Ελληνικό Μεσογειακό Πανεπιστήμιο

Διεύθυνση Πληροφορικής & Βιβλιοθήκης

Κανονιστικό Πλαίσιο Προστασίας Υποδομής ΤΠΕ

Περιεχόμενα

Σύμφωνα με το σχέδιο συμμόρφωσης τους Ιδρύματος, όπως εκπονήθηκε αρχικά από την ομάδα έργου της αναδόχου εταιρείας και παραδόθηκε τον Ιανουάριο του 2019, κρίνεται απαραίτητο να οριστούν πολιτικές για την αύξηση της προστασίας των προσωπικών δεδομένων που διατηρεί, επεξεργάζεται και συλλέγει το Ελληνικό Μεσογειακό Πανεπιστήμιο.
Με τη μετεξέλιξη του ΤΕΙ Κρήτης σε Ελληνικό Μεσογειακό Πανεπιστήμιο τον Μάϊο του 2019 δόθηκε προτεραιότητα στην προσαρμογή όλων των λειτουργιών και διαδικασιών προκειμένου η υπολογιστική και δικτυακή υποδομή του Ιδρύματος να προσαρμοστεί και να υποστηρίξει τη νέα δομή, ως εκ τούτου δεν κατέστη δυνατή η πλήρης συμμόρφωση σύμφωνα με τον ΓΚΠΔ. Βέβαια, πολλές υποδείξεις ενσωματώθηκαν στην ανάπτυξη της νέας υποδομής, π.χ. κανένας δικτυακός τόπος του domain hmu.gr δεν λειτουργεί χωρίς πιστοποιητικό ασφαλείας.
Λαμβάνοντας υπόψη ότι το θέμα της προστασίας των προσωπικών δεδομένων είναι κρίσιμο, και τα σχετικά θέματα που δημιουργούνται κατά την χρήση νέων τεχνολογιών συνεχώς αυξάνονται, εισηγούμαστε την ενσωμάτωση στην πολιτική λειτουργία της υπολογιστικής και δικτυακής υποδομής τον ορισμό των ακόλουθων πολιτικών:

Πολιτική Κωδικού πρόσβασης

Αύξηση της πολυπλοκότητας των κωδικών ασφαλείας των χρηστών. Σε πρώτη φάση θα πρέπει να κληθούν οι χρήστες να αλλάξουν κωδικό πρόσβασης και να ορίσουν έναν νέο που θα αποτελείται από τουλάχιστον 9 χαρακτήρες που θα περιλαμβάνει λατινικούς χαρακτήρες, αριθμούς και ειδικά σύμβολα, τουλάχιστον 1 από κάθε κατηγορία.
Παράλληλα να ενεργοποιηθεί λειτουργικότητα που θα υποχρεώνει τους χρήστες να αλλάζουν κωδικούς κάθε 12 μήνες.

Κλείδωμα οθόνης

Όλοι οι σταθμοί εργασίας πρέπει να ρυθμιστούν ώστε μετά από χρονικό διάστημα αδράνειας 15 λεπτών της ώρας, να κλειδώνουν, χωρίς αδρανοποίηση του σταθμού εργασίας, και να απαιτείται ξανά πιστοποίηση του χρήστη. Για μηχανήματα που δεν μπορεί να εφαρμοστεί η κεντρική πολιτική (policy) θα είναι ευθύνη του διαχειριστή του σταθμού εργασίας να εφαρμόζει σχετική πολιτική.

Δικαιώματα τοπικού διαχειριστή

Δεν παραχωρούνται δικαιώματα τοπικού διαχειριστή σε απλούς χρήστες.
Θα πρέπει να ανακληθούν, σε όλους τους σταθμούς εργασίας, τα δικαιώματα τοπικού διαχειριστή από όλους τους χρήστες και να αφαιρεθούν όσοι τοπικοί λογαριασμοί έχουν αντίστοιχα δικαιώματα και δεν ανήκουν σε συγκεκριμένο χρήστη.
Σε όσους σταθμούς εργασίας δεν υπάρχει κεντρική διαχείριση είναι υποχρέωση του διαχειριστή του σταθμού εργασίας να εφαρμόζει σχετική πολιτική.

