Δραστηριότητα: GDPR στην πράξη

Στόχος:
Οι συμμετέχοντες θα αναλύσουν μια πραγματική μελέτη περίπτωσης για να κατανοήσουν πώς μια εταιρεία εφάρμοσε με επιτυχία τη συμμόρφωση με τον GDPR μετά από μια παραβίαση δεδομένων. Στόχος είναι να διερευνήσουν τις προκλήσεις που αντιμετώπισαν, την αντίδραση της εταιρείας σύμφωνα με τον ΓΚΠΔ και τα διδάγματα που αποκόμισαν.

Διάρκεια:

30 λεπτά

Απαιτούμενα υλικά:

1. **Μελέτη περίπτωσης Φυλλάδιο ή διαφάνεια**: Σύντομη περιγραφή της πραγματικής μελέτης περίπτωσης, με έμφαση στην παραβίαση, την αντίδραση και το αποτέλεσμα.
2. **Προβολέας ή πίνακας** (προαιρετικά): Για την παρουσίαση των βασικών σημείων και τη διευκόλυνση της συζήτησης.
3. **Σημειωματάρια και στυλό** ή **φορητοί υπολογιστές/tablets**: Για να σημειώνουν οι συμμετέχοντες τις παρατηρήσεις τους και τα βασικά σημεία της συζήτησης.

Παράδειγμα μελέτης περίπτωσης: XYZ Telecom

Σενάριο:
XYZ Telecom, μια ευρωπαϊκή εταιρεία τηλεπικοινωνιών, υπέστη σημαντική παραβίαση δεδομένων κατά την οποία χάκερ απέκτησαν πρόσβαση σε προσωπικές πληροφορίες πελατών, συμπεριλαμβανομένων ονομάτων, διευθύνσεων, διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών τηλεφώνου. Η παραβίαση συνέβη λόγω μιας ευπάθειας στην πύλη υποστήριξης πελατών τους, την οποία εκμεταλλεύτηκαν οι χάκερ. Η εταιρεία έπρεπε να ανταποκριθεί σε πλήρη συμμόρφωση με τους κανονισμούς του GDPR.

Βασικά σημεία προς συζήτηση:

1. Η παραβίαση:

- **Πώς συνέβη**:

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.

- Οι χάκερ εκμεταλλεύτηκαν μια ευπάθεια ασφαλείας στην πύλη υποστήριξης πελατών της XYZ Telecom, αποκτώντας πρόσβαση σε προσωπικά δεδομένα πελατών που ήταν αποθηκευμένα στο σύστημα.

- **Δεδομένα εκτεθειμένα**:
  - Προσωπικά στοιχεία όπως ονόματα πελατών, διευθύνσεις, αριθμοί τηλεφώνου και διευθύνσεις ηλεκτρονικού ταχυδρομείου εκτέθηκαν, αλλά δεν παραβιάστηκαν λεπτομέρειες πληρωμών.

Ερώτηση συζήτησης:

- Ποια τρωτά σημεία ασφαλείας ή αποτυχίες οδήγησαν σε αυτή την παραβίαση; Πώς θα μπορούσε η XYZ Telecom να εντοπίσει και να επιδιορθώσει αυτή την ευπάθεια νωρίτερα;

---

2. Η απάντηση:

- **Ενημέρωση των επηρεαζόμενων ατόμων**:
  - Σύμφωνα με τον ΓΚΠΔ, η XYZ Telecom ενημέρωσε τους πελάτες που επηρεάζονται εντός του απαιτούμενου **παραθύρου των 72 ωρών**. Έστειλε μηνύματα ηλεκτρονικού ταχυδρομείου και γραπτά μηνύματα σε όλους τους επηρεαζόμενους πελάτες, εξηγώντας την παραβίαση, ποια δεδομένα εκτέθηκαν και προσφέροντας καθοδήγηση σχετικά με τα βήματα για την προστασία των πληροφοριών τους.

- **Αξιολόγηση της παραβίασης**:
  - Η XYZ Telecom διενήργησε **ανάλυση της αιτίας** και διαπίστωσε ότι η παραβίαση οφειλόταν σε αποτυχία του συστήματος διαχείρισης επιδιορθώσεων, η οποία άφησε ευάλωτη την πύλη υποστήριξης. Διόρθωσαν αμέσως την ευπάθεια και έκαναν πρόσθετες δοκιμές ασφαλείας.

- **Ενημέρωση πρωτοκόλλων ασφαλείας**:
  - Η εταιρεία ενίσχυσε την ασφάλειά της εφαρμόζοντας **έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)** τόσο για τους εσωτερικούς υπαλλήλους όσο και για τους πελάτες που έχουν πρόσβαση σε ευαίσθητα δεδομένα, πραγματοποίησε συχνότερους ελέγχους συστημάτων και προσέλαβε μια τρίτη εταιρεία κυβερνοασφάλειας για τη διενέργεια τακτικών δοκιμών διείσδυσης.

Ερώτηση συζήτησης:

- Πώς εναρμονίστηκε η απάντηση της XYZ Telecom με τον GDPR; Ποια μέτρα θα μπορούσαν να είχαν λάβει διαφορετικά για την καλύτερη προστασία των δεδομένων των πελατών;

---

3. Το αποτέλεσμα:

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.

- **Διδάγματα**:
    - Η XYZ Telecom έμαθε τη σημασία της τακτικής ενημέρωσης των συστημάτων ασφαλείας και την ανάγκη για αυστηρότερους ελέγχους πρόσβασης. Η παραβίαση ανέδειξε τρωτά σημεία στην υποδομή ΤΠ τους, τα οποία στη συνέχεια αντιμετωπίστηκαν.
- **Αλλαγές που εφαρμόστηκαν**:
    - Η εταιρεία επικαιροποίησε τις εσωτερικές της **πολιτικές προστασίας δεδομένων**, απαιτώντας συχνότερες σαρώσεις ευπάθειας και καλύτερη εκπαίδευση του προσωπικού σε θέματα κυβερνοασφάλειας. Δημιούργησε επίσης ένα **σχέδιο αντιμετώπισης παραβίασης** δεδομένων για να διασφαλίσει ταχείες, συμβατές αντιδράσεις σε τυχόν μελλοντικά περιστατικά.

Ερώτηση συζήτησης:

- Ποιες μακροπρόθεσμες αλλαγές εφάρμοσε η XYZ Telecom για να διασφαλίσει τη συμμόρφωση με τον ΓΚΠΔ και να αποτρέψει μελλοντικές παραβιάσεις; Πώς μπορούν αυτά τα διδάγματα να εφαρμοστούν σε άλλες εταιρείες;

Ροή δραστηριότητας:

1. Παρουσίαση περίπτωσης (10 λεπτά):

- Ο συντονιστής παρουσιάζει τη μελέτη περίπτωσης της XYZ Telecom, εξηγώντας την παραβίαση, τα δεδομένα που εκτέθηκαν και την απάντηση της εταιρείας σύμφωνα με τον GDPR.

2. Ομαδική συζήτηση (15 λεπτά):

- Οι συμμετέχοντες θα χωριστούν σε μικρές ομάδες για να συζητήσουν τα εξής:
    1. Πώς συνέβη η παραβίαση και ποιες αδυναμίες εκτέθηκαν.
    2. Η αποτελεσματικότητα της ανταπόκρισης της XYZ Telecom σε συμμόρφωση με τον ΓΚΠΔ.
    3. Τα διδάγματα που αντλήθηκαν και οι αλλαγές που εφάρμοσε η εταιρεία για την αποτροπή μελλοντικών παραβιάσεων.
    4. Ποιες άλλες ενέργειες θα μπορούσε να είχε λάβει η XYZ Telecom για να βελτιώσει την απόκριση και την προστασία των δεδομένων της;

3. Παρουσίαση των βασικών γνώσεων (5 λεπτά):

- Κάθε ομάδα θα παρουσιάσει εν συντομία τα συμπεράσματά της, τονίζοντας τα βασικά συμπεράσματα της συζήτησης. Στη συνέχεια, ο συντονιστής θα ολοκληρώσει τη δραστηριότητα συνοψίζοντας τα σημαντικότερα σημεία και ενθαρρύνοντας την υποβολή ερωτήσεων.

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.

Αναμενόμενα αποτελέσματα:

- **Κατανόηση της συμμόρφωσης με τον GDPR**: Συμμόρφωση με τον ΓΚΠΔ: Οι συμμετέχοντες θα κατανοήσουν πώς μια εταιρεία μπορεί να ανταποκριθεί σε μια παραβίαση δεδομένων σε συμμόρφωση με τον ΓΚΠΔ, συμπεριλαμβανομένης της ενημέρωσης των πελατών, της αξιολόγησης της παραβίασης και των ενημερώσεων του πρωτοκόλλου ασφαλείας.
- **Εφαρμογή στον πραγματικό κόσμο**: Οι συμμετέχοντες θα αναλύσουν τις προκλήσεις που αντιμετώπισε μια πραγματική εταιρεία και τα βήματα που λήφθηκαν για τη διασφάλιση της συμμόρφωσης, προσφέροντας πρακτικά μαθήματα που μπορούν να εφαρμοστούν και σε άλλους οργανισμούς.
- **Κριτική σκέψη**: Η ομαδική συζήτηση θα ενθαρρύνει τους συμμετέχοντες να σκεφτούν κριτικά σχετικά με τις ενέργειες που έλαβε η XYZ Telecom και να διερευνήσουν πιθανές βελτιώσεις στις στρατηγικές προστασίας δεδομένων.

Πρόσθετα σενάρια για δραστηριότητες μελέτης περίπτωσης

1. **Σενάριο: Πλατφόρμα ηλεκτρονικού εμπορίου**
    - **Πλαίσιο**: Η παραβίαση της ασφάλειας ενός μεγάλου διαδικτυακού εμπόρου λιανικής πώλησης, όπου οι πληροφορίες πληρωμής των πελατών εκτίθενται εξαιτίας μιας ευπάθειας στη διαδικασία πληρωμής. Πρέπει να αντιδράσουν σύμφωνα με τον ΓΚΠΔ.
    - **Εστίαση**: Πώς να χειρίζεστε παραβιάσεις που αφορούν οικονομικά δεδομένα και προστασία των πληροφοριών πληρωμών.
2. **Σενάριο: Διαρροή δεδομένων χρηματοπιστωτικού ιδρύματος**
    - **Πλαίσιο**: Μια τράπεζα ανακαλύπτει ότι ένας υπάλληλος διέρρευσε ακούσια στοιχεία λογαριασμού πελατών μέσω μη ασφαλούς επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου.
    - **Εστίαση**: Πώς να εφαρμόζετε πολιτικές συμβατές με τον ΓΚΠΔ για το εσωτερικό προσωπικό που χειρίζεται ευαίσθητα δεδομένα.
3. **Σενάριο: Παραβίαση δεδομένων παρόχου υγειονομικής περίθαλψης**
    - **Πλαίσιο**: Ένας οργανισμός υγειονομικής περίθαλψης αντιμετωπίζει μια παραβίαση όπου τα ιατρικά αρχεία ασθενών αποκτούν πρόσβαση από μη εξουσιοδοτημένο προσωπικό λόγω των αδύναμων ελέγχων πρόσβασης.
    - **Εστίαση**: Πώς να χειρίζεστε τις ευαίσθητες πληροφορίες υγείας στο πλαίσιο του ΓΚΠΔ και να συμμορφώνεστε με τους νόμους περί απορρήτου δεδομένων υγείας.

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.