Το/τα θέμα/τα προέρχεται και αντλήθηκε/αν από την πλατφόρμα της Τράπεζας Θεμάτων Διαβαθμισμένης Δυσκολίας που αναπτύχθηκε (MIS5070818-Τράπεζα θεμάτων Διαβαθμισμένης Δυσκολίας για τη Δευτεροβάθμια Εκπαίδευση, Γενικό Λύκειο-ΕΠΑΛ) και είναι διαδικτυακά στο δικτυακό τόπο του Ινστιτούτου Εκπαιδευτικής Πολιτικής (Ι.Ε.Π.) στη διεύθυνση (http://iep.edu.gr/el/trapezathematon-arxiki-selida)

Θέμα 1

Για να ικανοποιηθούν οι απαιτήσεις ασφαλείας ενός Πληροφοριακού Συστήματος (Π.Σ.) και να μειωθεί η επικινδυνότητα σχεδιάζονται κάποια μέτρα ασφαλείας. Κατηγοριοποιήστε τα είδη των μέτρων ασφαλείας στην πρώτη στήλη Α, ανάλογα με τις κατηγορίες που αυτά καλύπτουν στην δεύτερη στήλη Κ .

Α. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ	**Κ. ΚΑΤΗΓΟΡΙΕΣ**
Α1. Απογραφή λογισμικού και υλικού	Κ1. Διοικητικά μέτρα
Α2. Αντίγραφα ασφαλείας (backup)	Κ2. Τεχνικά μέτρα
Α3. Εκπαίδευση χρηστών για τις λειτουργίες του Π.Σ.	Κ3. Μέτρα φυσικής ασφάλειας
Α4. Διαβάθμιση πληροφοριών	
Α5. Αδιάλειπτη παροχή ρεύματος (UPS)	
Α6. Πρόσβαση στις κτιριακές εγκαταστάσεις	
Α7. Αρχεία καταγραφής (log files)	

Θέμα 2

Το ηλεκτρονικό κατάστημα «The Almond Tree» πραγματοποίησε μεγάλη διαφημιστική καμπάνια για την προώθηση των προϊόντων του, ενώ ταυτόχρονα κάνει προσφορές έως 90% σε όσους αγοράσουν προϊόντα μέσα στο Σαββατοκύριακο. Όσοι όμως προσπάθησαν να επισκεφτούν τον δικτυακό τόπο του καταστήματος εκείνες τις μέρες, διαπίστωσαν ότι αυτός έχει τεθεί εκτός λειτουργίας και δεν κατάφεραν να κάνουν αγορές. Αιτία ήταν το μικρό εύρος γραμμής (bandwidth) του εξυπηρετητή και η λήψη πάρα πολλών αιτήσεων προβολής του ηλεκτρονικού καταστήματος.

α. Ποια μέτρα πρόληψης έπρεπε να τηρούνται για την αποφυγή του παραπάνω περιστατικού;

β. Ποια από τις βασικές αρχές ασφάλειας πληροφοριακών συστημάτων καταστρατηγείται στο παραπάνω περιστατικό;

Θέμα 3

Έστω πως το Σαββατοκύριακο σε κάποιο υπολογιστικό σύστημα γίνεται το πλήρες αντίγραφο ασφαλείας (full Backup).

Την Δευτέρα τροποποιήθηκε το αρχείο Α , την Τετάρτη το αρχείο Β και το αρχείο Γ, ενώ την Πέμπτη, πάλι το αρχείο Β.

α) Τι θα πάρει το αυξητικό αντίγραφο ασφαλείας (incremental backup) την Τετάρτη

β) Τι θα πάρει το διαφορικό αντίγραφο ασφαλείας (differential backup) την Πέμπτη

Θέμα 4

Σε μια εταιρεία υπάρχουν μηχανογραφημένα τα τμήματα του ΛΟΓΙΣΤΗΡΙΟΥ, της ΑΠΟΘΗΚΗΣ, των ΠΕΛΑΤΩΝ και της ΔΙΕΥΘΥΝΣΗΣ. Τα αρχεία στα τμήματα αυτά τροποποιούνται σε εβδομαδιαία βάση, όπως φαίνεται στον παρακάτω πίνακα ως εξής:

Του ΛΟΓΙΣΤΗΡΙΟΥ τις ημέρες Δευτέρα, Τετάρτη, Παρασκευή, της ΑΠΟΘΗΚΗΣ την Τρίτη και Πέμπτη, των ΠΕΛΑΤΩΝ Δευτέρα, Τρίτη, Τετάρτη και της ΔΙΕΥΘΥΝΣΗΣ την Πέμπτη.

Το Σάββατο η εταιρεία «τραβάει» πλήρη αντίγραφα (full backup) σε όλα τα αρχεία από όλα τα τμήματα.

Ημέρες / Αρχεία	*Δευτέρα*	*Τρίτη*	*Τετάρτη*	*Πέμπτη*	*Παρασκευή*	*Σάββατο*
ΛΟΓΙΣΤΗΡΙΟΥ	√		√		√	*FULL BACKUP*
ΑΠΟΘΗΚΗΣ		√		√		*FULL BACKUP*
ΠΕΛΑΤΩΝ	√	√	√			*FULL BACKUP*
ΔΙΕΥΘΥΝΣΗΣ				√		*FULL BACKUP*

Με βάση τα παραπάνω απαντήστε σύντομα στα παρακάτω ερωτήματα:

α. Ποιων τμημάτων τα αρχεία θα περιλαμβάνει ένα διαφορικό αντίγραφο (differential backup) της Τρίτης;

β. Ποιων τμημάτων τα αρχεία θα περιλαμβάνει το αυξητικό αντίγραφο (incremental backup) της Τρίτης και της Πέμπτης;

Θέμα 5

Διαβάστε το παρακάτω κείμενο και απαντήστε συνοπτικά στις ερωτήσεις που ακολουθούν:

Στις 17 Σεπτεμβρίου 2020 σημειώθηκε στη Γερμανία ο πρώτος παγκόσμια θάνατος που αποδίδεται σε λογισμικό πληρωμής λύτρων (ransomware). Τέτοιο λογισμικό κλειδώνει συνήθως αρχεία ώστε να μην μπορούν να τα προσπελάσουν οι χρήστες χωρίς να γνωρίζουν κάποιο μυστικό κωδικό. Για να αποκτηθεί ο κωδικός και να ξεκλειδωθούν τα αρχεία απαιτείται η πληρωμή λύτρων που γίνεται συνήθως σε κάποιο κρυπτονόμισμα*,

ώστε να είναι πιο δύσκολος ο εντοπισμός των θυτών. Στην συγκεκριμένη περίπτωση, το κακόβουλο λογισμικό ‘μόλυνε’ υπολογιστές του νοσοκομείου του Ντύσελντορφ με αποτέλεσμα να ακυρωθούν χειρουργεία και οι γιατροί να αναγκαστούν να στείλουν τα επείγοντα περιστατικά σε γειτονικά νοσοκομεία. Σε μία τέτοια περίπτωση η ασθενής δεν άντεξε κατά την μεταφορά και απεβίωσε.

*τύπος ηλεκτρονικού χρήματος που δίνει τη δυνατότητα στους χρήστες να συναλλάσσονται χρησιμοποιώντας ψευδώνυμα και όχι την πραγματική τους ταυτότητα

α. Ποια από τις βασικές αρχές της ασφάλειας συστημάτων παραβιάστηκε στην περίπτωση που περιγράφεται στο κείμενο. Να αιτιολογήσετε την απάντησή σας.

β. Να εξηγήσετε τον ρόλο της διαδικασίας λήψης αντιγράφων ασφαλείας στην *αντιμετώπιση* παρόμοιων επιθέσεων. Να εστιάσετε ιδιαίτερα στον ρόλο και τη συχνότητα λήψης αυξητικών αντιγράφων ασφαλείας.

Θέμα 6

Μία εταιρεία θέλει να επιλέξει στρατηγική λήψης αντιγράφων ασφαλείας. Για τον σκοπό αυτό θα χρησιμοποιήσει στατιστικά στοιχεία για το μέγεθος των δεδομένων για τα οποία λαμβάνει αντίγραφο ασφαλείας και των αλλαγών που έγιναν σε αυτά την προηγούμενη εβδομάδα. Τα στατιστικά αυτά φαίνονται στον παρακάτω πίνακα:

Ημέρα	**Συνολικό Μέγεθος Δεδομένων**
Κυριακή	10GB
Δευτέρα (βράδυ μετά την λήξη εργασιών)	11GB
Τρίτη (βράδυ μετά την λήξη εργασιών)	13GB
Τετάρτη (βράδυ μετά την λήξη εργασιών)	14GB
Πέμπτη (βράδυ μετά την λήξη εργασιών)	16GB
Παρασκευή (βράδυ μετά την λήξη εργασιών)	17GB

Το τμήμα πληροφορικής πρότεινε τις παρακάτω 3 στρατηγικές:

1. Κάθε μέρα πλήρες backup.
2. Την Κυριακή πλήρες backup και κάθε μια από τις υπόλοιπες μέρες διαφορικό.
3. Την Κυριακή πλήρες backup και κάθε μέρα από τις υπόλοιπες αυξητικό.

Υποθέτουμε ότι η εταιρεία πρέπει να διατηρεί *όλα* τα εβδομαδιαία αντίγραφα ασφαλείας σε κάθε μία από τις παραπάνω περιπτώσεις. Επίσης υποθέτουμε ότι δεν εφαρμόζεται κανενός είδους συμπίεση στα αντίγραφα ασφαλείας.

α. Πόσος χώρος απαιτείται για να διατηρηθούν όλα τα εβδομαδιαία αντίγραφα ασφαλείας σε κάθε μία από τις παραπάνω περιπτώσεις. Σε ποια από αυτές καταλαμβάνουν το λιγότερο χώρο;

β. Ποια είναι τα αντίγραφα ασφαλείας που είναι απολύτως απαραίτητα για να γίνει η επαναφορά των δεδομένων, αν συμβεί αστοχία υλικού το Σάββατο το πρωί, σε κάθε μία από τις παραπάνω περιπτώσεις;

Θέμα 7

Για κάθε ένα από τα σενάρια που περιγράφονται στη στήλη Α γράψτε την έννοια της Ασφάλειας Πληροφοριακών Συστημάτων της στήλης Β με την οποία αντιστοιχεί.

(Α)	**(Β)**
1. Κενό ασφαλείας στο Λειτουργικό Σύστημα Windows που επιτρέπει την απομακρυσμένη πρόσβαση με δικαιώματα διαχειριστή στο σύστημα.	Α. Απειλή
2. Πιθανό συμβάν διακοπής ρεύματος στο κέντρο μηχανογράφησης μιας επιχείρησης	Β. Ευπάθεια
3. Διαγραφή σημαντικών αρχείων λόγω λάθους χειρισμού από χρήστη υπολογιστή.	Γ. Αντίμετρα
4. Εγκατάσταση ενημέρωσης που διορθώνει κενά ασφαλείας στο Λειτουργικό Σύστημα Linux.	
5. Εγκατάσταση συστήματος πυρόσβεσης στο κέντρο μηχανογράφησης μιας επιχείρησης.	
6. Χρήση εύκολα προβλέψιμου κωδικού πρόσβασης από έναν χρήστη ενός υπολογιστικού συστήματος.	
7. Κλείδωμα των αρχείων ενός οργανισμού από επιτιθέμενο χάκερ και απαίτηση καταβολής χρηματικού ποσού για την επαναφορά τους.	
8. Διοργάνωση σεμιναρίου στους υπαλλήλους μια επιχείρησης σχετικά με τις επιθέσεις τύπου κοινωνικής μηχανικής.	
9. Εγκατάσταση προγράμματος ανίχνευσης και αντιμετώπισης ιών σε υπολογιστές.	
10. Παράλειψη εγκατάστασης των σημαντικών ενημερώσεων ασφαλείας ενός Λειτουργικού Συστήματος	

Θέμα 8

Ο κ. Γεωργίου, ελεύθερος επαγγελματίας, δέχθηκε στο κινητό του τηλέφωνο το ακόλουθο μήνυμα:

«Μια εισερχόμενη μεταφορά στον λογαριασμό σας απορρίφθηκε λόγω πιθανών σφαλμάτων στο προφίλ σας. Κάντε κλικ εδώ και ακολουθήστε τις οδηγίες για την επεξεργασία της πληρωμής».

Ως αποστολέας του μηνύματος εμφανίζονταν το όνομα της τράπεζας με την οποία ο κ. Γεωργίου συνεργάζεται. Καθώς ο κ. Γεωργίου δέχεται συχνά ηλεκτρονικές πληρωμές

πάτησε στο σύνδεσμο που περιείχε το μήνυμα (στην λέξη «εδώ») και εισήγαγε το όνομα χρήστη και την συνθηματική του λέξη στην ιστοσελίδα που εμφανίσθηκε. Ύστερα από δύο ώρες διαπίστωσε ότι όχι μόνο δεν έλαβε κάποια πληρωμή, αλλά ένα σημαντικό χρηματικό ποσό έλλειπε από τον λογαριασμό του. Απαντήστε στις ακόλουθες ερωτήσεις:

α. Τι είδους επίθεση δέχθηκε ο κ. Γεωργίου και ποια τεχνική χρησιμοποιήθηκε για την απόσπαση των πληροφοριών σύνδεσης στον λογαριασμό του; Δικαιολογήστε την απάντησή σας.

β. Ποια ή ποιες από τις βασικές αρχές ασφαλείας Πληροφοριακών Συστημάτων παραβιάστηκαν στην συγκεκριμένη περίπτωση; Δικαιολογήστε την απάντησή σας.