Εργαστήριο 4.1 – Δημιουργία Μητρώου Κινδύνων

1. Επισκόπηση Εργαστηρίου

1.1 Περιγραφή Εργαστηρίου

Σε αυτό το εργαστήριο θα ανακαλύψετε πώς να δημιουργείτε και να διατηρείτε ένα **μητρώο κινδύνων** — το βασικό εργαλείο για τη διαχείριση κινδύνων και τη διακυβέρνηση της κυβερνοασφάλειας. Σε αντίθεση με τα τεχνικά εργαστήρια που επικεντρώνονται σε εργαλεία συστημάτων ή δικτύων, αυτή η άσκηση δίνει έμφαση στην **ανάλυση, τεκμηρίωση με δομή και στρατηγική σκέψη**.

Θα καταγράψετε τους κινδύνους με οργανωμένο τρόπο, θα αξιολογήσετε την πιθανότητα και τις επιπτώσεις τους, θα ορίσετε υπεύθυνους και θα τους κάνετε **ορατούς και εφαρμόσιμους**. Στο τέλος, θα έχετε το δικό σας λειτουργικό μητρώο κινδύνων — ένα έγγραφο που χρησιμοποιούν οι οργανισμοί καθημερινά για να καθοδηγούν αποφάσεις και να ενισχύουν την προστασία τους.

1.2 Μαθησιακοί Στόχοι

Με την ολοκλήρωση αυτού του εργαστηρίου, θα μπορείτε να:

- Να ορίσετε τι είναι το μητρώο κινδύνων και να εξηγήσετε τον σκοπό του.
- Να αναγνωρίσετε τα **βασικά στοιχεία** ενός μητρώου κινδύνων (περιγραφή κινδύνου, πιθανότητα, επίπτωση, βαθμολογία, υπεύθυνος, κατάσταση).
- Να μετατρέψετε μια πραγματική απειλή σε δομημένη εγγραφή κινδύνου.
- Να εφαρμόσετε ένα **μοντέλο αξιολόγησης κινδύνου** (επίπτωση × πιθανότητα).
- Να δημιουργήσετε εγγραφές κινδύνων τεχνικής φύσης και σχετικές με ανθρώπινα/πολιτικές παραμέτρους.
- Να κατανοήσετε με ποιον τρόπο το μητρώο κινδύνων ενισχύει τις **στρατηγικές αποφάσεις ασφάλειας**.

1.3 Προϋποθέσεις

Πριν ξεκινήσετε αυτό το εργαστήριο, καλό είναι να διαθέτετε:

- Βασική γνώση σχετικά με **απειλές, ευπάθειες και κινδύνους** (από προηγούμενες ενότητες).
- Εξοικείωση με τις **κλίμακες εκτίμησης επίπτωσης και πιθανότητας κινδύνου** (Χαμηλή, Μεσαία, Υψηλή).

- Ένα εργαλείο υπολογιστικών φύλλων (Excel, Google Sheets ή LibreOffice Calc) ή ένας απλός πίνακας σε Word/Docs.
- Ένα σημειωματάριο (ηλεκτρονικό ή χάρτινο) για τις ερωτήσεις αναστοχασμού.

1.4 Εκτιμώμενος Χρόνος Ολοκλήρωσης

Δραστηριότητα	**Εκτιμώμενος Χρόνος**
Εισαγωγή & πλαίσιο	30 λεπτά
Ανασκόπηση βασικών στοιχείων του μητρώου κινδύνων – 45 λεπτά	
Παράδειγμα εφαρμογής (κίνδυνος phishing)	30 λεπτά
Δοκιμασία: Δημιουργήστε 2 παραδείγματα εγγραφών	60 λεπτά
Στρατηγική αξιοποίηση & συζήτηση	30 λεπτά
Σκέψεις & απολογισμός κλείσιμο	15 λεπτά
Συνολικός Εκτιμώμενος Χρόνος	**~3,5–4 ώρες**

Σημείο Ελέγχου

Πριν συνεχίσετε, βεβαιωθείτε ότι:

- Έχετε στη διάθεσή σας ένα εργαλείο υπολογιστικών φύλλων.
- Γνωρίζετε τις βασικές έννοιες των κινδύνων, απειλών και ευπαθειών.
- Είστε έτοιμοι να δημιουργήσετε **τουλάχιστον δύο εγγραφές κινδύνου** (τεχνικές + ανθρώπινες/πολιτικές).
- Μπορείτε να αφιερώσετε περίπου **3,5–4 ώρες** για αυτό το εργαστήριο.

