EXCELLENCE
MANAGEMENT CONSULTANTS

Τομέας
Cyber Security & GDPR

Λ. Συγγρού 310 & Σπάρτης 1, 176 73 Καλλιθέα

T: 210-48.38.706, 712 & 714 | F: 210-48.22.091,

E: info@excellence.gr | www.excellence.gr

Περιεχόμενα

1. Συνοπτική παρουσίαση

Η **Excellence Management Consultants είναι εταιρία συμβούλων επιχειρήσεων** με παρουσία 30+ χρόνων που παρέχει ολοκληρωμένες λύσεις επιχειρησιακής αναδιοργάνωσης και οργανωτικής ανάπτυξης για τη βελτίωση απόδοσης των επιχειρήσεων, ειδικά διαμορφωμένες και προσαρμοσμένες στις ανάγκες του πελάτη μας, μέσα από συμβουλευτικές και εκπαιδευτικές υπηρεσίες.

Τομείς εξειδίκευσης στην Οργάνωση και Διοίκηση των επιχειρήσεων

- **ISO – Συστήματα Διαχείρισης**
- **Επιχειρησιακή Αναδιοργάνωση & Οργανωτική Ανάπτυξη**
- **Στρατηγική – Marketing – Οργάνωση Πωλήσεων**
- **Χρηματοοικονομική Οργάνωση**
- **Logistics – Supply Chain**
- **Cyber Security & GDPR**
- **HR Management**
- **Ανάπτυξη Ικανοτήτων – Training & Coaching**
- **Επιλογή Προσωπικού**

Η δυνατή ομάδα senior consultants

Ιδιαίτερο ανταγωνιστικό μας πλεονέκτημα αποτελεί, η **δυνατή ομάδα senior consultants** που:

- Αποτελείται από καταξιωμένα στελέχη, με σημαντικές εμπειρίες από μεγάλες ελληνικές και πολυεθνικές επιχειρήσεις, που καλύπτουν ένα ευρύ φάσμα αντικειμένων δραστηριότητας.
- Διαθέτει ικανότητα παροχής ολοκληρωμένης προσέγγισης στον κύκλο: «διάγνωση – μελέτη – εφαρμογή – εκπαίδευση – coaching» για την εφαρμογή και επίτευξη αποτελεσμάτων.
- Αξιοποιεί σύγχρονες μεθόδους και συστήματα από την διεθνή εμπειρία των επιτυχημένων επιχειρήσεων.
- Έχει προσανατολισμό προς τη βελτίωση απόδοσης και τη μείωση κόστους.

Η αποστολή μας

Χτίζουμε σχέσεις στρατηγικής συνεργασίας με τους πελάτες μας και συμβάλλουμε στην αναπτυξιακή τους πορεία, αξιοποιώντας και προσαρμόζοντας στις ιδιαίτερες ανάγκες τους, σύγχρονες μεθόδους και διεθνείς πρακτικές της αγοράς στην διοίκηση των επιχειρήσεων.

30+ χρόνια αξιόπιστης παρουσίας – 2.500 ικανοποιημένοι πελάτες

Τα **30+ χρόνια αξιόπιστης παρουσίας**, με **πάνω από 2.500 ικανοποιημένους πελάτες**, η μακροχρόνια και επιτυχημένη συνεργασία μας στους τομείς που δραστηριοποιούμαστε, αλλά και η ομάδα των έμπειρων συνεργατών μας, αποτελούν εγγύηση για μια αμοιβαία επωφελή συνεργασία.

Η συνδεδεμένη εταιρία ΕΞΥΠΠ Active Safety

Παρέχει υπηρεσίες Υγείας και Ασφάλειας της εργασίας και είναι αδειοδοτημένη ως Εξ.Υ.Π.Π από το Υπουργείο Εργασίας. Επίσης, είναι μέλος στο επίσημο όργανο του κλάδου ΠΑΣΥΜΕΠ και μέλος στο ΔΣ. Για περισσότερες πληροφορίες παραπέμπουμε στο www.active-safety.gr.

