

ΤΟ ΤΡΙΠΤΥΧΟ ΑΡΧΩΝ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ:

Εμπιστευτικότητα

Η εμπιστευτικότητα (Confidentiality) είναι ένας από τους βασικούς πυλώνες της κυβερνοασφάλειας και αναφέρεται στην προστασία των δεδομένων και των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Η διατήρηση της εμπιστευτικότητας είναι κρίσιμη για την προστασία της ιδιωτικότητας των χρηστών και των οργανισμών, καθώς και για την αποτροπή διαρροής ευαίσθητων δεδομένων. Η εμπιστευτικότητα διασφαλίζεται με:

Κρυπτογράφηση, μετατροπή των δεδομένων σε κρυπτογραφημένη μορφή για προστασία από μη εξουσιοδοτημένη πρόσβαση.

Έλεγχος Πρόσβασης, καθορισμό και διαχείριση των δικαιωμάτων πρόσβασης των χρηστών σε δεδομένα και συστήματα.

Αυθεντικοποίηση, επιβεβαίωση της ταυτότητας των χρηστών που προσπαθούν να αποκτήσουν πρόσβαση σε πληροφορίες.



Διαχείριση Κωδικών Πρόσβασης, χρήση ισχυρών και μοναδικών κωδικών πρόσβασης και εφαρμογή πολιτικών για την τακτική αλλαγή τους.

Ασφαλής Επικοινωνία, χρήση κρυπτογραφημένων πρωτοκόλλων για την προστασία των δεδομένων κατά τη μεταφορά τους μέσω δικτύων.



ΤΟ ΤΡΙΠΤΥΧΟ ΑΡΧΩΝ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ:

Ακεραιότητα

Η ακεραιότητα αναφέρεται στην ακρίβεια και την πληρότητα των δεδομένων και των πληροφοριών, διασφαλίζοντας ότι δεν έχουν τροποποιηθεί ή καταστραφεί από μη εξουσιοδοτημένους χρήστες ή διεργασίες και διασφαλίζεται με:

Χρήση Κατακερματισμού (Hashing), τη δημιουργία μοναδικών ψηφιακών αποτυπωμάτων για τα δεδομένα, ώστε να είναι δυνατή η ανίχνευση οποιασδήποτε αλλαγής.

Ψηφιακές Υπογραφές, που εξασφαλίζει την αυθεντικότητα και την ακεραιότητα των δεδομένων μέσω κρυπτογραφικών τεχνικών.

Έλεγχο Πρόσβαση, περιορισμό των δικαιωμάτων των χρηστών για την αποτροπή μη εξουσιοδοτημένων αλλαγών.



Διαχείριση Εκδόσεων, παρακολούθηση και διαχείριση των αλλαγών στα δεδομένα και τις εφαρμογές.

Διαγνωστικά και Ελέγχους, με τη χρήση εργαλείων και διαδικασιών για την ανίχνευση και την επιδιόρθωση παραβιάσεων ακεραιότητας.



ΤΟ ΤΡΙΠΤΥΧΟ ΑΡΧΩΝ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ:

Διαθεσιμότητα

Η διαθεσιμότητα διασφαλίζει ότι τα συστήματα, οι εφαρμογές και τα δεδομένα είναι προσβάσιμα και λειτουργικά όταν χρειάζονται από τους εξουσιοδοτημένους χρήστες και επιτυγχάνεται με:

Ανθεκτικότητα (Redundancy), τη χρήση εφεδρικών συστημάτων και υποδομών για την εξασφάλιση της συνέχισης της λειτουργίας σε περίπτωση αποτυχίας.

Σχεδιασμός για Ανάκαμψη από Καταστροφή (Disaster Recovery Planning), περιλαμβάνει τη δημιουργία και την εφαρμογή σχεδίων για την αποκατάσταση της λειτουργίας μετά από καταστροφές.

Δικτυακή Ασφάλεια, προστασία δηλαδή των συστημάτων από επιθέσεις που στοχεύουν στη διακοπή της λειτουργίας τους, όπως επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service- DoS) και καταναμεμημένων επιθέσεων άρνησης παροχής υπηρεσιών (Distributed Denial of Service- DDoS).



Παρακολούθηση και Συντήρηση, που απαιτεί την τακτική παρακολούθηση των συστημάτων και προληπτική συντήρηση για την αποφυγή προβλημάτων.

Διαχείριση Ενημερώσεων, εφαρμογή ενημερώσεων και διορθώσεων λογισμικού για την αποτροπή των τρωτών σημείων.



ΤΟ ΤΡΙΠΤΥΧΟ ΑΡΧΩΝ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ:

Η διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων είναι ζωτικής σημασίας για την προστασία των πληροφοριών από τις διάφορες απειλές.

Η σωστή εφαρμογή των μεθόδων και των πολιτικών ασφάλειας μπορεί να μειώσει τον κίνδυνο παραβίασης της ασφάλειας και να διασφαλίσει την αξιοπιστία και την ακεραιότητα των πληροφοριών.

Η επιτυχία της προστασίας στηρίζεται ιδιαίτερα σε έναν καλό σχεδιασμό πλάνων δράσης, αντιμετώπισης και πρόβλεψης απειλών και δράσεων αποφυγής και αντιμετώπισης.



Ο σωστός σχεδιασμός πριν από ένα περιστατικό θα μειώσει σημαντικά τους κινδύνους μιας επίθεσης και θα αυξήσει σημαντικά τις δυνατότητες έγκαιρης και αποτελεσματικής ανίχνευσης και αντίδρασης σε περίπτωση επίθεσης.

