Παιχνίδι ρόλων: Εφαρμογή των αρχών του GDPR

Στόχος:
Οι συμμετέχοντες θα συμμετάσχουν σε μια άσκηση ρόλων για την προσομοίωση της εφαρμογής των αρχών του ΓΚΠΔ ως απάντηση σε μια παραβίαση δεδομένων. Στόχος είναι να κατανοήσουν πώς να προστατεύουν τα δεδομένα, να συμμορφώνονται με τον ΓΚΠΔ και να λαμβάνουν τα κατάλληλα μέτρα σε περίπτωση παραβίασης.

Σενάριο:

Ένας φανταστικός οργανισμός, η **SecureFin**, διαχειρίζεται ευαίσθητα δεδομένα πελατών, συμπεριλαμβανομένων οικονομικών πληροφοριών και προσωπικών αναγνωριστικών στοιχείων. Έχει σημειωθεί παραβίαση δεδομένων, εκθέτοντας αυτές τις ευαίσθητες πληροφορίες. Η εταιρεία πρέπει να λάβει άμεσα μέτρα για την προστασία των δεδομένων, να συμμορφωθεί με τους κανονισμούς του GDPR και να ενημερώσει τα θιγόμενα μέρη.

Διάρκεια:

30 λεπτά

Απαιτούμενα υλικά:

1. **Χειρόγραφα σεναρίου ή διαφάνεια παρουσίασης**:
    - Σύντομη περιγραφή του σεναρίου παραβίασης δεδομένων (SecureFin), των σχετικών αρχών του ΓΚΠΔ και των ρόλων των συμμετεχόντων.
2. **Κάρτες ανάθεσης ρόλων**:
    - Προετοιμασμένες κάρτες ή οδηγίες που αναθέτουν σε κάθε συμμετέχοντα έναν ρόλο (υπεύθυνος προστασίας δεδομένων, νομικός σύμβουλος, ειδικός ασφάλειας πληροφορικής, εκπρόσωπος εξυπηρέτησης πελατών).
3. **Σημειωματάρια και στυλό** ή **φορητοί υπολογιστές/tablets** για να σημειώνουν οι συμμετέχοντες τις απαντήσεις τους, τα βήματα για τη συμμόρφωση και τα σχέδια δράσης.
4. **Χρονοδιακόπτης**:
    - Για να παρακολουθείτε τη δραστηριότητα των 30 λεπτών.
5. **Προβολέας ή πίνακας** (προαιρετικά):

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

- Για τους συμμετέχοντες να μοιραστούν τα τελικά τους σχέδια δράσης, εάν εργάζονται σε ομάδες.

Οδηγίες:

1. **Εντοπισμός παραβιάσεων GDPR**
   - Οι συμμετέχοντες πρέπει να προσδιορίσουν τι πήγε στραβά στο σενάριο (π.χ. έλλειψη κρυπτογράφησης, μη εξουσιοδοτημένη πρόσβαση).
   - Καθορίστε πώς συνέβη η παραβίαση και ποιες αρχές του ΓΚΠΔ παραβιάστηκαν (π.χ. συγκατάθεση, ελαχιστοποίηση δεδομένων, διαφάνεια, λογοδοσία).
2. **Περιγράψτε τα βήματα για τη συμμόρφωση**
   - **Ειδοποίηση πελατών**: Ειδοποίηση των επηρεαζόμενων πελατών εντός 72 ωρών, εξηγώντας την παραβίαση και τα μέτρα που λαμβάνονται.
   - **Εσωτερική αναθεώρηση**: Διερεύνηση της αιτίας της παραβίασης και επανεξέταση των πρωτοκόλλων ασφαλείας.
   - **Πρόληψη μελλοντικών περιστατικών**: Εφαρμόστε μέτρα ασφαλείας, πολιτικές διακυβέρνησης δεδομένων και εκπαίδευση του προσωπικού για την πρόληψη μελλοντικών παραβιάσεων.
3. **Ανάθεση ρόλων**
   - **Υπεύθυνος προστασίας δεδομένων (DPO)**: Ηγείται της έρευνας και διασφαλίζει τη συμμόρφωση με τον GDPR.
   - **Νομικός Σύμβουλος**: Συμβουλεύει σχετικά με τις νομικές ευθύνες και διασφαλίζει ότι η ενημέρωση των πελατών συμμορφώνεται με τον ΓΚΠΔ.
   - **Ειδικός ασφάλειας πληροφορικής**: Ερευνά την παραβίαση, εντοπίζει τα τρωτά σημεία και προτείνει βελτιώσεις στην ασφάλεια.
   - **Εκπρόσωπος εξυπηρέτησης πελατών**: Επικοινωνεί με τους πληγέντες πελάτες, εξηγώντας τις ενέργειες της εταιρείας και καθησυχάζοντάς τους.

