ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ
ΚΑΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ
ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΕΥΡΩΠΑΪΚΟΣ ΚΑΝΟΝΙΣΜΟΣ
(GENERAL DATA PROTECTION REGULATION, GDPR)

ΔΕΥΤΕΡΑ

20/11 **17:30**

Επιμελητήριο Έβρου

ΒΑΣΙΚΟΙ ΕΙΣΗΓΗΤΕΣ:
ΣΦΑΚΙΑΝΑΚΗΣ ΕΜΜΑΝΟΥΗΛ
ΜΑΚΡΥΠΟΥΛΙΑΣ ΙΩΑΝΝΗΣ

CSIi Cyber Security International Institute

ΔΙ.Β.Β.Α.Π. ΔΙΚΤΥΟ ΒΙΟΤΕΧΝΙΩΝ ΚΑΙ ΒΙΟΜΗΧΑΝΙΩΝ ΑΚΡΙΤΙΚΩΝ ΠΕΡΙΟΧΩΝ

ΣΥΝΔΕΣΜΟΣ ΒΙΟΤΕΧΝΙΩΝ ΒΙΟΜΗΧΑΝΙΩΝ ΕΒΡΟΥ

ΕΠΙΜΕΛΗΤΗΡΙΟ ΕΒΡΟΥ

Prisma Electronics

Ο ΝΕΟΣ ΕΥΡΩΠΑΪΚΟΣ ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR - 2016/679) της ΕΕ αποτελεί τη μεγαλύτερη αλλαγή στην νομοθεσία περί προστασίας των δεδομένων τα τελευταία 20 χρόνια.

Ο Ευρωπαϊκός Κανονισμός 2016/679 (General Data Protection Regulation, GDPR) ψηφίστηκε στις 27.04.2016 και τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο, χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας και καταργώντας την υφιστάμενη νομοθεσία. Ο νέος κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των επιχειρήσεων, ενώ το μέγεθος των προβλεπόμενων προστίμων τον τοποθετεί πολύ υψηλά στην ατζέντα της ανώτατης διοίκησης.

ΠΟΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΑΦΟΡΑ;

Όλες τις ιδιωτικές και δημόσιες επιχειρήσεις, καθώς και τις κρατικές αρχές που με οποιοδήποτε τρόπο διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, πελατών των πελατών τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων.

Ως εκ τούτου, ο GDPR αφορά πρακτικά όλες τις επιχειρήσεις, εντός και εκτός Ευρωπαϊκής Ένωσης, εφόσον έχουν την έδρα τους στην Ε.Ε. ή τα δεδομένα αφορούν Ευρωπαίους πολίτες.

ΟΙ ΒΑΣΙΚΕΣ ΑΛΛΑΓΕΣ ΠΟΥ ΕΠΙΦΕΡΕΙ Ο ΚΑΝΟΝΙΣΜΟΣ

1. Υψηλά πρόστιμα: Ο νέος κανονισμός εξουσιοδοτεί τις εκάστοτε Αρχές Προστασίας Προσωπικών Δεδομένων στην Ευρώπη, να επιβάλουν για σοβαρές παραβάσεις πρόστιμα σε ύψος έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών τους ή 20 εκατομμύρια ευρώ, ανάλογα πάντα με το ποιο είναι το μεγαλύτερο

2. Αυξημένα δικαιώματα των υποκειμένων των δεδομένων: Το υποκείμενο των δεδομένων έχει πλέον αυξημένα δικαιώματα που περιλαμβάνουν: δικαίωμα στη λήθη, δικαίωμα περιορισμού της επεξεργασίας, δικαίωμα διόρθωσης, δικαίωμα στη φορητότητα, υποχρέωση γνωστοποίησης σε περίπτωση παραβίασης.

3. Ενίσχυση της παιδικής προστασίας: Ενίσχυση της προστασίας των ανηλίκων που χαρακτηρίζονται ως “ευάλωτα φυσικά πρόσωπα” με αυστηρότερους κανόνες και υποχρεώσεις για τον υπεύθυνο επεξεργασίας καθώς και αυστηρότερο πλαίσιο για τη συναίνεση των υποκειμένων των δεδομένων.

4. Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα: Ο υπεύθυνος επεξεργασίας οφείλει, σε περίπτωση παραβιάσεως, να ενημερώσει εντός 72 ωρών τόσο το ίδιο το υποκείμενο όσο και την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

5. Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (Data protection by design and by default): Ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

6. Αυστηροποίηση των προϋποθέσεων της παροχής συγκατάθεσης των υποκειμένων των δεδομένων: Όταν η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου πρέπει πλέον να είναι ρητή και εν πλήρει επιγνώσει αυτού και επιπλέον παρέχεται σε αυτό η δυνατότητα ανάκλησης της.

7. Εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων: Στις περιπτώσεις που η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας οφείλει να διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

8. Αρχεία των δραστηριοτήτων επεξεργασίας: Κάθε υπεύθυνος επεξεργασίας οφείλει να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος.

9. Ορισμός Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer): Ορίζεται η θέση του Υπευθύνου Προστασίας Δεδομένων (DPO), η οποία σε πολλές περιπτώσεις καθίσταται υποχρεωτική.

ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΕΝΕΡΓΕΙΕΣ ΓΙΑ ΤΗΝ ΜΕΙΩΣΗ ΤΩΝ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΩΝ

Δεδομένου του χρόνου, των πόρων και των οικονομικών κινήτρων, ένας κακόβουλος χρήστης μπορεί να παραβιάσει σχεδόν οποιοδήποτε σύστημα. Όλες οι διαδικασίες ασφαλείας και οι διαθέσιμες τεχνολογίες δεν μπορούν να εγγυηθούν ότι όλα τα συστήματα είναι απολύτως ασφαλή. Η επιτυχία καθεμιάς από αυτές τις τεχνολογίες εξαρτάται από έναν αριθμό μεταβλητών, όπως:

- Την εμπειρία και την τεχνογνωσία των ανθρώπων που είναι υπεύθυνοι για την διαμόρφωση, την παρακολούθηση και την διατήρηση των τεχνολογιών.
- Την ικανότητα να αναβαθμιστούν τα συστήματα γρήγορα και αποτελεσματικά.
- Τη συνεχή ενημέρωση και συμβουλή από ειδικούς για νέα κενά ασφαλείας.
- Τη συμμόρφωση των εταιριών σύμφωνα με τα διεθνή πρότυπα ασφαλείας.
- Την ενημέρωση και την εκπαίδευση του προσωπικού για επιθέσεις κοινωνικής μηχανικής.
- Τη διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των ψηφιακών δεδομένων.

ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΠΕΙΛΕΣ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Οι κίνδυνοι που έχουν προκύψει τα τελευταία χρόνια στον κυβερνοχώρο προέρχονται κυρίως από το οργανωμένο έγκλημα, τους υπάλληλους ή τους συνεργάτες της ίδιας της επιχείρησης που έχουν πρόσβαση στα συστήματά της, τους ακτιβιστές του κυβερνοχώρου, τους τρομοκράτες του κυβερνοχώρου, αλλά και μεγάλα κράτη. Τα κίνητρά τους είναι ποικίλα, με κάποιους να ενδιαφέρονται για οικονομικό κέρδος και άλλους να παρακινούνται από εμπορικά, ιδεολογικά, πολιτικά ή γεωπολιτικά συμφέροντα.

ΣΥΝΕΠΕΙΕΣ ΜΙΑΣ ΕΠΙΤΥΧΗΜΕΝΗΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗΣ

Οι επιπτώσεις ενός περιστατικού παραβίασης ασφάλειας διαφέρουν ανάλογα με το είδος και το βαθμό επιτυχίας μιας επίθεσης. Αυτές μπορεί να περιλαμβάνουν:

1. Πλήγμα ως προς την εμπιστοσύνη προς την επιχείρηση
2. Υποβάθμιση της εμπορικής της επωνυμίας
3. Μείωση των εσόδων
4. Ποινικές διώξεις
5. Απώλεια πνευματικής ιδιοκτησίας
6. Πρόστιμο από τις ρυθμιστικές Αρχές
7. Κόστος ανάκαμψης της λειτουργίας τους
8. Κόστος των τεχνικών ερευνών
9. Κόστος εισαγωγής επιπρόσθετων μέτρων ασφάλειας

ΠΡΟΛΗΨΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΥΒΕΡΝΟΑΠΕΙΛΩΝ

Για την ενίσχυση των τεχνολογιών ασφαλείας, την προστασία της πληροφοριακής υποδομής και των ευαίσθητων δεδομένων μιας εταιρίας πρέπει να γίνει αποτίμηση κινδύνου των επιχειρησιακών αγαθών, αξιολόγηση των ευπαθειών, και ευαισθητοποίηση για θέματα ασφάλειας. Με αυτόν τον τρόπο, ελέγχονται τα πληροφοριακά συστήματα και το δίκτυο με τους ίδιους τρόπους όπως ακολουθεί και ο επιτιθέμενος.