2. Τομέας Cyber Security

Κυβερνοασφάλεια (Cyber Security)

Ο αυξανόμενος αριθμός ατόμων που συνδέονται με το διαδίκτυο αυξάνει τις απειλές για σοβαρές βλάβες σε επιχειρήσεις και μεμονωμένους χρήστες. Η κυβερνοασφάλεια μπορεί να βοηθήσει στην διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (Confidentiality, Integrity, Availability - CIA) στα δεδομένα και τις πληροφορίες

Η κυβερνοασφάλεια αναφέρεται στην προστασία των συνδεδεμένων στο διαδίκτυο συστημάτων από συμβάντα όπως διαρροή, επίθεση, αστοχία κλπ, συμπεριλαμβανομένου του εξοπλισμού (hardware), του λογισμικού (software) και των δεδομένων (data) από κυβερνοεπιθέσεις, καθώς και την ικανότητα ανάκτησης αυτών από τέτοια συμβάντα.

Η Κυβερνοασφάλεια σήμερα

Η πανδημία του κορονοϊού επιτάχυνε τον ψηφιακό μετασχηματισμό της οικονομίας και της κοινωνία καθώς έφερε νέες ευκαιρίες και προκλήσεις στο προσκήνιο.
125 δισεκατομμύρια συσκευές θα έχουν συνδεθεί στο διαδίκτυο μέχρι το 2030, από 27 δισεκατομμύρια το 2021, και το 90% των ανθρώπων άνω των 6 ετών εκτιμάται ότι θα έχει διαδικτυακή παρουσία. Ο κυβερνοχώρος από την φύση του βασίζεται στη διασύνδεση των κοινοτήτων κάθε μορφής και καθώς ο ψηφιακός και φυσικός κόσμος είναι όλο και πιο αλληλένδετοι, προκύπτουν νέοι κίνδυνοι.

Οι κυβερνοεπιθέσεις είναι από τις γρηγορότερα αναπτυσσόμενες μορφές εγκλήματος παγκοσμίως. Το 2020 το ετήσιο κόστος του κυβερνοεγκλήματος για την παγκόσμια οικονομία υπολογίζεται στα 5,5 τρις ευρώ, ποσό διπλάσιο από εκείνο του 2015.

Απειλές και Επιπτώσεις για τις επιχειρήσεις

<u>Κύριες απειλές</u>
- Διαρροή πληροφοριών ή μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές, φορητούς υπολογιστές, tablet, κινητά.
- Απομακρυσμένες επιθέσεις σε συστήματα πληροφορικής ή ιστοχώρους.
- Επίθεση σε πληροφορίες που κατέχει τρίτο μέρος, π.χ. φιλοξενούμενες υπηρεσίες ή τραπεζικό λογαριασμό της εταιρίας.
- Πρόσβαση σε πληροφορίες μέσω του προσωπικού των επιχειρήσεων.

<u>Επιπτώσεις επιθέσεων</u>
- Οικονομικές απώλειες από κλοπή πληροφοριών, οικονομικές λεπτομέρειες, τραπεζικά στοιχεία ή χρήματα.
- Οικονομικές απώλειες λόγω διακοπής των συναλλαγών στις επιχειρήσεις.
- Η κακή δημοσιότητα και βλάβη στη φήμης μιας επιχείρησης μπορεί να οδηγήσει σε απώλεια συμβολαίων με πελάτες.
- Κόστος για τον καθαρισμό των συστημάτων που έχουν επηρεαστεί και για τη ανάκτηση της λειτουργίας τους.
- Κόστος για πρόστιμα εάν χαθούν ή διακυβεύονται προσωπικά δεδομένα.
- Ζημιά σε άλλες εταιρείες στις οποίες μια επιχείρηση προμηθεύει υπηρεσίες ή συνδέεται με άλλο τρόπο.

