

ΕΞΩΦΥΛΛΟ

***ΑΝΑΠΤΥΞΗ ΕΦΑΡΜΟΓΗΣ ΣΕ PYTHON ΓΙΑ
ΔΙΑΧΕΙΡΙΣΗ ΧΡΗΣΤΩΝ***

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ	4
ΠΕΡΙΛΗΨΗ	5
ΚΕΦΑΛΑΙΟ 1: Βασικά γνωρίσματα της Python.....	6
1.1 Εισαγωγή	6
1.2 Ιστορικά στοιχεία	6
1.3 Ανάλυση της θεματικής της Python	7
1.4 Χαρακτηριστικά της Python.....	8
1.5 Εφαρμογές της Python	11
ΚΕΦΑΛΑΙΟ 2: Πληροφοριακά Συστήματα	12
2.1 Εισαγωγή	12
2.2 Ορισμός και λειτουργία πληροφοριακών συστημάτων	13
2.3 Πλεονεκτήματα και μειονεκτήματα πληροφοριακών συστημάτων 15	
2.4 Βασικές λειτουργίες πληροφοριακών συστημάτων	19
2.5 Κατηγορίες πληροφοριακών συστημάτων	20
2.6 Είδη πληροφοριακών συστημάτων	22
2.7 Ασφάλεια των πληροφοριακών συστημάτων	25
2.8 Επιθέσεις στα πληροφοριακά συστήματα ασφάλειας.....	26
ΚΕΦΑΛΑΙΟ 3: Αυθεντικοποίηση χρηστών.....	28
3.1 Έλεγχος αυθεντικότητας και διατήρησης δεδομένων	28
3.2 Συντελεστές και είδη αυθεντικοποίησης	29
3.3 Χρηστικότητα των μεθόδων αυθεντικοποίησης.....	30

3.4	Συστήματα κρυπτογράφησης δεδομένων	32
3.5	Κωδικοποίηση tokens	34
3.6	Πρότυπα χρηστικότητας αυθεντικοποίησης.....	36
3.7	Κωδικοποίηση one time password (OTP)	41
3.8	Πλεονεκτήματα και μειονεκτήματα των one time passwords.....	44
ΚΕΦΑΛΑΙΟ 4: Υλοποίηση Εφαρμογής Αυθεντικοποίησης 2		
παραγόντων		47
(two factor authentication).....		47
4.1	Αυθεντικοποίηση 2 παραγόντων	47
4.2	Πως λειτουργεί η αυθεντικοποίηση 2 παραγόντων	47
4.3	Λεπτομέρειες Υλοποίησης.....	48
4.4	Δημιουργία ενός απλού Flask Server	48
4.5	Αυθεντικοποίηση ενός παράγοντα.....	49
4.6	Αυθεντικοποίηση 2 παραγόντων χρησιμοποιώντας TOTP	52
Βιβλιογραφικές Αναφορές		58

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

Εικόνα 1: Πληροφοριακό σύστημα (Πηγή: Φωλίνας, 2007)	13
Εικόνα 2: Σχηματική αναπαράσταση ενός μοντέλου (Πηγή: Γιαννακόπουλος & Παπουτσής, 1995).....	15
Εικόνα 3: Βασικές λειτουργίες Πληροφοριακών Συστημάτων	20
Εικόνα 4: Προσκόμιση συστημάτων μιας εταιρείας.....	22
Εικόνα 5: Σχέση διαφόρων τύπων Πληροφοριακών Συστημάτων (Πηγή: τροποποιημένο Laudon K. C., Laudon J. P., 2002)	25
Εικόνα 6: Εφαρμογές των Tokens (Πηγή: Voshmgir, 2019).....	36
Εικόνα 7: Φόρμα εισαγωγής στοιχείων εισόδου.....	51
Εικόνα 8: Εισαγωγή λανθασμένων στοιχείων χρήστη και μήνυμα σφάλματος	52
Εικόνα 9: Εισαγωγή ορθών στοιχείων χρήστη και μήνυμα επιτυχούς αυθεντικοποίησης	52
Εικόνα 10: Οδηγίες εγκατάστασης και αυθεντικοποίησης Google Authenticator	56
Εικόνα 11: Περίπτωση εισαγωγής λανθασμένου token και μήνυμα σφάλματος	57
Εικόνα 12: Περίπτωση εισαγωγής έγκυρου token και μήνυμα εγκυρότητας	57

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία μελετά το φαινόμενο της αυθεντικοποίησης των χρηστών εντάσσοντας την στα πληροφοριακά συστήματα. Το φαινόμενο των πληροφοριακών συστημάτων τα τελευταία χρόνια επιδεικνύει αύξουσα πορεία και γίνεται εμφανές πως η κοινωνία, τα άτομα αλλά και οι εταιρείες έχουν διευκολυνθεί με τα πλεονεκτήματα που παρουσιάζουν τα πληροφοριακά συστήματα.

