Αξιότιμοι Κύριοι και Κυρίες,

Σας ευχαριστούμε για τη σημερινή σας παρουσία και είναι μεγάλη χαρά που σας φιλοξενούμε στο κτήριο του Εθνικού Κέντρου Δημόσιας Διοίκησης και Αυτοδιοίκησης.

Η ανταπόκριση στο κάλεσμα μας ξεπέρασε και τις πιο αισιόδοξες προσδοκίες. Η εκδήλωση ενδιαφέροντος υπήρξε υπερδιπλάσια του μέγιστου αριθμού ανθρώπων που μπορούμε να υποδεχτούμε. Λυπόμαστε που δεν είμαστε σε θέση να ικανοποιήσουμε όλα τα αιτήματα.

Θα θέλαμε να παραθέσουμε **μερικά στοιχεία**, διότι η σημερινή Ημερίδα αποτελεί επιστέγασμα όλων των προηγούμενων συστηματικών προσπαθειών του ΙΝ.ΕΠ. Το Ινστιτούτο Επιμόρφωσης (ΙΝ.ΕΠ.) πραγματοποίησε στις **11 Δεκεμβρίου 2017** την πρώτη δράση ενημέρωσης και ευαισθητοποίησης, με αντικείμενο τον Γενικό Κανονισμό, έξι περίπου μήνες πριν αυτός τεθεί σε ισχύ. Έκτοτε το ΙΝ.ΕΠ. σχεδίασε, σε συνεργασία, με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, το **επιμορφωτικό πρόγραμμα** «Γενικός Κανονισμός Προστασίας Δεδομένων: οι υποχρεώσεις της Δημόσιας Διοίκησης». Το πρόγραμμα έχει πραγματοποιηθεί **48 φορές**, αρχής γενομένης από τον **Μάρτιο του 2018**. Στις σχετικές δράσεις έχουν εκπαιδευτεί **1674** δημόσιοι λειτουργοί, από το σύνολο του φάσματος της Δημόσιας Διοίκησης.

Η προσπάθεια για την καλλιέργεια κουλτούρας ασφαλούς διαχείρισης δεδομένων πρέπει να είναι συνεχής και σωρευτική ως προς τα αποτελέσματα της. Πρέπει επιπλέον να εναρμονίζεται με τις εξελίξεις στο πεδίο της ασφαλείας πληροφοριακών συστημάτων και Κυβερνοασφάλειας.

Σε αυτό το πλαίσιο, πριν λίγες ημέρες πραγματοποιήθηκε στον ίδιο χώρο Ημερίδα για την Κυβερνοασφάλεια. **Κυβερνοασφάλεια** και **προστασία δεδομένων** είναι πεδία **αλληλένδετα** και διατρέχονται από κοινούς άξονες.

Αρκεί να δούμε τη σχετική ευρωπαϊκή και εθνική νομοθεσία σε σχέση με τα δύο αυτά θεματικά πεδία για να διακρίνουμε προφανείς ομοιότητες. Και στις δύο περιπτώσεις:

- ορίζεται ένα φυσικό πρόσωπο ως σημείο αναφοράς του Οργανισμού
- η ασφάλεια αποτελεί μέρος του σχεδιασμού
- η κοινοποίηση περιστατικών παραβίασης οφείλει να γίνεται εντός συγκεκριμένου χρονικού παραθύρου
- ενθαρρύνεται η χρήση διεθνών προτύπων και προδιαγραφών

Αυτό που δεν είναι προφανές σε μια πρώτη ανάγνωση είναι το **κοινό μοντέλο διαχείρισης** για την προστασία δεδομένων και την ασφάλεια πληροφοριακών συστημάτων.

Η θέσπιση του Υπευθύνου Προστασίας Δεδομένων, όπως και του Υπευθύνου Ασφάλειας Πληροφοριών Δικτύων και Πληροφοριών, δείχνει ότι το βάρος πλέον πέφτει στους ίδιους τους οργανισμούς. Δεν υφίσταται πλέον ένα κεντρικό σημείο διαχείρισης, που αποφασίζει συγκεντρωτικά και οι οργανισμοί απλά υλοποιούν.

Το νέο κοινό μοντέλο διαχείρισης είναι **αποκεντρωμένο**, με ένα εποπτικό κέντρο συντονισμού και αναφοράς για την παροχή κατευθυντήριων γραμμών. Η εφαρμογή αυτών των γραμμών βαρύνει τον ίδιο τον φορέα, ο οποίος οφείλει να βρει, με τρόπο αναλογικό, τα ιδιαίτερα εκείνα μέτρα που προσιδιάζουν στην φυσιογνωμία του και εκπληρώνουν το πνεύμα των νομοθετικών διατάξεων. Οι όποιες παραλείψεις εφαρμογής των διατάξεων επιφέρουν ιδιαίτερα αυστηρά πρόστιμα και κυρώσεις για τον φορέα. Στο αποκεντρωμένο αυτό μοντέλο:

- η ανάδειξη και διάχυση καλών πρακτικών
- η ανταλλαγή τεχνογνωσίας
- ο δημόσιος διάλογος
- η ανάπτυξη επιμορφωτικών δράσεων

καθίστανται επιβεβλημένες ενέργειες.

