Ασκήσεις Ερωτήσεις

Άσκηση

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)	

Άσκηση

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)	

Α1-Κ2
Α2-Κ2
Α3-Κ1
Α4-Κ1
Α5-Κ2
Α6-Κ3
Α7-Κ2

Άσκηση

Να αντιστοιχίσετε τις ενέργειες της στήλης Α με τις διαδικασίες της στήλης Β με τις οποίες σχετίζονται στα πλαίσια της διαχείρισης ασφάλειας ενός πληροφοριακού συστήματος.

Α. ΕΝΕΡΓΕΙΑ	**Β. ΔΙΑΔΙΚΑΣΙΑ**
Α1. Αναγνώριση ευπαθειών	**Β1.** Διαχείριση Κινδύνου
Α2. Περιγραφή νομικών περιορισμών που διέπουν τη λειτουργία του οργανισμού	**Β2.** Πολιτική Ασφάλειας
Α3. Αναγνώριση απειλών	**Β3**. Σχέδιο Επαναφοράς από καταστροφή
Α4. Χαρακτηρισμός εμπιστευτικότητας πληροφοριών	
Α5. Δημιουργία αντιγράφων ασφαλείας	
Α6. Περιγραφή Στόχων ασφάλειας	
Α7. Δοκιμές επαναφοράς συστήματος από αντίγραφα ασφαλείας	

Οι **διαδικασίες** που περιλαμβάνει συνοπτικά είναι:

1. Η **Διαχείριση Κινδύνου**, για να προσδιοριστεί το αποδεκτό **επίπεδο ασφαλείας**
2. Η **ανάπτυξη** και εφαρμογή **Σχεδίου Ασφαλείας** με την οποία θα μπορεί να επιτευχθεί το **επιθυμητό επίπεδο** ασφάλειας
3. Η **Επαναφορά** από **Καταστροφή** και η **Επιχειρησιακή Συνέχεια**.

Άσκηση

Να αντιστοιχίσετε τις ενέργειες της στήλης Α με τις διαδικασίες της στήλης Β με τις οποίες σχετίζονται στα πλαίσια της διαχείρισης ασφάλειας ενός πληροφοριακού συστήματος.

Α. ΕΝΕΡΓΕΙΑ	**Β. ΔΙΑΔΙΚΑΣΙΑ**
Α1. Αναγνώριση ευπαθειών	**Β1.** Διαχείριση Κινδύνου
Α2. Περιγραφή νομικών περιορισμών που διέπουν τη λειτουργία του οργανισμού	**Β2.** Πολιτική Ασφάλειας
Α3. Αναγνώριση απειλών	**Β3.** Σχέδιο Επαναφοράς από καταστροφή
Α4. Χαρακτηρισμός εμπιστευτικότητας πληροφοριών	
Α5. Δημιουργία αντιγράφων ασφαλείας	
Α6. Περιγραφή Στόχων ασφάλειας	
Α7. Δοκιμές επαναφοράς συστήματος από αντίγραφα ασφαλείας	

A1 – B1, A2 – B2, A3 – B1, A4 – B2, A5 – B3, A6 – B2, A7 – B3

Άσκηση

Σε ένα κατάστημα που εμπορεύεται ηλεκτρονικά είδη υπάρχει ένας υπολογιστής σε κοινόχρηστο χώρο όπου καταχωρούνται οι παραγγελίες των πελατών που το επισκέπτονται. Ο υπάλληλος που αναλαμβάνει την καταχώριση και την εκτέλεση των παραγγελιών δεν χρησιμοποιεί κωδικούς για την σύνδεσή του στον υπολογιστή αλλά ούτε και στο σχετικό πρόγραμμα, ενώ τον χρόνο που δεν εξυπηρετεί πελάτες παίζει παιχνίδια, στον υπολογιστή αυτόν, που "κατεβάζει" από το διαδίκτυο. Ποια περίπτωση ελέγχου της πρόσβασης θα έπρεπε να έχει εξασφαλιστεί για να ελαχιστοποιηθούν οι κίνδυνοι και γιατί

