο πάροχος, ουσιαστικά, τι κάνει; Παίρνει ένα αντικείμενο από τον αποστολέα και πρέπει να το δώσει στον παραλήπτη. Μεταξύ αποστολέα και παραλήπτη περιλαμβάνονται ορισμένα στάδια: της παραλαβής, της μεταφοράς, της διαλογής -εφόσον γίνεται διαλογή· ας μην ξεχνάμε ότι πολλές ταχυδρομικές εταιρίες δεν κάνουν διαλογή, αλλά το παίρνουν κατευθείαν από τον παραλήπτη και κάνουν την επίδοση αυθημερόν- και, τελικά, της επίδοσης.

Κατά την παραλαβή, ο πολίτης πάει στα γραφεία μιας ταχυδρομικής εταιρίας και δίνει το ταχυδρομικό αντικείμενο, είτε αυτό είναι επιστολή είτε είναι δέμα, ή πάει η εταιρία courier -γίνεται και αυτό- στην έδρα του αποστολέα και παραλαμβάνει το αντικείμενο, ή μπορεί ο πολίτης -όπως είπε και ο κύριος Σταμούλης- να εναποθέσει το ταχυδρομικό του δέμα στο κυτίο των ΕΛΤΑ, ανωνύμως αν θέλει.

Σε δεύτερο στάδιο, η μεταφορά ταχυδρομικών αντικειμένων στο εξωτερικό γίνεται αποκλειστικά αεροπορικώς, ενώ στο εσωτερικό γίνεται και αεροπορικώς και οδικώς, ή και με δίκυκλα τα οποία μεταφέρουν δέματα από αποστολέα σε παραλήπτη.

Όταν φτάσουμε στη διαλογή, ορισμένες εταιρίες διαφυλάσσουν τα ταχυδρομικά αντικείμενα σε ένα δωμάτιο, σε ένα «κέντρο διαλογής» όπως λέγεται, το οποίο -βασικά- πρέπει να προφυλάσσεται επαρκώς, είτε με το να υπάρχουν άνθρωποι φύλακες είτε με κάμερες είτε με οτιδήποτε

Μετέπειτα, αφού το ταχυδρομικό αντικείμενο είναι στο κέντρο διαλογής, το παίρνει ο διανομέας την επόμενη μέρα για να κάνει την επίδοση. Η επίδοση γίνεται σε υπαίθριες θυρίδες, όταν μιλάμε για επαρχία ή εκεί όπου δεν υπάρχει οδοαρίθμηση, η επίδοση επίσης γίνεται στην έδρα του παραλήπτη, είτε με δίκυκλο είτε με αυτοκίνητο, πλέον γίνεται και σε σταθμούς βενζίνης (Shell κ.λπ.), ενώ μελλοντικώς θα κάνουν επίδοση -νομίζω ότι έχει αρχίσει ήδη στην Ευρώπη- μέσω drone· κάποια ώρα, πιστεύω, θα έρθει και από εδώ.

Τα ανωτέρω είναι ό,τι κάνει ο πάροχος, το έργο του, αλλά ποια είναι τα μέτρα; Όταν αναφερόμαστε σε μέτρα, δεν είναι κάτι που δεν μπορούμε να φανταστούμε πολύ εύκολα. Κατά την παραλαβή, ένα ενδεικτικό μέτρο είναι να ζητάμε τα στοιχεία του αποστολέα· τα ζητάμε. Κατά τη μεταφορά, ένα ενδεικτικό μέτρο είναι να κλειδώνουμε το μηχανάκι, να μην το αφήνουμε ανοιχτό. Δεν ξέρω αν το έχετε προσέξει, αλλά στην Αθήνα τα μισά μηχανάκια όλων των παρόχων είναι ξεκλείδωτα, στην δε επαρχία όλα. Υπάρχουν εξαιρέσεις, απλά το λέω για να σας δείξω ότι δεν τηρούνται τα ενδεικτικά μέτρα ασφάλειας, αυτά τα λίγα που μπορούμε να κάνουμε. Κατά τη διαλογή, το κέντρο διαλογής πρέπει να βρίσκεται σε ξεχωριστό χώρο, να μην μπαίνει όποιος κι όποιος μέσα, παρά μόνο εξουσιοδοτημένα πρόσωπα από τον πάροχο και, φυσικά, να φυλάσσονται επαρκώς τα αντικείμενα. Κατά την επίδοση, πρέπει ο διανομέας να ζητάει τα στοιχεία του παραλήπτη. Άκρα του τάφου σιωπή! Όταν έχετε πα-

ραλάβει ένα ταχυδρομικό αντικείμενο, σας έχει ζητηθεί ποτέ να επιδείξετε ταυτότητα; Κι αν ναι, πόσες φορές; Αυτά για τα ενδεικτικά μέτρα.

Ένας άλλος μεγάλος παράγων, θα έλεγα, που έχει σχέση με τα μέτρα είναι -το είπε και ο κύριος Σταμούλης πριν- ο ανθρώπινος παράγων. Δεν ξέρω αν θυμάστε ή πόσοι θυμάστε τι έγινε 4 Νοεμβρίου του 2010, όταν παγιδευμένα πακέτα με εκρηκτικά πήγαν σε διάφορους -όχι σε έναν, αλλά σε αρκετούς- courier, διανεμήθηκαν μέσα στην Ελλάδα και στο εξωτερικό, και μάλιστα πέρασαν όλα. Εξαιτίας της παρατηρητικότητας κάποιας μικρής μεταφορικής εταιρίας εντοπίστηκαν αυτά τα πακέτα, συνέδραμε ένας υπάλληλος αυτής της εταιρίας να εντοπιστούν αυτά τα πακέτα και να μπορέσει η αστυνομία να ασκήσει κάποιον έλεγχο. Αυτά για τον ανθρώπινο παράγοντα από το ένα μέρος. Θέλω να πω ότι, εν προκειμένω, ο υπάλληλος έκανε καλά τη δουλειά του. Από το άλλο μέρος, όμως, όπως θυμάστε, πριν λίγο καιρό, το 2017, ένα παγιδευμένο πακέτο πέρασε από το αεροδρόμιο, έφτασε στο ΔΝΤ στη Γαλλία και τραυμάτισε την υπάλληλο που το παρέλαβε. Δεν εντοπίστηκε κατά την ακτινοσκόπηση ούτε ο screener είδε τι γινόταν καθώς περνούσε το πακέτο μέσα από το μηχάνημα. Και δεν είναι μόνο αυτά. Ο κύριος Σταμούλης από την ΥΠΑ είπε τη λέξη «αναίμακτα». Δεν είναι αναίμακτα! Δεν ξέρω αν θυμάστε, το 2010, τον Ιούνιο ή Ιούλιο, που σκοτώθηκε ο μακαρίτης Βασιλάκης, υπασπιστής του κυρίου Χρυσοχοΐδη όταν άνοιξε παγιδευμένο πακέτο. Του έσκασε στο πρόσωπο, σκοτώθηκε. Επικίνδυνα πράγματα, πρέπει να προσέχουμε.

Τι θα μπορούσαν να κάνουν οι πάροχοι; Οι τρεις πρώτες προτεραιότητες κάθε παρόχου πρέπει να είναι: η εκπαίδευση των υπαλλήλων, η εκπαίδευση των υπαλλήλων και η εκπαίδευση των υπαλλήλων· δεν μπορούν να κάνουν κάτι άλλο, αλλά αυτό τουλάχιστον μπορούν να το κάνουν, δεν είναι και τόσο δύσκολο.

Βέβαια, είπαμε τώρα για τα μέτρα που μπορούμε να πάρουμε, αλλά τι μέτρα να πάρουμε; Πρέπει να υπάρχει μια ισορροπία μεταξύ των μέτρων που παίρνουμε και του απορρήτου. Οι ταχυδρομικές επιχειρήσεις οφείλουν να τηρούν την αρχή της αναλογικότητας κατά τη λήψη μέτρων για την αποτροπή μεταφοράς αντικειμένων που είναι επικίνδυνα για την ασφάλεια και την υγεία του κοινού. Αυτά τα μέτρα και οι έλεγχοι που κάνουν όταν παίρνουν αυτά τα μέτρα δεν πρέπει να είναι δυσανάλογα επαχθή για το απόρρητο. Τι προσπαθώ να πω; Ότι δεν μπορούμε να καταργήσουμε το απόρρητο παίρνοντας μέτρα και μόνο αυτό. Πρέπει να υπάρχει μια ισορροπία μεταξύ των μέτρων και του απορρήτου. Άλλωστε, αυτό λέει και ο Κανονισμός της ΑΔΑΕ στο άρθρο 6 (παράγραφο ε΄) της Απόφασης 1001/Φ.21/24.03.2005.

Σας ευχαριστώ για την προσοχή σας.

ΠΑΠΑΝΙΚΟΛΑΟΥ ΑΙ. – Συντονίστρια:

Σας ευχαριστούμε πάρα πολύ, κύριε Μισαηλίδη, που στα ακριβώς 11 λεπτά, εντός των οποίων αυτοπεριοριστήκατε, καταφέρατε να εκπέμψετε περίσσεια υπηρεσιακού πατριωτισμού και αληθινό νοιάξιμο για τη διασφάλιση του ταχυδρομικού απορρήτου. Σας ευχαριστούμε πάρα πολύ.

Προχωρούμε στην εισήγηση του κυρίου Μαρκόπουλου.

Ο κύριος Μαρκόπουλος, ως έμπειρος δικαστής στο Συμβούλιο της Επικρατείας και νομικός της δικαστικής πράξης, θα μας πα-

ρουσιάσει μια -ίσως είναι λίγο υποκειμενική εκτίμηση, αλλά φαντάζομαι ότι θα πειστείτε όταν τον ακούσετε- από τις πιο ενδιαφέρουσες αποφάσεις του Συμβουλίου της Επικρατείας, σχετικά πρόσφατη, του έτους 2016, στην οποία υπήρξε εισηγητής. Η απόφαση αυτή βάζει -επιτρέψτε μου την έκφραση- τα πράγματα στη θέση τους σε σχέση με το κανονιστικό εύρος της προστασίας απορρήτου. Παίρνει θέση δηλαδή, στο ερώτημα εάν η έννοια του απορρήτου αφορά και το περιεχόμενο ή περιορίζεται απλώς στα εξωτερικά στοιχεία της επικοινωνίας. Πρόκειται για σημαντική δικαστική απόφαση, υψηλής μεθοδολογικής αξίας.

Παρακαλώ, κύριε Μαρκόπουλε, σας ακούμε.

ΜΑΡΚΟΠΟΥΛΟΣ Ν.:

Σας ευχαριστώ πολύ για την πρόσκληση που μου απευθύνατε να παρουσιάσω αυτό το πραγματικά πολύ επίκαιρο θέμα, για το οποίο υπάρχει διάσταση στη νομολογία των Ανωτάτων Δικαστηρίων, του Αρείου Πάγου και του Συμβουλίου της Επικρατείας, δυστυχώς· μάλιστα, σε αυτή την αίθουσα, που είναι συνδεδεμένη και με την ιστορία του Συμβουλίου της Επικρατείας, την αίθουσα της Γερουσίας.

Να υπενθυμίσω ξεκινώντας, λίγο-πολύ συνοπτικά, το συνταγματικό πλαίσιο.

Το άρθρο 19 του Συντάγματος κατοχυρώνει ως απόλυτα απαραβίαστο το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης της επικοινωνίας, το οποίο αίρεται μόνο υπό τις προϋποθέσεις που ορίζει η ίδια συνταγματική διάταξη, δηλαδή μόνο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, τα οποία είναι συγκεκριμένα, τα ορίζει ο εκτελεστικός Νόμος του Συντάγματος 2225/1994 (στο άρθρο 19), ο οποίος ορίζει και τις προϋποθέσεις και τη διαδικασία άρσης του απορρήτου. Η διαδικασία αυτή ολοκληρώνεται -και αυτό είναι πολύ σημαντικό- με μια ανακριτική πράξη, της έκδοσης ή επικύρωσης διάταξης άρσης του απορρήτου από το Δικαστικό Συμβούλιο.

Η ΑΔΑΕ, σε αυτό το συνταγματικό πλαίσιο, είχε πολύ σημαντικό ρόλο: την προστασία του απορρήτου και, μεταξύ άλλων, όπως ορίζει ο εκτελεστικός Νόμος 3115/2003, την αποστολή του ελέγχου της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, γεγονός που σημαίνει ότι μπορούν να υφίστανται περιπτώσεις όπου θα πρέπει πολύ διακριτικά να ελέγξεις αν τηρήθηκε η διαδικασία από τα Δικαστικά Συμβούλια. Συνήθως, αυτό το πράττει στους παρόχους.

