Χαιρετισμός του Προϊστάμενου Διεύθυνσης Διασφάλισης Υποδομών, Απορρήτου Υπηρεσιών και Εφαρμογών Διαδικτύου στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε), κ. Ιωάννη Ψαλλίδα.

5ο Ετήσιο Συνέδριο «ICT Security World»

"Ψηφιακός Μετασχηματισμός και ΚυβερνοΑσφάλεια εν μέσω Cloud, Mobile Apps, 5G και Artificial Intelligence"

Κυρίες και Κύριοι.

Ευχαριστώντας για την πρόσκληση προς την ΑΔΑΕ και μεταφέροντας τους χαιρετισμούς του Προέδρου μας, κ. Χρήστου Ράμμου, επιθυμώ να σας συγχαρώ για αυτό το συνέδριο που αφορά σε ένα επίκαιρο και σημαντικό θέμα, αυτό του "Ψηφιακού Μετασχηματισμού και της Κυβερνοασφάλειας."

Θα προσπαθήσω να εκθέσω τις σκέψεις μου που πηγάζουν από την 10ετη θητεία μου σε εταιρίες τηλεπικοινωνιών του ιδιωτικού τομέα ως μηχανικού και Product Manager, όσο και στην 11ετή θητεία μου στην ΑΔΑΕ, την Συνταγματικά κατοχυρωμένη Ανεξάρτητη Αρχή που σκοπό έχει την Διασφάλιση του Απορρήτου των Επικοινωνιών των Ελλήνων Πολιτών. Ως γνωστό η ΑΔΑΕ εποπτεύει και ελέγχει παρόχους τηλεπικοινωνιακών υπηρεσιών στο κοινό και λόγο του αντικειμένου τους είναι πρωτοπόρες στο θέμα του Ψηφιακού Μετασχηματισμού.

Ψηφιακός Μετασχηματισμός είναι ένα ευρύ πεδίο που στην ουσία αναφέρεται στην ολοένα αυξανόμενη υιοθέτηση της τεχνολογίας από φορείς τόσο του ιδιωτικού τομέα όσο και του δημόσιου τομέα για

- την βελτίωση της αλληλοεπίδρασης τους με τους πελάτες ή Πολίτες αντίστοιχα (οπουδήποτε και οποτεδήποτε) και
- για την υιοθέτηση συνεχώς βελτιστοποιημένων εσωτερικών διαδικασιών για την επίτευξη της καλύτερης απόδοσης τους.

Για την πραγματοποίηση του Ψηφιακού Μετασχηματισμού είναι απαραίτητο να εντοπιστούν

- Οι ανάγκες και τα προβλήματα των πελατών ή των Πολιτών.

- Οι απαραίτητες πληροφορίες που πρέπει να ληφθούν υπόψη .
- Οι απαραίτητες οργανικές δομές που εμπλέκονται στην αλυσίδα παραγωγής του προϊόντος ή της υπηρεσίας που προσφέρεται προς το κοινό.

Τα σημαντικότερα χαρακτηριστικά των στελεχών που πρέπει να ηγούνται τέτοιων προσπαθειών Ψηφιακού Μετασχηματισμού είναι

- Να έχουν πολύ καλή αίσθηση του τι θέλει ο αποδέκτης της υπηρεσίας ή του προϊόντος τώρα αλλά και την δυνατότητα να προβλέπουν τις μελλοντικές ανάγκες.
- Να έχουν την δυνατότητα να καταλαβαίνουν τόσο το επιχειρηματικό /επιχειρησιακό σκέλος όσο και την τεχνολογία που μπορεί να χρησιμοποιηθεί για την προσφορά των προϊόντων / υπηρεσιών .

Η τεχνολογίες σήμερα η οποίες επιτρέπουν αυτόν τον μετασχηματισμό είναι

- **Data Science** που επιτρέπει την συλλογή και επεξεργασία της πληροφορίας για την δημιουργία πολύτιμου business Intelligence**.**
- **AI και Machine Learning** οι οποίες είναι στον πυρήνα της εξατομικευμένης εξυπηρέτησης και είναι απαραίτητες για την βελτιστοποίηση της εμπειρίας του πελάτη, ωθώντας την πληροφορία σε πράξη.
- **Αυτοματοποίηση** η οποία ενισχύει την αποδοτικότητα της εταιρίας ή του οργανισμού που την υιοθετεί.
- **Το Cloud,** κυρίως ως προς τις υποδομές**,** που παρέχει την δυνατότητα της δυναμικής προσαρμογής των υπολογιστικών πόρων με τις εκάστοτε επιχειρησιακές ανάγκες.
- **5G δίκτυα** που θα επιτρέπουν γρήγορές ταχύτητες διασύνδεσης και μικρούς χρόνους απόκρισης μεταξύ οποιονδήποτε 5G συσκευών.