Ροή δραστηριοτήτων:

1. Εισαγωγή (5 λεπτά)

- Ο συντονιστής παρουσιάζει το σενάριο, εξηγώντας την παραβίαση και τον στόχο της δραστηριότητας παιχνιδιού ρόλων.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

2. Ανάθεση ρόλων (5 λεπτά)

- Οι συμμετέχοντες κατανέμονται σε ρόλους (DPO, Νομικός Σύμβουλος, Ειδικός Ασφάλειας ΤΠ, Εκπρόσωπος Εξυπηρέτησης Πελατών).

3. Ομαδική συζήτηση (15 λεπτά)

- Οι συμμετέχοντες, στους ρόλους τους, συνεργάζονται για να:
    - Εντοπισμός παραβιάσεων GDPR.
    - Σχεδιάστε την αντίδραση της εταιρείας, συμπεριλαμβανομένης της ενημέρωσης των πελατών, της διενέργειας εσωτερικής επανεξέτασης και της πρόληψης μελλοντικών παραβιάσεων.
    - Συζητήστε τις ευθύνες τους στο πλαίσιο των ρόλων τους.

4. Παρουσίαση (5 λεπτά)

- Κάθε ομάδα παρουσιάζει το σχέδιο δράσης της στους υπόλοιπους συμμετέχοντες.
- Ο συντονιστής και οι άλλοι συμμετέχοντες μπορούν να υποβάλουν ερωτήσεις ή να παράσχουν πρόσθετα σχόλια.

Αναμενόμενα αποτελέσματα:

- Σαφέστερη κατανόηση των **αρχών του ΓΚΠΔ** και του τρόπου εφαρμογής τους σε ένα πραγματικό σενάριο.
- Κατανόηση της σημασίας της **διατμηματικής συνεργασίας** για την αντιμετώπιση των παραβιάσεων δεδομένων (νομικά, πληροφορική, προστασία δεδομένων και εξυπηρέτηση πελατών).
- Πρακτικές στρατηγικές για την αντιμετώπιση παραβιάσεων δεδομένων και τη διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Παράδειγμα ολοκληρωμένης δραστηριότητας παιχνιδιού ρόλων: GDPR

Σενάριο: SecureFin, μια εταιρεία χρηματοοικονομικών υπηρεσιών, υπέστη παραβίαση δεδομένων, εκθέτοντας οικονομικές πληροφορίες και προσωπικά στοιχεία ταυτότητας πελατών. Η παραβίαση συνέβη λόγω μιας μη ασφαλούς βάσης δεδομένων στην οποία είχαν πρόσβαση μη εξουσιοδοτημένα άτομα. Η εταιρεία πρέπει να αντιδράσει σύμφωνα με τις αρχές του ΓΚΠΔ.