Η πτυχιακή εργασία αποτελείται από το θεωρητικό μέρος και στη συνέχεια ακολουθεί το εμπειρικό μέρος. Το θεωρητικό μέρος απαρτίζεται από τρία βασικά κεφάλαια, στα οποία βασίζεται το εμπειρικό μέρος και απαρτίζουν τη σημαντικότητα της παρούσης πτυχιακής εργασίας. Στο πρώτο κεφάλαιο γίνεται αναφορά στη γλώσσα Python, δίνοντας τα σημαντικά γνωρίσματα με βάση τη σύγχρονη ξενόγλωσση και ελληνόγλωσση βιβλιογραφία. Επισημαίνεται εννοιολογικά το τι είναι η γλώσσα Python και δίνοντας ορισμένα βασικά ιστορικά σημεία. Στη συνέχεια, αναλύεται η θεματική της γλώσσας Python, δίνοντας βαρύτητα στα σημαντικά χαρακτηριστικά που έχει και επισημαίνοντας τις εφαρμογές που λειτουργούν και έχουν δημιουργηθεί με τη γλώσσα Python.

Στο δεύτερο κεφάλαιο γίνεται λόγος για τα πληροφοριακά συστήματα. Επισημαίνονται εννοιολογικά η έννοια των πληροφοριακών συστημάτων καθώς και ποια είναι η λειτουργία τους. Στη συνέχεια, αναφέρονται ποια είναι τα πλεονεκτήματα και τα μειονεκτήματα που ενδέχεται να έχουν τα πληροφοριακά συστήματα καθώς και ποιες είναι οι βασικές τους λειτουργίες. Έπειτα, υπογραμμίζονται τα είδη και σε ποιες κατηγορίες διαίρονται πληροφοριακά συστήματα καθώς και την ασφάλεια που έχουν προκειμένου να αποτρέπονται οι τυχόν επιθέσεις σε λογισμικά, εφαρμογές και προγράμματα.

Τέλος, στο τρίτο θεωρητικό κεφάλαιο αναφέρεται η αυθεντικοποίηση που πρέπει να έχουν οι χρήστες σε προγράμματα και σε εφαρμογές. Δίνεται βαρύτητα η έννοια αυθεντικοποίηση καθώς και η κρυπτογράφηση σε θέματα ασφαλείας. Επίσης, υπογραμμίζεται στο πόσο χρησιμεύει η αυθεντικότητα και η τήρηση των δεδομένων κάνοντας αναφορά στη κωδικοποίηση tokens και τη κωδικοποίηση με one time password (OTP).

Λέξεις – κλειδιά:

Γλώσσα Python, πληροφοριακά συστήματα, αυθεντικοποίηση, tokens, κωδικοποίηση one time password (OTP).

ΚΕΦΑΛΑΙΟ 1: Βασικά γνωρίσματα της Python

1.1 Εισαγωγή

Η Python θεωρείται μια από τις πιο εύκολες στην μάθηση, καθώς λογίζεται ως μια από τις ισχυρές γλώσσες προγραμματισμού. Φέρνει γόνιμες δομές δεδομένων υψηλού τομέα, καθώς και μια απλή, αλλά εποικοδομητική γεφύρωση στον αντικειμενοστραφή προγραμματισμό. Η καλαίσθητη συγγραφή της Python και τα δυναμικά είδη της, συνάμα με τη λειτουργία της ως διερμηνευόμενη (σε αντίθεση μεταγλωττιζόμενης) γλώσσα, την κάνουν να φαίνεται ως μια ιδεώδης γλώσσα για το σχηματισμό υποθέσεων εντολών και για τη γρήγορη ανάπτυξη εφαρμογών σε αρκετούς κλάδους και σε πολλές πλατφόρμες.