Σκοπός της Κυβερνοασφάλειας είναι η κυβερνοανθεκτικότητα

Η κυβερνοανθεκτικότητα είναι η ικανότητα μιας εταιρίας να προετοιμάζεται, να ανταποκρίνεται και να ανακάμπτει από κυβερνοεπιθέσεις. Βοηθά τις εταιρείες να προστατεύονται από τους κινδύνους του κυβερνοχώρου, να υπερασπίζονται και να περιορίζουν τη σοβαρότητα των επιθέσεων, και να διασφαλίζουν τη συνεχή επιβίωσή τους παρά την επίθεση. Ο στόχος της κυβερνοανθεκτικότητας είναι η διατήρηση της ικανότητας της εταιρίας να παρέχει τα προϊόντα και τις υπηρεσίες της απρόσκοπτα, ακόμα και όταν οι συνηθισμένοι μηχανισμοί παροχής έχουν αποτύχει εξαιτίας μιας κυβερνοεπίθεσης.

Μια βέλτιστη πρακτική για την ενίσχυση της ανθεκτικότητας στον κυβερνοχώρο μιας εταιρίας είναι η εφαρμογή ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS – Information Security Management System). Ένα ISMS είναι ένα σύνολο πολιτικών και διαδικασιών για τη συστηματική διαχείριση των ευαίσθητων δεδομένων ενός οργανισμού. Ο στόχος ενός ISMS είναι η ελαχιστοποίηση του κινδύνου και η διασφάλιση της επιχειρησιακής συνέχειας, περιορίζοντας τον αντίκτυπο μιας παραβίασης της ασφάλειας.

3. Οι Υπηρεσίες Cyber Security της Excellence Management Consultants

3.1 Διάγνωση υφιστάμενης κατάστασης και εκπόνηση σχεδίου δράσης

Η διάγνωση της υφιστάμενη κατάστασης και η εκπόνηση του απαραίτητου σχεδίου δράσης πραγματοποιείται ορίζοντας τα απαραίτητα μέτρα βελτίωσης μέσω

1. Gap Analysis & Vulnerability Assessment:

Αφορά στον Τεχνικό έλεγχο ασφάλειας πληροφοριακών συστημάτων για τον εντοπισμό ευπαθειών, τρωτοτήτων και κενών ασφαλείας.

Με την χρήση εξειδικευμένου λογισμικού εξετάζονται με διάφορους τρόπους τα συστήματα, οι εφαρμογές και οι υπηρεσίες του πελάτη τόσο από εξωτερικές απειλές όσο και από εσωτερικές, με σκοπό τον εντοπισμό αδυναμιών που μπορεί να οδηγήσουν σε παραβίαση ασφαλείας.

Ο έλεγχος μπορεί να πραγματοποιηθεί είτε με φυσική είτε με εικονική (vpn) πρόσβαση στο υπό εξέταση σύστημα.

Το αποτέλεσμα του ελέγχου δίνει μία πλήρης περιγραφή των ευπαθειών με τις αντίστοιχες προτεινόμενες διορθωτικές ενέργειες.

2. Penetration Testing

Η Δοκιμή Διείσδυσης (Penetration Test) αποτελεί την εξελιγμένη επέκταση του τεχνικού ελέγχου ασφαλείας, λειτουργώντας ως ένα σύνθετο εργαλείο επιθετικής αξιολόγησης. Σκοπός της είναι να προσομοιώσει μία ή πολλαπλές επιθέσεις στα Συστήματα Πληροφορικής, εκμεταλλευόμενη τις αδυναμίες που έχουν εντοπιστεί κατά την διάρκεια της αρχικής εκτίμησης ασφαλείας.

Η Δοκιμή Διείσδυσης εξετάζει ενδελεχώς τις επιπτώσεις μιας επίθεσης και προσφέρει ακριβή εκτίμηση της πιθανής ζημίας ή βλάβης που θα προκύψει από μια παραβίαση ασφαλείας. Απαιτεί εξειδικευμένα εργαλεία και εξαρτάται από εξειδικευμένο προσωπικό, ενώ οι παράμετροι της δοκιμής διαμορφώνονται σύμφωνα με τις ανάγκες, τις προτεραιότητες και τα αποτελέσματα της αρχικής εκτίμησης ασφαλείας του πελάτη.