Βήμα 1: Εντοπισμός παραβιάσεων GDPR

- **Παραβίαση της εμπιστευτικότητας**:
  Η βάση δεδομένων που περιείχε ευαίσθητες χρηματοοικονομικές πληροφορίες δεν είχε ασφαλιστεί σωστά, με αποτέλεσμα να υπάρξει μη εξουσιοδοτημένη πρόσβαση. Αυτό παραβιάζει την αρχή της **εμπιστευτικότητας**
  του ΓΚΠΔ, καθώς η εταιρεία απέτυχε να προστατεύσει τα προσωπικά δεδομένα από μη εξουσιοδοτημένα άτομα.
- **Έλλειψη διαφάνειας**:
  παραβιάζοντας την αρχή **της διαφάνειας**
  του ΓΚΠΔ, η οποία απαιτεί από τις επιχειρήσεις να ενημερώνουν τα άτομα αμέσως για κάθε παραβίαση που επηρεάζει τα προσωπικά τους δεδομένα.
- **Συναίνεση**:
  Αυτό αποτελεί παραβίαση της αρχής της **συγκατάθεσης** σύμφωνα με τον ΓΚΠΔ.

Βήμα 2: Βήματα συμμόρφωσης

1. **Ειδοποίηση πελατών**:
   - **Χρονοδιάγραμμα κοινοποίησης**:
     SecureFin πρέπει να ειδοποιήσει όλους τους πελάτες που επηρεάζονται εντός **72 ωρών** από την ανακάλυψη της παραβίασης.
   - **Μήνυμα προς τους πελάτες**:
     "Αγαπητέ πελάτη, με λύπη μας σας ενημερώνουμε ότι σημειώθηκε παραβίαση δεδομένων, η οποία επηρέασε τις προσωπικές και οικονομικές σας πληροφορίες. Λαμβάνουμε άμεσα μέτρα για την ασφάλεια των δεδομένων σας και συνεργαζόμαστε στενά με τις ρυθμιστικές αρχές για την επίλυση του ζητήματος. Παρακαλούμε επικοινωνήστε με τη γραμμή βοήθειας για περαιτέρω βοήθεια".
2. **Εσωτερική αναθεώρηση**:

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

- **Ανασκόπηση Τμήματος Πληροφορικής**:
  Απαιτείται ενδελεχής επανεξέταση όλων των πρωτοκόλλων ασφαλείας της βάσης δεδομένων. Η ομάδα ασφάλειας του IT θα διερευνήσει πώς συνέβη η παραβίαση και θα εντοπίσει τυχόν ευπάθειες.

- **Έλεγχος των εντύπων συγκατάθεσης**:
  Η νομική ομάδα θα επανεξετάσει όλες τις μεθόδους συλλογής δεδομένων για να διασφαλίσει ότι ελήφθη η κατάλληλη συγκατάθεση από τους πελάτες. Για δεδομένα που συλλέγονται χωρίς συγκατάθεση, η εταιρεία πρέπει να διαγράψει ή να ανωνυμοποιήσει τα δεδομένα.

3. **Πρόληψη μελλοντικών παραβιάσεων**:

   - **Εφαρμογή κρυπτογράφησης**:
     για την αποφυγή μη εξουσιοδοτημένης πρόσβασης.

   - **Έλεγχος πρόσβασης βάσει ρόλων**:
     Περιορισμός της πρόσβασης σε ευαίσθητα δεδομένα με βάση τους ρόλους των εργαζομένων, περιορίζοντας τον αριθμό των ατόμων που μπορούν να έχουν πρόσβαση σε εμπιστευτικές πληροφορίες.

   - **Εκπαίδευση προσωπικού**:
     Εκπαίδευση για τη συμμόρφωση με τον ΓΚΠΔ για όλους τους υπαλλήλους, ώστε να διασφαλιστεί ότι κατανοούν τις αρχές και τις ευθύνες τους όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα.

Βήμα 3: Ρόλοι και αρμοδιότητες

1. **Υπεύθυνος προστασίας δεδομένων (DPO)**:

   - Ο ΥΠΔ είναι υπεύθυνος για το συντονισμό της αντίδρασης στην παραβίαση, τη διασφάλιση της ενημέρωσης των πελατών και τη σύνδεση με τις ρυθμιστικές αρχές για την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ.

