

Ασφάλεια πληροφοριακών συστημάτων

Τζήκας Δημήτριος
Αλεξάνδρειο ΤΕΙΘ

Καρανικόλας Γιώργος
Αλεξάνδρειο ΤΕΙΘ

29/4/2019

Contents

1	Περίληψη	4
2	Εισαγωγή	4
2.1	Τι είναι ένα πληροφοριακό σύστημα;	4
2.2	Η ιστορία των πληροφοριακών συστημάτων	5
3	Πληροφορία	6
3.1	Χαρακτηριστικά πληροφορίας	7
4	Ασφάλεια και ασφάλεια πληροφοριακών συστημάτων	8
4.1	Ιστορική αναφορά	8
4.2	Ασφάλεια πληροφοριακών συστημάτων	9
4.3	Πολιτική ασφάλειας	9
4.4	Βασικές αρχές	11
4.4.1	Ακεραιότητα	11
4.4.2	Διαθεσιμότητα	11
4.4.3	Εμπιστευτικότητα	11
5	Συμπεράσματα	12

1 Περίληψη

Το συγκεκριμένο έγγραφο αποτελεί τμήμα μιας εργασίας του μαθήματος Δεξιότητες Επικοινωνίας από τους φοιτητές Τζήκας Δημήτριος και Καρανικόλας Γιώργος του ΑΤΕΙ Θεσσαλονίκης. Όπως αναφέρεται και στον τίτλο το θέμα είναι η ασφάλεια των πληροφοριακών συστημάτων, το έγγραφο περιέχει 4 κεφάλαια όπου έχουν ως σκοπό την κατανόηση το τι είναι ένα πληροφοριακό σύστημα, πως κατασκευάζετε ένα πληροφοριακό σύστημα και για ποιο λόγο είναι σημαντική η ασφάλεια σε ένα πληροφοριακό σύστημα.

Το πρώτο κεφάλαιο είναι μια εισαγωγή στο τι είναι ένα πληροφοριακό σύστημα και μια περίληψη της ιστορίας των πληροφοριακών συστημάτων. Το δεύτερο κεφάλαιο αναφέρεται στην πληροφορία. Το τρίτο κεφάλαιο αναφέρεται στην ασφάλεια και επεκτείνεται στην ασφάλεια των πληροφοριακών συστημάτων. Το τέταρτο κεφάλαιο αναφέρεται σε γενικά συμπεράσματα.

Ελπίζουμε να βρείτε το περιεχόμενο ενδιαφέρον, χρήσιμο και καθώς να απολαύσετε την ανάγνωση αυτού του εγγράφου.

2 Εισαγωγή

Πριν γίνει οποιαδήποτε αναφορά στην ασφάλεια των πληροφοριακών συστημάτων θα πρέπει πρώτα να κατανοήσουμε το τι είναι ένα πληροφοριακό σύστημα, πως σχεδιάζονται και γιατί είναι απαραίτητη η ασφάλεια σε ένα πληροφοριακό σύστημα.

2.1 Τι είναι ένα πληροφοριακό σύστημα;

Πληροφοριακό σύστημα είναι ένα σύνολο από συνιστώντα στοιχεία που αλληλεπιδρούν για να παράγουν, αποθηκεύουν, ανακτούν και επεξεργάζονται την πληροφορία. Τα συνιστώντα στοιχεία μπορούν να διακριθούν σε πέντε κατηγορίες:

- Υλικό ηλεκτρονικών υπολογιστών
- Λογισμικό
- Δεδομένα
- Διαδικασίες
- Άνθρωποι

Ένα πληροφοριακό σύστημα μπορεί να μην περιέχει υλικό ηλεκτρονικών υπολογιστών και λογισμικό, γιαυτό τα πληροφοριακά συστήματα μπορούν να χωριστούν σε δύο κατηγορίες, στα πληροφορικά συστήματα όπου είναι υποστηριζόμενα από ηλεκτρονικούς υπολογιστές και στα πληροφοριακά συστήματα χωρίς την υποστήριξη ηλεκτρονικών υπολογιστών. Όμως πάντοτε θα πρέπει να περιέχει ως συνιστώντα στοιχεία τα δεδομένα, τις διαδικασίες και τους ανθρώπους. Ο λόγος που υπάρχει αυτός ο “περιορισμός” είναι επειδή τα πληροφοριακά συστήματα έχουν ως στόχο να βοηθήσουν τους χρήστες τους στην επίτευξη των στόχων τους.