Τώρα, όσον αφορά την έννοια των εξωτερικών στοιχείων της επικοινωνίας. Από τη χρήση των δημοσίων δικτύων ηλεκτρονικών επικοινωνιών παράγονται δεδομένα κατά την επικοινωνία. Αυτά τα δεδομένα παράγονται αυτοματοποιημένα και παράγουν πληροφορίες σχετικά με τις περιστάσεις της επικοινωνίας: τον τόπο, τον χρόνο, την ταυτότητα των επικοινωνούντων μερών, τη διάρκεια, τη συχνότητα της επικοινωνίας. Για παράδειγμα, στην περίπτωση της σταθερής τηλεφωνίας, εξωτερικά στοιχεία επικοινωνίας αποτελούν οι αριθμοί των εισερχόμενων ή εξερχόμενων κλήσεων, τα ονοματεπώνυμα, οι διευθύνσεις των προσώπων στα οποία ανήκουν οι τηλεφωνικές συνδέσεις, η ημερομηνία, η διάρκεια, η χρέωση κάθε επικοινωνίας.

Τα δεδομένα αυτά είναι παρελθοντικά, αποτελούν στοιχεία επικοινωνίας που ήδη έχει λήξει, αποθηκεύονται από τους παρόχους των ηλεκτρονικών επικοινωνιών, δηλαδή από τρίτους και όχι από τα υποκείμενα της

επικοινωνίας, διατηρούνται και τυγχάνουν επεξεργασίας από τους παρόχους, κατ' αρχήν για λόγους διεξαγωγής της επικοινωνίας και χρέωσης. Υπάρχει ένα ζήτημα με τη διατήρηση, αλλά δεν είναι το ζήτημα της εισηγήσεως. Τα δεδομένα αυτά ταξινομούνται σε δύο κατηγορίες, όπως ίσως οι περισσότεροι ξέρετε, και συγκεκριμένα σε δεδομένα κίνησης, που αφορούν τις περιστάσεις της επικοινωνίας (τόπος, χρόνος, διάρκεια), και σε δεδομένα θέσης, που αφορούν το γεωγραφικό στίγμα του τερματικού εξοπλισμού του χρήστη (πού βρίσκεται γεωγραφικά ο χρήστης την ώρα που επικοινωνεί).

Τώρα, η ισχύουσα νομοθεσία -δεν θα μιλήσω για το Σύνταγμα- στην Ελλάδα προβλέπει ότι τα εξωτερικά στοιχεία της επικοινωνίας καλύπτονται από το απόρρητο των επικοινωνιών. Πρακτικά, αυτό σημαίνει ότι, για παράδειγμα, ο ειδικός εφέτης ανακριτής που ζητά από έναν πάροχο στοιχεία τηλεφωνικών συνδέσεων - επικοινωνιών, αριθμούς κ.λπ., θα πρέπει προηγουμένως να έχει εξοπλιστεί με διάταξη άρσης του απορρήτου από το Δικαστικό Συμβούλιο. Αν δεν το κάνει αυτό, κατά τη νομοθεσία, δεν μπορεί ο πάροχος να δώσει τα στοιχεία· ο οποίος, φυσικά, θα βρεθεί σε πολύ δύσκολη θέση, καθώς από τη μια θα έχει την απειλή της ΑΔΑΕ και από την άλλη την απειλή της δικαστικής Αρχής.

Ενδεικτικά αναφέρω το Προεδρικό Διάταγμα 47/2005, το οποίο προβλέπει ότι αντικείμενο διάταξης μιας άρσης επικοινωνίας είναι τα εξωτερικά στοιχεία της επικοινωνίας, τα οποία και αναλύει εξαντλητικά, και τον Νόμο 3471/2006, που ενσωμάτωσε την Οδηγία για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, την 2002/58, που ορίζει ρητά και παραπέμπει στη χρήση της διαδικασίας άρσης του απορρήτου που προβλέπεται από το άρθρο 19 του Συντάγματος και τον εκτελεστικό Νόμο για την άρση του απορρήτου.

Μέχρι εδώ, όλα καλά· το ζήτημα που τίθεται είναι το εξής… Οι διατάξεις αυτής της νομοθεσίας, που επεκτείνουν το συνταγματικό πέπλο του απορρήτου της επικοινωνίας και σε εξωτερικά δεδομένα, στοιχούν με το άρθρο 19 του Συντάγματος; Ο Άρειος Πάγος απαντά αρνητικά και αφοριστικά, δηλαδή χωρίς κάποια ιδιαίτερη αιτιολογία, καθώς έχει ήδη δεχθεί από το 2006 -όπως στις σχετικές γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου- ότι το συνταγματικό απόρρητο των επικοινωνιών καλύπτει μόνο το περιεχόμενο, για παράδειγμα των τηλεφωνικών συνδιαλέξεων στο πεδίο της τηλεφωνίας, και όχι τα εξωτερικά στοιχεία των επικοινωνιών, παρά την περί του αντιθέτου πρακτική -πρέπει να επισημάνω- που τηρείται στη διαδικασία στα Δικαστικά Συμβούλια, όπου στις χιλιάδες διατάξεις άρσης του απορρήτου που εκδίδονται κάθε χρόνο, φυσικά, το μεγαλύτερο μέρος αυτών αφορά τα εξωτερικά στοιχεία της επικοινωνίας.

Τελικώς, φαίνεται ότι η ερμηνεία αυτή του Αρείου Πάγου περί του ότι το συνταγματικό απόρρητο των επικοινωνιών καλύπτει μόνο το περιεχόμενο και όχι τα εξωτερικά στοιχεία της επικοινωνίας παγιώνεται με τη δημοσίευση της 1/2017 Αποφάσεως της Ολομέλειας του Αρείου Πάγου. Με την απόφαση αυτή κρίθηκε ό,τι θα σας διαβάσω:

Στην έννοια του απορρήτου εμπίπτει, κατ' αρχήν, το περιεχόμενο της επικοινωνίας με όποιον τρόπο και αν αυτή διεξάγεται. Η συνταγματική προστασία του απορρήτου εντοπίζεται κατά το στάδιο της επικοινωνίας, δηλαδή κατά τον χρόνο που αυτή πραγματοποιείται και λήγει με τη λήξη της – δηλαδή

όταν κλείσετε το τηλέφωνο ή όταν στείλετε το e-mail, τελείωσε για το απόρρητο, δεν υφίσταται απόρρητο. Η προστασία του απορρήτου τελειώνει από τη στιγμή που ο παραλήπτης λάβει γνώση του περιεχομένου του μηνύματος. Από το χρονικό σημείο λήξης της επικοινωνίας κι έπειτα, κάθε στοιχείο (μήνυμα και εξωτερικά στοιχεία) μπορεί να εμπίπτει στο ρυθμιστικό πεδίο της συνταγματικής προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων, αλλά δεν καλύπτεται πλέον από τη συνταγματική προστασία του απορρήτου.

Οι συνέπειες αυτής της θέσης είναι αρκετά σοβαρές, νομίζω, διότι καταλαβαίνετε τι σημαίνει υπαγωγή εξωτερικών στοιχείων της επικοινωνίας στο γενικό πλαίσιο των προσωπικών δεδομένων, που μάλιστα αποτελούν απλά προσωπικά δεδομένα.

Η ερμηνεία αυτή του άρθρου 19 του Συντάγματος δεν είναι ορθή, κατά την άποψή μου, για τρεις λόγους:

Πρώτον, διότι παραβλέπει τη σχετική ευρωπαϊκή νομοθεσία, την Οδηγία 2002/58, του απορρήτου των επικοινωνιών, δηλαδή τον κοινό εκείνον υπερεθνικό - ευρωπαϊκό τόπο στον οποίο τα εξωτερικά στοιχεία της επικοινωνίας αποτελούν αναπόσπαστο μέρος αυτού.

Δεύτερον, ερμηνεύει -κατά την άποψή μου πάντα- εσφαλμένα το δικαίωμα που κατοχυρώνεται από το άρθρο 19 του Συντάγματος. Κυρίες και κύριοι, στο άρθρο 19 του Συντάγματος, επειδή το διαβάζω πάρα πολύ συχνά και το ακούω, δεν κατοχυρώνεται κανένα δικαίωμα ως απόρρητη επικοινωνία· κατοχυρώνεται το δικαίωμα στην απόρρητη ελεύθερη επικοινωνία, όπως πολύ ορθά -πάντα κατά την άποψή μου-επισημαίνει το Συμβούλιο της Επικρατείας. Πριν καταστεί απόρρητη η επικοινωνία, προϋποτίθεται ότι διεξάγεται ελεύθερα, δηλαδή χωρίς κανένας -πλην των υποκειμένων της επικοινωνίας- να γνωρίζει όχι μόνο το περιεχόμενο αλλά και την ίδια την πράξη της επικοινωνίας (τόπο, χρόνο, αποδέκτη), φυσικά. Συνεπώς αυτό που πράγματι προστατεύεται ως απόρρητο από το άρθρο 19 του Συντάγματος είναι το ίδιο το επικοινωνιακό γεγονός σε όλη του την έκταση, τόσο το περιεχόμενο της επικοινωνίας όσο και τα συναφώς παραγόμενα δεδομένα.

Στο πνεύμα αυτό, το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, κατά την ερμηνεία του άρθρου 8 της ΕΣΔΑ που κατοχυρώνει το δικαίωμα της επικοινωνίας και της ιδιωτικής ζωής, έχει κρίνει ότι όχι μόνο η παρακολούθηση του περιεχομένου της επικοινωνίας αλλά και η συλλογή, αποθήκευση και γνωστοποίηση παραγόμενων δεδομένων (αριθμοί εισερχόμενων κλήσεων, ημερομηνία, διάρκεια τηλεφωνικών συνδιαλέξεων), τα οποία αποτελούν αναπόσπαστο συστατικό στοιχείο της επικοινωνίας, συνιστούν επέμβαση στην απόλαυση των δικαιωμάτων αυτών.

Τρίτον, φαίνεται να παραβλέπει ότι το πλήρως εννοιολογικό περιεχόμενο της έννοιας «ελεύθερη επικοινωνία» προσδιορίζεται εξελικτικά, δηλαδή αναλόγως της τεχνολογικής προόδου στον τομέα των ηλεκτρονικών επικοινωνιών και, συνακόλουθα και κυρίως, του επιπέδου διακινδύνευσης που συνεπάγεται η τεχνολογική εξέλιξη για την ιδιωτική ζωή, την ελεύθερη ανάπτυξη προσωπικότητας και την ελευθερία της έκφρασης.

Υπό αυτό το πρίσμα, το Δικαστήριο της Ευρωπαϊκής Ένωσης ακύρωσε την Οδηγία 2002/64 η οποία επέβαλλε μια Οργουελιανή -θα έλεγα- γενική υποχρέωση αποθήκευσης, διατήρησης και επεξεργασίας για

κάποιο χρονικό διάστημα, έως 2 έτη, για όλους τους πολίτες της ΕΕ, επισημαίνοντας -μεταξύ άλλων- τη διακινδύνευση που συνεπάγεται η επεξεργασία για την ιδιωτική ζωή, και τούτο λόγω της δυνατότητας προσδιορισμού προφίλ των υποκειμένων της επικοινωνίας, δηλαδή της συναγωγής ιδιαιτέρως ακριβών συμπερασμάτων σε σχέση με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα διατηρούνται, όπως οι καθημερινές συνήθειες, οι μόνιμοι ή προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, οι δραστηριότητες, οι κοινωνικές σχέσεις και τα κοινωνικά περιβάλλοντα στα οποία τα πρόσωπα αυτά συχνάζουν.

Το Συμβούλιο της Επικρατείας, αντίθετα, προχώρησε σε μια λειτουργική ερμηνεία -υπό αυτή την οπτική που σας ανέλυσα- του άρθρου 19 του Συντάγματος και έκρινε:

Το δικαίωμα που κατοχυρώνεται από το άρθρο 19 του Συντάγματος είναι το δικαίωμα στην απόρρητη ελεύθερη επικοινωνία. Το απόρρητο της επικοινωνίας προστατεύεται έναντι πάντων, ιδιωτών και φορέων δημόσιας εξουσίας, από κάθε είδους προσβολή, και εκτείνεται στο σύνολο του επικοινωνιακού γεγονότος, δηλαδή καλύπτει όχι μόνο το περιεχόμενο της επικοινωνίας (φωνή, κείμενα, εικόνα, ήχος ιστοσελίδα) -στην Απόφαση του Συμβουλίου της Επικρατείας, στην παρένθεση αναφέρεται «ιστοσελίδα»· για όσους αμφισβήτησαν αν κατοχυρώνεται το δικαίωμα, υφίσταται δικαίωμα στο απόρρητο στο ίντερνετ- αλλά και τα συναφώς παραγόμενα δεδομένα επικοινωνίας, που προσδιορίζουν και εξατομικεύουν τις συνθήκες επικοινωνίας και τις περιστάσεις.