Άσκηση

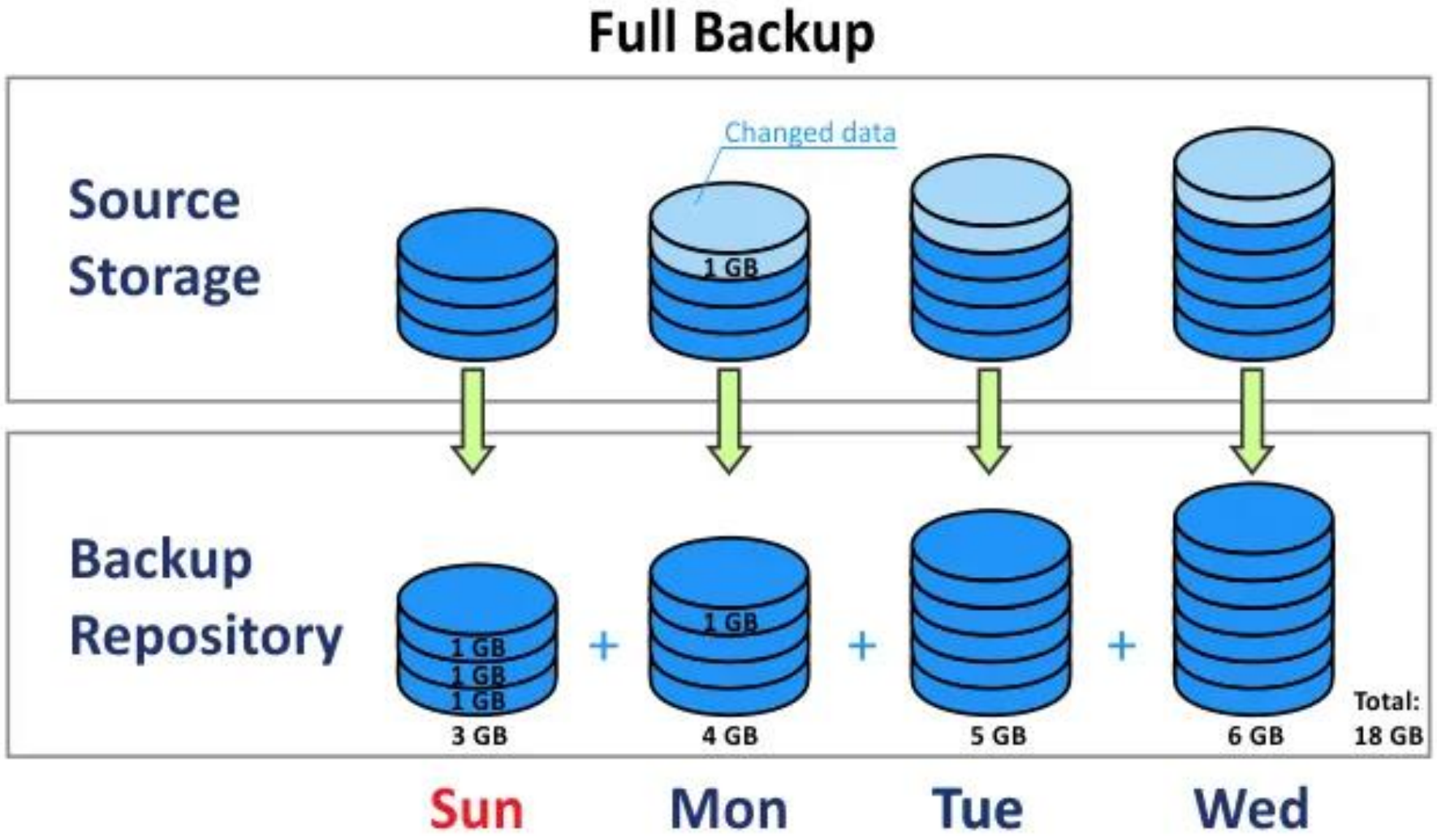
Σε ένα κατάστημα που εμπορεύεται ηλεκτρονικά είδη υπάρχει ένας υπολογιστής σε κοινόχρηστο χώρο όπου καταχωρούνται οι παραγγελίες των πελατών που το επισκέπτονται. Ο υπάλληλος που αναλαμβάνει την καταχώριση και την εκτέλεση των παραγγελιών δεν χρησιμοποιεί κωδικούς για την σύνδεσή του στον υπολογιστή αλλά ούτε και στο σχετικό πρόγραμμα, ενώ τον χρόνο που δεν εξυπηρετεί πελάτες παίζει παιχνίδια, στον υπολογιστή αυτόν, που "κατεβάζει" από το διαδίκτυο. Ποια περίπτωση ελέγχου της πρόσβασης θα έπρεπε να έχει εξασφαλιστεί για να ελαχιστοποιηθούν οι κίνδυνοι και γιατί