Τέτοιου είδους προληπτικές αξιολογήσεις ασφάλειας σε ένα πληροφοριακό σύστημα μπορούν να αποκαλύψουν πιθανά ζητήματα τα οποία μπορούν να αντιμετωπιστούν πριν τα εκμεταλλευτεί ο κακόβουλος χρήστης. Ο Ευρωπαϊκός Κανονισμός 2016/679 (General Data Protection Regulation, GDPR), βοηθάει την πρόληψη των κυβερνοαπειλών προστατεύοντας τις εταιρείες και κατ' επέκταση τα δεδομένα των πελατών.

ΠΡΟΓΡΑΜΜΑ

18:00 – 18:15 **Χριστόδουλος Τοψίδης** **Χρήστος Γιορδαμλής**	Ο Νέος Ευρωπαϊκός Κανονισμός για την προστασία των Δεδομένων.
18:15 – 18:45 **Εισαγωγή στο GDPR** Εισηγητές: **Εμμανουήλ Σφακιανάκης** **Ιωάννης Μακρυπούλιας**	Ποιες αλλαγές φέρνει ο νέος Ευρωπαϊκός Κανονισμός για τα προσωπικά δεδομένα; Ποιες εταιρείες αφορά και ποιες οι νέες υποχρεώσεις που προκύπτουν; Πόσο σημαντικό είναι μία επιχείρηση να λάβει τα απαραίτητα μέτρα και ποιες οι πιθανές συνέπειες μη συμμόρφωσης; Ο ρόλος της κυβερνοασφάλειας με πραγματικά παραδείγματα.
18:45 – 19:15 **GDPR: Νομική προσέγγιση** Εισηγητής: **Ρόντου Καλλιόπη**	Νομικά ζητήματα που ανακύπτουν από την εφαρμογή του Νέου Ευρωπαϊκού Κανονισμού GDPR: Ανάλυση και κατανόηση νομοθετικού πλαισίου, κανονιστική συμμόρφωση, νέοι ρόλοι, ευθύνη και κυρώσεις.
19:15 – 19:30	Σύντομο διάλειμμα
19:30 – 20:00 **Cyber Security** Εισηγητές: **Παπαντωνίου Παναγιώτης** **Βιέννας Αχιλλέας**	Τι είναι η ασφάλεια στον κυβερνοχώρο; Ποιος είναι ο στόχος της ασφάλειας των πληροφοριών μέσα σε έναν οργανισμό; Ποια είναι η διαφορά μεταξύ της απειλής, ευπάθειας και κινδύνου; Ποια είναι τα κρίσιμα σημεία τα οποία πρέπει να επικεντρωθούν οι επιχειρήσεις; Ποιες είναι οι επιπτώσεις ενός παραβιασμένου πληροφοριακού συστήματος για την επιχείρηση; Ποιες είναι και που ωφελούν οι αξιολογήσεις ασφάλειας; Ο ρόλος της κρυπτογραφίας, αυθεντικοποίησης και εξουσιοδότησης στα δεδομένα και στις επικοινωνίες.
20:00 – 20:20 **Best ICT Practices** Εισηγητής: **Καραγεωργίου Δημοσθένης**	Πληροφοριακά συστήματα επιχειρήσεων και καλές πρακτικές σήμερα. Προσωπικά δεδομένα πελατών – συνεργατών και ο έλεγχος πρόσβασης επί αυτών. Η διαχείριση του Περιεχόμενου και πρακτικές κατηγοριοποίησης αυτού. Παραδείγματα εφαρμογών και προτεινόμενες πρακτικές των κατασκευαστών λογισμικού.
20:20 – 20:30	Συζήτηση – Ερωτήσεις