Η γλώσσα προγραμματισμού Python θεωρείται μια υψηλού επιπέδου γλώσσα, η οποία επινοήθηκε από τον Ολλανδό Γκβίντο βαν Ρόσσουμ (Guido van Rossum) κατά το έτος 1990. Ο βασικός σκοπός της γλώσσας είναι ιδίως να αναγνωριστεί διεθνώς του κώδικά της, να αποσαφηνιστεί η ευχέρεια όταν χρησιμοποιείται από στελέχη και, τέλος το συντακτικό της εγκρίνει στους προγραμματιστές να φανερώσουν σημασίες σε πιο λίγες γραμμές κώδικα σε αντίθεση από άλλες γλώσσες όπως η C++ ή η Java. Παρατηρείται πως η γλώσσα αυτή έχει σημαντικές βιβλιοθήκες και έτσι διευκολύνεται η ταχύτητα της μάθησής της μέσα από πολλές καθορισμένες ενασχολήσεις. Οι διερμηνευτές της Python είναι σε θέση να την εγκαταστήσουν σε πολλά λειτουργικά μοντέλα, εγκρίνοντας στην Python την εφαρμογή κώδικα σε μεγάλη ποικιλία μοντέλων (Downey, 2012).

Κάνοντας χρήση άλλα εργαλεία, όπως για παράδειγμα το Py2exe ή το Pyinstaller, ο κώδικας της Python ενδέχεται να εφαρμοστεί σε αυτοδιοίκητα προγράμματα που εκτελούνται για ορισμένα από τα πιο γνωστά λειτουργικά μοντέλα, εγκρίνοντας τον καταμερισμό του βασισμένου σε Python λογισμικού για χρησιμοποίηση σε αυτά τους χώρους χωρίς να χρειάζεται να γίνει εγκατάσταση από τον διερμηνευτή της Python. Η Python ευδοκimei ως ανοιχτό λογισμικό (open source) και η χρήση της πραγματοποιείται από τη μη κερδοσκοπική εταιρεία Python Software Foundation. Ο κώδικας μοιράζεται με την εξουσιοδότηση Python Software Foundation License η οποία ταιριάζει με την GPL. (Downey, 2012).

1.2 Ιστορικά στοιχεία

Η γλώσσα Python, όπως προαναφέρθηκε θεωρείται μια διερμηνευόμενη (interpreted), αλληλεπιδραστική (interactive) και προσανατολισμένη σε

αντικείμενα (object – oriented) γλώσσα προγραμματισμού, η οποία αναπτύχθηκε από τον Ολλανδό Guido van Rossum, το 1990. Το όνομά της πηγάζει από ένα από τα αγαπημένες τηλεοπτικές εκπομπές του van Rossum, «Το Ιπτάμενο Τσίρκο» των Monty Python's. Η Python είναι μια γλώσσα, η οποία εναρμονίζει τη δηλωτική δύναμη με μια πολύ σαφή σύνταξη. Η ίδια κάνει χρήση διαφόρων ενοτήτων (modules), τάξεων (classes), εξαιρέσεων (exceptions) καθώς και αρκετά υψηλού τομέα δυναμικών τύπων δεδομένων.

Η διεθνής ιστοσελίδα της γλώσσας είναι η <http://www.python.org>. Η γλώσσα Python αναπτύχθηκε το 1990 στο CWI του Άμστερνταμ και εξακολουθεί μέχρι και σήμερα στο CNRI του Reston. Η γλώσσα αυτή, έχει μια κομψότητα αν και δεν θεωρείται ότι η σύνταξη της είναι τόσο απλή, έχοντας μια ελάχιστη ποσότητα από ανθεκτικούς και υψηλού επιπέδου τύπους στοιχείων. Η Python ενδέχεται να εξαπλωθεί συμπληρώνοντας νέες ενότητες που να είναι γραμμένες σε μια γλώσσα που μεταφράζεται, όπως είναι η C ή η C++. Αυτά οι ενότητες διεύρυνσης δύνανται να οριοθετήσουν νέες αλληλεξαρτήσεις και μεταβλητές, καθώς επίσης και σύγχρονους τύπους δεδομένων.

