Ενότητα 3: Χρήση της τεχνολογίας ως λύση

3.4. Ασφάλεια στον κυβερνοχώρο
Διάρκεια: 45 λεπτά
Θέμα διδασκαλίας: Προκλήσεις και λύσεις για την ασφάλεια στον κυβερνοχώρο στις έξυπνες πόλεις
- Υποθέμα 1 : Η φύση των απειλών στον κυβερνοχώρο στις έξυπνες πόλεις
- Υποθέμα 2: Στρατηγικές για τον μετριασμό και την πρόληψη

Μαθησιακοί στόχοι:
- Να κατανοήσουν τις μοναδικές προκλήσεις της ασφάλειας στον κυβερνοχώρο στο πλαίσιο των έξυπνων πόλεων
- Να γνωρίσουν αποτελεσματικές στρατηγικές και πρακτικές για τη διασφάλιση των έξυπνων αστικών περιβαλλόντων

Μεθοδολογία:
- Παρακολούθηση της πρώτης παρουσίασης (15 λεπτά)
- Απάντηση σε ερωτήσεις πολλαπλής επιλογής (5 λεπτά)
- Παρακολούθηση της δεύτερης παρουσίασης (15 λεπτά)
- Απάντηση σε ερωτήσεις drag&drop (10 λεπτά)

Υπο-θέμα πρώτο: Η φύση των απειλών στον κυβερνοχώρο στις έξυπνες πόλεις
Διάρκεια: 20 λεπτά
Περιεχόμενο: Αύξηση της διάρκειας του μαθήματος: 1: Αυτή η ενότητα θα επικεντρωθεί στην εκπαίδευση των εκπαιδευομένων σχετικά με τους διάφορους τύπους απειλών στον κυβερνοχώρο που αντιμετωπίζουν οι έξυπνες πόλεις, όπως παραβιάσεις δεδομένων, επιθέσεις ransomware, ευπάθειες IoT και εσωτερικές απειλές. Θα χρησιμοποιηθούν παραδείγματα από τον πραγματικό κόσμο για να απεικονιστούν αυτές οι απειλές και οι πιθανές επιπτώσεις τους στις υποδομές των έξυπνων πόλεων

Μεθοδολογία
- Παρακολούθηση της παρουσίασης: (15 λεπτά)
- Απάντηση σε ερωτήσεις πολλαπλής επιλογής (5 λεπτά)

Υλικό
- Παρουσίαση PowerPoint: 3.4. Ασφάλεια στον κυβερνοχώρο-Η φύση των απειλών στον κυβερνοχώρο στις έξυπνες πόλεις.pptx

Σύνδεσμος Canva
- Σύνδεση στο Διαδίκτυο

Υπο-θέμα δεύτερο: Στρατηγικές μετριασμού και πρόληψης
Διάρκεια: 20 λεπτά
Περιεχόμενο: Ακολουθείται η συζήτηση για την αντιμετώπιση των κινδύνων και την καταπολέμηση των κινδύνων: Αυτή η ενότητα διερευνά στρατηγικές για τον μετριασμό και την πρόληψη των απειλών στον κυβερνοχώρο,

συμπεριλαμβανομένου του ασφαλούς σχεδιασμού, της προληπτικής διαχείρισης κινδύνων και της επιχειρησιακής ανθεκτικότητας.

Μεθοδολογία

● Παρακολούθηση της παρουσίασης: (15 λεπτά)
● Συνέχιση της δραστηριότητας drag&drop (5 λεπτά)

Υλικό

● Παρουσίαση PowerPoint: 3.4. Ασφάλεια στον κυβερνοχώρο-στρατηγικές για μετριασμό και πρόληψη.pptx
Canva
● Σύνδεση στο Διαδίκτυο

Υποθέμα 1 : Η φύση των απειλών στον κυβερνοχώρο στις έξυπνες πόλεις

Ερωτήσεις πολλαπλής επιλογής

IMG 
Ερώτηση: Ποιος είναι ο πρωταρχικός σκοπός των έξυπνων πόλεων;
● Να αυξηθεί ο πληθυσμός της πόλης (Λάθος)
● Να χρησιμοποιηθεί προηγμένη τεχνολογία για τη βελτίωση των αστικών υπηρεσιών (Σωστό)
● Να μειώσει το κόστος ζωής (Λάθος)
● Να επεκτείνει τις αστικές περιοχές (Λάθος)

IMG 
Ερώτηση: Τι ρόλο παίζει η κυβερνοασφάλεια στις έξυπνες πόλεις;

• ● Προστατεύει πρωτίστως τις φυσικές υποδομές (Λάθος)
• ● Εξασφαλίζει την αποδοτική χρήση της ενέργειας (Λάθος)
• ● Προστατεύει τα δεδομένα και διατηρεί αδιάλειπτες τις υπηρεσίες της πόλης (Σωστό)
• ● Προστατεύει μόνο τις χρηματοοικονομικές συναλλαγές (Λάθος)

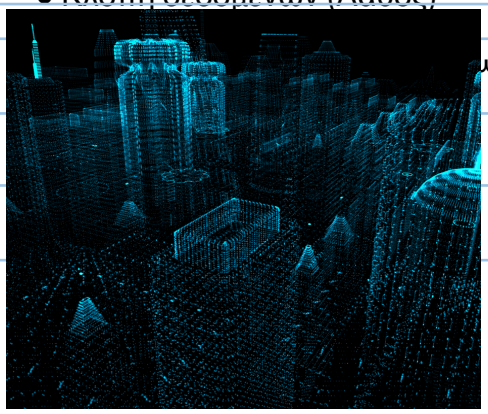
IMG 
Ερώτηση: Ποια είναι τα τρία επίπεδα υποδομής σε ένα οικοσύστημα έξυπνης πόλης;
● Το στρώμα νέφους, το στρώμα χρήστη και το στρώμα επικοινωνίας (Λάθος)
● Το στρώμα IoT, το στρώμα δεδομένων και το φυσικό στρώμα (Λάθος)
● Το στρώμα άκρων, ο πυρήνας και τα κανάλια επικοινωνίας (Σωστό)
● Το στρώμα αισθητήρων, το στρώμα επεξεργασίας και το στρώμα δικτύου (Λάθος)

IMG 
Ερώτηση: Η επίθεση στον κυβερνοχώρο της γερμανικής χαλυβουργίας το 2014 είναι ένα παράδειγμα:
• ● Κλοπή δεδομένων (Λάθος)
• ● Επίθεση «άνθρωπος στο μέσο» (Λάθος)

• ● Φυσική ζημία λόγω απειλής στον κυβερνοχώρο (Σωστό)
• ● Επίθεση DDoS (Λάθος)

IMG 
Ερώτηση: Ποια από τις ακόλουθες είναι μια κοινή απειλή στον κυβερνοχώρο στις έξυπνες πόλεις;
● Παραβίαση συσκευής (Σωστό)
● Ηλεκτρονική απάτη (Λάθος)
● Λογοκρισία στο Διαδίκτυο (Λάθος)
● Ψάρεμα μέσω ηλεκτρονικού ταχυδρομείου (Λάθος)

IMG 

Ερώτηση: Ποιο είδος επίθεσης περιλαμβάνει την υποκλοπή της επικοινωνίας μεταξύ δύο συστημάτων από έναν χάκερ;
● Κλοπή δεδομένων (Λάθος)
ωστό)
IMG 
Ερώτηση: Πώς ενσωματώνονται ο φυσικός και ο κυβερνοχώρος στις έξυπνες πόλεις;
● Μέσω ξεχωριστών αλλά παράλληλων συστημάτων (Λάθος)
● Με τη χρήση μόνο συσκευών IoT (Λάθος)
● Μέσω διασυνδεδεμένων δικτύων και τεχνολογιών (Σωστό)
● Τα φυσικά συστήματα δεν ενσωματώνονται με τα συστήματα στον κυβερνοχώρο. (Λάθος)

Υπο-θέμα 2 : Στρατηγικές μετριασμού και πρόληψης

Συμπληρώστε το κενό

Δραστηριότητα Drag the Words- Κυβερνοασφάλεια στις έξυπνες πόλεις
Σύρετε τη σωστή λέξη ή φράση από τον κατάλογο στο κατάλληλο κενό χώρο κάθε πρότασης. Κάθε λέξη ή φράση μπορεί να χρησιμοποιηθεί μόνο μία φορά. Συμπληρώστε σωστά όλες τις προτάσεις για να ολοκληρώσετε τη δραστηριότητα.
Η κυβερνοασφάλεια στις έξυπνες πόλεις προστατεύει τα *δεδομένα* και διατηρεί τις *αδιάλειπτες υπηρεσίες της πόλης*. Στις έξυπνες πόλεις, ο φυσικός και ο κυβερνοχώρος ενσωματώνονται μέσω *συνδεδεμένων δικτύων και τεχνολογιών*. Η παραβίαση δεδομένων του 2015 στο Γραφείο Διαχείρισης Προσωπικού των ΗΠΑ προκλήθηκε κυρίως από τη χρήση *πεπαλαιωμένων συστημάτων και ανεπαρκούς κρυπτογράφησης*. Η επίθεση *Man-in-the-Middle Attack* περιλαμβάνει έναν χάκερ που υποκλέπτει την επικοινωνία μεταξύ δύο συστημάτων.

Μια βασική πρόκληση για την προστασία των έξυπνων πόλεων από απειλές στον κυβερνοχώρο είναι η *ενσωμάτωση παλαιών συστημάτων με νέες τεχνολογίες*.

Το κακόβουλο λογισμικό* CRASHOVERRIDE* έθεσε εκτός λειτουργίας το ουκρανικό δίκτυο ηλεκτρικής ενέργειας το 2016.

Η πρωταρχική απειλή που συνιστά το Mirai Botnet είναι η *συμβιβασμός μη ασφαλών συσκευών IoT*.

Η επίθεση ransomware στην Ατλάντα το 2018 διέκοψε *τις υπηρεσίες της πόλης και προκάλεσε οικονομικές προκλήσεις*

Κατάλογος λέξεων/φράσεων που πρέπει να σύρετε:

- δεδομένα
- αδιάλειπτες υπηρεσίες της πόλης
- διασυνδεδεμένα δίκτυα και τεχνολογίες
- απαρχαιωμένα συστήματα και ανεπαρκής κρυπτογράφηση
- Επίθεση «άνθρωπος στο μέσο» (Man-in-the-Middle Attack)
- ενσωμάτωση παλαιών συστημάτων με νέες τεχνολογίες
- CRASHOVERRIDE
- παραβίαση μη ασφαλών συσκευών IoT
- υπηρεσίες της πόλης και προκαλούμενες οικονομικές προκλήσεις