Επιπροσθέτως, ένα κρίσιμο στοιχείο της Δοκιμής Διείσδυσης αποτελεί η Δοκιμή Διείσδυσης σε Εφαρμογές Διαδικτύου (Web Application Penetration Test).Αυτό το στοιχείο απαιτεί διαφορετική τεχνογνωσία και

εργαλεία και μπορεί να παρέχεται είτε ανεξάρτητα, είτε ως μέρος του γενικότερου Penetration Test, ανάλογα με την υποδομή και τις απαιτήσεις του πελάτη.

3. **Asset Management & Risk Assessment**

Έλεγχος, αξιολόγηση και ανάλυση του τρόπου διαχείρισης και καταγραφής των ψηφιακών μέσων και Εκτίμηση κινδύνου που προκύπτει από την ανάλυση των παραπάνω – Μέσα, Κενά, Αδυναμίες.

3.2 Ενέργειες βελτίωσης με την υλοποίηση του σχεδίου δράσης

1. Συμβουλευτικές υπηρεσίες – Μέτρα ασφαλείας

Αφορούν στην ανάλυση απαιτήσεων, σχεδιασμό και προτεινόμενους τρόπους υλοποίησης και εγκατάστασης μέτρων ασφαλείας, Περιμετρική ασφάλεια, όπως:

- Προστασία σταθμών εργασίας (endpoints/workstations/laptops)
- Συστήματα Εντοπισμού Παραβιάσεων
- Συστήματα διαχείρισης συμβάντων,
- Συστήματα συνεχούς παρακολούθησης και εντοπισμού περιστατικών ασφαλείας
- Συνεχής παρακολούθηση και εντοπισμός αδυναμιών και ευπαθειών
- Ασφαλής Διαμόρφωση των πληροφοριακών συστημάτων (εκτίμηση τρέχουσας διαμόρφωσης, σημεία διόρθωσης ρυθμίσεων, αξιολόγηση ρυθμίσεων - CIS benchmarks)

2. Εκπαίδευση χρηστών

Διαμορφώνεται και υλοποιείται, το κατάλληλο πρόγραμμα εκπαίδευσης για τις επιμέρους κατηγορίες χρηστών.

Οι εκπαιδεύσεις σχετικά με την κυβερνοασφάλεια και το phishing είναι απαραίτητες για τη διασφάλιση της προστασίας των ψηφιακών πόρων των επιχειρήσεων και των ατόμων. Παρέχουν πολλά οφέλη, όπως:

- **Αυξημένη επίγνωση:** Οι εκπαιδεύσεις κυβερνοασφάλειας βοηθούν το προσωπικό να κατανοήσει και να αναγνωρίσει τις απειλές, όπως τις επιθέσεις phishing, πριν προκληθεί ζημιά.
- **Προφύλαξη από απώλειες:** Η πρόληψη των επιθέσεων phishing μπορεί να αποτρέψει την κλοπή πολύτιμων πληροφοριών ή χρημάτων, προφυλάσσοντας τόσο τις εταιρείες όσο και τους ιδιώτες από σημαντικές οικονομικές απώλειες.
- **Ενίσχυση της κυβερνο-ανθεκτικότητας:** Μέσω της εκπαίδευσης, τα άτομα και οι επιχειρήσεις μπορούν να αποκτήσουν τις δεξιότητες και τις γνώσεις που χρειάζονται για να αντιμετωπίσουν και να ανακάμψουν από τις επιθέσεις κυβερνοασφάλειας, ενισχύοντας την κυβερνο-ανθεκτικότητά τους.
- **Δημιουργία μιας θετικής κουλτούρας ασφάλειας:** Μια καλά εκπαιδευμένη ομάδα μπορεί να προωθήσει μια θετική κουλτούρα ασφάλειας σε μια οργάνωση, όπου οι εργαζόμενοι γνωρίζουν, εκτιμούν και εφαρμόζουν τις βέλτιστες πρακτικές ασφάλειας.
- **Εκπλήρωση των νομικών και ρυθμιστικών απαιτήσεων:** Σε πολλές περιπτώσεις, οι εκπαιδεύσεις κυβερνοασφάλειας και phishing μπορεί να είναι απαραίτητες για την εκπλήρωση των νομικών και ρυθμιστικών απαιτήσεων, ιδιαίτερα σε ορισμένες βιομηχανίες όπως οι χρηματοπιστωτικές υπηρεσίες.
- **Αποφυγή επιπτώσεων στη φήμη:** Μια επιτυχής επίθεση phishing μπορεί να προκαλέσει σοβαρή ζημιά στη φήμη μιας επιχείρησης. Η εκπαίδευση μπορεί να βοηθήσει στην αποφυγή τέτοιων επιπτώσεων.
- **Ενθάρρυνση της συνεχούς μάθησης:** Οι απειλές κυβερνοασφάλειας εξελίσσονται συνεχώς. Οι εκπαιδεύσεις δίνουν την ευκαιρία για συνεχή εκμάθηση και προσαρμογή στις τελευταίες τάσεις και τεχνικές που χρησιμοποιούν οι επιτιθέμενοι.