Η γλώσσα Python παραβάλλεται συχνά με άλλες διερμηνευόμενες γλώσσες προγραμματισμού, όπως για παράδειγμα οι Java, JavaScript, Perl, Tcl και η Smalltalk, αλλά αντιπαραβολές δύνανται να παραχθούν και με τις C++, Common Lisp και Scheme. Η Python 2.0 βγήκε σε κυκλοφορία στις 16 Οκτωβρίου του 2000. Στη συνέχεια, στις 3 Δεκεμβρίου 2008 δημοσιεύθηκε η έκδοση 3.0 (αναγνωρισμένη και ως py3k ή python 3000). Αρκετά από τα σύγχρονα γνωρίσματα αυτής της έκδοσης έχουν μετακινηθεί στις εκδόσεις 2.6 και 2.7 που είναι προς τα πίσω συμβατές. Η python 3 θεωρείται ιστορικά ως η πρώτη γλώσσα προγραμματισμού που «τσακίζει» την προς τα πίσω τη συμφωνία με προγενέστερες εκδόσεις, προκειμένου να διορθωθούν κάποια σφάλματα που ενδημούσαν σε παλαιότερες εκδόσεις και να γίνει ακόμα πιο καταληπτός ο απλός τρόπος με τον οποίο δύνανται να παραχθούν ορισμένα πράγματα.

1.3 Ανάλυση της θεματικής της Python

Η Python αποτελεί μια ενεργή γλώσσα και γλώσσα προγραμματισμού. Αυτό εννοεί ότι εάν και είναι μια διερμηνευόμενη γλώσσα, δηλαδή δεν χρειάζεται να γίνει μεταγλώττιση ο κώδικας, απλά σώζεται στην εφαρμογή, διαφυλάσσει τα μεγαλύτερα προτερήματα μιας συνηθισμένης γλώσσας προγραμματισμού (π.χ. Java, VB.). Παρακάτω αναλύεται πιο συγκεκριμένα η γλώσσα Python:

- Θεωρείται μια «απλή γλώσσα προγραμματισμού», ενώ πολλές φορές κατηγοριοποιείται στις πολύ υψηλού επιπέδου γλώσσες. Αυτοί οι δύο

χαρακτήρες σχετίζονται ιδίως στην απλή σύνταξη και στους «γενικούς» τύπους στοιχείων, που της εγκρίνουν σημαντικό τομέα εφαρμογής).

- Συγκατατίθεται στο σχηματισμό ενοτήτων που δύνανται να χρησιμοποιηθούν ευχερώς από άλλες εφαρμογές που έχουν γραφτεί σε Python γλώσσα.
- Είναι προσανατολισμένη στην σύνταξη ελασσόνων και συμπυκνωμένων εφαρμογών. Έτσι, τα σχέδια σε Python είναι εκδήλως ελάσσονα από τα ομόλογά τους σε γλώσσες όπως οι C / C++ ή Java.
- Το όνομά της συνδέεται με το show του BBC «Το Ιπτάμενο Τσίρκο» και όχι με το αναγνωρισμένο ερπετό.

Ο κώδικας σε γλώσσα προγραμματισμού Python δύναται:

1. Να ενταχθεί σε πολλά λειτουργικά μοντέλα.
2. Να διαβαστεί με ευχέρεια και να τροποποιηθεί / αναπτυχθεί από άλλα μέλη, επινοώντας ένα συλλογικό αγώνα πολύ πιο δυνατό και εφικτό.
3. Να αποσαφηνιστούν ευχερώς τυχόν απροσεξίες στον κώδικα και να διορθωθούν.
4. Να ανακαλυφθούν ευχερώς οι ικανότητες του προγράμματος με τις λεγόμενες ενότητες στην Python.

1.4 Χαρακτηριστικά της Python

Τα χαρακτηριστικά της Python κατηγοριοποιούνται ως εξής (Τερζίδου & Δασυγένης, 2016):

1. Απλή

Η Python θεωρείται μια απλή και μινιμαλιστική γλώσσα. Η μελέτη ενός καλού σχεδίου σε Python παρομοιάζεται ως τη μελέτη των Αγγλικών. Αυτή η συμφωνία της Python με ψευδοκώδικα είναι ένα από τα πιο σθεναρά τμήματα της. Επιτρέπει να συγκεντρώνεται κάποιος για να ανακαλύψει τη λύση του ζητήματος σε αντίθεση με την ίδια τη γλώσσα.

2. Εύκολη στην εκμάθηση

Η Python είναι εύκολη γλώσσα στο να ξεκινήσει κάποιος να τη μαθαίνει. Η Python κατέχει μια ασυνήθιστα απλή συγγραφή, όπως έχει ήδη προαναφερθεί.