Υπηρεσίες καταλόγου

Ενσωμάτωση όλων των σταθμών εργασίας γραφείων και εργαστηρίων (εκπαιδευτικών και ερευνητικών), που λειτουργούν εντός του δικτύου του Ιδρύματος, στην υπηρεσία καταλόγου, ώστε όλοι οι χρήστες να χρησιμοποιούν τον ιδρυματικό λογαριασμό για την πρόσβαση σε αυτούς. Παράλληλα, για να μειωθεί ο κίνδυνος ευαλωσημότητας, να μπουν πίσω από το

τείχος προστασίας (firewall) του Ιδρύματος όλοι οι σταθμοί εργασίας, ανεξάρτητα από την χρήση τους.
Όλα τα ασύρματα δίκτυα που λειτουργούν εντός του Ιδρύματος πρέπει να ρυθμιστούν κατάλληλα ώστε να χρησιμοποιούν την κεντρική υπηρεσία πιστοποίησης για να επιτρέπουν την πρόσβαση.
Να δημιουργηθεί υπηρεσία δημιουργία προσωρινών λογαριασμών (π.χ. μέχρι 20 ενεργούς) την οποία θα χρησιμοποιούν όσοι επιθυμούν να παρέχουν πρόσβαση στο διαδίκτυο σε επισκέπτες. Η συγκεκριμένη υπηρεσία θα είναι διαθέσιμη μόνο για τα μέλη του μόνιμου εκπαιδευτικού προσωπικού και τους προϊσταμένους διευθύνσεων και αυτόνομων τμημάτων, η διάρκεια ισχύος των λογαριασμών θα είναι δέκα (10) ημέρες, με δυνατότητα παράτασης όποτε απαιτείται.
Σε όσους σταθμούς εργασίας δεν υπάρχει κεντρική διαχείριση είναι υποχρέωση του διαχειριστή του σταθμού εργασίας να εφαρμόζει σχετική πολιτική.

Υπηρεσίες δικτύου

Υποχρεωτική χρήση ταυτοποίησης από τους χρήστες που επιθυμούν να έχουν πρόσβαση στο εσωτερικό δίκτυο του Ιδρύματος που διαχειρίζεται η Διεύθυνση Πληροφορικής & Βιβλιοθήκης. Για την ταυτοποίηση θα πρέπει να χρησιμοποιείται ο Ιδρυματικός λογαριασμός (το HMU ID της μορφής username@hmu.gr), χρησιμοποιώντας την κεντρική υπηρεσία πιστοποίησης του Ιδρύματος, είτε άλλη υπηρεσία του Ιδρύματος (π.χ. CAS, Ldap) που πιστοποιεί τους χρήστες από την Κεντρική Υπηρεσία Καταλόγου του Ιδρύματος.
Παράλληλα, όλα τα ασύρματα δίκτυα που λειτουργούν εντός του Ιδρύματος πρέπει να ρυθμιστούν ώστε να χρησιμοποιούν την συγκεκριμένη διαδικασία πρόσβασης.

Απομάκρυνση υπολογιστών με λειτουργικά συστήματα που δεν υποστηρίζονται.

Απόσυρση όλων των σταθμών εργασίας που λειτουργούν με λειτουργικά συστήματα που έχει περάσει ο χρόνος υποστήριξης τους (π.χ. Windows XP, Windows 7, Ubuntu 14.04 LTS, κτλ.). Οι σταθμοί εργασίας θα παραδίδονται στην Διεύθυνση Πληροφορικής και Βιβλιοθήκης, για να αξιολογηθούν και να κριθεί αν μπορούν να αναβαθμιστούν με χρήση εκδόσεων λειτουργικού που λαμβάνουν ενημερώσεις, ώστε να είναι αποδοτικοί και ασφαλείς.
Οι διαχειριστές της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης, πρέπει να εκτελούν διαδικασία αυτοματοποιημένης σάρωσης του δικτύου, τουλάχιστον μια φορά τον χρόνο, για να εντοπίζουν σταθμούς εργασίας που χρησιμοποιούν λειτουργικά συστήματα που δεν υποστηρίζονται, και να ξεκινούν την διαδικασία της απόσυρσής τους.
Όσοι σταθμοί εργασίας δεν είναι στην διαχείριση της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης, ο διαχειριστής τους έχει την υποχρέωση να εφαρμόζει σχετική πολιτική.