Για να κατανοήσουμε καλύτερα αυτόν τον “περιορισμό” θα δούμε ως παράδειγμα ένα πληροφοριακό σύστημα μιας τράπεζας. Μια τράπεζα χρειάζεται το πληροφοριακό σύστημα για να ενημερώνονται η συναλλαγές χρημάτων. Μόνο από αυτή τη φράση μπορούμε να καταλάβουμε πως είδη έχουμε βάλει τρεις συνιστώσες όπου αυτές είναι: Οι διαδικασίες όπου είναι η συναλλαγή χρημάτων, τα δεδομένα όπου είναι το ποσό της συναλλαγής αλλά ακόμη και η ίδια η συναλλαγή και τέλος οι άνθρωποι όπου κάνουν τις συναλλαγές. Αυτές είναι οι τρεις απαραίτητες συνιστώσες. Όπως ξέρουμε από την καθημερινή μας ζωή, οι τράπεζες έχουν υλικό ηλεκτρονικών υπολογιστών και λογισμικό όπως είναι και περιέχει το ATM αλλά αυτό δεν το κάνει απαραίτητο καθώς μια τράπεζα μπορεί να λειτουργήσει χωρίς ηλεκτρονικούς υπολογιστές, όπως γινόταν περίπου πριν το 1970-1980. Φυσικά, στις μέρες μας κάτι τέτοιο είναι αδιανόητο καθώς μια τέτοια τράπεζα δεν θα μπορούσε να είναι ανταγωνιστική, γιαυτό όσο συνεχίζει η ανάπτυξη την επιστήμης τον υπολογιστών βλέπουμε όλο και περισσότερα πληροφοριακά συστήματα να χρησιμοποιούν ηλεκτρονικού υπολογιστές για να αυξήσουν την ασφάλεια και την ταχύτητα του πληροφοριακού συστήματος.

Τα πληροφοριακά συστήματα εξελίσσονται γρήγορα όπως και η επιστήμη της πληροφορικής, αυτό δημιουργεί θέματα ασφάλειας καθώς τα συστήματα γίνονται ολοένα και πιο περίπλοκα αλλά μαζεύουν και περισσότερη πληροφορία ως αποτέλεσμα να δημιουργούνται περισσότερες τρύπες ασφάλειας αλλά και περισσότερη λόγος για να θελήσει κάποιος να επιτεθεί ένα πληροφοριακό σύστημα. Η επόμενη υποενότητα αναφέρει περιληπτικά την ιστορία των πληροφοριακών συστημάτων, ο στόχος της θα είναι να δούμε πως ξεκίνησε ο τομέας της ασφάλειας στα πληροφοριακά συστήματα.

2.2 Η ιστορία των πληροφοριακών συστημάτων

Η ιστορία των πληροφοριακών συστημάτων συμπίπτει με την ιστορία της επιστήμης των υπολογιστών, όπου ξεκίνησε πολύ πριν από την σύγχρονη επιστήμη των υπολογιστών όπου εμφανίστηκε τον εικοστό αιώνα. Τα πρώτα πληροφοριακά συστήματα που εμφανίστηκαν ήταν πολύ διαφορετικά από τα σύγχρονα τους. Μπορούμε να χωρίσουμε τα πληροφοριακά συστήματα των επιχειρήσεων