Αρχικά, εφόσον ο χρήστης δεν χρησιμοποιεί κωδικούς για την σύνδεσή του στον υπολογιστή αλλά ούτε και στο πρόγραμμα διαχείρισης των πελατών, θα πρέπει να εφαρμοστεί έλεγχος πρόσβασης στα δεδομένα και ο χρήστης να αποκτήσει ατομικό λογαριασμό σύνδεσης με όνομα χρήστη και κωδικό τα οποία να μην κοινοποιήσει σε τρίτους. Έτσι προστατεύεται η Ακεραιότητα Δεδομένων. Ακόμα, επειδή ο υπάλληλος συνδέεται στο διαδίκτυο από τον συγκεκριμένο υπολογιστή για να παίξει παιχνίδια, θέτοντας έτσι σε κίνδυνο τα δεδομένα των πελατών από ιούς ή άλλες κακόβουλες ενέργειες, ακόμα και αν ο υπολογιστής διαθέτει κάποιου είδους προστασία (πχ antivirus) θα πρέπει να εφαρμοστεί έλεγχος δικτυακής πρόσβασης. Δηλαδή να μπουν κάποιοι περιορισμοί στη σύνδεση στο διαδίκτυο αν όχι να καταργηθεί εντελώς. Επίσης, καλό θα ήταν να υπάρχουν Αρχεία Καταγραφής συμβάντων (Log files) για κάθε ενέργεια που μπορεί να προκαλέσει απώλεια ή βλάβη ώστε να μπορεί να αναζητηθεί η πηγή (π.χ. Η/Υ ή χρήστης) που την προκάλεσε.