Τείχος Προστασίας (firewall)

Ανάπτυξη πολιτικών στο τείχος προστασίας που θα αποτρέπουν τις εσωτερικές και εξωτερικές επιθέσεις.
Το εσωτερικό εικονικό δίκτυο του ΕΛΜΕΠΑ, θα ενώνει τις κεντρικές εγκαταστάσεις στο Ηράκλειο με όλα τις υπόλοιπες εγκαταστάσεις σε: Σητεία, Άγιο Νικόλαο, Ρέθυμνο (εγκαταστάσεις εκπαίδευσης και έρευνας (Τρία Μοναστήρια)), Χανιά και όσες άλλες εγκαταστάσεις επεκταθεί το Πανεπιστήμιο στο μέλλον. Όλες οι υπολογιστικές υποδομές (σταθμοί εργασίας, φορητές συσκευές, εξυπηρετητές, κτλ.) πρέπει να ενταχθούν πίσω από το τείχος προστασίας, εκτός αν για λόγους υποστήριξης της υποδομής και της φύσης της εργασίας που εκτελούν πρέπει να είναι εκτός (π.χ. εξωτερικοί DNS). Υπεύθυνοι για να

ορίσουν και να χρησιμοποιούν αυτόν τον εξοπλισμό είναι αποκλειστικά το προσωπικό της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης και ειδικότερα οι εκτελούντες χρέη κεντρικού διαχειριστή.

Το τείχος προστασίας θα υλοποιεί τις πολιτικές χρήσης του δικτύου και θα ρυθμίζει την πρόσβαση σε διάφορους πόρους ανάλογα με τα δικαιώματα χρήσης που διαθέτει ο κάθε χρήστης. Η λειτουργία αυτή είναι απαραίτητη, γιατί ο κίνδυνος κακόβουλων επιθέσεων από το εσωτερικό δίκτυο παρουσιάζεται αυξημένος, σύμφωνα με την εμπειρία χρήσης.

Το τείχος προστασίας θα υλοποιεί πολιτική καταγραφής της κίνησης κάθε χρήστη, ώστε σε περίπτωση που ζητηθεί από αρμόδιο φορέα, στα πλαίσια του υφιστάμενου νομικού πλαισίου, το Ίδρυμα να μπορεί να παρέχει τις ζητούμενες πληροφορίες για την χρήση των υποδομών του. Η περίοδος διατήρησης των στοιχείων καταγραφής πρέπει να ακολουθεί όσα ορίζονται από το υφιστάμενο νομικό πλαίσιο και όχι λιγότερο από 6 μήνες.

Για να αποτρέπονται προσπάθειες παράκαμψης των κανόνων λειτουργίας με χρήση της σύνδεσης σε εξωτερικές υπηρεσίες VPN (είτε μέσω του λειτουργικού συστήματος, είτε μέσω χρήσης επεκτάσεων σε προγράμματα περιήγησης (browsers), είτε με χρήση άλλων τεχνολογιών) πρέπει το τείχος προστασίας (firewall) να απαγορεύει την εγκατάσταση συνδέσεων VPN, εσωτερικά ή εξωτερικά, χωρίς άδεια.