2. Ξεκινώντας

2.1 Τι είναι το Μητρώο Κινδύνων;

Το **μητρώο κινδύνων** είναι ένα οργανωμένο έγγραφο (συχνά σε μορφή υπολογιστικού φύλλου ή βάσης δεδομένων) που καταγράφει, παρακολουθεί και διαχειρίζεται τους κινδύνους ασφαλείας.

Κάθε καταχώρηση στο μητρώο αντιστοιχεί σε έναν συγκεκριμένο κίνδυνο και περιλαμβάνει στοιχεία όπως:

- Ποιος είναι ο κίνδυνος (περιγραφή)
- Από πού προέρχεται (απειλές + ευπάθειες)
- Πόσο πιθανό είναι να συμβεί (πιθανότητα)
- Πόσο σοβαρές θα ήταν οι συνέπειες (επίπτωση)
- Με ποιον τρόπο αντιμετωπίζεται (μέτρα, κατάσταση, υπεύθυνος)

Σκεφτείτε το μητρώο κινδύνων σαν τον **«πύργο ελέγχου»** σας για την παρακολούθηση των κινδύνων — σας προσφέρει μια ολοκληρωμένη εικόνα του τοπίου κινδύνου του οργανισμού σας.

2.2 Γιατί τα Μητρώα Κινδύνων Είναι Σημαντικά στην Κυβερνοασφάλεια

Τα μητρώα κινδύνων δεν είναι απλώς έγγραφα· αποτελούν **στρατηγικά εργαλεία**. Όταν διατηρούνται σωστά, βοηθούν τους οργανισμούς να:

- **Θέστε προτεραιότητες στις ενέργειες** → Τα ζητήματα υψηλού κινδύνου αντιμετωπίζονται πρώτα.
- **Υποστηρίξτε τη λήψη αποφάσεων** → Η διοίκηση διακρίνει ποιοι κίνδυνοι είναι κρίσιμοι.
- **Παρακολουθήστε τις αλλαγές με την πάροδο του χρόνου** → Ελέγξτε αν οι κίνδυνοι αυξάνονται, μειώνονται ή αντιμετωπίζονται.
- **Παρέχετε αποδείξεις για ελέγχους και συμμόρφωση** → Δείξτε μια μεθοδική προσέγγιση στη διαχείριση κινδύνων.

2.3 Λίστα Ελέγχου για τη Ρύθμιση του Εργαστηρίου

Πριν ξεκινήσετε, βεβαιωθείτε ότι έχετε τα εξής:

Ένα εργαλείο λογιστικών φύλλων (όπως Excel, Google Sheets ή LibreOffice Calc).

Ένα κενό πρότυπο μητρώου κινδύνων (ή δημιουργήστε έναν πίνακα με τις στήλες που χρειάζεστε).

Παραδείγματα κινδύνων που θέλετε να καταγράψετε (τεχνικοί, ανθρώπινοι ή σχετικοί με πολιτικές).
Συμβουλευτείτε τις σημειώσεις από προηγούμενες ενότητες (απειλές, ευπάθειες, αξιολόγηση κινδύνου).

Προαιρετικά: Αν εργάζεστε σε ομάδα ή τάξη, να είστε έτοιμοι να **συγκρίνετε τις καταγραφές κινδύνων** — συχνά έτσι προκύπτουν διαφορετικές οπτικές για τον ίδιο κίνδυνο.