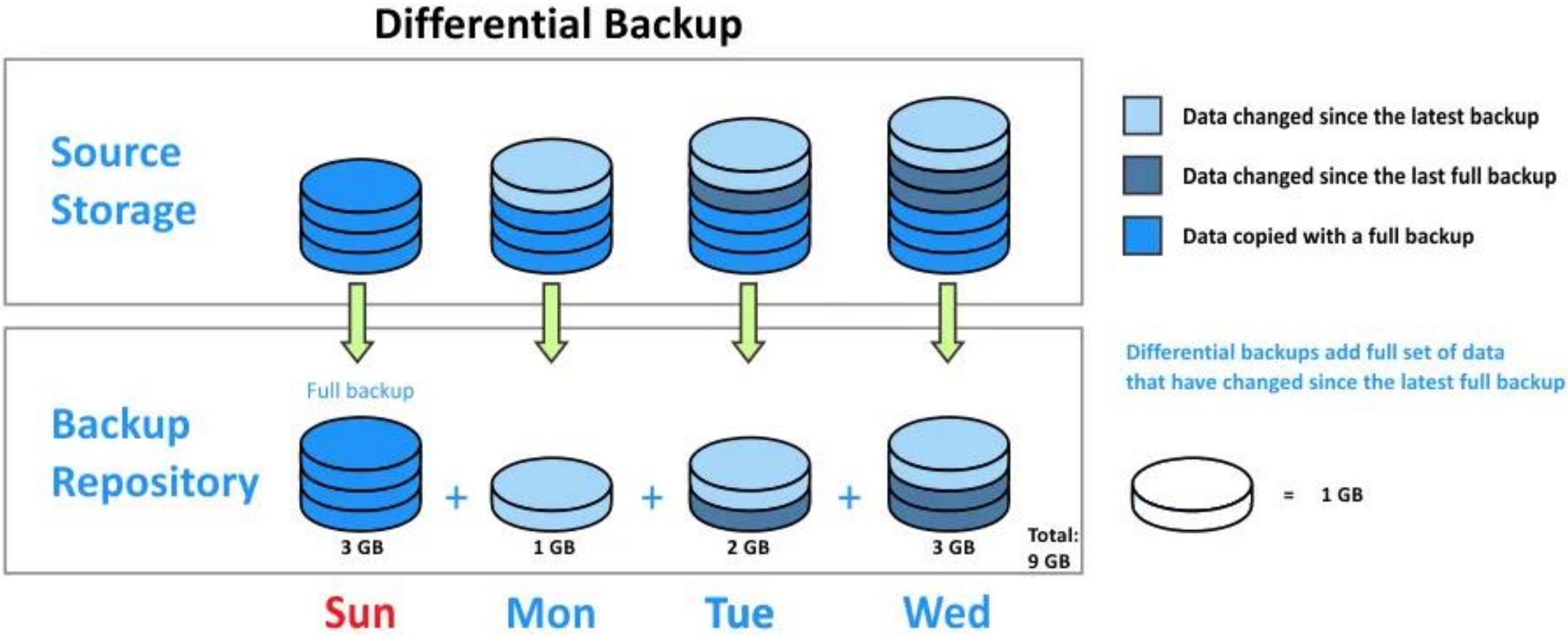
Ασκήσεις Ερωτήσεις

Αντίγραφα Ασαφαλείας

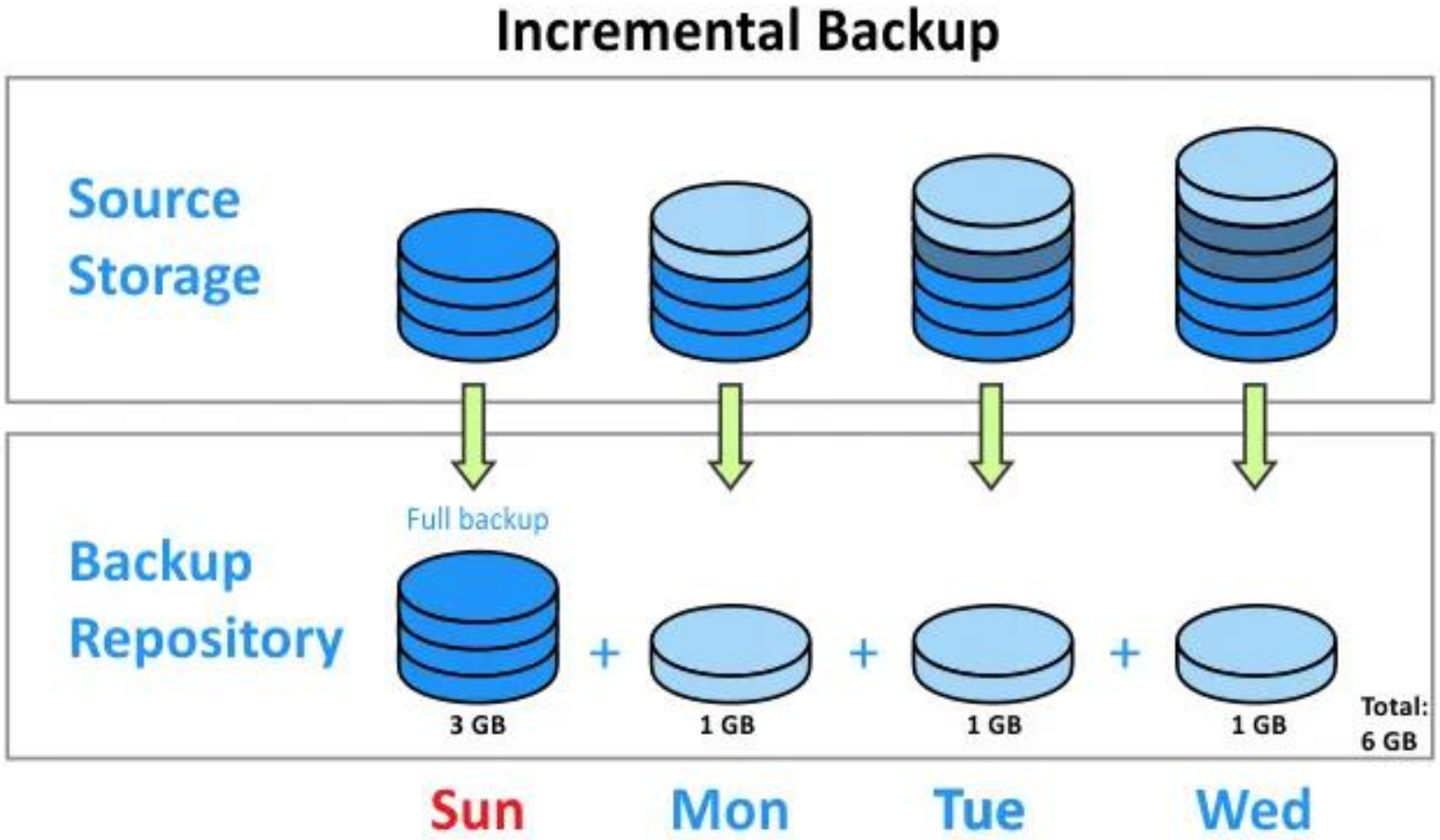
Πλήρες Αντίγραφο Ασφαλείας



Διαφορικό Αντίγραφο Ασφαλείας



Αυξητικό Αντίγραφο Ασφαλείας



Incremental backup copies only data that have changed since the latest backup job

Άσκηση

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 (μον 4) και
β) Τι θα πάρει το διαφορικό αντίγραφο ασφαλείας (differential backup) την Πέμπτη (μον 5);

Παρ	Σαβ	Κυρ	Δευ	Τρι	Τετ	Πεμ	Παρ
			Α		Β,Γ	Β	
Full B/U		v					
Dif B/U			Α	Α	Α,Β,Γ	Α,Β,Γ	
Inc B/U			Α		Β,Γ	Β	

Το αυξητικό αντίγραφο ασφαλείας (incremental backup) της Τετάρτης θα πάρει το αρχείο Β και το αρχείο Γ. Το διαφορικό αντίγραφο ασφαλείας (differential backup) της Πέμπτης θα πάρει όλα τα αρχεία δηλ. Το αρχείο Α που τροποποιήθηκε την Δευτέρα, το αρχείο Γ που τροποποιήθηκε την Τετάρτη και το αρχείο Β που τροποποιήθηκε τελευταία φορά την Πέμπτη.

Άσκηση 18014