Χρήση προγράμματος προστασίας από ιούς (Antivirus)

Όλοι οι σταθμοί εργασίας θα πρέπει να διαθέτουν πρόγραμμα προστασίας από ιούς (Antivirus), το οποίο θα εφαρμόζει πολιτική καθημερινής γρήγορης σάρωσης καθώς και πλήρους εβδομαδιαίας. Σε περίπτωση που το πρόγραμμα που χρησιμοποιείται δεν είναι το προσφερόμενο από το Ίδρυμα, που ακολουθεί κεντρικά ορισμένη πολιτική (policy), είναι ευθύνη του διαχειριστή που εγκαθιστά το συγκεκριμένο πρόγραμμα να ρυθμίζει την σχετική πολιτική.

Όσοι σταθμοί εργασίας δεν είναι στην διαχείριση της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης, ο διαχειριστής τους έχει την υποχρέωση να εφαρμόζει σχετική πολιτική.

Παραβίαση ασφαλείας

Η **τεκμηριωμένη απόπειρα** ενός χρήστη ενάντια στην ασφάλεια στα εσωτερικά συστήματα (πληροφοριακά συστήματα, δίκτυα κτλ. του Ιδρύματος ή απομακρυσμένων συστημάτων επιφέρει προσωρινό κλείδωμα του λογαριασμού του χρήστη και περαιτέρω έλεγχο της δραστηριότητάς του. Στην συνέχεια, για την ενεργοποίηση του λογαριασμού του θα πρέπει να καταθέσει έντυπη απολογία την οποία θα αξιολογήσει η Επιτροπή «Στρατηγικού Σχεδιασμού Υποδομών Πληροφορικής και Δικτύων» και θα εισηγηθεί για την αφαίρεση του λογαριασμού ή την επαναλειτουργία του.

Απενεργοποίηση λογαριασμού

Η Διεύθυνση Πληροφορικής και Βιβλιοθήκης έχει το δικαίωμα να προβεί σε αναστολή λειτουργίας λογαριασμών που είναι ανενεργοί για χρονικό διάστημα μεγαλύτερο του ενός (1) έτους. Πριν την αναστολή θα πρέπει να γίνει προσπάθεια επικοινωνίας με τον κάτοχο του λογαριασμού, για την διερεύνηση των προθέσεών του, όσον αφορά την χρήση του λογαριασμού.

Όρια Ηλεκτρονικής Αλληλογραφίας

Για την διασφάλιση της ομαλής λειτουργίας των συστημάτων και ιδιαίτερα της υπηρεσίας ηλεκτρονικής αλληλογραφίας απαγορεύεται η αποστολή μεγάλου αριθμού μηνυμάτων. Το ακριβές του πλήθους των μηνυμάτων που μπορεί να αποστείλει ένας χρήστης θα ορίζεται από την διεύθυνση Πληροφορικής και Βιβλιοθήκης ανάλογα με τις δυνατότητες του εξοπλισμού, τις απαιτήσεις ασφαλείας και τις ανάγκες των διοικητικών υπηρεσιών. Προτείνεται ο αριθμός των παραληπτών να μην υπερβαίνει τους εκατό (150) ανά μήνυμα, προκειμένου να αποφευχθεί κίνδυνος καταχώρησης των διακομιστών ηλεκτρονικής αλληλογραφίας του Πανεπιστημίου μας σε spam lists.

Επιμόρφωση προσωπικού (επισήμανση αναγκαιότητας)

Η επιμόρφωση μελών της κοινότητας είναι το μοναδικό μη τεχνικό μέσο περιορισμού των κινδύνων παραβίασης αλλά ίσως και το σημαντικότερο.
Μέσω της επιμόρφωσης περιορίζεται η πιθανότητα επιτυχούς επίθεσης, με στόχο προσωπικά δεδομένα, αφού οι χρήστες ενημερώνονται για τους κινδύνους και εκπαιδεύονται να τους αποφεύγουν.
Η εκπαίδευση θα παρέχεται μέσω σεμιναρίων ενημέρωσης για νέες τεχνολογίες από τη διεύθυνση Πληροφορικής και Βιβλιοθήκης ή από άλλους φορείς. Κατά την εκπαίδευση πρέπει να γίνεται χρήση προσομοίωσης ρεαλιστικού σεναρίου κυβερνοεπίθεσης.