- **Προστασία των πελατών:** Η κατάρτιση των υπαλλήλων σε θέματα κυβερνοασφάλειας και phishing μπορεί να βοηθήσει στην προστασία των πελατών της εταιρίας από απάτες και κλοπή δεδομένων.

3.3 Υπηρεσίες συμβούλου κυβερνοασφάλειας

Αφορά στην παροχή συμβουλευτικών υπηρεσιών σε θέματα Cyber Security, από στελέχη με σημαντική εμπειρία στον τομέα της κυβερνοασφάλειας. Σκοπός είναι ο τακτικός έλεγχος των συνδεδεμένων στο διαδίκτυο συστημάτων και η προστασία αυτών καθώς και η ανάκτηση των συστημάτων από τυχόν συμβάντα.

3.4 Ανάπτυξη & Εφαρμογή Συστήματος Διαχείρισης Πληροφοριών (Information Security) κατά ISO 27001

Επιπλέον των ανωτέρω απαραίτητων ελέγχων για την αναγνώριση των κενών ασφαλείας πληροφοριών σε σχέση με το πρότυπο ISO 27001 υλοποιούνται ενέργειες προετοιμασίας για επιθεώρηση από αρμόδιο φορέα για πιστοποίηση κατά ISO 27001, που αφορούν σε:

- Χαρτογράφηση Δεδομένων (data mapping – data flow – data repository)
- Συλλογή πληροφοριών για χαρακτηριστικά δεδομένων (τι, που, ποιος, πως)
- Τεκμηρίωση πληροφοριών
- Ανάλυση συνολικής χαρτογράφησης δεδομένων (data workflow analysis) για να κατανοηθεί σε βάθος ο πλήρης κύκλος ζωής και διακίνησης των δεδομένων ώστε να βελτιωθεί από πλευράς ασφάλειας.
- Εκπόνηση του Privacy Impact Assessment - PIA (Μελέτη Εκτίμησης Αντικτύπου),
- Ανάπτυξη Πολιτικών, Διεργασιών και Διαδικασιών στα πλαίσια του προτύπου.

Η μεθοδολογία της Excellence Management Consultants

Για τη Βελτίωση της Ασφάλειας των Επιχειρήσεων, συνολικά ή επιμέρους τμημάτων τους, η εταιρία μας παρέχει μια ολοκληρωμένη προσέγγιση στον κύκλο διάγνωση – βελτίωση – εκπαίδευση στους βασικούς παράγοντες που εμπλέκονται στην Κυβερνοασφάλεια και αφορούν:

- Στην Τεχνολογία, το Software και το Hardware που απαιτείται για την προστασία
- Στις Διαδικασίες που τηρεί ο οργανισμός ή κάποιος ατομικά
- Στους Χρήστες (ανθρώπινος παράγοντας)

Σκοπός: Η επίτευξη του μεγίστου ποσοστού ασφάλειας πληροφοριακών συστημάτων ώστε να είναι ασφαλή τα εταιρικά και προσωπικά δεδομένα.