Με τον τρόπο αυτό, με την προστασία του συνόλου του επικοινωνιακού γεγονότος, ο συνταγματικός νομοθέτης εγγυάται ένα περιβάλλον ιδιαίτερα αυξημένης προστασίας της εμπιστευτικότητας κατά τη διεξαγωγή της επικοινωνίας και, συνακόλουθα, της ιδιωτικής ζωής. Τούτο καθίσταται ιδιαίτερα σημαντικό εν όψει της διακινδύνευσης που συνεπάγεται για την ιδιωτική ζωή και την άσκηση του δικαιώματος ελεύθερης επικοινωνίας η συστηματική επεξεργασία -ειδικώς- των δεδομένων επικοινωνίας από ιδιωτικούς και κρατικούς φορείς και για διάφορους σκοπούς, η οποία -υπενθυμίζω την ιστορία της Cambridge Analytica, η έκταση της οποίας δεν έχει συνειδητοποιηθεί ακόμα- είναι ικανή να οδηγήσει όχι μόνο στην άντληση πληροφοριών για όλο το δίκτυο των ιδιωτικών και κοινωνικών σχέσεων των ανθρώπων αλλά και στην ανίχνευση των προσωπικών, πολιτικών, φιλοσοφικών και θρησκευτικών στάσεων ή πεποιθήσεών τους.

Εν όψει της ερμηνείας αυτής του άρθρου 19 του Συντάγματος από το Συμβούλιο της Επικρατείας, το Δικαστήριο έκρινε ότι νομίμως επιβλήθηκε από την ΑΔΑΕ σε βάρος παρόχου τηλεφωνίας η διοικητική κύρωση προστίμου λόγω του ότι ο πάροχος παρέδωσε σε ειδικό εφέτη ανακριτή, σε πάρα πολύ σοβαρή υπόθεση, κατόπιν εγγράφου αιτήματος αυτού, κατάλογο με τα δεδομένα επικοινωνίας τηλεφωνικής σύνδεσης συγκεκριμένου φυσικού προσώπου (αριθμού εισερχόμενων και εξερχόμενων κλήσεων μαζί με ονοματεπώνυμα και διευθύνσεις των προσώπων στα οποία ανήκαν αυτές οι κλήσεις), χωρίς προηγουμένως να έχει κατατεθεί διάταξη άρσης του απορρήτου, ήτοι κρίθηκε ότι μη νομίμως απεστάλησαν τα στοιχεία αυτά από τον πάροχο.

Ελπίζω η εισήγησή μου να ήταν διαφωτιστική και σας ευχαριστώ πολύ για την προσοχή σας.

ΠΑΠΑΝΙΚΟΛΑΟΥ ΑΙ. - Συντονίστρια:

Σας ευχαριστούμε πάρα πολύ κύριε Μαρκόπουλε· δεν εξαντλήσατε καν τον προβλεπόμενο χρόνο και είπατε τόσο σημαντικά πράγματα.

Αν πρέπει κάτι να κρατήσουμε -ήταν όλα εξαιρετικά ενδιαφέροντα- ως παιδαγωγικώς ιδιαίτερα χρήσιμο από όσα μόλις ακούσαμε γι' αυτή τη σπουδαία απόφαση, είναι οι σημαίνουσες επισημάνσεις του κυρίου Μαρκόπουλου ως προς το περιεχόμενο της ελεύθερης επικοινωνίας και τη δυναμική έννοιά του, τη διαρκή διαμόρφωσή του δηλαδή, σε συνάρτηση με τις τεχνολογικές εξελίξεις.

Σας ευχαριστούμε πάρα πολύ.

Προχωρούμε στον κύριο Γιαννόπουλο, Επίκουρο Καθηγητή στη Νομική Σχολή του Πανεπιστημίου Αθηνών, με ιδιαιτέρως ενδιαφέρον γνωστικό αντικείμενο, τη Νομική Πληροφορική. Ο κος Γιαννόπουλος είναι παράλληλα, Διευθυντής στο Εργαστήριο Νομικής Πληροφορικής· σπάνιος -η αλήθεια είναι- και πλεονεκτικός ο συνδυασμός νομικού ιδιαιτέρως μυημένου στην επιστήμη της Πληροφορικής.

Σας ακούμε με ιδιαίτερο ενδιαφέρον, κύριε Γιαννόπουλε, για ένα ζήτημα που αφορά την ταυτοποίηση της IP διεύθυνσης (IP address).

ΓΙΑΝΝΟΠΟΥΛΟΣ Γ.:

Σας ευχαριστώ πολύ, κυρία Πρόεδρε.

Να ευχαριστήσω και την ΑΔΑΕ για την προσωπική πρόσκληση, καθώς και τον Πρόεδρο για την πρόσκληση γι' αυτή την ομιλία και για τη διοργάνωση.

Κύριοι Πρόεδροι και Μέλη των Ανεξαρτήτων Αρχών, κυρίες και κύριοι, εγώ προχωράω ένα βήμα παραπέρα από εκεί που σταμάτησε ο κύριος Μαρκόπουλος, πάμε σε ένα ειδικότερο θέμα, στην περιβόητη διεύθυνση πρωτοκόλλου Internet, την IP address.

Θα ξεκινήσω με ένα-δύο τεχνικά ζητήματα, για να δούμε λίγο τι είναι αυτή η IP address, ιδίως για όσους δεν έχουν τεχνικό υπόβαθρο. Για οποιαδήποτε επικοινωνία στο Internet -ίσως είναι γνωστό- χρησιμοποιείται συγκεκριμένο πρωτόκολλο επικοινωνίας, δηλαδή συγκεκριμένο λογισμικό, το οποίο αποκαλείται πρωτόκολλο TCP/IP από τα αρχικά Transmission Control Protocol / Internetworking Protocol. Τι σημαίνει αυτό; Σημαίνει ότι οι υπολογιστές, για να επικοινωνήσουν στο διαδίκτυο, δεν χρειάζεται απλώς να συνδεθούν με ένα καλώδιο αλλά πρέπει να «τρέχουν» και αυτό το συγκεκριμένο λογισμικό.

Κατά την εφαρμογή αυτού του πρωτοκόλλου, οποιαδήποτε συσκευή συνδεθεί στο Internet αποκτά μια 12ψηφια -υπάρχει και μία άλλη εκδοχή, θα σας την πω- αριθμητική διεύθυνση. Η εταιρία που είχε αναλάβει αρχικά την ονοματοδοσία στο Internet, η IANA (Internet Assigned Numbers Authority) στις Ηνωμένες Πολιτείες, επιβλέπει την απονομή αυτών των αριθμητικών διευθύνσεων. Αυτές οι διευθύνσεις, όπως είπα, ήταν αρχικά 12ψηφιες, λειτουργούσε το πρωτόκολλο IP version 4 (IPV4), που είχε περιορισμένο αριθμό -περίπου 4 δισεκατομμύρια- διευθύνσεων παγκοσμίως. Υπήρχε, ωστόσο, η πρόβλεψη ότι αυτός ο αριθμός δεν θα αντέξει για πάρα πολύ καιρό διότι υπάρχει μεγάλη ζήτηση για αυτές τις διευθύνσεις, επομένως έχουμε οδηγηθεί τώρα στο πρωτόκολλο IP version 6 (IPV6), το οποίο έχει μια διαφορετική μορφή· ας μην πάμε στο βάθος των τεχνι-

κών επιλογών, απλά το ζήτημα τώρα είναι ότι μπορούμε να έχουμε όσες διευθύνσεις θέλουμε, ουσιαστικά δεν είναι πεπερασμένος ο αριθμός.

Τι σημαίνει αυτή η 12ψηφια διεύθυνση; Επιτελεί δύο λειτουργίες. Πρώτον, ταυτοποιεί μονοσήμαντα όποια οντότητα συνδέεται στο Internet, η οποία μπορεί να είναι συσκευή, μπορεί να είναι κινητό τηλέφωνο, μπορεί να είναι ιστοσελίδα. Δεύτερον, χρησιμεύει για την επικοινωνία αυτών των συσκευών. Για να το πω πιο απλά, λειτουργεί ακριβώς όπως ο αριθμός του τηλεφώνου. Ο αριθμός του τηλεφώνου είναι από τη μια π.χ. ο αριθμός του Γιώργου, ξέρουμε ότι είναι ο αριθμός κάποιου, όμως χρησιμεύει και τεχνικά καθώς, όταν θέλουμε να καλέσουμε τον Γιώργο, πληκτρολογούμε τον αριθμό στο τηλέφωνο ή στη συσκευή.

Από την τεχνική πλευρά, έχουμε δύο είδη τέτοιων διευθύνσεων που αποδίδονται στις συσκευές, και αυτό έχει σημασία γι' αυτά που θα εκθέσω παρακάτω. Έχουμε τις δυναμικές διευθύνσεις, που αλλάζουν κάθε φορά που συνδέεται μια συσκευή, και τις στατικές διευθύνσεις, που απονέμονται μια φορά και μετά εξακολουθούν να είναι οι ίδιες.

Επίσης, υπάρχει ένα άλλο ζήτημα, το ότι μια τέτοια διεύθυνση μπορεί να αντιστοιχεί σε πάρα πολλούς υπολογιστές. Ιδίως όταν έχουμε εσωτερικά δίκτυα, εταιριών, επιχειρήσεων και οργανισμών, συνήθως, προς τον έξω κόσμο υπάρχει μια διεύθυνση IP, ενώ στο εσωτερικό δίκτυο υπάρχουν πάρα πολλοί συνδεδεμένοι υπολογιστές. Αντίστοιχο παράδειγμα είναι αυτό του τηλεφωνικού κέντρου από όπου μας καλούν και βλέπουμε μόνο τον αριθμό του τηλεφωνικού κέντρου, δεν βλέπουμε ποια είναι η εσωτερική γραμμή. Το λέω αυτό γιατί στο παρελθόν είχαμε τέτοια παραδείγματα, με προβλήματα που δημιουργήθηκαν, και μάλιστα κι από τον χώρο που μιλάμε, καθώς υπήρχαν μηνύματα που στάλθηκαν από τον χώρο της Βουλής με μια IP address και δεν μπορούσε να ανακαλυφθεί από ποιον συγκεκριμένο υπολογιστή είχαν σταλεί.

Τώρα, σε αυτές τις περιπτώσεις, ιδίως της δυναμικής IP, που αλλάζει, είναι κρίσιμο εάν ο πάροχος -το είπε προηγουμένως και ο κύριος Μαρκόπουλος- τηρεί κάποια στοιχεία· ο πάροχος είναι υποχρεωμένος να τηρεί κάποια στοιχεία. Ας μην μπούμε στην ιστορία της κατάργησης της Οδηγίας για το Data Retention, που εμφανίζεται στη διαφάνεια διαγραμμένη, για να τη θυμηθούμε. Εκτός από αυτήν και από την Οδηγία 2002/58/ΕΚ, τη λεγόμενη e-privacy, και εσωτερικά, από τη δική μας νομοθεσία και από τον Κανονισμό της ΑΔΑΕ για την ασφάλεια και την ακεραιότητα των δικτύων, υπάρχουν συγκεκριμένες υποχρεώσεις των παρόχων ως προς συγκεκριμένα αρχεία καταγραφής. Ακόμα, υπάρχει και το σχέδιο νέου Κανονισμού για το e-privacy, που θα αντικαταστήσει -υποτίθεται ότι θα είχε γίνει αυτό μέχρι τις 25 Μαΐου, μαζί με τον Κανονισμό για τα προσωπικά δεδομένα, αλλά δεν έχει γίνει μέχρι τώρα- την Οδηγία 2002/58/ΕΚ. Θα δούμε, λοιπόν, ότι και στο άρθρο 7 και στο άρθρο 8 του σχεδίου του Κανονισμού προβλέπεται -κι εκεί- υποχρέωση των παρόχων να τηρούν αυτά τα αρχεία καταγραφής.

Για να συμπληρώσω την εικόνα, στις κινητές επικοινωνίες, επειδή έχουμε και το τεράστιο θέμα των κινητών τηλεφώνων, προστίθεται η καταγραφή της κάρτας δικτύου, συνήθως της συσκευής. Όλες οι συσκευές που συνδέονται στο Internet έχουν μια

κάρτα δικτύου, με μια MAC address (Media Access Control address), που και αυτή πιθανώς καταγράφεται.

Επίσης, μετά τη νομοθεσία για την ταυτοποίηση -αυτή η νομοθεσία είχε τεθεί σε ισχύ μετά την απόδραση του Παλαιοκώστα, που είχαν γίνει συνεννοήσεις με καρτοκινητά τηλέφωνα και υποτίθεται ότι εισάγει μια αυστηροποίηση του πλαισίου- όλων των κινητών τηλεφώνων έχουμε τους τρεις αριθμούς που καταγράφονται από το κινητό τηλέφωνο, που είναι: ο αριθμός του συνδρομητή κινητής τηλεφωνίας (IMSI), η ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI) και, βέβαια, ο αριθμός της κάρτας SIM που χρησιμοποιεί το κινητό τηλέφωνο.

