

# Μήνυμα Προσκεκλημένου Εκδότη

## Κυβερνοασφάλεια: προκλήσεις και προοπτικές στην ψηφιακή εποχή



**Ελευθέριος Αθουσάκης**  
**Μέντορας ΑΛΛΗΛΟΝ**  
**Cyber Security Specialist**  
[Eleftherios Athousakis | LinkedIn](#)

Σε συνέχεια του αφιερώματος στην κυβερνοασφάλεια στο ένθετο αυτού του τεύχους θεωρήθηκε σκόπιμο ν' αγγίξουμε θέματα που έχουν να κάνουν με την κυβερνοασφάλεια και την ηγεσία, ένα σημείο που συχνά παραβλέπεται αλλά παραμένει από τα πιο απαραίτητα, την σημασία της εκπαίδευσης στον τομέα καθώς και τις απαραίτητες ενέργειες για να μπορέσουμε να μειώσουμε το χάσμα ικανοτήτων και γνώσεων στο χώρο. Μαθαίνουμε τι είναι τα "Deerfake" αλλά και πώς οι "Πιλότοι της κυβερνοασφάλειας" μας βοηθούν να κερδίσουμε την καθημερινή μάχη για να εξασφαλίσουμε την ασφάλεια των δεδομένων μας.

Κάτω από αυτή την ομπρέλα έχουμε συμπεριλάβει πέντε άρθρα με σκοπό την ενημέρωσή σας. Του Δρ Ιωάννη Ηλιάδη, του κυρίου Δημήτρη Τακετζή, της κυρίας Σπυριδούλας Κλειδί, του κυρίου Αθανασίου Πανδή και του υπογράφοντα.

Το άρθρο του Δρ Ι. Ηλιάδη μας εισάγει στον σύγχρονο ψηφιακό κόσμο, όπου η αποτελεσματική επικοινωνία των ζητημάτων κυβερνοασφάλειας στην εταιρική ηγεσία είναι κρίσιμη. Το άρθρο αναλύει τρεις προσεγγίσεις: την παρουσίαση της κυβερνοασφάλειας ως μόδα (που μπορεί να αποξενώσει), τη χρήση τακτικών φόβου (FUD) (που μπορεί να δημιουργήσει άγχος), και την προτεινόμενη μέθοδο παρουσίασης της κυβερνοασφάλειας ως κέντρου επενδύσεων.

Στο άρθρο του ο κύριος Δ. Τακετζής αναλύει την εξέλιξη της εκπαίδευσης στην κυβερνοασφάλεια, από τις παραδοσιακές μεθόδους στη σύγχρονη εποχή της Τεχνητής Νοημοσύνης (TN). Το άρθρο τονίζει τα οφέλη της TN στην εκπαίδευση κυβερνοασφάλειας, όπως η βελτιωμένη συμμετοχή των εκπαιδευομένων και η προσαρμογή στις σύγχρονες απειλές, ενώ παράλληλα επισημαίνει τους πιθανούς κινδύνους και ηθικά ζητήματα

που προκύπτουν από τη χρήση της TN.

Στη συνέχεια η κυρία Σ. Κλειδί στο άρθρο της εξετάζει την άνοδο της τεχνολογίας Deerfake και τις επιπτώσεις της στην κοινωνία. Αναλύει τους κινδύνους που ενέχει αυτή η τεχνολογία, όπως η διάβρωση της εμπιστοσύνης, η πολιτική χειραγώγηση, η διάδοση ψευδών ειδήσεων και οι απειλές για την ασφάλεια. Παρουσιάζει παραδείγματα πραγματικών επιθέσεων Deerfake και προτείνει στρατηγικές για την προστασία οργανισμών από αυτές τις απειλές.

Στο άρθρο του ο κύριος Α. Πανδής συγκρίνει τους Incident Responders στην κυβερνοασφάλεια με τους πιλότους μαχητικών αεροσκαφών, τονίζοντας τη σημασία της ταχείας αντίδρασης και της εκτεταμένης προετοιμασίας. Οι Incident Responders πρέπει να έχουν άριστη γνώση των συστημάτων, να αντιδρούν γρήγορα και να διαχειρίζονται το άγνωστο.

Τέλος στο άρθρο του ο υπογράφοντας, αναλύει το χάσμα δεξιοτήτων στην κυβερνοασφάλεια και προτείνει λύσεις για τη μείωσή του. Εξετάζει τις αιτίες του προβλήματος, αναλύει τον ρόλο των πανεπιστημίων, των κυβερνήσεων και των οργανισμών στην αντιμετώπιση του ζητήματος, προτείνοντας στρατηγικές όπως η ενημέρωση προγραμμάτων σπουδών, η χρηματοδότηση εκπαιδευτικών προγραμμάτων και η επένδυση στην εκπαίδευση των υπαλλήλων. Παρέχει επίσης συμβουλές για νεοεισερχόμενους στον τομέα, τονίζοντας τη σημασία της πρακτικής εξάσκησης, της συνεχούς μάθησης και της δικτύωσης.

Και μην ξεχνάτε η κυβερνοασφάλεια θεωρείται πάντα υπερβολική μέχρι να γίνει αντιληπτό ότι δεν ήταν αρκετή!