2. **Νομικός Σύμβουλος**:

   - Η νομική ομάδα διασφαλίζει ότι η κοινοποίηση προς τους πελάτες συμμορφώνεται με τον ΓΚΠΔ και συμβουλεύει την εταιρεία σχετικά με τις νομικές υποχρεώσεις και τις πιθανές ευθύνες της.

3. **Ειδικός ασφάλειας πληροφορικής**:

   - Η ομάδα πληροφορικής διερευνά τον τρόπο με τον οποίο συνέβη η παραβίαση, διασφαλίζει το σύστημα και εφαρμόζει ισχυρότερα μέτρα ασφαλείας για την αποτροπή μελλοντικών περιστατικών.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

4. **Εκπρόσωπος εξυπηρέτησης πελατών**:
    - Επικοινωνεί με τους επηρεαζόμενους πελάτες, παρέχοντας πληροφορίες και υποστήριξη και αντιμετωπίζοντας τυχόν ανησυχίες των πελατών σχετικά με την ασφάλεια των δεδομένων τους.

Τελειωμένο παράδειγμα του αποτελέσματος του παιχνιδιού ρόλων:

Σχέδιο δράσης:

- **Εντοπισμός παραβίασης**: Η μη ασφαλής βάση δεδομένων επέτρεψε μη εξουσιοδοτημένη πρόσβαση σε οικονομικές πληροφορίες πελατών.
- **Βήματα συμμόρφωσης**:
    1. **Ειδοποιήστε τους πελάτες** εντός 72 ωρών.
    2. **Εσωτερική αναθεώρηση**: Ενίσχυση της ασφάλειας της βάσης δεδομένων, αναθεώρηση των εντύπων συγκατάθεσης.
    3. **Πρόληψη**: Κρυπτογράφηση ευαίσθητων δεδομένων, εφαρμογή ελέγχων πρόσβασης και εκπαίδευση του προσωπικού.
- **Εκχωρημένοι ρόλοι**:
    - **DPO**: Συντονίζει την αντίδραση και διασφαλίζει τη συμμόρφωση.
    - **Νομικός Σύμβουλος**: Διασφαλίζει ότι η κοινοποίηση είναι σύμφωνη με τον GDPR.
    - **Ειδικός ασφάλειας πληροφορικής**: Ερευνά την παραβίαση και ενισχύει τα μέτρα ασφαλείας.
    - **Εξυπηρέτηση πελατών**: Καθησυχάζει τους πελάτες και παρέχει υποστήριξη.

Πρόσθετα σενάρια για παιχνίδι ρόλων

Σενάριο 2: Παραβίαση δεδομένων εταιρείας λιανικού εμπορίου (πλατφόρμα ηλεκτρονικού εμπορίου)

Πλαίσιο:
Μια μεγάλη πλατφόρμα ηλεκτρονικού εμπορίου, η **ShopAll**, υφίσταται παραβίαση δεδομένων, εκθέτοντας στοιχεία πληρωμών πελατών, συμπεριλαμβανομένων πληροφοριών πιστωτικών καρτών και προσωπικών διευθύνσεων. Η παραβίαση συνέβη μέσω μιας επίθεσης phishing σε έναν από τους υπαλλήλους της εταιρείας, δίνοντας στους χάκερ πρόσβαση στο σύστημα επεξεργασίας πληρωμών.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Βήματα για τους συμμετέχοντες:

1. **Εντοπισμός παραβιάσεων**:
    - Συμβιβασμός των στοιχείων πληρωμής των πελατών (παραβίαση εμπιστευτικότητας).
    - Δεν υπάρχει άμεση ενημέρωση των πελατών (θέμα διαφάνειας).
2. **Συμμόρφωση**:
    - Ειδοποιήστε τους πελάτες εντός 72 ωρών.
    - Διερεύνηση της επίθεσης phishing και ενίσχυση της εκπαίδευσης των εργαζομένων σε θέματα κυβερνοασφάλειας.
    - Εφαρμόστε έλεγχο ταυτότητας δύο παραγόντων (2FA) για την πρόσβαση στην επεξεργασία πληρωμών.
3. **Πρόληψη**:
    - Εκπαίδευση ευαισθητοποίησης των εργαζομένων σε θέματα phishing.
    - Ασφάλεια πολλαπλών επιπέδων για συστήματα πληρωμών, συμπεριλαμβανομένης της κωδικοποίησης των στοιχείων της κάρτας.