Στον υπολογιστή του λογιστηρίου μιας εταιρείας είναι αποθηκευμένα τα αρχεία Α, Β, Γ και Δ. Ο παρακάτω πίνακας δείχνει πότε τροποποιούνται τα αρχεία αυτά κατά την διάρκεια 4 εβδομάδων. Τα αρχεία τροποποιούνται κατά τις εργάσιμες ημέρες ενώ στο τέλος κάθε εβδομάδας, το Σάββατο, δημιουργούνται τα αντίγραφα ασφαλείας.

	1η Εβδομάδα	2η Εβδομάδα	3η Εβδομάδα	4η Εβδομάδα
Α	✓		✓	
Β			✓	
Γ		✓		
Δ				✓

Α) Πότε είναι προτιμότερο ο διαχειριστής του υπολογιστή να πάρει αυξητικό αντίγραφο ασφαλείας (incremental backup) που θα περιέχει τα αρχεία Α και Γ;

Β) Πότε πρέπει να πάρουμε αντίγραφο ασφαλείας που θα περιέχει όλα τα τροποποιημένα αρχεία, και τι είδους αντίγραφο ασφαλείας μπορεί να είναι αυτό;

Άσκηση

	1η Εβδομάδα	2η Εβδομάδα	3η Εβδομάδα	4η Εβδομάδα
Α	✓		✓	
Β			✓	
Γ		✓		
Δ				✓

Α) Εφόσον τα αρχεία τροποποιούνται κατά τις εργάσιμες ημέρες και ώρες ενώ τα αντίγραφα ασφαλείας δημιουργούνται το Σάββατο, μπορούμε να πάρουμε αυξητικά αντίγραφα ως εξής: για το αρχείο Α το Σάββατο της 1ης και 3ης Εβδομάδας και για το αρχείο Γ το Σάββατο της 2ης εβδομάδας. Με τον τρόπο αυτό στο τέλος κάθε εβδομάδας θα έχουμε backup όλων των εκδόσεων των Α και Γ.

