

**ΣΥΝΕΔΡΙΟ «Γυναίκες στην κυβερνοασφάλεια:
Προκλήσεις, Εμπειρίες και Σχέδια για το Μέλλον»**

1η Ιουνίου 2023, Lemon Park, Λευκωσία

Κατά πρώτον θα ήθελα να ευχαριστήσω τον φίλο Επίτροπο Επικοινωνιών για τη πρόσκληση να απευθύνω χαιρετισμό στην στοχευμένη και επίκαιρη σημερινή ημερίδα.

Από μία απλή έρευνα στο διαδίκτυο, εύκολα διαπιστώνει κάποιος ότι υπάρχει άπλετη βιβλιογραφία για το θέμα των γυναικών στην κυβερνοασφάλεια. Κάποια από αυτά τα επιστημονικά άρθρα, φαίνονται να συγκλίνουν στα εξής συμπεράσματα. Το φύλο δεν φαίνεται να είναι καθοριστικός παράγοντας στην διάπραξη κυβερνό-αδικημάτων, οι γυναίκες φαίνεται να είναι πιο ευάλωτες σε κάποια είδη κυβερνό-αδικημάτων και ότι, σε κάποιες χώρες οι γυναίκες έχουν ψηλότερη πιθανότητα να είναι θύματα κυβερνό-επιθέσεων, παρά σε άλλες χώρες.

Σε ένα άρθρο μάλιστα που δημοσιεύτηκε το 2018, η συγγραφέας Winifred R. Poster εισηγείται ότι, ο τομέας της κυβερνό-ασφάλειας χρειάζεται περισσότερες γυναίκες καθώς, όπως εξηγεί, η διασφάλιση της ψηφιακής ασφάλειας απαιτεί δεξιότητες και εμπειρίες που ξεφεύγουν των αρρενωπών στερεότυπων του χάκερ ή του στρατιώτη.

Αναντίλεκτα βιώνουμε και θα συνεχίσουμε να βιώνουμε κυβερνοεπιθέσεις. Το ζητούμενο είναι, οι οργανισμοί, είτε υπέχουν ρόλο του υπεύθυνου επεξεργασίας, είτε ρόλο εκτελούντος, να είναι σε θέση να αποδείξουν ότι έλαβαν όλα εκείνα τα τεχνικά και οργανωτικά μέτρα τα οποία αποτελούν όσο το δυνατό αδιαπέραστο τοίχος, το οποίο να αποτρέπει την όποια διαρροή και την όποια παραβίαση προσωπικών δεδομένων, με όλες τις αναρίθμητες επιπτώσεις που μπορεί να έχει αυτό.

Νομικό πλαίσιο το οποίο έχουν υποχρέωση να εφαρμόζουν οι οργανισμοί προκειμένου να επιτύχουν ασφάλεια δεδομένων υπάρχει και είναι ισχυρό. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ) και ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (Νόμος 125(Ι)/2018).

Η παρακολούθηση της συμμόρφωσης με το ως άνω πλαίσιο ελέγχεται από το Γραφείο μου τόσο κατά την διερεύνηση παραπόνων, ή και αυτεπαγγέλτως.

Για την επιλογή των κατάλληλων τεχνικών και οργανωτικών μέτρων που πρέπει να τηρούνται ούτως ώστε να διασφαλίζεται κατάλληλο επίπεδο ασφάλειας των προσωπικών δεδομένων από τυχαία ή παράνομη πρόσβαση, αλλοίωση ή καταστροφή των δεδομένων, θα πρέπει να λαμβάνονται υπόψιν:

- οι τελευταίες τεχνολογικές εξελίξεις,
- η φύση των δεδομένων (π.χ. οικονομικά δεδομένα, ιατρικά δεδομένα),
- η σοβαρότητα και πιθανότητα επέλευσης των κινδύνων.

Απαραίτητη επίσης η συμμόρφωση με την πρόνοια για την διενέργεια Εκτίμησης Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ) στις περιπτώσεις όπου μια επεξεργασία,

ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η πρόνοια αυτή συνδράμει στην διαχείριση των κινδύνων και την πλήρωση της υποχρέωσης λογοδοσίας. Στις περιπτώσεις όπου η ΕΑΠΔ υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου, ο υπεύθυνος επεξεργασίας έχει υποχρέωση διαβούλευσης με το Γραφείο μου για λήψη πρόσθετων μέτρων, εκεί και όπου ενδείκνυται.

Τέλος εργαλείο που αποδεικνύει διάθεση συμμόρφωσης είναι η επιβαλλόμενη Γνωστοποίηση περιστατικών παραβίασης στο Γραφείο μου εντός 72 ωρών, καθώς επίσης και η σχετική ανακοίνωση της παραβίασης στα επηρεαζόμενα πρόσωπα στις περιπτώσεις όπου το περιστατικό ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες τους. Ενδεικτικά αναφέρω ότι κατά το 2023 και μέχρι σήμερα έχουν γνωστοποιηθεί στο Γραφείο μου 46 συμβάντα ενώ κατά το 2022 είχαν Γνωστοποιηθεί 67 και κατά το 2021 108, κάποια εκ των οποίων έχουν καταλήξει στην επιβολή διοικητικών κυρώσεων συμπεριλαμβανομένων και προστίμων. Κάποια από αυτά αφορούσαν σε περιστατικά κυβερνοεπιθέσεων. Κατά το 2022 είχα επιβάλει

- στο Υπουργείο Άμυνας διοικητικό πρόστιμο ύψους €5.000 σχετικά με επίθεση σε διαδικτυακό σύστημα του (και διοικητικό πρόστιμο ύψους €7.500 στην εταιρεία εκτελούντα την επεξεργασία για το σύστημα αυτό).
- σε εταιρεία διοικητικό πρόστιμο ύψους €6.000 σχετικά με επίθεση σε ένα από τα συστήματα της (και διοικητικό πρόστιμο €5.000 στην εταιρεία εκτελούντα την επεξεργασία για το σύστημα αυτό).
- σε εταιρεία διοικητικό πρόστιμο ύψους €9.000 για επίθεση κατά την οποία ζητήθηκαν και λύτρα.

Θα πρέπει βεβαίως να αναφέρω ότι στους οργανισμούς που θεωρούνται ως κρίσιμες υποδομές υπάρχει η συνεργασία και με την Αρχή Ψηφιακής Ασφάλειας.

Οι προκλήσεις για το Γραφείο μου και για μένα προσωπικά πάρα πολλές και πολυεπίπεδες, ειδικά τώρα με την τιμητική εκλογή μου στην Αντιπροεδρία του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.