σε τέσσερα χρονολογικά τμήματα, το πρώτο ξεκίνησε το 1970 όπου χρειαζόταν η γλώσσα Cobol για τον προγραμματισμό του πληροφοριακού συστήματος, χρησιμοποιούνταν mainframe συστήματα όπου τα δεδομένα ήταν συγκεντρωμένα σε ένα σημείο και οι κύριες λειτουργίες που προσπαθούσαν να υλοποιήσουν τα πληροφοριακά συστήματα ήταν η μισθοδοσία, καταγραφή εμπορευμάτων και η τιμολόγηση. Το 1980 άρχισε να εμφανίζεται η υποστήριξη των προσωπικών υπολογιστών από τα πληροφοριακά συστήματα καθώς και βασικές λειτουργίες δικτύου, κάθε τμήμα της επιχείρησης άρχισε να έχει το δικό της υπολογιστικό σύστημα και οι τελικοί χρήστες χρησιμοποιούσαν υπολογιστές με κειμενογράφους και υπολογιστικά φύλλα έτσι ώστε να μειωθεί η εξάρτηση των τμημάτων από το τμήμα του IT. Το 1990 η ανάγκη για υποστήριξη δικτύων έγινε μεγαλύτερη καθώς τα WAN έγιναν το ντε φάκτο για τις επιχειρήσεις καθώς και τα stand-alone συστήματα άρχισαν να εξαφανίζονται γιατί υπήρχε η ανάγκη για ενσωμάτωση περισσότερων συστημάτων όπως συστήματα διαχείρισης βάσεων δεδομένων έτσι ώστε να υλοποιηθεί ο κεντρικός έλεγχος και η επιχειρησιακή μάθηση. Το 2000 η υποστήριξη του δικτύου άρχισε να αλλάζει μορφή καθώς τα WAN επεκταθήκαν με την διάδοση του Ιντερνετ έτσι ώστε να μπορούν να συνεργάζονται επιχειρήσεις για να πετύχουν γρηγορότερους χρόνους στην παραγωγή και στην παράδοση των προϊόντων.

3 Πληροφορία

Σαφώς εφόσον μιλάμε για πληροφοριακά συστήματα δεν γίνεται να μην κάνουμε μια αναφορά στο τι είναι η πληροφορία και πως την αποθηκεύουμε σε ένα πληροφοριακό σύστημα, σε αυτό το κεφάλαιο θα δούμε τι ακριβώς είναι η πληροφορία έτσι ώστε να κατανοήσουμε γιατί είναι η ασφάλεια των πληροφοριακών συστημάτων σημαντική.

Όλοι μας γνωρίζουμε το τι είναι πληροφορία αλλά μας είναι συνήθως λίγο δύσκολο να δώσουμε έναν ορισμό για το τι είναι πληροφορία, υπάρχουν και περιπτώσεις που σε βιβλία όπως το βιβλίο της πληροφορικής της τρίτης λυκείου, όπου υπάρχει λάθος στον ορισμό της πληροφορίας. Τι είναι όμως η πληροφορία; Ένας ορισμός της πληροφορία είναι αυτός: πληροφορία είναι η γνώση που προκύπτει από τα δεδομένα, όπου τα δεδομένα είναι τα στοιχεία που συγκεντρώνονται και καταχωρούνται ή πληροφορία είναι δεδομένα που έχουν παρουσιασθεί κατά τρόπο που να προσδίδει σε αυτά νόημα. Για να κατανοήσουμε την λεπτή διαφορά των δεδομένων από την πληροφορία μπορούμε να δούμε το εξής παράδειγμα: έχουμε ένα φίλο που μας λέει διάφορους αριθμούς και εμείς τους γράφουμε σε ένα χαρτί, οι αριθμοί που γράψαμε είναι τα δεδομένα μας αλλά δεν μας δίνουν κάποια πληροφορία, αν όμως ο φίλος μας πει πως αυτοί οι αριθμοί είναι η μέση θερμοκρασία ανά ημέρα τότε μπορούμε να βγάλουμε πολ-