ΟΜΙΛΗΤΕΣ

ΣΦΑΚΙΑΝΑΚΗΣ ΕΜΜΑΝΟΥΗΛ

Ο Αντιστράτηγος ε.α. Εμμανουήλ Σφακιανάκης εργαζόταν στην Αστυνομία 34 έτη εκ των οποίων τα 23 ασχολείτο με τη διερεύνηση των ηλεκτρονικών εγκλημάτων. Σπούδασε Ανάλυση και Προγραμματισμό Η/Υ. Εκπαιδεύθηκε στο Λονδίνο στο έγκλημα του Πλαστικού χρήματος (Plastic Crime) και στο FBI σε θέματα για Τρομοκρατία στο διαδίκτυο (Cyber Terrorism). Έχει χειρισθεί περισσότερες από 10.000 σοβαρές υποθέσεις σε σύνολο 28.000 που αφορούν το κυβερνοέγκλημα. Έχει συμμετάσχει ως βασικός ομιλητής από το 2001 έως 2016 σε 875 συνέδρια Εθνικά και Διεθνή της INTERPOL - EUROPOL - Πανεπιστημιακών Ιδρυμάτων - Διεθνών Οργανισμών κ.α. Είναι κάτοχος Μεταπτυχιακών Διπλωμάτων α] στις «Ποινικές Επιστήμες» και β] στην «Εγκληματολογία» του Τμήματος της Νομικής Σχολής του ΕΚΠΑ. Είναι υποψήφιος Διδάκτωρ στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς. Είναι καθηγητής στο ΠΑ.ΠΕΙ στην Αστυνομική Ακαδημία, και Εθνική Σχολή Δικαστών. Είναι συγγραφέας των: α) Εθισμός στο διαδίκτυο και άλλες διαδικτυακές συμπεριφορές, β) Ο κώδικας του Διαδικτύου, γ) Τα κλειδιά του Διαδικτύου. Έχει λάβει, μέχρι το 2016, 90 τίτλους τιμής από: α) τον Πρόεδρο της Δημοκρατίας, β) την Ακαδημία Αθηνών για την ιδιαιτέρως μεγάλη κοινωνική του προσφορά, γ) από τη UNICEF ως ο "άνθρωπος των παιδιών", δ) το FBI -3- φορές για διερεύνηση διαδικτυακών εγκλημάτων, κ.α. Επίσης εμπνεύστηκε την εφαρμογή CYBERKID και βραβεύτηκε στο Mobility Forum & Apps Awards 2015 με το Χρυσό Βραβείο. Είναι συνιδρυτής της εταιρείας GDPR Greece.

ΜΑΚΡΥΠΟΥΛΙΑΣ ΙΩΑΝΝΗΣ

Εργάστηκε στη Δίωξη Ηλεκτρονικού Εγκλήματος επί πέντε και πλέον έτη ως Αξιωματικός Ειδικών Καθηκόντων στο Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων και στο Ειδικό Τμήμα Εγκλημάτων Υψηλής Τεχνολογίας. Σπούδασε Μηχανικός Ηλεκτρονικών Υπολογιστών στο Πανεπιστήμιο Πατρών και απέκτησε Μεταπτυχιακό Τίτλο Σπουδών στο Τμήμα Επιστήμης των Υπολογιστών του Οικονομικού Πανεπιστημίου Αθηνών με ειδίκευση στην ασφάλεια πληροφοριακών συστημάτων, κατακτώντας υποτροφία για τις επιδόσεις του. Συμμετείχε σε πλήθος ερευνητικών εργασιών για σημαντικά και επίκαιρα θέματα της τεχνολογίας, τα αποτελέσματα των οποίων έχουν δημοσιευθεί σε διεθνή συνέδρια και περιοδικά. Σήμερα εργάζεται στον ιδιωτικό τομέα στην ανάπτυξη πληροφοριακών συστημάτων, ιστοσελίδων και συστημάτων διαχείρισης με ειδικότητα στην ασφάλεια και τη βελτιστοποίηση της απόδοσης και λειτουργίας τους. Κατά την υπηρεσία του στη Δίωξη Ηλεκτρονικού Εγκλήματος εκπαιδεύτηκε από το FBI και τη Europol, συμμετείχε ως ομιλητής σε διεθνή συνέδρια με θέμα την κυβερνοασφάλεια, ασχολήθηκε με πλήθος σημαντικών υποθέσεων παραβίασης υπολογιστικών συστημάτων και συμμετείχε σε επιτροπές για την αξιολόγηση και βελτίωση μερικών εκ των σημαντικότερων κρατικών πληροφοριακών συστημάτων. Είναι συγγραφέας του βιβλίου "Τα κλειδιά του διαδικτύου" και συνιδρυτής της εταιρείας GDPR Greece.