Σημείο Ελέγχου

Πριν προχωρήσετε:

- Γνωρίζεις τι είναι το μητρώο κινδύνων και γιατί έχει σημασία;
- Έχεις έτοιμο κάποιο υπολογιστικό φύλλο ή πίνακα για να καταγράψεις πιθανούς κινδύνους;
- Έχεις ξανακοιτάξει τις σημειώσεις σου σχετικά με απειλές, ευπάθειες και αξιολόγηση κινδύνου;

3. Κύρια Στοιχεία του Μητρώου Κινδύνων

3.1 Βασικές Στήλες

Ένα απλό μητρώο κινδύνων μπορεί να έχει διάφορα επίπεδα πολυπλοκότητας, αλλά συνήθως περιλαμβάνει τις παρακάτω στήλες:

1. **Περιγραφή Κινδύνου** → Σαφής αναφορά του κινδύνου (π.χ. «Λειτουργικό σύστημα χωρίς ενημερώσεις μπορεί να αποτελέσει στόχο επίθεσης»).
2. **Επηρεαζόμενο Περιουσιακό Στοιχείο** → Το σύστημα, τα δεδομένα ή η διαδικασία που διατρέχει κίνδυνο (π.χ. «Διακομιστής οικονομικής διαχείρισης»).
3. **Πηγή Απειλής** → Ποιος ή τι μπορεί να προκαλέσει τον κίνδυνο (π.χ. «Εξωτερικός εισβολέας», «Κακή χρήση από εσωτερικό προσωπικό»).
4. **Ευπάθεια** → Το αδύναμο σημείο που επιτρέπει την απειλή (π.χ. «Λογισμικό χωρίς ενημερώσεις»).
5. **Πιθανότητα** → Πόσο συχνά μπορεί να συμβεί ο κίνδυνος (π.χ. Χαμηλή, Μεσαία, Υψηλή).
6. **Επίπτωση** → Ποιες θα είναι οι συνέπειες αν συμβεί ο κίνδυνος (π.χ. Χαμηλή, Μεσαία, Υψηλή).
7. **Βαθμολογία Κινδύνου** → Αριθμητική ή ποιοτική αξιολόγηση (συχνά υπολογίζεται ως **Επίπτωση × Πιθανότητα**).
8. **Στρατηγική Μείωσης** → Τι θα κάνετε για να μειώσετε τον κίνδυνο (π.χ. «Μηνιαία ενημέρωση συστήματος»).
9. **Υπεύθυνος Κινδύνου** → Το άτομο ή η ομάδα που διαχειρίζεται τον κίνδυνο.
10. **Κατάσταση** → Η τρέχουσα φάση (π.χ. Ανοιχτό, Σε εξέλιξη, Μειώθηκε, Έγινε αποδεκτό).

3.2 Πώς λειτουργεί η αξιολόγηση κινδύνου

Η αξιολόγηση κινδύνου βοηθά να δώσουμε προτεραιότητα στους κινδύνους που πρέπει να αντιμετωπιστούν πρώτοι.

- **Ποιοτικό μοντέλο** (συνηθίζεται σε πιο απλά μητρώα):
    - Η πιθανότητα και οι συνέπειες αξιολογούνται ως **Χαμηλή, Μεσαία, Υψηλή**.
    - Ο συνδυασμός τους βοηθά στην κατηγοριοποίηση του κινδύνου (π.χ. «Κρίσιμη», «Μετρία», «Χαμηλή»).
- **Ποσοτικό μοντέλο** (πιο εξελιγμένο):

- Αναθέστε αριθμητικές τιμές (π.χ. Χαμηλό = 1, Μεσαίο = 2, Υψηλό = 3).
- Υπολογίστε Βαθμολογία Κινδύνου = Πιθανότητα × Επίπτωση.
- Παράδειγμα: Πιθανότητα = 3 (Υψηλό), Επίπτωση = 2 (Μεσαίο) → Βαθμολογία = 6.

Ακόμα και μια απλή μέθοδος αξιολόγησης είναι χρήσιμη, καθώς σε αναγκάζει να **συγκρίνεις τους κινδύνους μεθοδικά** και όχι υποκειμενικά.