λές πληροφορίες από τα δεδομένα μας. Παραδείγματος χάρη πληροφορία είναι η γνώση της θερμοκρασίας που είχε μια συγκεκριμένη ημέρα, επίσης μπορούμε να βγάλουμε από τα δεδομένα μας και άλλες πληροφορίες, μπορούμε να συγκρίνουμε όλες της θερμοκρασίες και να πούμε ποια μέρα ήταν πιο ζεστή ή ποια μέρα ήταν πιο κρύα. Μπορούμε να δούμε μέσα από αυτό το απλό παράδειγμα πως τα δεδομένα μπορούν να μας δώσουν πολλές πληροφορίες, ανάλογα με το τι σημασία δίνουμε στα δεδομένα μπορούμε να βγάλουμε διάφορες πληροφορίες από αυτά. Ειδικά όταν ενώσουμε τα δεδομένα με αλλά δεδομένα τότε το ποσό των πληροφοριών που μπορούμε να βγάλουμε από αυτά είναι πάρα πολύ μεγάλο, γιαυτό συνηθίζουμε να αποθηκεύουμε τα δεδομένα σε πρωτογενή μορφή και σε περίπτωση που θέλουμε κάποια συγκεκριμένη πληροφορία μπορούμε να επεξεργαστούμε κατάλληλα τα δεδομένα.

3.1 Χαρακτηριστικά πληροφορίας

Για να μπορέσουμε να αποθηκεύσουμε την πληροφορία πρέπει να έχουμε τον εκάστοτε αποθηκευτικό χώρο όπου κοστίζει λεφτά γιαυτό διακρίνουμε κάποια χαρακτηριστικά στη πληροφορία έτσι ώστε να γνωρίζουμε διάφορα πράγματα για την πληροφορία όπως το άμα αξίζει να την κρατήσουμε, τα χαρακτηριστικά είναι τα εξής:

- Ακρίβεια

Η καλή πληροφορία είναι και ακριβής. Για να είναι ακριβής θα πρέπει τα δεδομένα που χρησιμοποιήθηκαν για να παραχθεί να είναι ακριβή και πλήρη, και η επεξεργασία να είναι σωστή.

- Επίκαιρη

Η καλή πληροφορία είναι και επίκαιρη, δηλαδή έχει παραχθεί σε χρονική στιγμή που να είναι κατάλληλη για τη χρήση της. Παραδείγματα, επεξεργασίας που διαφέρουν ως προς το χρόνο παραγωγής της πληροφορίας είναι η λεγόμενη επεξεργασία πραγματικού χρόνου και η επεξεργασία κατά ομάδες. Η πρώτη διαθέτει την πληροφορία αμέσως ενώ η δεύτερη μετά την επεξεργασία ενός συνόλου δεδομένων. Βέβαια η πρώτη είναι και δυσκολότερη να επιτευχθεί και κατά συνέπεια ακριβότερη για να υλοποιηθεί.

- Σχετική

Η καλή πληροφορία είναι και σχετική τόσο στο υποκείμενο που τη δέχεται όσο και στο πλαίσιο και το περιβάλλον για το οποίο έχει παραχθεί. Για παράδειγμα, να είναι η πληροφορία που χρειάζεται κάποιος και όχι κάτι άλλο. Να είναι στο επίπεδο λεπτομέρειας που είναι κατάλληλο για το

υποκείμενο. Να μπορεί να ανευρεθεί εύκολα η συγκεκριμένη πληροφορία που απαιτείται μέσα στο σύνολο όλων των πληροφοριών που παράγονται.

- **Στοχευμένη**

Η καλή πληροφορία είναι στοχευμένη. Επειδή σήμερα παράγονται τεράστιες ποσότητες πληροφοριών ενώ ο χρόνος των ανθρώπων που θέλει να τις χρησιμοποιήσει είναι περιορισμένος πρέπει η πληροφορία να είναι στοχευμένη, δηλαδή κατάλληλη για την χρήση της.

- **Ανταποδοτική ως προς το κόστος της**

Η καλή πληροφορία είναι και ανταποδοτική ως προς το κόστος που απαιτείται για να παραχθεί. Το κόστος αυτό αφορά την ανάπτυξη του πληροφοριακού συστήματος που την παράγει, την συντήρηση του, τους ανθρώπους που εργάζονται σε αυτό κλπ. Πρέπει δηλαδή η αξία της πληροφορίας να είναι μεγαλύτερη από το κόστος της.