4. Τομέας GDPR

Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου (General Data Protection Regulation, GDPR) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία αυτών, έχει ως στόχο τη θέσπιση κανόνων σύννομης επεξεργασίας προσωπικών δεδομένων στον Ευρωπαϊκό Οικονομικό Χώρο.

Δημοσιεύτηκε στην επίσημη εφημερίδα της Ε.Ε. στις 27.04.2016, θέτοντας υποχρεωτική εφαρμογή για όλα τα Κράτη Μέλη της Ευρωπαϊκής Ένωσης την 25η Μαίου 2018. Σε περίπτωση μη συμμόρφωσης επιβάλλονται από τις Εποπτικές Αρχές (εθνικές αρχές Προστασίας Δεδομένων) υψηλότατα πρόστιμα κατά των παραβατών, τα οποία, επί σοβαρών παραβιάσεων, μπορούν να ανέλθουν μέχρι ποσοστού 4% επί του ετήσιου κύκλου εργασιών του οργανισμού ή της επιχείρησης, ή μέχρι 20 εκ. Ευρώ, όποιο ποσό είναι υψηλότερο.
Ο νέος Κανονισμός αφορά κάθε υπεύθυνο επεξεργασίας, και, φυσικά, όλες τις επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα, ανεξαρτήτως κλάδου οικονομικής δραστηριότητας και μεγέθους.
Το 2019 δημοσιεύτηκε και ο Ελληνικός Νόμος 4624/2019 (ΦΕΚ Α' 137/ 29.8.2019) που ορίζει τις αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τα μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

5. Οι Υπηρεσίες GDPR της Excellence Management Consultants

Κατά την ανάπτυξη του έργου Συμμόρφωσης με τον GDPR και τον Ν. 4624/2019 παρέχονται οι ακόλουθες υπηρεσίες

- **Διάγνωση Υφιστάμενης Κατάστασης**
- **Χαρτογράφηση της Επιχείρησης (Data Flow Mapping)**
- **Εντοπισμός Αποκλίσεων**
- **Έκθεση Εκτίμησης Αντικτύπου (Privacy Impact Assessment)**
- **Σχεδιασμός Πλάνου Συμμόρφωσης**
- **Ανάπτυξη και Εφαρμογή Συστημάτων Ασφάλειας Δεδομένων και Πληροφοριών**
- **Υπηρεσίες Νομικής Συνδρομής**
- **Υπηρεσίες Εκπαίδευσης**
- **Επιθεωρήσεις Συμμόρφωσης**

Διάγνωση υφιστάμενης κατάστασης: Αφορά στην αξιολόγηση του βαθμού συμμόρφωσης της επιχείρησης, με επισκόπηση του χειρισμού των δεδομένων προσωπικού χαρακτήρα με πληροφορίες που αντλούνται από όλες τις οργανωτικές μονάδες της επιχείρησης. Η επισκόπηση πραγματοποιείται μέσω ερωτηματολογίου, συναντήσεων και συνεντεύξεων.

Χαρτογράφηση της επιχείρησης (Data Flow Mapping): Γίνεται πλήρης απογραφή των προσωπικών δεδομένων που διαχειρίζεται ο οργανισμός με χάρτη ροής και διαδικασίες. Στη χαρτογράφηση εντοπίζονται:

- οι κατηγορίες των προσώπων των οποίων τα δεδομένα επεξεργάζεται η επιχείρηση (π.χ.προσωπικό, πελάτες-ασφαλισμένους, ασφαλισμένους ομαδικών ασφαλίσεων, προμηθευτές),
- τα δεδομένα των ανωτέρω προσώπων που επεξεργάζεται η επιχείρηση (προσωπικά στοιχεία, φορολογικά, οικογενειακή κατάσταση, δεδομένα υγείας, κ.α.)
- οι χρήσεις αυτών, καθώς και η νομική βάση της επεξεργασίας τους.