Από τα παραπάνω μπορεί κάποιος να καταλάβει ότι ο Ψηφιακός Μετασχηματισμός παρέχει ένα ευρύ φάσμα δυνατοτήτων και ευκαιριών τόσο για φορείς που μπαίνουν στην διαδικασία αυτού του μετασχηματισμού όσο και στους αποδέκτες των προσφερόμενων υπηρεσιών /προϊόντων.

Το γεγονός ότι υιοθετούνται όλο και περισσότερο οι τεχνολογίες που προαναφέρθηκαν παραπάνω, το *πεδίο δράσης* των κακόβουλων αντίστοιχα

μεγαλώνει και μάλιστα ασύμμετρα. Υπάρχουν δυνητικά περισσότερα σημεία εισόδου, δυσκολεύοντας τους επαγγελματίες κυβερνοασφάλειας να γνωρίζουν και να καλύπτουν όλα τα κενά. Και όταν παραβιαστεί ένα σύστημα, τότε είναι σχετικά εύκολη η ψηφιακή περιήγηση των κακόβουλων σε όλα τα υπόλοιπα συστήματα του φορέα.

Παλαιότερα οι εταιρίες βασιζόταν σε ψηφιακές υποδομές εγκατεστημένες σε ιδιόκτητους χώρους με πλήρη έλεγχο του κύκλου ζωής τόσο των υποδομών όσο και των εφαρμογών που χρησιμοποιούσαν. Αυτό ίσως ισχύει και σήμερα για κάποιες μεγάλες εταιρίες οι οποίες διαχειρίζονται εξαιρετικά ευαίσθητες πληροφορίες. Αρκετές όμως είναι και οι εταιρίες οι οποίες κάνουν χρήση εφαρμογών ή Servers οι οποίες φιλοξενούνται σε υποδομές τρίτων στο Cloud. Οι δυνητικές επιπτώσεις σε περίπτωση παραβίασης είναι μεγαλύτερες δεδομένου ότι οι Πληροφορίες και τα συστήματα στα οποία βρίσκονται είναι διασυνδεδεμένα διαδικτυακά και μπορούν είτε να υποκλαπούν, είτε να αλλοιωθούν, είτε να καθίστανται μη διαθέσιμα, με τις οποιεσδήποτε επιπτώσεις στους φορείς που παραβιάζονται (οικονομικές, φήμης, νομικές κλπ). Αυτό ισχύει ακόμα περισσότερο όταν μιλούμε για κρίσιμες υποδομές που χρησιμοποιούνται για την εύρυθμη λειτουργία της κοινωνίας, όπως, νοσοκομεία, τράπεζες, ενεργειακά δίκτυα, μέσα μεταφοράς, τηλεπικοινωνίες κλπ.

Οι τεχνολογικές εξελίξεις είναι ραγδαίες και παρόλο που αυτό παρέχει πολλά οφέλη δημιουργεί προβλήματα στην έγκαιρη επικαιροποίηση μέτρων ασφάλειας που υιοθετούνται από τους φορείς, επιτρέποντας την δημιουργία κενών ασφάλειας εκεί που πρόσφατα δεν υπήρχαν.

Οι ίδιες τεχνολογίες και εργαλεία που χρησιμοποιούνται σήμερα από τις εταιρίες υιοθετούνται και από κακόβουλους, οι οποίοι δημιουργούν σύνθετους τρόπους προκειμένου να παρεισφρήσουν απαρατήρητοι στα συστήματα των θυμάτων τους. Η πρόσβαση σε AI και Machine Learning πλατφόρμες είναι εκτεταμένη και το κόστος για τον σχεδιασμό και ανάπτυξη κακόβουλων εργαλείων έχει μειωθεί δραστικά. Δεν μπορεί να θεωρηθεί επιστημονική φαντασία το σενάριο όπου εργαλεία βασισμένα σε AI θα χρησιμοποιούνται εναντίων AI εργαλείων κυβερνοασφάλειας.

Σε επίπεδο Ευρωπαϊκής Ένωσης τα τελευταία χρόνια έχει δοθεί έμφαση στην Ενιαία Ψηφιακή Αγορά με επενδύσεις στις απαραίτητες υποδομές, σε έρευνα, στην τόνωση του ηλεκτρονικού εμπορίου, στην ενημέρωση του κοινού, αλλά και με παρεμβάσεις σε θέματα κυβερνοασφάλειας, και αναπροσαρμογές του νομικού πλαισίου.