Άδειες Εξαίρεσης

Σύμφωνα με το Αρθρο 89 του Γ.Κ.Π.Δ δύναται στα Μέλη ΔΕΠ/ΕΔΙΠ/ΕΤΕΠ του πανεπιστημίου να παρεκκλίνουν με την επεξεργασία δεδομένων για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς με το κανονιστικό πλαίσιο λειτουργίας.
Για τις περιπτώσεις που μέλος ΔΕΠ, προϊστάμενος διεύθυνσης ή αυτόνομου τμήματος επιθυμεί να υπάρξει εξαίρεση για κάποιον από τους κανόνες λειτουργίας που αναφέρονται παραπάνω για εκπαιδευτικούς ή ερευνητικούς λόγους ή άλλο αίτιο θα πρέπει να υποβάλει αίτημα όπου θα αναφέρει τους λόγους που χρειάζεται να υλοποιηθεί η συγκεκριμένη εξαίρεση, τον χρήστη που αφορά, τον εξοπλισμό που αφορά, το είδος της εργασίας που θα εκτελείται, το χρονικό διάστημα και κυρίως το εξειδικευμένο προσωπικό που θα αναλάβει την διαχείριση του εξοπλισμού (εφόσον απαιτείται). Στην περίπτωση αυτή ο αιτών αναλαμβάνει την ευθύνη λειτουργίας των συστημάτων και της τήρησης του Γενικού Κανονισμού Προστασίας Δεδομένων.

Η αίτηση θα υποβάλλεται μέσω της πλατφόρμας ΜΙΤΟΣ και θα περιλαμβάνει α) τις εξαιρέσεις που αιτούνται, β) τα στοιχεία του υπεύθυνου υποστήριξης, γ) τον υπεύθυνο λειτουργίας των συστημάτων και τήρησης των κανόνων του Γενικού Κανονισμού Προστασίας Δεδομένων, δ) το χρονικό διάστημα που ζητείται η/οι εξαίρεση/εις, ε) την περιγραφή της αναγκαιότητας που υπάρχει ώστε να υλοποιηθεί η εξαίρεση, στ) την υπηρεσία που αφορά η εξαίρεση.

Αφού ζητηθεί η γνώμη του Υπεύθυνου Προστασίας Δεδομένων και αφού αξιολογηθεί η αίτηση από την Επιτροπή «Επιτροπή «Στρατηγικού Σχεδιασμού Υποδομών Πληροφορικής και Δικτύων» και είναι θετική η απάντηση θα προχωράει η υλοποίηση της εξαίρεσης. Η εξαίρεση θα υλοποιείται με χρονική διάρκεια, το μέγιστο τέσσερα (4) χρόνια και στην συνέχεια θα πρέπει να γίνει ανανέωση της άδειας εξαίρεσης. Αιτία για τον χρονικό περιορισμό της εξαίρεσης είναι ότι υπάρχουν περιπτώσεις υποδομών που αναπτύχθηκαν από

εξειδικευμένο προσωπικό μεν αλλά με το πέρας της συνεργασίας, λήξη συμβάσεων ή άλλους λόγους, οι υποδομές βρέθηκαν χωρίς εποπτεία και συντήρηση. Από την πρότερη εμπειρία, αυτό δημιουργεί κινδύνους για κακόβουλες επιθέσεις εντός και εκτός Ιδρύματος.

Η Επιτροπή ορίζει ότι η αίτηση για εξαιρέσεις γίνεται αποδεκτή όταν αφορά μία από τις ακόλουθες περιπτώσεις:

1) Καινοτόμο έρευνα που δεν μπορεί να υλοποιηθεί στα πλαίσια λειτουργίας των κεντρικών υποδομών
2) Συνεργασία του Πανεπιστημίου με εξωτερικούς Φορείς (Ιδρύματα, Οργανισμούς, Φορείς, κτλ.)
3) Χρήση καινοτόμων εκπαιδευτικών εργαλείων ή τεχνολογίας
4) Χρήση τεχνολογίας τρίτων για διοικητικές εργασίες
5) Δοκιμή τεχνολογιών
6) Άλλες ειδικές περιπτώσεις που πρέπει να τεκμηριωθεί επαρκώς η απαίτηση.