ΡΟΝΤΟΥ ΚΑΛΛΙΟΠΗ

Δικηγόρος Παρ' Αρείω Πάγω, μέλος του Δικηγορικού Συλλόγου Αθηνών, νομικός σύμβουλος και μέλος της Ένωσης Σηματούχων Εταιρειών Ελλάδος και Κύπρου (ESIMET), νομικός σύμβουλος μεγάλων ανωνύμων εταιρειών στο χώρο του φαρμάκου, της βιομηχανίας και του εμπορίου. Απόφοιτος Νομικής Σχολής Αθηνών με Μεταπτυχιακό Τίτλο Σπουδών στο Αστικό Δικονομικό και Διεθνές Δικονομικό Δίκαιο, με ειδίκευση στην Κατάσχεση των Τραπεζικών Λογαριασμών στην ημεδαπή και διεθνή έννομη τάξη. Από το έτος 2004 ασκεί μαχόμενη δικηγορία στην Αθήνα με πολύχρονη εμπειρία στο αστικό και ποινικό δίκαιο, σε ζητήματα προσβολής εμπορικών σημάτων, αθέμιτου ανταγωνισμού, πνευματικής και βιομηχανικής ιδιοκτησίας, domain names και νομικά θέματα ιστοσελίδων. Έχει συμμετάσχει σε διεθνείς υποθέσεις προσβολής πνευματικών δικαιωμάτων και σημάτων φήμης εταιρειών μεγάλης εμπορικής εμβέλειας. Τα τελευταία έτη συμβάλει, στα πλαίσια του σκοπού της ένωσης ESIMET, στην καταπολέμηση παραποιημένων ειδών στην Ελλάδα και στην Κύπρο σε συνεργασία με τους αρμόδιους ελληνικούς οργανισμούς. Έχει χειριστεί υποθέσεις προσβολής προσωπικών δεδομένων και ειδικότερα ζητήματα διαγραφής προσωπικών και ευαίσθητων προσωπικών δεδομένων βάσει του "δικαιώματος στη λήθη". Έχει φέρει εις πέρας μεγάλο αριθμό υποθέσεων παραβίασης πληροφοριακών συστημάτων, έχει

εκπαιδευτεί και εξειδικευτεί σε θέματα συμμόρφωσης με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) και έχει λάβει επιμόρφωση σχετικά με τα καθήκοντα και το ρόλο του DPO .

ΠΑΠΑΝΤΩΝΙΟΥ ΠΑΝΑΓΙΩΤΗΣ

Ο Παναγιώτης Παπαντωνίου είναι ειδικός ερευνητής και εμπειρογνώμονας ασφάλειας πληροφοριακών συστημάτων με πάνω από 7 χρόνια εργασιακής εμπειρίας. Ειδικεύεται στη διαδικτυακή ασφάλεια, την αναζήτηση 0day ευπαθειών, το ηθικό hacking, τις τεχνολογίες blockchain, την αντιμετώπιση συμβάντων και ηλεκτρονικών εγκληματολογικών ερευνών. Έχει συμμετάσχει σε εγκληματολογικές έρευνες υποθέσεων δημοσίου ενδιαφέροντος σε συνεργασία με τις ελληνικές αρχές, διατέλεσε εξωτερικός σύμβουλος ασφάλειας πληροφοριών στην Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης, μια εταιρεία του δημοσίου που διαχειρίζεται το έργο της ηλεκτρονικής συνταγογράφησης. Έχει συμμετάσχει και έχει διακριθεί στην εθνική άσκηση κυβερνοάμυνας «ΠΑΝΟΠΤΗΣ», είναι συνιδρυτής της διαγωνιστικής ομάδας «Greunion» με αρκετές παγκόσμιες διακρίσεις στον χώρο της κυβερνοασφάλειας. Έχει διατελέσει αρχηγός και κατέχει την θέση του προπονητή της εθνικής ομάδας κυβερνοασφάλειας που αντιπροσωπεύει την χώρα μας για δεύτερη συνεχή χρονιά στον πανευρωπαϊκό διαγωνισμό κυβερνοασφάλειας «ECSC»

ΒΙΕΝΝΑΣ ΑΧΙΛΛΕΑΣ

Ο Βιέννας Αχιλλέας, ως ελεύθερος επαγγελματίας, ασχολείται από το 2007 με θέματα πληροφορικής σε επαγγελματικό και προσωπικό επίπεδο. Είναι πτυχιούχος Μηχανικός Υπολογιστικών συστημάτων Τ.Ε και Μεταπτυχιακός φοιτητής στο τμήμα πληροφορικής και τηλεπικοινωνιών του Πανεπιστημίου Πειραιά με ειδίκευση στην διαχείριση τεχνολογιών ασφάλειας σε προηγμένα συστήματα πληροφορικής. Βάση της ακαδημαϊκής και επαγγελματικής του πορείας, εξειδικεύτηκε σε θέματα ασφάλειας και εύρεσης βέλτιστων λύσεων σε πληροφοριακά συστήματα. Αναλαμβάνει εταιρικά και ιδιωτικά έργα πληροφορικής που αφορούν δημιουργία, διαμόρφωση και διαχείριση ιστοσελίδων. Επιπροσθέτως, ασχολείται με την ασφάλεια στον κυβερνοχώρο, την αξιολόγηση και την εκμετάλλευση ευπαθειών, και τους ελέγχους παρείσδυσης. Παράλληλα, ειδικεύεται στην εύρεση, ανάλυση και διαχείριση κακόβουλου λογισμικού και την καταγραφή-οργάνωση των διαδικασιών και πολιτικών των επιχειρήσεων ώστε να συμμορφώνονται στον γενικό κανονισμό προστασίας των δεδομένων (GDPR) καθώς και στο ISO 27001. Μέσα από την συμμετοχή του, σε ελληνικό και παγκόσμιο επίπεδο, σε διαγωνισμούς hacking, έχει δείξει ιδιαίτερο ενδιαφέρον για θέματα που αφορούν στην έρευνα και ανάπτυξη στο τομέα της ασφάλειας και στην εφαρμογή διεθνών προτύπων στον τρόπο διεξαγωγής των αξιολογήσεων ασφάλειας. Είναι μέλος της ομάδας CTF «Greunion», με την οποία κατέκτησε την πρώτη θέση στην εθνική άσκηση κυβερνοπολέμου 'ΠΑΝΟΠΤΗΣ' του γενικού επιτελείου εθνικής άμυνας το 2017.

ΚΑΡΑΓΕΩΡΓΙΟΥ ΔΗΜΟΣΘΕΝΗΣ

Ο Καραγεωργίου Δημοσθένης, είναι Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών, με ειδίκευση στις τεχνολογίες του internet και στα social media. Από το 2008 εργάζεται στην Πρίσμα Ηλεκτρονικά. Έχει μεγάλη εμπειρία στην υλοποίηση και διαχείριση μεγάλων δημόσιων έργων με αντικείμενα όπως: σχεδιασμό και υλοποίηση δικτύων (LAN, WAN, MAN), σχεδιασμό και εγκατάσταση οπτικών ινών, σχεδιασμό και εγκατάσταση ευρυζωνικών-ασύρματων δικτύων, Portals ηλεκτρονικής διακυβέρνησης, εφαρμογές internet καθώς επίσης έχει συμμετάσχει σε πλήθος εθνικών-ευρωπαϊκών ερευνητικών προγραμμάτων πληροφορικής. Είναι υπεύθυνος ανάπτυξης και σχεδιασμού του XENAGOS το οποίο είναι σύστημα διαχείρισης και παρουσίασης πληροφορίας σχεδιασμένο για μουσεία, αρχαιολογικούς και εκθεσιακούς χώρους καθώς και για ξεναγήσεις σε πόλεις και περιοχές. Έχει συμμετάσχει ως επόπτης και σύμβουλος σε έργα του Υπουργείο Δικαιοσύνης όπως το Εθνικό Ποινικό Μητρώο και το Ολοκληρωμένο Πληροφορικό Σύστημα Διοικητικών Δικαστηρίων. Ασχολείται με την οργάνωση και την τήρηση διαδικασιών των προτύπων ISO 27001 και ISO 20000 στον τομέα IT και Ασφάλειας Πληροφοριών. Παράλληλα, ειδικεύεται στην σχεδίαση ηλεκτρονικών καταστημάτων (e-shops), ιστοσελίδων καθώς και με την προβολή - προώθηση εταιρειών και οργανισμών μέσω των κοινωνικών δικτύων.