4 Ασφάλεια και ασφάλεια πληροφοριακών συστημάτων

4.1 Ιστορική αναφορά

Η ασφάλεια πληροφοριακών συστημάτων μελετήθηκε για πρώτη φορά στις αρχές της δεκαετίας του 1970. Η πρώτη σχετική δημοσίευση, από την Ομάδα Εργασίας του Συμβουλίου Αμυντικής Επιστήμης του υπουργείου Άμυνας των ΗΠΑ, εξέτασε το πρόβλημα της χρήσης υπολογιστών εξ αποστάσεως (μέσω τερματικών). Προηγουμένως, η πρόσβαση στους υπολογιστικούς πόρους προϋπέθετε την φυσική παρουσία και πρόσβαση του χρήστη ή του διαχειριστή στον κεντρικό υπολογιστή. Η προσέγγιση στην λύση των προβλημάτων ασφάλειας μέχρι τότε βασιζόταν στην φυσική απομόνωση και προστασία του κεντρικού υπολογιστή καθώς και στον έλεγχο πρόσβασης σε αυτόν. Ένα από τα συμπεράσματα στην αναφορά της Ομάδας Εργασίας ήταν ότι ο χρήστης δεν θα έπρεπε να δημιουργήσει το δικό του κωδικό πρόσβασης, μια πρόταση που ποτέ δεν υιοθετήθηκε ευρέως. Άλλες καινοτόμες ιδέες που εκφράστηκαν στην ανάλυση είχαν μεγαλύτερη απήχηση. Για παράδειγμα, αναγνωρίστηκε από τους ερευνητές η αρχή της ισορροπίας μεταξύ της ευκολίας της εργασίας του χρήστη και της προστασίας των πληροφοριών και σήμερα έχει καταλήξει θεμέλιος λίθος στη δημιουργία πολιτικών ασφάλειας.

Ο πρώτος ιός, ο Creeper, εμφανίστηκε επίσης στις αρχές της δεκαετίας του 1970 στο ARPANET, και το πρώτο δίκτυο "σουλήχι", το σουλήχι Morris,

κυκλοφόρησε το 1998. Εκτιμάται ότι 6.000 συστήματα προσβλήθηκαν από το "σκουλήκι". Το 2007 ανακαλύφθηκαν περισσότεροι από 711.000 καινούργιοι ιοί.

Παρόλο που ο πρώτος υπολογιστής με το λειτουργικό σύστημα Multics εγκαταστάθηκε το 1967 με κωδικό πρόσβασης για χρήστες και με άλλα μέτρα ασφάλειας στο σχεδιασμό του, και δύο από τους δημιουργούς του, ο Ken Thompson και ο Dennis Ritchie, έπαιζαν κρίσιμο ρόλο στην ανάπτυξη του Unix, η πρώτη έκδοση του Unix δεν διέθετε κωδικούς. Η λειτουργία αυτή προστέθηκε αργότερα, το 1973. Σήμερα η χρήση αδύναμων κωδικών πρόσβασης παραμένει μία από τις κυριότερες δυσκολίες που αντιμετωπίζει ο επαγγελματίας στον τομέα. Χρησιμοποιούνται και άλλες μέθοδοι αυθεντικοποίησης, για παράδειγμα οι έξυπνες κάρτες, αλλά μόνο σε συγκεκριμένους τομείς.

4.2 Ασφάλεια πληροφοριακών συστημάτων

Με τον όρο ασφάλεια αναφερόμαστε στο κατά πόσο ένα σύστημα μπορεί να ανταπεξέλθει σε τυχαία ή σκόπιμη απειλή. Με το όρο απειλή αναφερόμαστε σε οτιδήποτε θα μπορούσε να δημιουργήσει πρόβλημα στο πληροφοριακό σύστημα, παραδείγματος χάρη η κλοπή ή η χρήση, διαγραφή δεδομένων από μη αρμόδια άτομα θα μπορούσε να είναι ολέθρια για έναν οργανισμό ή επιχείρηση. Μπορούμε πολύ εύκολα να κατανοήσουμε το πόσο σημαντικός είναι ο ρόλος της ασφάλειας των πληροφοριακών συστημάτων, επίσης μπορούμε να αναφερόμαστε σε αυτό το γνωστικό πεδίο ως ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών.