Απαραίτητη προϋπόθεση για την παροχή της εξαίρεσης είναι να υπάρχει ανάληψη ευθύνης, από μόνιμο εκπαιδευτικό ή ερευνητικό ή διοικητικό προσωπικό, της λειτουργίας των συστημάτων και τήρηση των κανόνων του Γενικού Κανονισμού Προστασίας Δεδομένων.

Καλές πρακτικές

α) Λίστες Αλληλογραφίας (Mailing Lists)

Να εφαρμοστεί πολιτική που θα αποτρέπει την δημοσιοποίηση διευθύνσεων ηλεκτρονικής αλληλογραφίας αναίτια. Θα πρέπει όταν χρησιμοποιούνται οι λίστες ηλεκτρονικής αλληλογραφίας α) οι διευθύνσεις των παραληπτών να αποκρύβονται με χρήση της επιλογής "BCC", β) όταν προωθούνται μηνύματα, θα πρέπει να γίνεται αφαίρεση των ηλεκτρονικών διευθύνσεων που εμφανίζονται στο σώμα του νέου κειμένου αν δεν προσθέτουν χρήσιμη πληροφορία, δυσκολεύοντας την ανάγνωση και προκαλώντας δημοσιοποίηση διευθύνσεων.

β) Φιλοξενία Δικτυακού Τόπου

Όποιος, επιθυμεί να χρησιμοποιήσει πόρους του Ιδρύματος για να φιλοξενηθεί ο δικτυακός τόπος εργαστηρίου ή ο προσωπικός, πρέπει να κάνει αίτηση μέσω της πλατφόρμας ΜΙΤΟΣ. Στην αίτηση θα πρέπει να αναφέρουν την χρήση του δικτυακού τόπου, την χρονική διάρκεια της φιλοξενίας, τον υπεύθυνο διαχείρισης του δικτυακού τόπου, τον τύπο της σχέσης του υπεύθυνου με το Ίδρυμα, τα στοιχεία επικοινωνίας (κινητό, e-mail, κτλ.) όλων των εμπλεκομένων.

Η αίτηση αφού αξιολογηθεί από την αρμόδια επιτροπή ή διαχειριστή και είναι θετική η απάντηση, θα παρέχεται φιλοξενία με χρονική διάρκεια που θα εξαρτάται από την χρονική διάρκεια της σύμβασης του προσωπικού που θα υποστηρίζει και θα διαχειρίζεται τον δικτυακό τόπο, και δεν θα μπορεί να ξεπερνάει τα δύο (2) χρόνια. Με το πέρας της χρονικής περιόδου θα πρέπει να γίνεται αίτηση ανανέωσης. Αιτία για τον χρονικό περιορισμό της φιλοξενίας είναι ότι έχει παρατηρηθεί να δημιουργούνται κίνδυνοι από περιπτώσεις δικτυακών τόπων που αναπτύχθηκαν από εξειδικευμένο προσωπικό (π.χ. στα πλαίσια προγραμμάτων) μεν αλλά με το πέρας των συμβάσεων τους ή άλλους λόγους οι δικτυακοί τόποι βρέθηκαν χωρίς εποπτεία και συντήρηση και αποτέλεσαν εύκολο στόχο για παραβίαση

και πραγματοποίηση κακόβουλων ηλεκτρονικών επιθέσεων εντός και εκτός του Πανεπιστημίου.

Ορισμός Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών

Σύμφωνα με το Ν 4961/2022 άρθρο 18 , παράγραφος 1, το ΕΛΜΕΠΑ έχει ορίσει υπεύθυνο και αναπληρωτή υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών.