

# Μήνυμα Προσκεκλημένου Εκδότη

## Κυβερνοασφάλεια: προκλήσεις και προοπτικές στην ψηφιακή Εποχή



**Ελευθέριος Αθουσάκης**  
**Μέντορας ΑΛΛΗΛΟΝ (Τομέα Κυβερνοασφάλειας)**  
**Ειδικός σε θέματα Κυβερνοασφάλειας**  
[Eleftherios A. | LinkedIn](#)

Η κυβερνοασφάλεια έχει αναδειχθεί σε κρίσιμο ζήτημα στη σύγχρονη ψηφιακή εποχή, καθώς ο κόσμος μας γίνεται ολοένα και πιο διασυνδεδεμένος. Με την εκθετική αύξηση των ψηφιακών συσκευών, την ευρεία χρήση του διαδικτύου και την αυξανόμενη εξάρτηση από ψηφιακά συστήματα σε όλους τους τομείς της ζωής μας, η ανάγκη για προστασία από κυβερνοαπειλές έχει καταστεί επιτακτική. Οι κυβερνοεπιθέσεις μπορούν να έχουν καταστροφικές συνέπειες, από την κλοπή προσωπικών δεδομένων και οικονομικές απώλειες μέχρι τη διατάραξη κρίσιμων υποδομών και την απειλή της εθνικής ασφάλειας. Συνεπώς, η κυβερνοασφάλεια δεν αποτελεί πλέον μόνο τεχνικό ζήτημα, αλλά έχει εξελιχθεί σε θεμελιώδη πυλώνα για τη διαφύλαξη της ψηφιακής μας ακεραιότητας και ευημερίας. Στο ένθετο αυτού του τεύχους θεωρήσαμε αναγκαίο να αναφερθούμε στον τομέα της κυβερνοασφάλειας καθώς και ο Οκτώβρης έχει θεσπιστεί ως μήνας Κυβερνοασφάλειας από την ΕΕ.

Κάτω από αυτή την ομπρέλα έχουμε συμπεριλάβει τέσσερα (4) άρθρα με σκοπό την ενημέρωσή σας.

1. Του κυρίου Π. Σούλου
2. Του κυρίου Δ. Γεωργίου
3. Του κυρίου Κ. Νασόπουλου και του υπογράφοντα.

Το άρθρο του κυρίου Π. Σούλου μας εισάγει στην έννοια της «Κυβερνοϋγιεινής» και αναδεικνύει τη σημασία της εφαρμογής της στην καθημερινή μας ζωή. Ο συγγραφέας τονίζει πώς η υιοθέτηση πρακτικών κυβερνοϋγιεινής μπορεί να θωρακίσει τόσο εμάς όσο και τον περίγυρό μας απέναντι στους πολυάριθμους κινδύνους του ψηφιακού κόσμου ώστε να μας καταστήσει πιο ασφαλείς.

Στο άρθρο του ο κύριος Δ. Γεωργίου αναλύει τις κυβερνοεπιθέσεις σε επιχειρήσεις, εστιάζοντας στην πρόληψη, αντιμετώπιση και διερεύνηση. Τονίζει τη σημασία της κυβερνοασφάλειας ως στρατηγικό ζήτημα και παρουσιάζει βασικές πρακτικές πρόληψης,

όπως η ανάπτυξη στρατηγικής ασφαλείας, τακτικές αξιολογήσεις κινδύνου, πολιτικές πρόσβασης, προστασία δεδομένων και εκπαίδευση προσωπικού. Αναφέρεται στην αντιμετώπιση περιστατικών μέσω σχεδίων απόκρισης και συνεργασίας με ειδικούς. Τέλος, υπογραμμίζει τη σημασία της ψηφιακής εγκληματολογίας στη διερεύνηση επιθέσεων και την ενίσχυση της συνολικής ασφάλειας των επιχειρήσεων.

Σε επαφή με το προηγούμενο άρθρο ο κύριος Κ. Νασόπουλος αναλύει τη σημασία και τις εφαρμογές της Ψηφιακής Εγκληματολογίας και Αντιμετώπισης Περιστατικών (DFIR) στην καθημερινότητα. Τονίζει τον ρόλο του DFIR στην προστασία προσωπικών δεδομένων, την ασφάλεια στο διαδίκτυο και την εξιχνίαση εγκλημάτων. Επισημαίνει τη σημασία του στον επιχειρηματικό τομέα για την προστασία εταιρικών δεδομένων και τη συμμόρφωση με κανονισμούς. Αναφέρεται στη χρήση του DFIR για την ασφάλεια έξυπνων συσκευών και την ανάκτηση δεδομένων. Τέλος, παρουσιάζει τις προκλήσεις που αντιμετωπίζει ο τομέας, όπως οι εξελισσόμενες απειλές, και τις μελλοντικές τάσεις, συμπεριλαμβανομένης της ενσωμάτωσης τεχνητής νοημοσύνης και μηχανικής μάθησης στις τεχνικές DFIR.

Τέλος στο άρθρο του υπογράφοντα θα βρείτε περιστατικά που συνέβησαν το τελευταίο χρονικό διάστημα σε διαφορετικούς τομείς και ηπείρους. Θα διαπιστώσετε ότι δεν υπάρχουν σύνορα για το κυβερνοέγκλημα και ότι οι τρόποι να προφυλαχτούμε είναι οι ίδιοι και επαναλαμβάνονται σ' όλα τα άρθρα και απ' όλους τους ειδικούς είτε αφορούν την προσωπική σας ζωή είτε την επαγγελματική σας δραστηριότητα.

Ακολουθήστε τις οδηγίες των επαγγελματιών κυβερνοασφάλειας και μείνετε όσο το δυνατόν πιο ασφαλείς.