Ρόλοι:
DPO, Νομικός Σύμβουλος, Ειδικός Πληροφορικής, Υποστήριξη Πελατών.

Σενάριο 3: Παραβίαση δεδομένων παρόχου υγειονομικής περίθαλψης (νοσοκομειακά αρχεία)

Πλαίσιο:
Το νοσοκομείο **HealthCare** Central υπέστη παραβίαση κατά την οποία μη εξουσιοδοτημένα άτομα απέκτησαν πρόσβαση σε ιατρικά αρχεία ασθενών, συμπεριλαμβανομένων διαγνώσεων και σχεδίων θεραπείας. Η παραβίαση οφειλόταν σε αδύναμο έλεγχο πρόσβασης στη βάση δεδομένων των ασθενών τους.

Βήματα για τους συμμετέχοντες:

1. **Εντοπισμός παραβιάσεων**:
    - Έκθεση ιατρικών αρχείων (παραβίαση εμπιστευτικότητας και ευαισθησίας).
    - Έλλειψη κατάλληλου ελέγχου πρόσβασης (ζήτημα λογοδοσίας).
2. **Συμμόρφωση**:
    - Ειδοποιήστε τους ασθενείς και τις ρυθμιστικές αρχές για την παραβίαση.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

- Διεξαγωγή εσωτερικής επανεξέτασης των πολιτικών πρόσβασης σε βάσεις δεδομένων.

3. **Πρόληψη**:
   - Εφαρμογή πρόσβασης σε δεδομένα ασθενών βάσει ρόλων.
   - Ενισχύστε την ασφάλεια μέσω κρυπτογράφησης και τακτικών ελέγχων του συστήματος.

Ρόλοι:
Ιατρικός Διαχειριστής: DPO, Νομικός Σύμβουλος, Ειδικός Ασφάλειας Πληροφορικής.

Σενάριο 4: Διαρροή δεδομένων τραπεζικού ιδρύματος (χρηματοπιστωτικές υπηρεσίες)

Πλαίσιο:
Ένα τραπεζικό ίδρυμα, η **GlobalBank**, υφίσταται παραβίαση όπου τα στοιχεία των λογαριασμών των πελατών, συμπεριλαμβανομένου του ιστορικού των συναλλαγών, αποκτήθηκαν και διέρρευσαν στο διαδίκτυο λόγω απειλής εκ των έσω (ένας δυσαρεστημένος υπάλληλος).

Βήματα για τους συμμετέχοντες:

1. **Εντοπισμός παραβιάσεων**:
   - Απειλή εκ των έσω που εκθέτει ευαίσθητα οικονομικά δεδομένα πελατών.
   - Παραβίαση της εμπιστευτικότητας και της λογοδοσίας.
2. **Συμμόρφωση**:
   - Ειδοποιήστε τους πελάτες και ενημερώστε τους για τα μέτρα που λαμβάνονται.
   - Διεξαγωγή εσωτερικής έρευνας σχετικά με την πρόσβαση των εργαζομένων σε ευαίσθητα δεδομένα.
3. **Πρόληψη**:
   - Περιορίστε την πρόσβαση των εργαζομένων σε ευαίσθητα οικονομικά δεδομένα.
   - Εφαρμογή εργαλείων παρακολούθησης για τον εντοπισμό ασυνήθιστων προτύπων πρόσβασης.

Ρόλοι:
DPO, Νομικός Σύμβουλος, Ειδικός Ασφάλειας Πληροφορικής, Υπεύθυνος Πρόληψης Απάτης.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.