Αυτά, για να ολοκληρώσω το τεχνικό κομμάτι των διευθύνσεων IP.

Γιατί όμως μας ενδιαφέρουν όλα αυτά; Διότι υπάρχει το ενδεχόμενο, προκειμένου να ανιχνεύσουμε μια παράνομη πράξη στο Internet, να βρούμε ποιος έχει παρανομήσει με γνώση της IP address. Τι χρειαζόμαστε για να βρούμε ποιος έχει παρανομήσει; Χρειαζόμαστε τον χρόνο έναρξης και τον χρόνο λήξης της επικοινωνίας και την IP address που χρησιμοποιήθηκε. Αυτό, τεχνικά, γίνεται είτε με ειδική δοκιμή είτε μέσω ειδικής εφαρμογής (software)· ας μην αναπτύξω ειδικά το τεχνικό ζήτημα.

Από εκεί και πέρα, αν οι διευθύνσεις ανήκουν στην κατηγορία των δυναμικών διευθύνσεων και αλλάζουν, ο καταχωρητής -που είναι η IANA (Internet Assigned Names Authority), η οποία διαθέτει και τοπικούς καταχωρητές στην Ευρώπη, δηλαδή υπάρχουν ειδικές εταιρίες που αναλαμβάνουν την καταχώρηση αυτών των αριθμών- αποδίδει ειδικές ομάδες διευθύνσεων IP σε συγκεκριμένους παρόχους. Για να το πω πιο απλά, όπως παλιότερα θυμόμασταν ότι τα τηλέφωνα που αρχίζουν από 36 είναι τα τηλέφωνα του κέντρου των Αθηνών, έτσι και εδώ, οι διευθύνσεις που έχουν ένα συγκεκριμένο αριθμητικό εύρος αποδίδονται σε συγκεκριμένους παρόχους, άρα από αυτή την ομάδα αριθμών μπορούμε να βρούμε ποιος είναι ο πάροχος της IP address. Τώρα, εάν ήταν σταθερή η IP address, θα πρέπει να ανατρέξουμε στο αρχείο των πελατών του παρόχου, άρα μπορούμε να ανακαλύψουμε ποιος είναι ο πελάτης. Εάν ήταν δυναμική, εδώ έχει μεγάλη σημασία αυτό που ανέφερα προηγουμένως για το αρχείο καταγραφής. Εάν ο πάροχος διατηρεί αρχείο καταγραφής, θα πρέπει να ελέγξουμε το αρχείο καταγραφής και να βρούμε την ώρα έναρξης και την ώρα λήξης της συνεδρίας. Συνήθως, καταγράφεται και το συνθηματικό, το password προκειμένου κάποιος να αποκτήσει σύνδεση, και το όνομα χρήστη. Μετά από αυτά τα στοιχεία θα πρέπει να ανατρέξουμε στους καταλόγους του παρόχου για να βρούμε το πραγματικό όνομα του πελάτη -όχι το όνομα χρήστη- και την πραγματική διεύθυνση. Συνήθως, καταγράφουν και το τηλέφωνο, την τηλεφωνική σύνδεση από όπου προήλθε η σύνδεση, γιατί στις περισσότερες περιπτώσεις η σύνδεση θα έχει προέλθει από μια τηλεφωνική σύνδεση. Επομένως, συμπερασματικά, για να μπορέσουμε να βρούμε κάτι με την IP address, πρέπει να διαθέτουμε πρόσβαση στο αρχείο αυτών των διευθύνσεων, να γνωρίζουμε τις ώρες της πρόσβασης και -τελευταίο- ο πάροχος να διατηρεί το αρχείο καταγραφής.

Όλα αυτά -τελείωσα με τα τεχνικά- δημιουργούν τεράστια νομικά προβλήματα, διότι υπάρχει τεράστια επέμβαση στην ιδιωτική σφαίρα, όπως καταλαβαίνετε.

Αυτομάτως, δημιουργούνται δύο ερωτήματα:

Πρώτον, είναι η IP address προσωπικό δεδομένο; Η άποψή μου αλλά και η άποψη -νομίζω- της νομολογίας είναι ότι, εφόσον συνδεθεί με συγκεκριμένο πρόσωπο, η IP address αποτελεί προσωπικό δεδομένο και προστατεύεται σύμφωνα με τη νομοθεσία των προσωπικών δεδομένων. Εξάλλου, και ο καινούργιος Κανονισμός, 2016/679, ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, αναφέρει ρητά ότι τα online αναγνωριστικά στοιχεία ταυτότητας -πάντα προτιμώ το "online" και το «απευθείας» από το πολύ κακό «επιγραμμικό» που έχει επινοήσει η μεταφραστική υπηρεσία των Βρυξελλών- προστατεύονται ως προσωπικά δεδομένα και, μεταξύ αυτών, αναφέρει ως παράδειγμα τις διευθύνσεις διαδικτυακού πρωτοκόλλου - και εδώ η μετάφραση είναι λίγο περίεργη· όταν λέμε «διευθύνσεις διαδικτυακού πρωτοκόλλου» εννοούμε τις IP address.

Το ίδιο, νωρίτερα, είχε υποστηρίξει και η ομάδα του άρθρου 29, η επικεφαλής όλων των Αρχών προστασίας προσωπικών δεδομένων στην ΕΕ, που ήταν υπερεθνικό Όργανο, τώρα θα γίνει -με βάση τον καινούργιο Κανονισμό- Συμβούλιο Προσωπικών Δεδομένων. Παλαιότερα, λοιπόν, το 2007, είχε καταλήξει ερμηνευτικά ότι η IP address προστατεύεται ως προσωπικό δεδομένο.

Το δεύτερο ερώτημα, που είναι και το αντικείμενο της ημερίδας, το αν προστατεύεται με το απόρρητο, νομίζω ότι δεν υπάρχει καμιά αμφιβολία. Αν πάμε στην ίδια τη νομοθεσία, η Οδηγία 2002/58/ΕΚ, η e-privacy που έχει μεταφερθεί -τα είπε και ο κύριος Μαρκόπουλος προηγουμένως- στην Ελλάδα με τον Ν. 3471/2006, καλύπτει αυτό το ζήτημα σε δύο σημεία. Είτε θα θεωρήσουμε ότι πρόκειται για δεδομένα κίνησης, γιατί η IP address αποκαλύπτει την ταυτότητα της σύνδεσης, είτε θα θεωρήσουμε ότι αποκαλύπτει δεδομένα θέσης καθόσον, ανάλογα με την αριθμητική σειρά, προκύπτει σε ποια γεωγραφική τοποθεσία έχει απονεμηθεί η IP address. Άρα, είτε με το άρθρο 2 παρ. 3 είτε με το άρθρο 2 παρ. 4, εφόσον υποδεικνύεται η γεωγραφική θέση του εξοπλισμού, προστατεύεται με το απόρρητο.

Εφόσον ισχύουν αυτά, να δούμε πού έχει καταλήξει η νομολογία.

Ήδη έγινε αναφορά και στην παλιά υπόθεση Malone, μεταγενέστερα και στην υπόθεση Copland κατά Ηνωμένου Βασιλείου, όπου το Δικαστήριο του Στρασβούργου έχει πει ότι προστατεύονται και τα εξωτερικά στοιχεία, που αποτελούν αναπόσπαστο τμήμα της τηλεφωνικής επικοινωνίας. Αργότερα, στην υπόθεση KU κατά Φιλανδίας, και εκεί στα πραγματικά περιστατικά είχαμε τη μη αποκάλυψη της IP address σε υπόθεση συκοφαντικής δυσφήμισης, και εκεί το Δικαστήριο είπε ότι καλύπτονται και τα εξωτερικά στοιχεία της επικοινωνίας. Επίσης, πολύ πρόσφατα, σε απόφαση που εκδόθηκε πριν από μια εβδομάδα περίπου, Benedik κατά Σλοβενίας, πολύ σοβαρή υπόθεση, υπόθεση παιδικής πορνογραφίας, όπου -για να ανακαλυφθεί ποιος είναι ο υπαίτιος- χρειάστηκε να αποκαλυφθεί η IP address. Το Δικαστήριο κατέληξε ότι έχουμε παράβαση του άρθρου 8 της ΕΣΔΑ, διότι το άρθρο 37 του Συντάγματος της Σλοβενίας -που εξεταζόταν στη συγκεκριμένη περίπτωση- προέβλεπε ότι, προκειμένου να αποκαλυφθούν τα δεδομένα κίνησης, έπρεπε να υπάρξει δικαστική απόφαση· δεν υπήρξε τέτοια απόφαση, άρα είχαμε παραβίαση.

Ερχόμαστε στο ΔΕΕ τώρα, στην άλλη μεριά, στο Λουξεμβούργο.

Ήδη, από την υπόθεση Scarlet, τη γνωστή υπόθεση για τα φίλτρα που τοποθετούνται για να εμποδιστεί το παράνομο κατέβασμα περιεχομένου, που προστατεύεται με την πνευματική ιδιοκτησία, εκεί αναφέρθηκε ότι οι IP συνιστούν δεδομένα προσωπικού χαρακτήρα καθ' όσον καθιστούν δυνατή την πλήρη αναγνώριση των εν λόγω χρηστών. Αλλά και αργότερα, στην πολύ σημαντική απόφαση Breyer, αναφέρθηκε -ο Breyer ήταν ένας πολίτης της Γερμανίας που διαμαρτυρήθηκε επειδή οι δημόσιες υπηρεσίες της Γερμανίας, σε διάφορες επικοινωνίες, διατηρούσαν την IP address- ότι η δυναμική διεύθυνση IP αποτελεί δεδομένο προσωπικού χαρακτήρα και όταν ο πάροχος έχει στη διάθεσή του νόμιμα μέσα βάσει των οποίων μπορεί να τη διατηρήσει.

Επίσης, όπως βλέπετε, σε δύο Αποφάσεις που συνεκδικάσθηκαν, την Tele2 και την άλλη, στην Αγγλία, με τρεις ενδιαφερόμενους, αναφέρθηκε ότι μετά την κατάργηση της Οδηγίας για τη διατήρηση των δεδομένων έχει τεθεί το ζήτημα του τι γίνεται από εδώ και πέρα. Ουσιαστικά, σε αυτό απαντούν αυτές οι Αποφάσεις του Ευρωπαϊκού Δικαστηρίου. Και εδώ ο Νόμος -ο 3917/2011- έχει μείνει μετέωρος, και εδώ αυτές οι Αποφάσεις κατέληξαν ότι τα δεδομένα μπορούν να διατηρηθούν, εφ' όσον αφορούν σοβαρά εγκλήματα.

Έχουμε μια πολύ τελευταία ανατροπή με την απόφαση που βγήκε μόλις χτες, την απόφαση Ministerio Fiscal· δεν είναι η απόφαση, είναι οι προτάσεις του εισαγγελέα -δεν ξέρω αν θα γίνουν δεκτές από το Δικαστήριο- που, αν τις διαβάζω σωστά, λένε ότι πρέπει να αναθεωρήσουμε την έννοια του σοβαρού εγκλήματος - μετά από εμένα, όμως, ακολουθεί ο συνάδελφος ο Γιώργος Τριανταφύλλου, που νομίζω ότι στα ποινικά είναι πολύ καλύτερος από εμένα. Τι λέει, λοιπόν; Αναφέρει ότι η έννοια του σοβαρού εγκλήματος, για το οποίο αίρεται το απόρρητο, δεν πρέπει να κριθεί αποκλειστικά από τον χρόνο της ποινής. Στα πραγματικά της περιστατικά, από κάποιον στην Ισπανία έκλεψαν το πορτοφόλι και το κινητό και, προκειμένου να βρει το πορτοφόλι, ζήτησε να αρθεί το απόρρητο για να εντοπίσει τις κλήσεις από το κινητό. Η ποινή γι' αυτό το αδίκημα είναι μόνο 3 χρόνια, και όχι 5 χρόνια που προβλέπει η ισπανική διαδικασία για την άρση του απορρήτου.

Στις ΗΠΑ είναι εξαιρετικά ευαίσθητοι μετά από τα γεγονότα της 11ης Σεπτεμβρίου, όπου και εκεί αίρεται το απόρρητο. Ωστόσο, υπάρχουν αντίβαρα κι εκεί, υπάρχει η Electronic Communications Privacy Act, για να υποστηριχτούν απόψεις υπέρ του απορρήτου.

ΓΙΑΝΝΟΠΟΥΛΟΣ Γ.:

Στη Γερμανία αποκάλυπταν τα στοιχεία του πελάτη μόνο για ποινική δίωξη, και τα έδιναν γιατί θεωρούσαν και ισχυρίζονταν ότι αυτά δεν είναι εξωτερικά στοιχεία της επικοινωνίας. Αντίθετα, δεν τα έδιναν για να αποκαλυφθούν παραβιάσεις - προσβολές της πνευματικής ιδιοκτησίας.