3.3 Ανακεφαλαίωση: Μετατροπή των δεδομένων κινδύνου σε χρήσιμα πεδία

Στήλη	**Σκοπός**
Περιγραφή Κινδύνου	Αποτυπώνει με σαφήνεια τον κίνδυνο
Επηρεαζόμενο Περιουσιακό Στοιχείο	Δείχνει τι μπορεί να υποστεί ζημιά
Πηγή Απειλής	Προσδιορίζει τον παράγοντα ή την αιτία
Ευπάθεια	Εξηγεί το σημείο αδυναμίας που αξιοποιείται
Πιθανότητα	Αξιολογεί το πόσο πιθανό είναι να συμβεί το συμβάν
Επίπτωση	Βαθμολογεί τη σοβαρότητα των συνεπειών
Βαθμολογία Κινδύνου	Θέτει αντικειμενική προτεραιότητα στους κινδύνους
Στρατηγική Αντιμετώπισης	Περιγράφει τα μέτρα προστασίας
Υπεύθυνος Κινδύνου	Καθορίζει υπευθυνότητα
Κατάσταση	Παρακολουθεί την πρόοδο

Σημείο Ελέγχου

Πριν συνεχίσετε:

- Γνωρίζετε τι σημαίνει κάθε στήλη σε ένα μητρώο κινδύνου;
- Μπορείτε να εξηγήσετε πώς ο συνδυασμός πιθανότητας και αντίκτυπου οδηγεί στη βαθμολογία κινδύνου;
- Νιώθετε έτοιμοι να συμπληρώσετε την πρώτη σας εγγραφή;

4. Παράδειγμα Καταχώρησης – Κίνδυνος Phishing

4.1 Παρουσίαση: Κίνδυνος Επίθεσης Phishing

Ας δημιουργήσουμε ένα παράδειγμα για έναν συχνό οργανωσιακό κίνδυνο: **το προσωπικό να παραπλανηθεί από phishing emails**.

Στήλη	**Ενδεικτική Καταχώρηση**
Περιγραφή Κινδύνου	Υπάλληλοι ίσως κάνουν κλικ σε κακόβουλους συνδέσμους σε phishing emails.
Επηρεαζόμενο Περιουσιακό Στοιχείο	Διαπιστευτήρια εταιρείας και εταιρικοί λογαριασμοί email.
Πηγή Απειλής	Εξωτερικοί επιτιθέμενοι που εκτελούν εκστρατείες phishing.
Τρωτό Σημείο	Έλλειψη ενημέρωσης των χρηστών και ανεπαρκές φιλτράρισμα email.
Πιθανότητα	Υψηλή
Επίπτωση	Υψηλή
Βαθμολογία Κινδύνου	Κρίσιμος (Υψηλή × Υψηλή)
Στρατηγική Αντιμετώπισης	Διεξαγωγή εκπαιδευτικών σεμιναρίων για την ασφάλεια + εφαρμογή εικονικών δοκιμών phishing.
Υπεύθυνος Διαχείρισης Κινδύνου	Ομάδα Ενημέρωσης για την Ασφάλεια
Κατάσταση	Σε εξέλιξη

4.2 Γιατί Αυτό το Παράδειγμα Είναι Σημαντικό

- **Συχνός κίνδυνος** → Το phishing παραμένει ένας από τους βασικούς τρόπους που παραβιάζονται οι οργανισμοί.
- **Ανθρώπινος παράγοντας** → Αναδεικνύει πώς οι άνθρωποι μπορούν να αποτελούν είτε το ισχυρότερο μέτρο προστασίας είτε τον πιο αδύναμο κρίκο.
- **Πρακτική αντιμετώπιση** → Η εκπαίδευση και οι προσομοιώσεις είναι αποτελεσματικά μέτρα για τη μείωση αυτού του κινδύνου.

- **Ορισμός υπευθύνου** → Οι κίνδυνοι παρακολουθούνται μέχρι κάποιος να αναλάβει την ευθύνη για την επίλυσή τους.

4.3 Ανακεφαλαίωση: Πώς να δομήσετε τη δική σας καταχώρηση

Όταν δημιουργείτε δικές σας εγγραφές κινδύνων:

1. Ξεκινήστε με μια **σαφή περιγραφή** (αποφεύγετε ασαφείς όρους όπως «κακή ασφάλεια»).
2. Συνδέστε τον κίνδυνο με το **περιουσιακό στοιχείο, την απειλή και την ευπάθεια**.
3. Αξιολογήστε **πιθανότητα και αντίκτυπο** με συνέπεια (χρησιμοποιήστε Χαμηλό/Μεσαίο/Υψηλό ή αριθμούς).
4. Υπολογίστε μια **βαθμολογία κινδύνου** για να ιεραρχήσετε τις ενέργειές σας.
5. Καθορίστε μια **πραγματική στρατηγική αντιμετώπισης**, όχι απλώς «θα το φτιάξουμε αργότερα».
6. Ορίστε έναν **υπεύθυνο κινδύνου** ώστε να είναι ξεκάθαρη η λογοδοσία.