3. Ελεύθερη και Ανοικτού Κώδικα

Η γλώσσα Python θεωρείται ένα παράδειγμα ΕΛΛΑΚ (Ελεύθερο Λογισμικό και Λογισμικό Ανοικτού Κώδικα). Συνεπώς, υπάρχουν αντίγραφα για αυτό το λογισμικό, προκειμένου να διαβαστεί ο πηγαίος κώδικάς του, και να γίνουν μετατροπές σ' αυτό, ώστε να χρησιμοποιηθούν τμήματα του σε σύγχρονα ελεύθερα προγράμματα. Το ΕΛΛΑΚ συναρτάται στην αντίληψη μιας κοινότητας που μοιράζεται τη πληροφορία. Η Python είναι τόσο καλή, διότι παρήχθη και αναβαθμίζεται όλο και πιο πολύ από μια ομάδα που το μόνο που επιθυμεί είναι μια βελτιωμένη Python.

4. Φορητή

Εξαιτίας του ανοικτού της κώδικα, η Python έχει πραγματοποιηθεί σε αρκετές εφαρμογές. Όλα τα Python προγράμματα δύνανται να λειτουργήσουν σε οποιαδήποτε από αυτές τις εφαρμογές δίχως να απαιτούνται καθόλου μεταβολές. Χρησιμοποιώντας την Python στο Linux, στα Windows, στο FreeBSD, σε Macintosh, στο Solaris, στο OS/2, στην Amiga, στο AROS, στο AS/400, στο BeOS, στο OS/390, στο z/OS, στο Palm OS, στο QNX, στο VMS, στο Psion, στο Acorn RISC OS, στο WxWorks, σε PlayStation, στο SharpZaurus, στα Windows CE ακόμα και σε PocketPC.

5. Γλώσσα υψηλού επιπέδου

Όταν γίνεται συγγραφή σε προγράμματα στην Python, δεν θεωρείται απαραίτητο να δίνεται σημασία στις χαμηλού επιπέδου μικρά στοιχεία όπως η διαχείριση της μνήμης που γίνεται χρήση από τα προγράμματα.

6. Διερμηνευόμενη

Ένα πρόγραμμα που συντάσσεται σε μια μεταφρασμένη γλώσσα όπως η C ή η C++ μεταβάλλεται από την πηγαία γλώσσα, σε μια γλώσσα που «μιλάει ο υπολογιστής» (δυαδικός κώδικας δηλαδή 0 και 1) κάνοντας χρήση ένα μεταγλωττιστή με πολλές σημαίες και επιλογές. Καθώς «τρέχει» ένα πρόγραμμα, ο συνδέτης απομιμείται το πρόγραμμα στη μνήμη και ξεκινά να το «τρέχει». Η Python, από την άλλη, δε έχει ανάγκη μετάφρασης σε δυαδικό αρχείο. Απλώς «τρέχει» το πρόγραμμα αμέσως από τον πηγαίο κώδικα. Η Python τροποποιεί τον πηγαίο κώδικα σε μια μεσαία θωριά επονομαζόμενη bytecode και στη συνέχεια το ερμηνεύει στη γλώσσα του υπολογιστή και μετά

το «τρέχει». Αυτή η διαδικασία, στην πραγματικότητα χρησιμοποιεί την Python πιο εύκολα, εφόσον δεν απαιτείται η ανησυχία για τη μετάφραση του προγράμματος, τη συνοχή με τις αρμόζουσες βιβλιοθήκες. Επιπροσθέτως κάνει τα προγράμματα της Python εξαιρετικά φορητά, εφόσον δύναται να γίνει αντιγραφή του προγράμματος Python που δημιουργήθηκε σε έναν άλλο υπολογιστή λειτουργώντας με ευχέρεια.

7. Επεκτάσιμη

Αν υπάρχει ανάγκη να δημιουργηθεί ένα σημαντικό τμήμα κώδικα, ώστε να «τρέχει» πολύ γρήγορα ή αν πρέπει να υπάρχει ένα τμήμα ενός αλγόριθμου που να είναι κλειδωμένο, τότε υπάρχει πιθανότητα προγραμματισμού αυτού του τμήματος σε C ή C++ και μετά να γίνει χρήση στο Python πρόγραμμα.