Εντοπισμός των αποκλίσεων: Αφορά στην λεπτομερή αξιολόγηση και έλεγχο των προσωπικών δεδομένων της επιχείρησης με βάση τον Κανονισμό και κυρίως με τις βασικές αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία δείχνει την τρέχουσα συμμόρφωση του οργανισμού με τον GDPR. Ανάδειξη των κενών και κάθε ασυμβατότητας με την νέα νομοθεσία και πρόταση σχεδίων πρόληψης, αντιμετώπισης και αποκατάστασης κενών και κινδύνων μέσω εκπόνησης σχετικής μελέτης (Gap Analysis).

Έκθεση Εκτίμησης Αντικτύπου (Privacy Impact Assessment): Αφορά στην Αξιολόγηση κινδύνων ανά κατηγορία. Εκτιμάται η πιθανότητα εμφάνισης, η αξιολόγηση κρισιμότητας, εμπλεκόμενων μερών, προληπτικής διαχείρισης / πρόληψης και θεραπείας/αποκατάστασης μέσω εκπόνησης Έκθεσης Εκτίμησης Αντικτύπου (Privacy Impact Assessment).

Σχεδιασμός Πλάνου συμμόρφωσης: Αφορά στην Δημιουργία και εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, διαδικασιών και υπηρεσιών πλήρους συμμόρφωσης με βάση τον Κανονισμό, με συνεχή υποστήριξη, έλεγχο και παροχή συμβουλευτικού έργου στην υλοποίησή τους.

Ανάπτυξη και εφαρμογή συστημάτων ασφάλειας δεδομένων και πληροφοριών: Αφορά στην εφαρμογή του ISO 27001που αφορά στην ασφάλεια δεδομένων και πληροφοριών, καθώς και στο ISO 22301 που αφορά στο Business Continuity, εφόσον κριθεί σκόπιμο

Υπηρεσίες νομικής συνδρομής: Προετοιμασία με υπηρεσίες νομικής συνδρομής για την προσαρμογή συμβάσεων, συμβολαίων και φορμών συναίνεσης.

Υπηρεσίες εκπαίδευσης: Αφορά στην ενημέρωση, ευαισθητοποίηση και εκπαίδευση ειδικά προσαρμοσμένη για τις απαιτήσεις του οργανισμού.

Επιθεωρήσεις συμμόρφωσης: Αφορά σε επιθεωρήσεις μετά την εφαρμογή των μέτρων

6. Επικεφαλής Τομέα: Άγης Σολέας

Ο Α. Σολέας είναι απόφοιτος του τμήματος Φυσικής από το τμήμα Θετικών Επιστημών του Πανεπιστημίου Πατρών, με μεταπτυχιακές σπουδές στην Ασφάλεια Δικτύων και Ασφάλεια Πληροφοριών.

Από το 2016 είναι πιστοποιημένος Επικεφαλής Επιθεωρητής και επιθεωρεί Συστήματα Διαχείρισης Ποιότητας, Ασφάλειας Δεδομένων & Πληροφοριών, Διαχείρισης Προσωπικών Δεδομένων, Επιχειρησιακής Συνέχειας.

Εργάζεται ως Σύμβουλος Ασφάλειας Πληροφοριών σε εταιρείες και οργανισμούς του δημόσιου και ιδιωτικού τομέα, μεταξύ των οποίων και στην Βουλή των Ελλήνων.

7. Επικοινωνήστε μαζί μας

Είμαστε στην διάθεσή σας για να δούμε τα μέτρα που απαιτούνται για την ασφάλεια της επιχείρησής σας στα ακόλουθα στοιχεία επικοινωνίας:

Άγης Σολέας, Επικεφαλής Τομέα
T: 210 48 38 706, 712 & 714 | E: info@excellence.gr