Σκοπός είναι η ανάπτυξη **δικτύων ανθρώπων** και **δικτύων απρόσκοπτων ροών πληροφορίας** για μια ολιστική διαχείριση σχετικά με την προσαρμογή των φορέων στο σύγχρονο τοπίο της προστασίας δεδομένων και της ασφάλειας πληροφοριακών συστημάτων.

Το **κοινό νήμα** που διατρέχει τα πεδία της προστασίας δεδομένων και της Κυβερνοασφάλειας είναι **η προτεραιοποιημένη διαχείριση του κινδύνου** και των **απειλών**.

- Ποιες προτεραιότητες πρέπει να θέσει ένας οργανισμός, ώστε να προφυλάξει, με τον πιο αποτελεσματικό τρόπο, τους πόρους τους, χωρίς να παρακωλυθεί η επιχειρησιακή και παραγωγική λειτουργία του;
- Ποιους από τους πόρους του οφείλει να προστατεύσει περισσότερο ο οργανισμός σε σχέση με τους υπόλοιπους;

- Ποιο είναι τελικά το **αποδεκτό επίπεδο κινδύνου** στο οποίο μπορεί εκτεθεί ένα οργανισμός;

Ο προσδιορισμός του αποδεκτού επιπέδου κινδύνου είναι μέρος της γνώσης ενός οργανισμού. Αφορά το εσωτερικό του και τις ιδιαίτερες επιχειρησιακές διαδικασίες του. Γι' αυτό και δεν μπορεί να υποδειχθεί από ένα εξωτερικό παρατηρητή. Οι ίδιοι οι άνθρωποι του οργανισμού καλούνται να υποδείξουν και να εφαρμόσουν λύσεις. Εξ ου και η **μετατόπιση υποδείγματος** από την κεντρική διαχείριση σε ένα αποκεντρωμένο μοντέλο διαχείρισης, με την παρουσία ενός εποπτικού κέντρου.

Τι σημαίνουν τα παραπάνω για τον κόσμο της Δημόσιας Διοίκησης; Σίγουρα μια σειρά υποχρεώσεις και καθήκοντα, αλλά ταυτόχρονα και ένα **παράθυρο ευκαιρίας** για μια περισσότερο ποιοτική λειτουργία του οργανισμού. **Στοιχεία ποιότητας** ενός οργανισμού είναι:

- η καταγραφή των δεδομένων
- η τήρηση αρχείων πράξεων επεξεργασίας δεδομένων
- η γνώση των νομιμοποιητικών βάσεων των πράξεων αυτών
- η κατάρτιση κωδίκων δεοντολογίας
- η διενέργεια εκτίμησης αντίκτυπου
- η άμεση και προσήκουσα διαχείριση περιστατικού παραβίασης

Ομοίως:

- η καταλογο-γράφηση των υπολογιστικών πόρων,
- η κατάρτιση διαγραμμάτων δικτύων,
- η δημιουργία και συντήρηση αρχείων καταγραφής (log events) και αρχείων δικτυακής κίνησης,
- η ανάπτυξη συστημάτων ενδείξεων παραβίασης,

ενισχύουν την υγεία ενός οργανισμού. Οι προκλήσεις, επομένως, για τη Δημόσια Διοίκηση, η οποία έρχεται αντιμέτωπη με καινοφανείς θεσμικές διατάξεις, που απορρέουν από την ευρωπαϊκή και εθνική νομοθεσία, είναι πολλαπλές και κοινής υφής.

Εν κατακλείδι, η επιτυχής προσαρμογή στις απαιτήσεις του Γενικού Κανονισμού θα συμβάλει τα μέγιστα στη επιτυχή εφαρμογή των προβλέψεων της Οδηγίας NIS περί ασφάλειας δικτύων και πληροφοριών και το αντίστροφο.

Πρόκειται για σχέση **αμφίδρομη**, στην οποία η Δημοσία Διοίκηση θα πρέπει να επενδύσει τις προσπάθειες της, με ιδιαίτερη έμφαση και στον τομέα της επιμόρφωσης. Σε αυτή την προσπάθεια, συμβάλει καθημερινά το ΙΝ.ΕΠ.

Σας ευχαριστούμε πολύ για τη σημερινή παρουσία σας εδώ.

Με εκτίμηση,

ΓΕΩΡΓΙΟΣ ΚΑΤΣΙΚΑΤΣΟΣ,

Ε.Ε.Π., ΙΝ.ΕΠ.