Σημείο ελέγχου

Πριν συνεχίσετε:

- Μπορείς να εξηγήσεις γιατί το phishing αξιολογείται ως Υψηλή Πιθανότητα και Υψηλή Επίπτωση;
- Βλέπεις πώς το μέτρο αντιμετώπισης στοχεύει άμεσα την ευπάθεια;
- Είσαι έτοιμος να δημιουργήσεις τις δικές σου εγγραφές στο μητρώο κινδύνων;

5. Εργαστηριακή Πρόκληση – Δημιουργήστε τις δικές σας Καταχωρήσεις

5.1 Δημιουργία Καταχώρησης Τεχνικού Κινδύνου

Η πρώτη σας αποστολή είναι να εντοπίσετε και να καταγράψετε έναν **τεχνικό κίνδυνο**.
Παραδείγματα:

- Ένα **μη ενημερωμένο σύστημα** ευάλωτο σε γνωστές επιθέσεις.
- Ένα **ανοιχτό θύρα δικτύου** προσβάσιμη από το διαδίκτυο.
- Ένας **λανθασμένος κανόνας firewall** που εκθέτει υπηρεσίες.

Για τον κίνδυνο που επιλέξατε, συμπληρώστε όλα τα πεδία:

Στήλη	**Η Καταχώρησή σας**
Περιγραφή Κινδύνου	...
Επηρεαζόμενο Περιουσιακό Στοιχείο	...
Πηγή Απειλής	...
Τρωτό Σημείο	...
Πιθανότητα	...
Επίπτωση	...
Βαθμολογία Κινδύνου	...
Στρατηγική Αντιμετώπισης	...
Υπεύθυνος Κινδύνου	...
Κατάσταση	...

5.2 Δημιουργία Εγγραφής Κινδύνου Ανθρώπινου Παράγοντα ή Πολιτικής

Έπειτα, καταγράψτε έναν **μη τεχνικό κίνδυνο** που σχετίζεται με άτομα, διαδικασίες ή πολιτικές. Παραδείγματα:

- **Αδύναμη χρήση κωδικών πρόσβασης** από το προσωπικό.

- **Κοινή χρήση στοιχείων εισόδου**από πολλά μέλη προσωπικού.
- **Απουσία διαδικασίας ένταξης/αποχώρησης**στη διαχείριση λογαριασμών.

Ακολουθήστε την ίδια δομή:

Στήλη	**Η καταχώρισή σας**
Περιγραφή Κινδύνου	…
Επηρεαζόμενο Περιουσιακό Στοιχείο	…
Πηγή Απειλής	…
Ευπάθεια	…
Πιθανότητα	…
Επίπτωση	…
Βαθμός Κινδύνου	…
Στρατηγική αντιμετώπισης	…
Υπεύθυνος κινδύνου	…
Κατάσταση	…

5.3 Ερωτήσεις Αναστοχασμού

Αφού ολοκληρώσετε τις εγγραφές σας, σκεφτείτε τα εξής:

1. Ποιον κίνδυνο αξιολογήσατε ως πιο σημαντικό — τον τεχνικό ή αυτόν που αφορά ανθρώπους/πολιτικές; Γιατί;
2. Σας ήταν πιο εύκολο να περιγράψετε την **τεχνική πλευρά** (ευπάθειες, στοιχεία) ή την **ανθρώπινη/πολιτική πλευρά** (διαδικασίες, συμπεριφορές);
3. Αν έπρεπε να **παρουσιάσετε τις εγγραφές σας στη διοίκηση**, πώς θα εξηγούσατε γιατί αυτοί οι κίνδυνοι χρειάζονται προσοχή;
4. Τι ενέργειες θα μπορούσατε να κάνετε μέσα στις επόμενες 30 ημέρες για να μειώσετε έναν από αυτούς τους κινδύνους;

Σημείο Ελέγχου

Πριν προχωρήσετε:

- Έχετε καταχωρίσει τουλάχιστον **δύο ολοκληρωμένες εγγραφές κινδύνων**;
- Έχετε αποδώσει **τιμές πιθανοτήτων και επιπτώσεων** με συνέπεια;
- Έχετε συμπεριλάβει μια **σαφή στρατηγική αντιμετώπισης** για κάθε κίνδυνο;
- Έχετε ορίσει **υπεύθυνο για τον κίνδυνο** (ακόμη και θεωρητικό);

6. Αξιοποίηση Μητρώων Κινδύνου για Στρατηγικές Αποφάσεις

6.1 Ιεράρχηση Υψηλών και Χαμηλών Κινδύνων

Ένα μητρώο κινδύνου δεν είναι απλώς μια λίστα — είναι εργαλείο για **προτεραιοποίηση ενεργειών**.

- **Οι υψηλού κινδύνου ενέργειες** (υψηλή πιθανότητα + υψηλός αντίκτυπος) πρέπει να αντιμετωπίζονται πρώτες.
- **Οι μεσαίου κινδύνου ενέργειες** ίσως χρειάζονται παρακολούθηση ή μερική αντιμετώπιση.
- **Οι χαμηλού κινδύνου ενέργειες** μπορεί να θεωρούνται αποδεκτές και να καταγράφονται ως «αποδεκτοί κίνδυνοι».

Αυτό βοηθά τις ομάδες να μην σπαταλούν χρόνο σε κάθε μικρό πρόβλημα, αλλά να επικεντρώνονται εκεί που έχει τη μεγαλύτερη σημασία.

6.2 Παρακολούθηση Ρίσκου με την Πάροδο του Χρόνου

Οι κίνδυνοι δεν παραμένουν σταθεροί. Εμφανίζονται νέες ευπάθειες, οι απειλές αλλάζουν, και τα μέτρα μείωσης μειώνουν τα επίπεδα κινδύνου. Το μητρώο κινδύνων σας βοηθά να:

- Ενημερώνετε την **κατάσταση** (Ανοιχτό → Σε εξέλιξη → Μειώθηκε/Αποδεκτό).
- Καταγράφετε πότε εισήχθη κάθε κίνδυνος και πότε ενημερώθηκε.
- Εντοπίζετε τάσεις, όπως αν τα περιστατικά phishing μειώνονται μετά από εκπαίδευση ή αν τα μη ενημερωμένα συστήματα παραμένουν πρόβλημα.

6.3 Αναφορά Κινδύνων στη Διοίκηση

Τα στελέχη και οι διευθυντές συνήθως δε θέλουν να βλέπουν τεχνικές λεπτομέρειες — ενδιαφέρονται όμως ιδιαίτερα για **συνοπτικές παρουσιάσεις των κινδύνων**.

Το μητρώο κινδύνων σας δίνει τη δυνατότητα να:

- Αναδείξετε τους **5 πιο κρίσιμους κινδύνους** σε κατανοητή γλώσσα.
- Δείξετε πρόοδο παρουσιάζοντας κινδύνους που μετακινήθηκαν από «Κρίσιμος» σε «Μεσαίος».
- Παραθέσετε αποδείξεις ότι οι κίνδυνοι έχουν ανατεθεί και διαχειρίζονται σωστά.

6.4 Συμμόρφωση και Υποστήριξη Ελέγχων

Τα μητρώα κινδύνων αποτελούν επίσης βασικό εργαλείο για κανονιστικά πλαίσια όπως:

- **ISO 27001** (Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών)
- **Πλαίσιο Κυβερνοασφάλειας NIST**
- **GDPR** (για κινδύνους που σχετίζονται με την προστασία δεδομένων)

Οι ελεγκτές συχνά ζητούν να δουν το μητρώο κινδύνων, επειδή:

- Αποδεικνύει ότι οι κίνδυνοι είναι **καταγεγραμμένοι** και **παρακολουθούνται ενεργά**.
- Δείχνει πως ο οργανισμός δεν αγνοεί γνωστές απειλές.
- Συνδέει τους κινδύνους με τα μέτρα αντιμετώπισης και την ανάληψη ευθύνης.