Ειδικότερα για την κυβερνοασφάλεια, οι πιο σημαντικές δράσεις επιγραμματικά είναι

- **Οδηγία 2016/1148/ΕΕ** - **Network & Information Security Directive** (**NIS**) (με ενσωμάτωση στο ελληνικό δίκαιο τον Δεκέμβριο του 2018 με τον ν 4577/2018)
- **Κανονισμός (ΕΕ) 2016/679 -** (**GDPR**) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων (με ενσωμάτωση στο ελληνικό δίκαιο τον Αύγουστο του 2019 με τον νόμο 4624/2019)
- **Κανονισμός (ΕΕ) 2019/881**- **Ενδυνάμωση του Οργανισμού Της Ευρωπαϊκής Ένωσης Για Την Κυβερνοασφάλεια-ENISA** και την πρόβλεψη **δημιουργίας πλατφόρμας εθελοντικής πιστοποίησης προϊόντων πληροφορικής και τηλεπικοινωνιών**.
- **Οδηγία 2018/1972** - **(ECC code**) για τη **θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών.**
- **Ειδικότερα σε ότι αφορά την ΑΔΑΕ** προτάθηκε από την Ευρωπαϊκή Επιτροπή τον **Ιανουάριο 2017** και από το Ευρωπαϊκό Κοινοβούλιο τον Οκτώβριο του ίδιου έτους, σχέδιο για τον νέο κανονισμό **ePrivacy,** το οποίο σε επίπεδο Συμβούλιου της ΕΕ μελετάται από τους εκπροσώπους των κυβερνήσεων των 28 κρατών μελών, χωρίς να έχουν ακόμη ολοκληρωθεί οι διαβουλεύσεις.

Για την περίοδο 2021-2027 η ευρωπαϊκή επιτροπή έχει προτείνει χρηματοδότηση 9.2 δις Ευρώ με στόχο την τόνωση των επενδύσεων σε τομείς όπως supercomputing, artificial intelligence, Ψηφιακές Δημόσιες Υπηρεσίες, την ανάπτυξη Ψηφιακών Δεξιοτήτων, και την κυβερνοασφάλεια με το μερίδιο χρηματοδότησης της τελευταίας να ανέρχεται στα 2 δις Ευρώ που αντιστοιχεί στο 21,7% της συνολικής χρηματοδότησης.

Από την εμπειρία της εποπτείας και των ελέγχων που έχει κάνει η ΑΔΑΕ τα τελευταία 15 χρόνια σε παρόχους τηλεπικοινωνιών, κάποια πράγματα τα οποία θα πρέπει να θεωρούνται δεδομένα για την αντιμετώπιση θεμάτων κυβερνοασφάλειας και να εφαρμόζονται από τους ψηφιακά μετασχηματιζόμενους φορείς είναι

- Οι αποφάσεις για τον σχεδιασμό και υλοποίηση σχεδίου κυβερνοασφάλειας να είναι με βάση ένα πλαίσιο διαχείρισης ρίσκου.
- Ο κύκλος ζωής των υιοθετημένων ψηφιακών συστημάτων να εμπλέκει την κυβερνοασφάλεια σε όλες τις φάσεις, από την σχεδιασμό μέχρι την απόσυρση τους.
- Όσον το δυνατό περισσότερη αυτοματοποίηση διεργασιών που αφορούν την κυβερνοασφάλεια με σκοπό την επικαιροποιημένη παρακολούθηση, εντοπισμό και αντίδραση σε περίπτωση σχετικών περιστατικών ασφάλειας.
- Να γίνονται στοχευόμενοι τακτικοί εσωτερικοί έλεγχοι προκειμένου να εντοπίζονται κενά στην εφαρμογή τεχνικών, διαδικαστικών και οργανωτικών μέτρων ασφάλειας και να δοκιμάζονται τα σχέδια επιχειρησιακής συνέχειας.
- Να υπάρχει διαρκείς ενημέρωση και εκπαίδευση σε θέματα ασφάλειας τόσο σε εξειδικευμένο προσωπικό επωμισμένο με την κυβερνοάμυνα του φορέα, όσο και του υπολοίπου προσωπικού.

Οι παραπάνω γενικές αρχές σε συνδυασμό με την εποπτεία και έλεγχο που έχει ασκήσει η ΑΔΑΕ όλα αυτά τα χρόνια πιστεύουμε ότι τουλάχιστον για τους μεγάλους τηλεπικοινωνιακούς παρόχους έχουν συμβάλει στο να είναι πολύ πιο ώριμοι στην διαχείριση θεμάτων κυβερνοασφάλειας και έχουν αποκτήσει κουλτούρα που θα τους επιτρέψει να αντιμετωπίσουν τις προκλήσεις που έρχονται στο άμεσο μέλλον.

Σας ευχαριστώ πολύ και εύχομαι καλή επιτυχία στο ενδιαφέρον αυτό Συνέδριο.