4.3 Πολιτική ασφάλειας

Ένας τρόπος για να μπορέσουμε να έχουμε καλύτερη ασφάλεια σε ένα πληροφοριακό σύστημα είναι με το να σχεδιάσουμε μια πολιτική ασφάλειας. Η πολιτική ασφάλειας έχει ως σκοπό την μείωση κινδύνων και συνδέεται άμεσα τόσο με τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με ηθικό-κοινωνικές αντιλήψεις, αρχές και παραδοχές. Ο σχεδιασμός της πολιτικής ασφάλειας είναι ένα δύσκολο και σημαντικό βήμα, επίσης οφείλει κάθε πολιτική ασφάλειας να τηρεί την αρχή της αποκέντρωσης, της ύπαρξης αντικατάστασης και της άμυνας σε βάθος. Θέλει πολύ σκέψη καθώς μια λάθος πρακτική θα μπορούσε να στοιχίσει πολλά στον οργανισμό καθώς και η αλλαγή μιας πρακτικής είναι δύσκολη ως και αδύνατη καθώς το πληροφοριακό σύστημα σχεδιάζεται με γνώμονα αυτών των πρακτικών. Συνηθίζεται από οργανισμούς να ακολουθούν πρότυπα πολιτικής ασφάλειας καθώς η δημιουργία πολιτικής ασφάλειας από την αρχή είναι συνήθως άσκοπη, χρονοβόρα και στοιχίζει πολλά λεφτά.

Επιπλέον θεμελιώνεται η σημασία της ασφάλειας του πληροφοριακού συστήματος για τα μέλη του οργανισμού, δημιουργείται μια κουλτούρα ασφαλείας

καθώς πολλές φορές αποτελεί νομική υποχρέωση και αποτελεί παράγοντα εμπιστοσύνης μεταξύ οργανισμού και πελατών. Τα είδη των πολιτικών ασφαλείας είναι α)τα τεχνικά συστήματα πληροφοριών, λειτουργικά συστήματα και δίκτυα υπολογιστών β)τα οργανωτικά και γ)τα ατομικά. Περιλαμβάνει αποσπασματική διαχείριση της ασφάλειας πληροφοριακών συστημάτων και μεγάλη πολυπλοκότητα στη συντήρηση ενώ είναι αποτελεσματική σε αυτόνομες εφαρμογές και υπολογιστικά συστήματα που δεν συνδέονται μεταξύ τους.

Σε ένα ενιαίο έγγραφο μη εύχρηστο λόγω όγκου και με πληροφορίες γενικού επιπέδου αναφέρονται όλα τα υπολογιστικά συστήματα, οι εφαρμογές και η διαδικασία του πληροφοριακού συστήματος.

Τις απαιτήσεις για την ασφάλεια του πληροφοριακού συστήματος πρέπει να την ικανοποιεί η πολιτική ασφάλεια που προέρχονται από όλους τους εμπλεκόμενους στη χρήση και στη λειτουργία του πληροφοριακού συστήματος ενός οργανισμού που είναι οι χρήστες και οι διαχειριστές του πληροφοριακού συστήματος, η διοίκηση του οργανισμού, οι πελάτες του οργανισμού, οι νομικές και κανονιστικές διατάξεις που διέπουν την λειτουργία τους.

Ο καθορισμός της πολιτικής ασφάλειας του πληροφοριακού συστήματος θα πρέπει να καλύπτουν οι ακόλουθες κατηγορίες:

- Ζητήματα προσωπικού
- Φυσική ασφάλεια
- Έλεγχος πρόσβασης στο πληροφοριακό σύστημα
- Διαχείριση υλικών και λογισμικών
- Νομικές υποχρεώσεις
- Διαχείριση της πολιτικής ασφάλειας
- Οργανωτική δομή
- Σχέδιο συνέχισης λειτουργίας

Όταν εφαρμόζουμε μια πολιτική ασφαλείας επιδιώκουμε: οι οδηγίες και τα μέτρα προστασίας οφείλουν να καλύπτουν το σύνολο των αγαθών και όλες τις λειτουργίες(πληρότητα) να λάβουμε υπόψη τις τρέχουσες τεχνολογικές εξελίξεις (επικαιρότητα) με κάποιες τροποποιήσεις ή προσθήκες να μπορεί η πολιτική να καλύπτει μικρές αλλαγές ή επεκτάσεις στο πληροφοριακό σύστημα (γενικευσιμότητα). Επιπλέον πρέπει να υπάρχει σαφήνεια και εύκολη κατανόηση, τεχνολογική ανεξαρτησία και καταλληλότητα ανάλογα με τον οργανισμό που απευθύνεται.

4.4 Βασικές αρχές

Η ασφάλεια πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές ιδέες.

4.4.1 Ακεραιότητα

Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα. Ακριβώς αυτό συνέβη το 1995, όταν άγνωστα άτομα κατάφεραν να εξουδετερώσουν τα μέτρα ασφάλειας της Ελευθεροτυπίας και να εισαγάγουν πρωτοσέλιδο άρθρο για τον πρόωρο θάνατο του Ανδρέα Παπανδρέου, που εκείνη τη στιγμή νοσηλευόταν στο Ωνάσειο.

4.4.2 Διαθεσιμότητα

Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών, που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι είτε προσωρινά, είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα.

4.4.3 Εμπιστευτικότητα

Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή, π.χ. με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας εταιρίας. Το 2006 μια μελέτη με τη συνεργασία 480 εταιριών έδειχνε ότι 80% των εταιριών είχε πρόβλημα με διαρροή πληροφοριών λόγω κλοπής φορητού.

5 Συμπεράσματα

Τα πληροφοριακά συστήματα είναι ένας μεγάλος κλάδος της τεχνολογίας της πληροφορίας και εξελίσσεται με γρήγορους ρυθμούς και με το πέρασμα του χρόνου προστίθενται ολοένα και περισσότερες τεχνολογίες. Στις μέρες μας για να δημιουργηθεί ένα πληροφοριακό σύστημα είναι αρκετά δύσκολη υπόθεση και απαιτεί πολύ εργασία από πολλά άτομα, η ασφάλεια του πληροφοριακού συστήματος είναι ζωτικής σημασίας και είναι αδύνατο να δημιουργήσουμε ένα ασφαλές πληροφοριακό σύστημα αλλά αυτό δεν σημαίνει πως δεν πρέπει να έχουμε μέτρα ασφάλειας. Για να μπορέσουμε να έχουμε ένα ασφαλές πληροφοριακό σύστημα θα πρέπει να ενημερωνόμαστε για τις τελευταίες τρύπες ασφάλειας και να τηρούνται οι αρχές ασφάλειας χωρίς εξαιρέσεις, επίσης θα πρέπει να υπάρχουν πάντα σενάρια επιδιορθώσεων και αντιμετώπισης επιθέσεων έτσι ώστε η ζημιά που θα δεχτεί το πληροφοριακό σύστημα να είναι όσο το δυνατό λιγότερη.

Αναφορές

- [1] Μαυρίδης, Ι., *Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών*, «Ασφάλεια πληροφοριών στο διαδίκτυο», ηλεκτρ. βιβλ., 2019, (ΙΣΒΝ 978-960-603-193-9)
- [2] *uwosh.edu*, The History of Information Systems in Business ιστοσελίδα, 25/4/2019, (http://www.uwosh.edu/faculty_staff/wresch/311ISHistory.htm)
- [3] Antony Bryant, *Journal of Information Technology (2013)*, Information Systems history ιστοσελίδα, 2013, (<https://link.springer.com/content/pdf/10.1057%2Fjit.2013.3.pdf>)
- [4] Sean Boran, (2003), «IT Security Cookbook» 25/4/2019,
- [5] DeNardis, L. (2007). "Chapter 24: A History of Internet Security". In de Leeuw, K.M.M.; Bergstra, J. (eds.). *The History of Information Security: A Comprehensive Handbook*. Elsevier. pp. 681–704. ISBN 9780080550589.
- [6] Εφαρμογές Πληροφορικής Υπολογιστών (Α, Β, Γ Γενικού Λυχείου - Γενικής Παιδείας), (<http://ebooks.edu.gr/modules/ebook/show.php/DSGL-C127/577/3745,16422>), 24/4/2019