Επίσης, κατά τη μεταφορά -ήθελα αυτή την επισήμανση- της Οδηγίας για το ηλεκτρονικό εμπόριο στην Ελλάδα, ενώ η Οδηγία λέει ότι πρέπει οι πάροχοι να αποκαλύπτουν τα στοιχεία, εδώ είχαμε μια ελληνική ιδιαιτερότητα, το ότι προστέθηκε η φράση που έχω με έντονα στοιχεία στη διαφάνεια, και συγκεκριμένα αναφέρει «…χωρίς να παραβιάζονται οι διατάξεις περί προστασίας του απορρήτου και των προσωπικών δεδομένων.».

Πού καταλήγουμε: Στο τι έχουν κάνει οι Αρχές μέχρι τώρα.

Η Αρχή Προστασίας Προσωπικών Δεδομένων, με παλαιότερες γνωμοδοτήσεις, στη δεκαετία του 2000, είχε ακολουθήσει έναν διαφορετικό δρόμο και είχε διακρίνει -κακώς κατά την άποψή μου- μεταξύ εξωτερικών και εσωτερικών στοιχείων της επικοινωνίας.

Αντίθετα, η ΑΔΑΕ έχει διατηρήσει σταθερή τη θέση υπέρ της προστασίας, και μάλιστα πρέπει να πω ότι τη διατήρησε σταθερή και εκείνο το καλοκαίρι, του 2008 ή του 2009, που διαπιστώθηκε καταιγισμός εισαγγελικών γνωμοδοτήσεων -και μιλάω για τις γνωμοδοτήσεις, διαδοχικά, των Εισαγγελέων Σανιδά, Τέντε, Κατσιρώδη, ενώ νομίζω ότι μετά υπάρχει και άλλη μία, του κυρίου Βουρλιώτη- ότι προστατεύονται και τα εξωτερικά στοιχεία της επικοινωνίας. Τα εξωτερικά στοιχεία της επικοινωνίας θεωρώ κι εγώ ότι είναι πολύ σημαντικά, μπορεί να αποκαλύπτουν πολύ περισσότερα πράγματα, ενώ ας μην ξεχνάμε πώς προέκυψε η Οδηγία για τη διατήρηση των δεδομένων· προέκυψε μετά τις τρομοκρατικές επιθέσεις στη Μαδρίτη και το Λονδίνο, όπου η πυροδότηση των μηχανισμών είχε γίνει με αναπάντητες κλήσεις.

Τελειώνω με ένα γενικότερο θέμα. Τι θέλουμε στο Internet; Επιθυμούμε την ανωνυμία ή όχι; Αυτό είναι το γενικότερο ζήτημα. Η αποκάλυψη, δηλαδή, της IP address συνδέεται με αυτό. Πρώτον, η ανωνυμία στο Internet, έτσι κι αλλιώς, είναι δεδομένη. Από εκεί και πέρα, θα πρέπει και το δικαίωμα στην ελευθερία της έκφρασης να σταθμιστεί σε σχέση με τα υπόλοιπα άρθρα του Συντάγματος, τα υπόλοιπα δικαιώματα, δηλαδή το δικαίωμα του ιδιωτικού βίου, την προστασία των προσωπικών δεδομένων, την προστασία του απορρήτου.

Προσωπικά, θεωρώ ότι η προσπάθεια καταστολής με νομοθετικούς περιορισμούς είναι μια μάχη χαμένη. Οι νέες τεχνολογίες δεν υποτάσσονται εύκολα. Πολύ γνωστό παράδειγμα ο Ν. 3783/2009, που ανέφερα προηγουμένως, για την ταυτοποίηση των κινητών τηλεφώνων. Κάλλιστα, κάποιος που θα αγοράσει μια SIM κάρτα, νόμιμα, όχι πακιστανική, όχι εκτός Ευρωπαϊκής Ένωσης, αλλά από χώρα της ΕΕ, παίρνει SIM κάρτα που δεν είναι ταυτοποιημένη και άρα μπορεί να τη χρησιμοποιήσει για να αποδράσει κάποιος από τον Κορυδαλλό. Αναφέρεται συχνά ως αντίβαρο ότι την ανωνυμία τη θέλουμε γιατί σε ανελεύθερα καθεστώτα δεν υπάρχει άλλος τρόπος να εκφράσει κανείς την άποψή του, αλλά αυτό είναι μια δικαιοπολιτική συζήτηση, που μπορεί την κάνουμε για πολύ ώρα.

Προσωπικά πιστεύω ότι πρέπει στα εργαλεία -και αυτή είναι η πρότασή μου- να στραφούμε πιο πολύ σε αυτορρυθμιστικές μεθόδους και σε δεοντολογικούς κανόνες, και οι πάροχοι -οι ενδιάμεσοι- μπορούν να βοηθήσουν πάρα πολύ σε αυτό, κάτι που το έχω υποστηρίξει έντονα.

Επίσης, θαρρώ ότι η ελληνική προσοχή έχει στραφεί πάρα πολύ στην ανεύρεση του δράστη, να βρούμε ποιος το έκανε. Δεν είναι κατά τη γνώμη μου κρίσιμο αυτό στο Internet. Στο Internet, με την πολλαπλασιαστική διάδοση της πληροφορίας, κρισιμότερο θεωρώ το να αφαιρεθεί όσο το δυνατόν γρηγορότερα η επιβλαβής πληροφορία.

Σας ευχαριστώ πολύ.

ΠΑΠΑΝΙΚΟΛΑΟΥ Αl. - Συντονίστρια:

Κι εμείς σας ευχαριστούμε πάρα πολύ, κύριε Γιαννόπουλε. Μπήκα στον πειρασμό πολλές φορές να διακόψω, αλλά ήταν τόσο

επικαιροποιημένες -μέχρι και χθεσινή νομολογία αναφέρατε- οι πληροφορίες σας, οπότε θα ήταν άδικο να στερήσω το ακροατήριο της ημερίδας από μια τέτοια προνομιακή ενημέρωση. Σας ευχαριστούμε λοιπόν, πάρα πολύ.

Προχωρούμε στον κύριο Τριανταφύλλου, Επίκουρο Καθηγητή του Ποινικού Δικαίου στη Νομική Σχολή του Πανεπιστημίου Αθηνών, ο οποίος θα μας παραθέσει σκέψεις για την ποινική διάσταση της παραβίασης του απορρήτου των επικοινωνιών· ζητήματα στάθμισης -και πάλι- έχουμε εδώ μεταξύ του προστατευόμενου δικαιώματος και άλλων δικαιωμάτων, όπως είναι η δικαστική προστασία, τα παρανόμως κτηθέντα μέσα απόδειξης και λοιπά.

Σας ακούμε, κύριε Καθηγητά.

ΤΡΙΑΝΤΑΦΥΛΛΟΥ Γ.:

Σας ευχαριστώ πολύ, κυρία Πρόεδρε.

Θα ήθελα, εισαγωγικώς, να αναφέρω ορισμένα βασικά χαρακτηριστικά του συστήματος ποινικής προστασίας των επικοινωνιών που ισχύει στην ελληνική έννομη τάξη.

Ένα πρώτο βασικό χαρακτηριστικό είναι ότι η προσέγγιση των ποινικών ζητημάτων που αναφύονται στην πράξη προϋποθέτει όχι μόνο ερμηνεία και εφαρμογή διατάξεων του ουσιαστικού ποινικού Δικαίου κατά βάση του ποινικού κώδικα αλλά -επιπρόσθετα- και άλλων διατάξεων, συνταγματικών κατά κύριο λόγο, με σημαντικότερη συνταγματική διάταξη εδώ το άρθρο 19 του Συντάγματος, αλλά και δικονομικών διατάξεων. Ο χώρος της ποινικής προστασίας της επικοινωνίας αποτελεί, νομίζω, το πιο χαρακτηριστικό παράδειγμα της αλληλεξάρτησης ουσιαστικού και δικονομικού Δικαίου, και αυτών των δυο με το συνταγματικό Δίκαιο, η συνδυασμένη εφαρμογή και ερμηνεία των οποίων μπορεί να δώσει επιτυχή λύση στα προβλήματα που αναφύονται.

Ένα δεύτερο βασικό χαρακτηριστικό, αρνητικό της σχετικής νομοθεσίας και του σχετικού συστήματος προστασίας, είναι η αφόρητη πολυνομία, καθόσον έχουμε πολλές διατάξεις που ρυθμίζουν από ποινικής απόψεως το ίδιο ζήτημα, διατάξεις του ποινικού κώδικα στο κεφάλαιο περί απορρήτων, διατάξεις σε ειδικούς ποινικούς νόμους που, κατά την προσφιλή συνήθεια του Έλληνα νομοθέτη, περιέχουν στο τέλος και μια ποινική διάταξη για την προστασία των επικοινωνιών. Επίσης, έχουμε συνεχείς τροποποιήσεις του νομοθετικού πλαισίου σε σύντομα χρονικά διαστήματα με συνέπεια να εγείρονται και σοβαρά ζητήματα διαχρονικού Δικαίου, δηλαδή ανευρέσεως του νόμου ο οποίος πρέπει να εφαρμοστεί στη συγκεκριμένη περίπτωση με βάση τις αρχές του ποινικού Δικαίου. Στο πλαίσιο αυτό, δεν προξενεί καμία εντύπωση ότι πολλές διατάξεις της -ειδικής κυρίως- ποινικής νομοθεσίας βαρύνονται και με την υπόνοια αντισυνταγματικότητάς τους λόγω αφόρητης αοριστίας τους. Μια τέτοια διάταξη είναι, λόγου χάριν, το άρθρο 10 του νόμου 3115/2003, που έχει κατακριθεί στη θεωρία ως αντισυνταγματική, μια διάταξη σύμφωνα με την οποία τιμωρείται όποιος με οποιονδήποτε τρόπο παραβιάσει οποιαδήποτε μορφή επικοινωνίας, και τίποτε άλλο. Μια τέτοια διάταξη δύσκολα αντέχει στα κριτήρια συνταγματικότητας των ποινικών διατάξεων που θέτει το άρθρο 7 του Συντάγματος αλλά και στα όρια που θέτει η θεωρία στην ποινικοποίηση κάποιων ανθρώπινων συμπεριφορών.

Ένα άλλο βασικό χαρακτηριστικό του συστήματος ποινικής προστασίας είναι η επικέντρωση της προστασίας στο λεγόμενο «τυπικό απόρρητο». Προστατεύεται, δηλαδή, το απαραβίαστο του διαύλου ή του τρόπου επικοινωνίας, για παράδειγμα η πρόσβαση σε μία επιστολή, η πρόσβαση σε μία επικοινωνία, σε μία τηλεφωνική συνδιάλεξη, χωρίς να ενδιαφέρει εάν όντως και η πληροφορία που μεταδίδεται εκείνη τη στιγμή έχει απόρρητο χαρακτήρα. Μπορεί δύο πρόσωπα να αναφέρονται σε γεγονότα γνωστά σε όλους, σε γεγονότα της επικαιρότητας, ο τρίτος που τους ακούει με μια αθέμιτη παρέμβαση διαπράττει την αξιόποινη συμπεριφορά, ανεξάρτητα από τον εμπιστευτικό ή μη χαρακτήρα της πληροφορίας. Κατ' εξαίρεση μόνο απαιτείται για τη θεμελίωση ποινικής ευθύνης η παραβίαση απορρήτου κατά κυριολεξία, δηλαδή η πρόσβαση σε μια πληροφορία το υποκείμενο της οποίας έχει ένα εύλογο ενδιαφέρον για την τήρηση της εμπιστευτικότητάς της.

Αυτά για τα βασικά χαρακτηριστικά του σχετικού συστήματος προστασίας, να αναφερθούμε τώρα στους τρόπους προσβολής.

Ποιους τρόπους προσβολής στην επικοινωνία θέλει να προλάβει ο νομοθέτης και, κατ' επέκταση, ποιους τρόπους ποινικοποιεί; Μπορούμε να κατηγοριοποιήσουμε τις προσβολές σε τρεις μεγάλες κατηγορίες. Η πρώτη κατηγορία είναι η αθέμιτη πρόσβαση σε μια επικοινωνία, λόγου χάριν κάποιος παγιδεύει ένα τηλέφωνο ή μια σύνδεση και ακούει την τηλεφωνική συνδιάλεξη δύο ατόμων. Η δεύτερη κατηγορία αξιόποινων προσβολών είναι η αποτύπωση μιας επικοινωνίας στην οποία έχει προηγηθεί αθέμιτη πρόσβαση, δηλαδή η καταγραφή της σε έναν υλικό φορέα που τη διαιωνίζει. Τρίτη αξιόποινη συμπεριφορά που μπορούμε να εντοπίσουμε στις σχετικές διατάξεις είναι η χρήση πληροφοριών που έχουν αποκτηθεί με τους δύο παραπάνω τρόπους αξιόποινης συμπεριφοράς.