Σημείο ελέγχου

Πριν συνεχίσετε:

- Μπορείτε να περιγράψετε πώς το μητρώο κινδύνων βοηθά στην ιεράρχηση των μέτρων ασφάλειας;
- Κατανοείτε πώς το μητρώο κινδύνων συμβάλλει στην αναφορά και τη συμμόρφωση;
- Έχετε ενημερώσει τις δικές σας εγγραφές με **κατάσταση** και **υπευθυνότητα** ώστε να αποτυπώνουν πραγματική πρόοδο;

7. Ανασκόπηση

7.1 Βασικά Συμπεράσματα

Σε αυτό το εργαστήριο, καταφέρατε να:

Μάθετε τι είναι το **μητρώο κινδύνων** και γιατί είναι σημαντικό.

Ανακαλύψετε τα **βασικά στοιχεία** (περιγραφή, περιουσιακό στοιχείο, απειλή, ευπάθεια, πιθανότητα, επίπτωση, βαθμολογία, υπεύθυνος, κατάσταση).

Αναλύσετε ένα **παράδειγμα phishing** για να κατανοήσετε πώς οργανώνονται οι κίνδυνοι.

Δημιουργήσατε **δικές σας καταχωρήσεις κινδύνων** (τεχνικές και ανθρώπινες/πολιτικές).

Κατανοήσατε πώς το μητρώο κινδύνων συμβάλλει στην **ιεράρχηση, την παρακολούθηση, την αναφορά και τη συμμόρφωση**.

7.2 Δεξιότητες που αποκτήσατε

Με την ολοκλήρωση αυτού του εργαστηρίου, έχετε αποκτήσει πρακτική εμπειρία σε:

- Μετατροπή απειλών και ευπαθειών σε δομημένες καταχωρήσεις κινδύνων.
- Εφαρμογή **βαθμολόγησης πιθανοτήτων × επιπτώσεων** για την προτεραιοποίηση των κινδύνων.
- Ανάθεση υπευθύνων και παρακολούθηση της κατάστασης των κινδύνων.
- Χρήση του μητρώου κινδύνων ως **στρατηγικό εργαλείο**, όχι απλώς ως τεκμηρίωση.

7.3 Επόμενο Βήμα: Τελικό Κουίζ Ενότητας 4

Έφτασες στο τέλος της **Ενότητας 4: Διαχείριση Κινδύνων και Πολιτικές Ασφάλειας**.
Σειρά έχει το **Τελικό Κουίζ Ενότητας 4**, όπου θα δοκιμαστούν οι γνώσεις σου σχετικά με:

- Βασικές έννοιες κινδύνου (απειλές, ευπάθειες, περιουσιακά στοιχεία, έλεγχοι).
- Τον ρόλο της διακυβέρνησης και των πολιτικών στην κυβερνοασφάλεια.
- Τη πρακτική αξιοποίηση του **μητρώου κινδύνων**.

Τελικός Έλεγχος

Πριν ξεκινήσεις το κουίζ:

- Έχετε αποθηκεύσει τουλάχιστον δύο πλήρεις εγγραφές κινδύνου στο μητρώο σας;
- Μπορείτε να εξηγήσετε πώς υπολογίζεται μια βαθμολογία κινδύνου;
- Μπορείτε να περιγράψετε τον τρόπο με τον οποίο το μητρώο κινδύνων ενισχύει τη στρατηγική ασφάλειας;

Αν ναι — είστε έτοιμοι για το τεστ!

8. Παράρτημα

8.1 Πρότυπο Μητρώου Κινδύνων (Διάταξη Υπολογιστικού Φύλλου)