Β) Το διαφορικό αντίγραφο ασφαλείας(differential backup) της 4ης εβδομάδας θα περιέχει τα αρχεία Α, Β, Γ και Δ με τις τροποποιήσεις τους. Επίσης και το πλήρες αντίγραφο (full backup) αν θα δημιουργηθεί την 4η εβδομάδα θα περιέχει τα τροποποιημένα Α,Β,Γ και Δ

Άσκηση 22653

Ο κ. Ιωάννου, δημόσιος υπάλληλος, βρήκε στα εισερχόμενα μηνύματα της ημέρας το ακόλουθο:
«Ο ΛΟΓΑΡΙΑΣΜΌΣ ΣΑΣ ΕΊΝΑΙ ΚΛΕΙΔΩΜΈΝΟΣ
Αγαπητέ, ενημερώνουμε το σύστημα ασφαλείας μας, για το λόγο αυτό κλειδώσαμε το λογαριασμό σας μέχρι να αναβαθμίσετε την ασφάλειά σας. Ο λογαριασμός σας έχει κλειδωθεί προσωρινά. Για να τον ξεκλειδώσετε, πρέπει να επαληθεύσετε τα στοιχεία σας.
ΕΙΣΟΔΟΣ
Πολιτική για Cookies | Προστασία Προσωπικών Δεδομένων |Copyright 2020© |»

Ως αποστολέας του μηνύματος εμφανιζόταν το όνομα της τράπεζας με την οποία ο κ. Ιωάννου συνεργάζεται. Καθώς ο κ. Ιωάννου χρησιμοποιεί συστηματικά το σύστημα ηλεκτρονικών πληρωμών, ανησύχησε και πάτησε πάνω στο σύνδεσμο που περιείχε το μήνυμα (στη λέξη «ΕΙΣΟΔΟΣ») και εισήγαγε το όνομα χρήστη και την συνθηματική του λέξη στην ιστοσελίδα που εμφανίσθηκε. Την επόμενη ημέρα διαπίστωσε ότι ένα σημαντικό χρηματικό ποσό έλειπε από τον λογαριασμό του.

Με βάση αυτό το περιστατικό, απαντήστε στις ακόλουθες ερωτήσεις:
1 Σχολιάστε την επίθεση που δέχθηκε ο κ. Ιωάννου. Πώς είναι γνωστή διεθνώς αυτή η τεχνική;
2. Ποια από τις τρεις βασικές αρχές ασφαλείας των Πληροφοριακών Συστημάτων θεωρείτε ότι παραβιάστηκε στην συγκεκριμένη περίπτωση; Αιτιολογήστε.
3 Πώς λέγεται το ηλεκτρονικό έγκλημα που τελέσθηκε στην περίπτωση αυτή και πως λέγεται το άτομο που το διέπραξε;
4 Πώς θα μπορούσε να προστατευθεί ο κ. Ιωάννου από την επίθεση;

Άσκηση 22653

Με βάση αυτό το περιστατικό, απαντήστε στις ακόλουθες ερωτήσεις:
1 Σχολιάστε την επίθεση που δέχθηκε ο κ. Ιωάννου. Πώς είναι γνωστή διεθνώς αυτή η τεχνική;
2. Ποια από τις τρεις βασικές αρχές ασφαλείας των Πληροφοριακών Συστημάτων θεωρείτε ότι παραβιάστηκε στην συγκεκριμένη περίπτωση; Αιτιολογήστε.
3 Πώς λέγεται το ηλεκτρονικό έγκλημα που τελέσθηκε στην περίπτωση αυτή και πως λέγεται το άτομο που το διέπραξε;
4 Πώς θα μπορούσε να προστατευθεί ο κ. Ιωάννου από την επίθεση;

1 Ο σκοπός του παραπλανητικού μηνύματος ήταν να αποκαλύψει ο κ. Ιωάννου τον προσωπικό λογαριασμό του σύνδεσης με το e-banking της τράπεζάς του. Αυτό ανήκει στο χώρο της κοινωνικής μηχανικής. Η τεχνική αυτή απόσπασης πληροφοριών ονομάζεται ψάρεμα (phishing)
2 Προφανώς παραβιάστηκε η αρχή της εμπιστευτικότητας καθώς οι κωδικοί σύνδεσής του κ. Ιωάννου στο online σύστημα της τράπεζας έγιναν διαθέσιμα σε αγνώστους.
3 Πρόκειται για κλοπή δεδομένων και απάτη, ενώ το άτομο ανήκει στην κατηγορία των black hat hackers ή crackers
4 Θα έπρεπε να ελέγξει με προσοχή τη διεύθυνση του αποστολέα του μηνύματος και να το διαγράψει αμέσως. Εννοείται ότι πρέπει απαραίτητα να έχει εγκαταστημένο στο η/υ του ένα ενημερωμένο λογισμικό προστασίας των ηλεκτρονικών μηνυμάτων