Ποιο είναι το έννομο αγαθό, τι προστατεύει ο νομοθέτης μας με τις ποινικές διατάξεις περί προστασίας των επικοινωνιών; Εδώ, οι απόψεις διίστανται. Έχει υποστηριχθεί ότι προστατεύεται η ιδιωτική ζωή, έχει υποστηριχθεί ότι προστατεύεται το απόρρητο της επικοινωνίας, όμως θα συνταχθώ κι εγώ με την άποψη που ανέφερε προηγουμένως ο κύριος Μαρκόπουλος, το ότι στην πραγματικότητα αυτό που προστατεύεται είναι η ελευθερία της επικοινωνίας, ο αυθόρμητος χαρακτήρας της επικοινωνίας, η δυνατότητα να μιλάμε ελεύθερα, απερίσκεπτα, χωρίς να είναι αναγκαίο να σκεπτόμαστε κάθε φορά ότι ένας τρίτος μπορεί να ακούσει την αυθόρμητη επικοινωνία μας και να την εκμεταλλευτεί παραπέρα. Αυτή είναι η άποψη που επικρατεί και στη γερμανική επιστήμη αλλά υποστηρίζεται ευρέως και στην ελληνική επιστήμη και στη νομολογία κάποιων αποφάσεων των Δικαστηρίων μας.

Τώρα, ποια είδη επικοινωνίας προστατεύονται;

Η πρώτη μορφή επικοινωνίας που προστατεύτηκε ποινικά στην Ελλάδα ήταν η επικοινωνία με επιστολές, με έγγραφες επιστολές. Το άνοιγμα κλειστής επιστολής αποτελεί αξιόποινη συμπεριφορά ήδη από το 1951, οπότε και τέθηκε σε ισχύ ο ποινικός μας Κώδικας. Εκεί η ποινή είναι ιδιαίτερα χαμηλή, ιδιαίτερα μικρή, είναι ποινή φυλακίσεως έως ένα έτος, είναι μία διάταξη που αντιμετωπίζει τις επιστολές ως ένα αντικείμενο χρήζον ήσσονος προστασίας, κάτι βεβαίως που δεν είναι ορθό, κατά την άποψή μου.

Η δεύτερη μορφή αξιόποινης συμπεριφοράς περί τις επικοινωνίες, που ποινικοποιήθηκε, ήταν η διείσδυση, η παρακολούθηση της τηλεφωνικής επικοινωνίας, της τηλεφωνικής συνδιάλεξης όπως την ορίζει το άρθρο 370Α του ποινικού Κώδικα που θεσπίστηκε το 1982. Στη διάταξη αυτή δεν ποινικοποιείται μόνο η πρόσβαση στην απόρρητη πληροφορία αλλά, όπως συμβαίνει και σε άλλες ποινικές διατάξεις, προστατεύονται ήδη πρόδρομες προσπάθειες πρόσβασης της πληροφορίας που μεταδίδεται τηλεφωνικώς. Η παγίδευση και η σύνδεση είναι καθεαυτές αξιόποινες συμπεριφορές, ανεξάρτητα αν ο δράστης καταφέρει να αποκτήσει -εν τέλει- πρόσβαση στο περιεχόμενο της επικοινωνίας, δηλαδή εδώ καθιερώνεται ένα έγκλημα αφηρημένης διακινδύνευσης, ένα έγκλημα με το οποίο ποινικοποιείται συμπεριφορά η οποία μπορεί να μην προσβάλλει -εν τέλει- την επικοινωνία καθεαυτή. Αυτό είναι σύνηθες στη σχετική νομοθεσία, και μάλιστα εδώ η ποινή είναι δρακόντεια, απειλείται ποινή καθείρξεως, η πράξη είναι κακούργημα, σε αντίθεση με την πρόσβαση στις επιστολές όπου έχουμε τη χαμηλή ποινή της φυλακίσεως μέχρι ένα έτος.

Προστατεύεται επίσης ποινικά η προφορική επικοινωνία, με μια προσθήκη που έγινε στο άρθρο 370Α, που τιμωρεί την παραβίαση της τηλεφωνικής επικοινωνίας. Το να ακούει κάποιος με τεχνικά μέσα την προφορική επικοινωνία μεταξύ τρίτων, ή το να καταγράφει την επικοινωνία που ο ίδιος έχει με έναν άλλο εν αγνοία του τελευταίου, είναι αξιόποινη συμπεριφορά, τιμωρούμενη και αυτή σε βαθμό κακουργήματος. Με πρόσφατες διατάξεις του νόμου 4411/2016, που κύρωσε μία σύβαση του Συμβουλίου της Ευρώπης και μετέφερε στην ελληνική έννομη τάξη Οδηγία της ΕΕ, του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου, ποινικοποιούνται και αθέμιτες παραβιάσεις της ηλεκτρονικής επικοινωνίας, δηλαδή το λεγόμενο hacking, η πρόσβαση σε αποθηκευμένα στοιχεία πληροφοριακών συστημάτων και συστημάτων μετάδοσης επικοινωνιών, επομένως το να έχει κάποιος πρόσβαση σε ένα αποθηκευμένο e-mail αποτελεί αξιόποινη συμπεριφορά η οποία -βέβαια- τιμωρείται και με άλλες διατάξεις της ειδικής νομοθεσίας του νόμου 3471/2006. Τώρα, στο πλαίσιο του γνωστού φαινομένου της πολυνομίας, στο οποίο αναφέρθηκα ήδη, έχουμε και άλλη διάταξη, η οποία απειλεί ποινή πλημμελληματική, και όχι κακουργηματική. Προσετέθη, δε, με τον πρόσφατο Νόμο 4411/2006, και μια ακόμα τελευταία διάταξη, το άρθρο 370Δ του ποινικού Κώδικα, που τιμωρεί αυτή τη φορά σε βαθμό κακουργήματος την παρακολούθηση μη δημόσιων διαβιβάσεων που γίνονται με συστήματα επικοινωνιών, επομένως και εδώ η παρακολούθηση με τεχνικά μέσα -όπως απαιτείται στη διάταξη- μιας εικονοδιάσκεψης που γίνεται μεταξύ κάποιων προσώπων τιμωρείται και αυτή σε βαθμό κακουργήματος.

Αυτά για τις μορφές επικοινωνίας που προστατεύονται ποινικώς.

Να προχωρήσουμε γρήγορα, γιατί δεν έχει μείνει πολύς χρόνος, στις συγκρούσεις συμφερόντων που γεννώνται. Η ποινική προστασία του απορρήτου, της επικοινωνίας γενικότερα, είναι ένα συμφέρον, δημόσιο και ατομικό συμφέρον, γιατί αφορά τα υποκείμενα της επικοινωνίας. Συχνά όμως, πολύ συχνά θα έλεγε κανείς, το συμφέρον αυτό συγκρούεται -όπως ανέφερε και η κυρία Πρόεδρος- με άλλα συμφέροντα, που ευλόγως αξιώνουν προστασία. Τα συμφέροντα αυτά είναι το δικαίωμα δικαστικής ακρόασης

και προστασίας, επίσης το συμφέρον αποκάλυψης της δικαιοσύνης, τα συμφέροντα προστασίας της παιδικής ηλικίας και κάποια άλλα.

Ένα χαρακτηριστικό παράδειγμα που βρίσκεται στον πυρήνα της σχετικής προβληματικής. Ένας κατηγορούμενος για ένα σοβαρό κακούργημα είναι αθώος, δεν έχει άλλο τρόπο να αποδείξει την αθωότητά του παρά μόνο να παρέμβει σε μια τηλεφωνική επικοινωνία, να παγιδεύσει τη συνομιλία δύο μαρτύρων κατηγορίας, του μηνυτή του ενδεχομένως, και με την παγίδευση αυτή να αποκαλύψει ότι, εν τέλει, η μήνυση εις βάρος του είναι ψευδής, πρόκειται για μια ψευδομήνυση. Αναθέτει, λοιπόν, σε έναν ιδιώτη ερευνητή να προβεί σε αυτή την παγίδευση και, όντως, από τη συνομιλία που καταφέρνει να αποτυπώσει, προκύπτει η αθωότητά του για το σοβαρό κακούργημα που του αποδίδεται, λόγου χάριν για μια ανθρωποκτονία με πρόθεση, η οποία τιμωρείται με ισόβια κάθειρξη. Μπορεί να επικαλεστεί στο ποινικό δικαστήριο αυτή την αποτύπωση; Και, μιας και βρισκόμαστε ακόμα στον χώρο του ουσιαστικού ποινικού Δικαίου, αυτή η αξιόποινη κατ' αρχήν συμπεριφορά είναι -εν τέλει- αξιόποινη ή μήπως αίρεται ο άδικος χαρακτήρας της με βάση κάποιες γενικές αρχές, με βάση κάποιους λόγους άρσης του αδίκου που προβλέπονται στην ποινική μας νομοθεσία;

Αυτό το περιστατικό περιγράφεται με την κωδική ονομασία «αποδεικτική κατάσταση ανάγκης», είναι ένα πρόβλημα που έχει απασχολήσει επανειλημμένα τη διεθνή θεωρία και νομολογία, αλλά και την ελληνική νομολογία, καθόσον μέχρι και σήμερα εκδίδονται πολλές αποφάσεις, και του Αρείου Πάγου ακόμα, του Ακυρωτικού μας. Εν γένει, στη θεωρία και στη διεθνή νομολογία γίνεται δεκτό ότι, εφόσον συντρέχουν οι προϋποθέσεις της κατάστασης ανάγκης, εφόσον προσβάλλεται ένα ήσσονος αξίας αγαθό, εν προκειμένω το απόρρητο, χάριν διασφαλίσεως ενός μείζονος αξίας νόμιμου αγαθού, εν προκειμένω της αθωότητας ενός ανθρώπου ο οποίος κινδυνεύει να βρεθεί στη φυλακή με την ποινή της ισοβίου καθείρξεως, μπορούμε να πούμε ότι είναι δικαιολογημένη αυτή η παρέμβαση και η αποτύπωση και να μην την τιμωρήσουμε με ποινική κύρωση.

Ο Άρειος Πάγος δεν δέχεται την άποψη αυτή. Επειδή όμως φοβάται να κάνει και το βήμα προς μια απόλυτη θέση η οποία θα οδηγήσει -σε κάποιες ακραίες περιπτώσεις- σε ανεπιεική αποτελέσματα, έχει λάβει την εξής θέση, η οποία αποτυπώνεται και σε μια σχετικά πρόσφατη Απόφασή του, την Απόφαση 453/2006. Τι δέχεται ο Άρειος Πάγος; Δέχεται ότι, κατ' αρχήν, το απόρρητο είναι ένα έννομο αγαθό που έχει μεγαλύτερη αξία από την ελευθερία του κατηγορουμένου, την τιμή του και την περιουσία του, επομένως δεν μπορεί να αποτελέσει αντικείμενο στάθμισης, δεν μπορεί να θυσιαστεί το απόρρητο κατ' εφαρμογή του άρθρου 25 του ποινικού Κώδικα, το οποίο προϋποθέτει και επιτρέπει την προσβολή ενός ήσσονος αξίας εννόμου αγαθού χάριν της διαφυλάξεως ενός υπέρτερου αγαθού. Υπό αυτή την έννοια, απορρίπτει σε αφηρημένο επίπεδο την εφαρμογή του άρθρου 25 του ποινικού Κώδικα, που προβλέπει ως γενικό λόγο άρσης του αδίκου την κατάσταση ανάγκης. Παρά ταύτα, και εδώ υπάρχει μια προφανής αντίφαση στη θέση του Ακυρωτικού, δέχεται ότι αν γίνει μια αντίθετη στάθμιση από δικαστήριο της ουσίας -μα πώς να γίνει αντίθετη στάθμιση αν αυτή δεν είναι νομικά ορθή;…- δεν υπόκειται στον αναιρετικό έλεγχο του Αρείου Πάγου. Όπως αναφέρει χαρακτηριστικά η πρόσφατη αυτή

Απόφαση, σταθμίσεις από τα δικαστήρια της ουσίας που καταλήγουν στο αντίθετο αποτέλεσμα -έχει δεχτεί ο Άρειος Πάγος- δεν είναι δεκτικές αναιρετικού ελέγχου.

Απόλυτα συναφές είναι το πρόβλημα, ανεξαρτήτως από την άρση του αδίκου μιας πράξης ενός ιδιώτη, αν το ίδιο το ποινικό δικαστήριο μπορεί να αξιοποιήσει αποτυπώσεις επικοινωνιών που έχουν αποσπαστεί με αθέμιτο τρόπο, δηλαδή με κάποια από τις πράξεις του κεφαλαίου που εξετάζουμε, χωρίς ενδεχομένως να τις προσκομίσει ο κατηγορούμενος, αλλά ενδεχομένως μπορεί να τις έχει προσκομίσει και ο πολιτικός ενάγων για να αποδείξει ότι ένας κατηγορούμενος τέλεσε ένα σοβαρό έγκλημα εις βάρος του. Εδώ υπεισέρχεται η προβληματική της εμβέλειας και των συνεπειών που έχουν για το ποινικό Δίκαιο το άρθρο 19 παρ. 3 του Συντάγματος, που εισάγει -κακώς κατά την άποψή μου- μια απόλυτη απαγόρευση αξιοποίησης ενώπιον των δικαστηρίων αποτυπώσεων που έχουν αποκτηθεί με παραβίαση του άρθρου 19.1 και 9Α του Συντάγματος, καθώς και η διάταξη του άρθρου 177.2 του ποινικού Κώδικα, που και αυτή -κακώς- καθιερώνει μια απόλυτη απαγόρευση αξιοποίησης αποδεικτικών μέσων που έχουν αποκτηθεί με αξιόποινες συμπεριφορές. Εν τέλει, και εδώ ο Άρειος Πάγος δεν τηρεί απόλυτα τη συνταγματική διάταξη του άρθρου 19 παρ. 3 του Συντάγματος, δεχόμενος ότι σε ακραίες περιπτώσεις όπου διακυβεύεται η αθωότητα του κατηγορουμένου, ή ακόμα όταν είναι αναγκαία η αποκάλυψη ενός σοβαρού εγκλήματος, λόγου χάριν τιμωρουμένου με ισόβια κάθειρξη, μπορούν να αξιοποιηθούν στην ποινική διαδικασία και αποδεικτικά μέσα που έχουν αποκτηθεί με παραβίαση του 19.1. Είναι όντως εντυπωσιακό ότι το Ακυρωτικό δεν εφαρμόζει μια απόλυτη συνταγματική απαγόρευση η οποία τέθηκε σε ισχύ κατά την συνταγματική αναθεώρηση του 2001.

Αυτά ως προς τις ρυθμίσεις.

Θα ήθελα να τελειώσω με ορισμένα συμπεράσματα, στα οποία μπορώ να θεμελιώσω και κάποιες προτάσεις.

Νομίζω, αποτελεί αδήριτη ανάγκη να αναθεωρηθεί το πλαίσιο ποινικής προστασίας, να ενοποιηθούν οι διατάξεις σε ένα κωδικοποιημένο σύνολο το οποίο θα ενταχθεί στον ποινικό μας Κώδικα. Με τον τρόπο αυτό θα αποφευχθούν αντιφάσεις, θα αποφευχθούν αοριστίες ποινικών διατάξεων και θα περιγραφούν με την απαιτούμενη καθαρότητα οι τρόποι προσβολής των επικοινωνιών, δηλαδή η προσβολή των εξωτερικών στοιχείων της επικοινωνίας, η πρόσβαση στο περιεχόμενο της επικοινωνίας και οι λοιποί τρόποι.

Θα πρέπει να αναθεωρηθεί το πλαίσιο ποινών ούτως ώστε να μην έχουμε ακραίες αντιφάσεις μεταξύ πλημμελημάτων - κακουργημάτων, αλλά οι ποινές να διαβαθμιστούν ανάλογα με την απαξία της συμπεριφοράς που κολάζεται κάθε φορά.

Τέλος, θα πρέπει -νομίζω- να καταργηθεί η δικονομική διάταξη του άρθρου 177 παρ. 2 του Κώδικα Ποινικής Δικονομίας, που εισάγει απόλυτη απαγόρευση αξιοποίησης παρανόμων αποδεικτικών μέσων που έχουν κτηθεί με τις πράξεις που μας απασχολούν, ακόμα και υπέρ του κατηγορουμένου· φαίνεται να δέχεται ο Κώδικας Ποινικής Δικονομίας ότι μπορεί να καταδικαστεί κάποιος σε ισόβια κάθειρξη παρά το γεγονός ότι υπάρχει ένα παράνομο αποδεικτικό μέσο υπέρ του.

Με αυτές τις παρατηρήσεις κλείνω την εισήγησή μου.

Σας ευχαριστώ.

ΠΑΠΑΝΙΚΟΛΑΟΥ ΑΙ. - Συντονίστρια:

Σας ευχαριστούμε πολύ, κύριε Καθηγητά· τροφή για σκέψη, όχι εύπεπτη είναι η αλήθεια, με δύσκολες σταθμίσεις σε μείζονα διακυβεύματα, που σίγουρα δεν προσφέρονται για μονοσήμαντες λύσεις.

Καλώ στο βήμα τον ακροτελεύτιο ομιλητή της σημερινής ημερίδας, του οποίου η προστιθέμενη αξία συνίσταται στην ιδιότητά του. Ως νομικός σύμβουλος της ΑΔΑΕ, ο κύριος Ηλίας Θεοδωράτος με τις εξαιρετικές νομικές συνεργάτιδές του που στελεχώνουν τη Διεύθυνση Νομικών Υπηρεσιών της Αρχής, έχουν συμβάλει -και δεν υπερβάλλω- τα μέγιστα στη διαμόρφωση της νομολογίας της Αρχής, από ιδρύσεώς της, επί ζητημάτων που αφορούν το απόρρητο της επικοινωνίας.

Η εισήγηση του κυρίου Θεοδωράτου αφορά μια κλασσική αρχή του Δικαίου, την αρχή "ne bis in idem", ή -αλλιώς- «διακριτές ποινές για διακριτά έννομα αγαθά».

Παρακαλώ, κύριε Θεοδωράτε.

ΘΕΟΔΩΡΑΤΟΣ Η.:

Ευχαριστώ πολύ.

Κι εγώ με τη σειρά μου να ευχαριστήσω τους διοργανωτές και την ΑΔΑΕ, της οποίας έχω την τιμή να είμαι Νομικός Σύμβουλος, για τον ορισμό μου ως ομιλητή στο σημερινό συνέδριο, πρωτίστως διότι πιστεύω ότι η δημόσια διοίκηση υπάρχει για να ακούει, αλλά όσο σημαντικό είναι να ακούς εξίσου σημαντικό είναι -κατά την άποψή μου- να διατυπώνεις τις απόψεις σου και να τις θέτεις υπό τη βάσανο και της δημοσιότητας και της κριτικής.

Τελικά, το ότι μιλάω τελευταίος δεν είναι μόνο για λόγους αβρότητας απέναντι στους συναδέλφους μου οι οποίοι μας τίμησαν με την παρουσία τους στο σημερινό συνέδριό μας αλλά είναι ίσως και θεματολογικά επιτυχημένο, και αυτό γιατί μέχρι τώρα ακούσαμε ότι υπάρχουν δεδομένα κίνησης, δεδομένα θέσης, στοιχεία της επικοινωνίας που είναι και προσωπικά δεδομένα. Το ζήτημα αυτό θέτει ένα ζήτημα ως προς την ύπαρξη στην εθνική έννομη τάξη περισσοτέρων Αρχών που ασχολούνται με την προστασία διαφορετικών εννόμων αγαθών; Αυτό ακριβώς είναι το θέμα της ομιλίας μου.

Η ομιλία μου αφορά την εφαρμογή της αρχής "non bis in idem" στις Ανεξάρτητες Αρχές, και πιο ειδικά στις συνταγματικώς Ανεξάρτητες Αρχές, επ' ευκαιρία μιας πρόσφατης Απόφασης του Συμβουλίου Επικρατείας, της υπ' αριθμ. 3473/2017 Απόφασης της 7μελους σύνθεσης του 4ου τμήματος του Συμβουλίου της Επικρατείας. Για τους μη μυημένους στα νομικά, που μάλλον είστε και οι περισσότεροι, να εξηγήσω ότι η αρχή "non bis in idem" σημαίνει ότι δεν επιβάλλονται δύο ποινές για την ίδια αιτία. Προέκυψε, κατ' αρχάς, από το ποινικό δίκαιο, ως θεμελιώδη αρχή του ποινικού δικαίου, η οποία απαγορεύει να διωχθεί ή να καταδικαστεί κάποιος για μια παράβαση για την οποία είτε αθωώθηκε είτε καταδικάστηκε με αμετάκλητη απόφαση ποινικού δικαστηρίου.

Το Δικαστήριο του Στρασβούργου και το Δικαστήριο της ΕΕ αναγνώρισαν την αρχή αυτή ως θεμελιώδη -επίσης- αρχή του κοινοτικού Δικαίου. Μάλιστα, η αρχή αυτή κατοχυρώθηκε και νομοθετικά, στο άρθρο 4 παρ. 1 του 7ου πρωτοκόλλου της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), που κυρώθηκε με τον Νόμο 1705/87, αλλά και στο άρθρο 50 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Το ΕΔΔΑ αναγνώρισε ότι η αρχή αυτή -η αρχή "non bis in idem"- δεν εφαρμόζεται μόνο

επί ποινικών αλλά και επί διοικητικών κυρώσεων, εφόσον στοιχειοθετείται και ποινικό αδίκημα, λαμβάνοντας μάλιστα υπ' όψιν όχι τη συγκεκριμένη ποινή που επιβάλλεται στη συγκεκριμένη υπόθεση, αλλά τη μέγιστη δυνατή ποινή που προβλέπει ο νομοθέτης. Το ΔΕΕ, το Δικαστήριο της ΕΕ, δέχεται ότι δεν απαγορεύεται η σώρευση περισσοτέρων της μιας ποινής, όταν αυτό αποβλέπει στην προστασία των οικονομικών συμφερόντων της Ένωσης.

Εν όψει αυτού του νομικού πλαισίου, εξεδόθη η Απόφαση 3474/2017 του 4ου τμήματος του Συμβουλίου της Επικρατείας. Τι είχε να κρίνει στην Απόφαση αυτή το Συμβούλιο της Επικρατείας; Τη νομιμότητα ενός διοικητικού προστίμου που επέβαλε η ΑΔΑΕ εις βάρος ενός τηλεοπτικού σταθμού για την αναμετάδοση παρανόμως μιας υποκλαπείσας τηλεφωνικής συνομιλίας χωρίς τη συναίνεση των μερών και εν γνώσει της προέλευσής της. Ο τηλεοπτικός σταθμός προέβαλε, ουσιαστικά, τρία επιχειρήματα. Το πρώτο επιχείρημα είναι ότι ως τέτοιος δεν υπάγεται στην κυρωτική αρμοδιότητα της ΑΔΑΕ, διότι δεν ελέγχεται από αυτήν. Ο δεύτερος ισχυρισμός είναι ότι ο τηλεοπτικός σταθμός και ο δημοσιογράφος δεν εμπλέκονται στην καταγραφή της παρανόμως αποκτηθείσας τηλεφωνικής συνομιλίας. Ως τρίτο, το ότι για το ζήτημα αυτό, για την παράβαση αυτή, έχει ήδη επιβληθεί ποινή, διοικητικό πρόστιμο από το Εθνικό Συμβούλιο Ραδιοτηλεόρασης· μάλιστα, το πρόστιμο αυτό έχει προσβληθεί δικαστικά ενώπιον του ΣτΕ, έχει απορριφθεί η αίτηση ακυρώσεως του τηλεοπτικού σταθμού και, κατά συνέπεια, το διοικητικό πρόστιμο που επέβαλε το Εθνικό Συμβούλιο Ραδιοτηλεόρασης έχει καταστεί οριστικό.

Το Συμβούλιο της Επικρατείας, επί των τριών αυτών ισχυρισμών, έκρινε τα ακόλουθα:

Πρώτον, δεν επηρεάζει το γεγονός -ακόμα και αληθές υποτιθέμενο- ότι ο τηλεοπτικός σταθμός δεν εμπλέκεται στην καταγραφή της παρανόμως αποκτηθείσας - υποκλαπείσας τηλεφωνικής συνομιλίας. Αρκεί μόνο το γεγονός ότι το αναμετάδωσε, ότι αυτό ήταν σε γνώση του και χωρίς τη συναίνεση των επικοινωνούντων μερών.

Δεύτερον, και πολύ σημαντικό, το ότι η κυρωτική αρμοδιότητα της ΑΔΑΕ, η δυνατότητά της να επιβάλλει διοικητικά πρόστιμα κατά τον ιδρυτικό της νόμο, ασκείται όχι μόνο έναντι των δημοσίων υπηρεσιών, δηλαδή των φορέων και οργανισμών που απασχολούνται με την επικοινωνία και την αλληλογραφία, αλλά και έναντι των ιδιωτών, όπως είναι ο συγκεκριμένος τηλεοπτικός σταθμός, και τούτο διότι το άρθρο 19 του Συντάγματος κατοχυρώνει απολύτως την προστασία και, πρωτίστως, την ελευθερία -θα έλεγα κι εγώ συγκλίνοντας προς την άποψη του κυρίου Μαρκόπουλου- της επικοινωνίας έναντι πάντων, άρα έναντι και των ιδιωτών, και του συγκεκριμένου τηλεοπτικού σταθμού.

Το τρίτο το οποίο είπε η Απόφαση αυτή του Συμβουλίου της Επικρατείας είναι πως είναι δυνατή η σώρευση δύο διοικητικών κυρώσεων που επιβάλλονται από διαφορετικά διοικητικά Όργανα και διαφορετικές Αρχές στον ίδιο παραβάτη και για τα ίδια πραγματικά περιστατικά, εφόσον τούτο αποβλέπει στην προστασία διαφορετικών σημαντικών εννόμων αγαθών, και τούτο διότι εάν εμείς κάναμε αυτή την εξαίρεση στην αρχή "non bis in idem" τότε θα υπήρχαν συνταγματικές διατάξεις -και αυτό είναι σημαντικό που είπε το Συμβούλιο της Επικρατείας- που θα έμεναν ανεφάρμοστες, παρ' ότι αυτές οι συνταγματικές διατάξεις θέλησαν να υπάρχουν διακριτές Ανεξάρτητες Αρχές, που προστατεύουν διακριτά και σημαντικά έννομα αγαθά.

Στην Απόφαση αυτή, βεβαίως, υπήρξε και μειοψηφία. Η μειοψηφία, όμως, ήταν ενός μόνο μέλους του Δικαστηρίου, και τολμώ να πω ότι θα μπορούσα να μην τη συμμερίζομαι. Και αυτό γιατί, σε αντιπαραβολή με τις συνταγματικές διατάξεις, με τις προαναφερόμενες συνταγματικές διατάξεις, έθεσε σε μείζονα μοίρα την ανάγκη εφαρμογής της αρχής "non bis in idem", λέγοντας ότι, αφού κάθε Ανεξάρτητη Αρχή έχει διαφορετική νομοθεσία, σε αυτή την περίπτωση θα εφαρμόζονται διαφορετικές νομοθεσίες, θα προστατεύονται διαφορετικά έννομα αγαθά και η αρχή "non bis in idem" θα μένει ανεφάρμοστη.

Να δούμε όμως -και αυτό προέχει- ποιες είναι οι προεκτάσεις, ίσως ίσως οι συνέπειες αυτής της συγκεκριμένης πρόσφατης δικαστικής Απόφασης του Συμβουλίου της Επικρατείας.

Θα μπορούσε, για παράδειγμα, να υπάρξει συγχώνευση συνταγματικώς κατοχυρωμένων Ανεξαρτήτων Αρχών με την αιτιολογία της ταυτότητας των πραγματικών περιστατικών, της ταυτότητας του παραβάτη και της παράβασης, όταν ισχύουν διαφορετικές συνταγματικές διατάξεις που προστατεύουν ξεχωριστά σημαντικά δικαιώματα, όπως είπε το Συμβούλιο της Επικρατείας, και -άραεφαρμόζεται η ειδικότητα του σκοπού της κάθε συνταγματικής διάταξης;

Δεύτερο ζήτημα… Απαιτείται παραπομπή από τη μία Αρχή στην άλλη όσον αφορά την άσκηση της κυρωτικής της αρμοδιότητας, όπως προβλέπει -για παράδειγμα- ο Νόμος 3674/2008, για να αποφύγουμε να επιβάλλεται η ίδια ποινή για τα ίδια πραγματικά περιστατικά στον ίδιο παραβάτη;

Τρίτο ζήτημα… Επιτρέπεται και είναι σωστό η αρμοδιότητα μιας συνταγματικώς κατοχυρωμένης Ανεξάρτητης Αρχής, και μάλιστα μέρος αυτής της αρμοδιότητας, να υπόκειται στον έλεγχο του Διοικητικού Εφετείου, όταν οι αντίστοιχες κυρωτικές αρμοδιότητες των υπολοίπων συνταγματικώς κατοχυρωμένων Ανεξαρτήτων Αρχών, όπως της Αρχής Προστασίας Προσωπικών Δεδομένων και του Εθνικού Συμβουλίου Ραδιοτηλεοράσεως, για παράδειγμα, υπόκεινται στον έλεγχο του Συμβουλίου της Επικρατείας;

Και στα τρία αυτά ερωτήματα θεωρώ ότι η απάντηση -μετά την Απόφαση αυτή του Συμβουλίου της Επικρατείας- πρέπει να είναι αρνητική. Για παράδειγμα, επειδή τίθεται μεγάλο ζήτημα ως προς την ταύτιση αρμοδιοτήτων ανάμεσα στην Αρχή Προστασίας Προσωπικών Δεδομένων και στην ΑΔΑΕ λόγω της εγγύτητας του περιεχομένου των προστατευομένων εννόμων αγαθών, όταν τα προσωπικά δεδομένα διέρχονται μέσω του διαύλου επικοινωνίας, το πρώτιστο αγαθό είναι η προστασία του απορρήτου της επικοινωνίας, δεν είναι η προστασία των προσωπικών δεδομένων, γιατί αν δεν υπήρχε παραβίαση του απορρήτου της επικοινωνίας δεν θα υπήρχε και παραβίαση των προσωπικών δεδομένων - η κοινή λογική το λέει αυτό. Θα έλεγα επίσης ότι, ακόμα και αν υπάρχει εγγύτητα περιεχομένου εννόμων αγαθών που προστατεύονται, το Συμβούλιο της Επικρατείας -καθαρά, πια- είπε ότι επιτρέπεται η σώρευση διοικητικών κυρώσεων όταν αυτές προβλέπονται/επιβάλλονται από διαφορετικές συνταγματικές Αρχές, που προβλέπονται και θεσμοθετούνται από το Σύνταγμα, και προστατεύονται διακριτά έννομα αγαθά.

Η σημαντικότερη συμβολή της Απόφασης αυτής είναι ότι οι συνταγματικές διατάξεις πρέπει να ερμηνεύονται σύμφωνα με τους όρους και περιορισμούς του Δικαίου της ΕΕ και της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου, θα πρέπει όμως να γίνεται αποδε-

κτή η ιδιαιτερότητά τους λόγω της ειδικότητας του σκοπού και της διαφορετικότητας των ενόμων αγαθών που προστατεύονται.

Κλείνοντας, θα μου επιτρέψετε να διαβάσω μια άποψη της οποίας έλαβα γνώση σε μια θεσσαλική εφημερίδα επιστρέφοντας από ένα ταξίδι από τη Θεσσαλία προς την Αθήνα, άποψη η οποία έλεγε:

«Η τεχνολογία είναι πολύτιμη επειδή έχει δώσει τη δυνατότητα στον οποιονδήποτε καθημερινό άνθρωπο, με μια απλή σύνδεση στο ίντερνετ και ένα-δύο λογαριασμούς στα social media, να κατανοήσει και μόνος του ότι ελπίδα δεν υπάρχει για την ανθρωπότητα.»

Υπογραφή, «Μαργαρίτες Μάντολες».

Σε αυτές τις «Μαργαρίτες Μάντολες», λοιπόν, θα ήθελα να απαντήσω ότι αυτή ακριβώς την άποψη καλούνται οι Ανεξάρτητες Αρχές και να αντιμετωπίσουν και να διαψεύσουν, όμως αυτό επιτυγχάνεται όταν η κυρωτική τους αρμοδιότητα ασκείται αποτελεσματικά και χωρίς στερεότυπα. Προϋπόθεση αυτού, βεβαίως, είναι οι Ανεξάρτητες Αρχές να στελεχώνονται και να εξοπλίζονται επαρκώς, όχι ευκαιριακά και όχι ανάλογα με τις πολιτικές συγκυρίες.

Ευχαριστώ πολύ.

ΠΑΠΑΝΙΚΟΛΑΟΥ ΑΙ. - Συντονίστρια:

Ευχαριστούμε πολύ, κύριε Θεωδωράτε.

Δανειζόμαστε το πολύ ενδιαφέρον φιλοσοφικό επιμύθιο του τέλους ως επιμύθιο της ημερίδας, αφού προηγουμένως απευθυνόμενη σε εσάς, ακούσω αν υπάρχουν κάποια λίγα ερωτήματα που επιθυμείτε να θέσετε στους ομιλητές - εισηγητές. Υπάρχει κάτι από πλευράς ακροατηρίου;... Κανείς, νομίζω ότι τους καλύψαμε όλους. Ωραία, αυτό είναι πολύ ευχάριστο.

Με τη σειρά μου θα ήθελα να ευχαριστήσω πάρα πολύ τους εξαιρετικούς και έγκυρους εισηγητές, τόσο της δεύτερης συνεδρίας όσο και εν συνόλω, των σημερινών εργασιών.

Θα ήθελα επίσης να ευχαριστήσω κυρίως όλους εσάς που είχατε την υπομονή, από το ξεκίνημα της ημερίδας μέχρι αυτή την ώρα, να παραμείνετε στις θέσεις προσηλωμένοι και να καλέσω στη συνέχεια τον Πρόεδρο της Αρχής, αν θέλει να κλείσει τις εργασίες της σημερινής ημερίδας. Πέρα από την αυτονόητη τελετουργία της συνέχειας, που μετά τόσο επαρκή τροφοδοσία της σκέψης, συνίσταται προφανώς σε πρόσκληση για ελαφρύ γεύμα, στο οποίο σας περιμένουμε με μεγάλη χαρά-, να αναγγείλω και μία έκπληξη της τελευταίας στιγμής. Οι υπηρεσίες της Βουλής, τις οποίες θερμά ευχαριστούμε τόσο για τη φιλοξενία της σημερινής εκδήλωσης, όσο επίσης και για τη συνολική τους υποστήριξη, είχαν την ευγενή πρόνοια να εξασφαλίσουν για μας τη δυνατότητα να επισκεφτούμε από 15.00 μέχρι 15.30 την αίθουσα «Ελευθερίου Βενιζέλου». Η αίθουσα αυτή βρίσκεται ακριβώς έξω από την αίθουσα της Γερουσίας, όπου βρισκόμαστε τώρα και φιλοξενεί τεκμήρια της διαχρονικής ελληνικής ιστορίας, με ιδιαίτερες αναφορές σε κυβερνήτες της Ελλάδας, Βενιζέλος, Καποδίστριας κ.α. Έχει ενδιαφέρον, και ακόμα περισσότερο ενδιαφέρον με δεδομένο ότι θα υπάρχει ξενάγηση στο διάστημα από 15.00 μέχρι 15.30.

Νομίζω ότι είμαστε ακριβέστατοι ως προς τον χρόνο, κύριε Πρόεδρε, άρα υπάρχει χρόνος και για το γεύμα και για την ξενάγηση.

Σας ευχαριστούμε πολύ όλους.

Λήξη Β΄ Ενότητας

Η ημερίδα έκλεισε με τις ευχαριστίες του Προέδρου της ΑΔΑΕ προς τους συμμετέχοντες.

ΟΛΟΚΛΗΡΩΣΗ ΕΡΓΑΣΙΩΝ ΗΜΕΡΙΔΑΣ

Ομιλητές – Σελίδες Αναφοράς

ΒΟΥΤΣΗΣ Ν.:	13
ΓΙΑΝΝΟΠΟΥΛΟΣ Γ.:	69
ΖΑΜΠΙΡΑΣ Χ.:	3, 12, 15, 16, 17, 19, 20, 22, 25
ΘΕΟΔΩΡΑΤΟΣ Η.:	80
ΚΑΛΛΟΝΙΑΤΗΣ Χ.:	38
ΚΑΨΑΛΗΣ Χ.:	35
ΚΟΝΔΥΛΗΣ Β.:	44
ΜΑΓΛΑΡΑΣ Λ.:	16, 26
ΜΑΡΙΝΟΣ Λ.:	31
ΜΑΡΚΟΠΟΥΛΟΣ Ν.:	65
ΜΑΣΣΕΛΟΣ Κ.:	19
ΜΕΝΟΥΔΑΚΟΣ Κ.:	18
ΜΙΣΑΗΛΙΔΗΣ Α.:	62
ΠΑΠΑΝΙΚΟΛΑΟΥ ΑΙ. - Συντονίστρια:	58, 62, 64, 69, 75, 80, 83
ΠΑΠΑΠΡΟΔΡΟΜΟΥ Γ.:	22
ΣΑΚΚΑΣ Μ. - Συντονιστής:	15, 26, 31, 34, 38, 44, 49, 53, 57
ΣΤΑΜΟΥΛΗΣ Π.:	58
ΤΑΦΥΛΛΗΣ Ι.:	21
ΤΡΑΚΑΔΑΣ Π.:	49
ΤΡΙΑΝΤΑΦΥΛΛΟΥ Γ.:	75
ΨΑΛΛΙΔΑΣ Ι.:	53

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
Ιερού Λόχου 3, 151 24 Μαρούσι Τηλ. 210 6387601-2, Fax. 210 6387666