Κωδικός Κινδύνου	Περιγραφή Κινδύνου	Επηρεαζόμενο Περιουσιακό Στοιχείο	Πηγή Απειλής	Ευπάθεια	Πιθανότητα	Επίπτωση	Σκορ Κινδύνου	Στρατηγική Αντιμετώπισης	Υπεύθυνος	Κατάσταση
R-001	Υπάλληλοι ενδέχεται να πατήσουν σε παραπλανητικούς συνδέσμους	Διαπιστευτήρια email	Εξωτερικός εισβολέας	Έλλειψη ενημέρωσης	Υψηλό	Υψηλό	Εκπαίδευση ευαισθητοποίησης + Προσομοιώσεις phishing υψηλής επικινδυνότητας		Ομάδα Εκπαίδευσης Ασφάλειας	Σε εξέλιξη
R-002	Μη ενημερωμένος διακομιστής ευάλωτος σε CVE	Διακομιστής οικονομικών	Εκμετάλλευση κακόβουλου λογισμικού	Απουσία ενημερώσεων ασφαλείας	Μεσαίο	Υψηλό	Κύκλος μηνιαίας διαχείρισης ενημερώσεων		Ομάδα Υποδομών Πληροφορικής	Ανοιχτό
R-003	Αδύναμοι κωδικοί πρόσβασης επαναχρησιμοποιούνται από το προσωπικό	Εσωτερικοί λογαριασμοί	Κακή χρήση από εσωτερικούς χρήστες	Ανεπαρκής πολιτική για κωδικούς πρόσβασης	Υψηλό	Μεσαίο	Υψηλό	Εφαρμογή αυστηρών πολιτικών για κωδικούς πρόσβασης και MFA	IAM (Ομάδα Διαχείρισης Ταυτοτήτων)	Σε εξέλιξη

8.2 Ενδεικτικές Κατηγορίες Κινδύνων

Όταν εντοπίζετε κινδύνους, εξετάστε τις παρακάτω κατηγορίες:

- **Τεχνικοί Κίνδυνοι**: μη ενημερωμένα συστήματα, ανοιχτές θύρες, μη ασφαλείς ρυθμίσεις.
- **Ανθρώπινοι Κίνδυνοι**: phishing, ασθενείς κωδικοί πρόσβασης, κατάχρηση από εσωτερικούς χρήστες.
- **Κίνδυνοι Πολιτικών/Διαδικασιών**: έλλειψη πολιτικών, ανεπάρκεια εκπαίδευσης, αδύναμη διαδικασία εισαγωγής/αποχώρησης.
- **Κίνδυνοι από Τρίτους**: παραβιάσεις προμηθευτών, επιθέσεις στην εφοδιαστική αλυσίδα, εξωτερικές υπηρεσίες.

Χρήσιμη συμβουλή: Προσπαθήστε να καταγράψετε **τουλάχιστον έναν κίνδυνο ανά κατηγορία** για πιο ολοκληρωμένο μητρώο.

8.3 Συνηθισμένα Λάθη προς Αποφυγή

Όταν οι φοιτητές δημιουργούν για πρώτη φορά μητρώα κινδύνων, συχνά:

- **Γράφουν αόριστες περιγραφές κινδύνων** (π.χ., «θέμα ασφάλειας» αντί για «μη ενημερωμένη ευπάθεια λειτουργικού συστήματος»).

- **Αν δεν ορίσετε υπεύθυνο** → κανείς δεν αναλαμβάνει ευθύνη και δεν υπάρχει πρόοδος.
- **Υπερεκτιμάτε όλα ως υψηλού κινδύνου** → η ιεράρχηση χάνει το νόημά της.
- **Αμελείτε την ενημέρωση** → τα μητρώα πρέπει να προσαρμόζονται σε νέες απειλές.
- **Μην μπερδεύετε τις απειλές με τις ευπάθειες** → σημειώστε:
    - Απειλή = πιθανός κίνδυνος (π.χ. εισβολέας).
    - Ευπάθεια = αδυναμία που μπορεί να αξιοποιηθεί (π.χ. ανοιχτή θύρα).

8.4 Επιπλέον Πηγές

- **Πλαίσιο Κυβερνοασφάλειας NIST (CSF)** – Κατευθυντήριες γραμμές για τη διαχείριση κινδύνου: https://www.nist.gov/cyberframework
- **ISO/IEC 27005** – Διεθνές πρότυπο για τη διαχείριση κινδύνων στην ασφάλεια πληροφοριών.
- **Οδηγίες Διαχείρισης Κινδύνων ENISA** – Πρακτικοί οδηγοί από τον Ευρωπαϊκό Οργανισμό για την Κυβερνοασφάλεια.
- **Μεθοδολογία Αξιολόγησης Κινδύνων OWASP** – Για την αξιολόγηση κινδύνων σε εφαρμογές και ιστό: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Προτεινόμενη Ανάγνωση: *Managing Risk in Information Systems* (Darril Gibson) — μια προσιτή εισαγωγή στη δημιουργία και διατήρηση μητρώων κινδύνων.