8. Αντικειμενοστραφής

Η Python ενισχύει τόσο το διαδικασιοστρεφή προγραμματισμό όσο και τον αντικειμενοστραφή προγραμματισμό. Στο διαδικασιοστρεφή προγραμματισμό, η μέθοδος διαρθρώνεται πάνω σε λειτουργίες ή αλληλεξαρτήσεις, οι οποίες δεν θεωρούνται επαναχρησιμοποιήσιμα τμήματα από σχέδια. Στις αντικειμενοστραφείς γλώσσες, το σχέδιο διαρθρώνεται πάνω σε αντικείμενα, τα οποία εναρμονίζουν στοιχεία και λειτουργικότητα. Η Python έχοντας έναν ισχυρό αλλά και απλό τρόπο για αντικειμενοστραφή προγραμματισμό, μπορεί να συγκριθεί με μεγάλες γλώσσες, όπως η C++ ή η Java.

9. Ενσωματώσιμη

Ενσωματώνεται η Python μέσα στα προγράμματα σε C/C++ για να δοθεί δυνατότητα ενεργειών για μέλη.

10. Εκτεταμένες βιβλιοθήκες

Η πρότυπη βιβλιοθήκη της Python είναι ουσιαστικά υπερβολικά μεγάλη. Βοηθά στο να δοθούν πολλά πράγματα συναρτώμενα με κανονικές αποδώσεις, σχηματισμό απόδειξης, έλεγχοι μονάδων, νημάτωση, βάσεις δεδομένων, περιηγητές ιστού, CGI, FTP, email, XML, XML-RPC, HTML, αρχεία WAV, κρυπτογράφηση, γραφικές διεπαφές χρήστη (GUI – graphical user interfaces), Tk, τα οποία εξαρτώνται από το μοντέλο. Τα παραπάνω είναι διαθέσιμα όποτε έχει εγκατασταθεί η Python. Αυτό καλείται ως η φιλοσοφία «Batteries Included» της Python. Τέλος, από την πρότυπη βιβλιοθήκη, υπάρχουν πολλές άλλες βιβλιοθήκες υψηλής ιδιοσυστασίας όπως η wxPython, η Twisted, η Python Imaging Library και άλλες πολλές.

1.5 Εφαρμογές της Python

Οι εφαρμογές της Python ταξινομούνται ως εξής (GitHub, 2019 & Matthes, 2016 & Mertz, 2015):

1. Δικτυακές εφαρμογές

Ενδέχεται να χρησιμοποιηθεί για το σχηματισμό επεκτάσιμων διαδικτυακών εφαρμογών με περιθώρια και μοντέλα χρήσης περιεχομένου, τα οποία βρίσκονται στην Python. Ορισμένες αναγνωρισμένες διαδικτυακές ιστοσελίδες όπως το Mozilla, το Reddit και το Instagram, όπου έχουν γραφτεί σε γλώσσα Python.

2. Σχηματισμός καινοτόμων λογισμικών

Η γλώσσα Python θεωρείται μια αργή γλώσσα σε αντιπαράβολή με τις άλλες γλώσσες όπως η C ++ και η Java. Δεν θεωρείται ποιοτική διαλογή, εάν οι πόροι είναι καθορισμένοι και έτσι απαιτούν ικανοποιητικές επιδόσεις. Όμως, η Python θεωρείται η γλώσσα, που δύναται να χρησιμοποιηθεί για το σχηματισμό καινοτόμων εφαρμογών. Για παράδειγμα το Pygame, βιβλιοθήκη για την δημιουργία παιχνιδιών) δύναται να δημιουργήσει ένα καινοτόμο παιχνίδι, το οποίο εάν θέλει κάποιος στη συνέχεια να το αξιοποιήσει παραπάνω μπορεί να κάνει χρήση της γλώσσας C ++ για την δημιουργία του.

3. Καλή γλώσσα για να αφομοιώσει κάποιος προγραμματισμό

Η Python χρησιμοποιείται από αρκετές εταιρείες και οργανισμούς για την διδασκαλία προγραμματισμού σε μαθητευομένους.

ΚΕΦΑΛΑΙΟ 2: Πληροφοριακά Συστήματα

2.1 Εισαγωγή

Στον κόσμο των εταιρειών τα πληροφοριακά συστήματα διαδραματίζουν καίριο ρόλο για την επιβίωση μιας εταιρείας μέσα σε ένα πλαίσιο, όπου η αναμέτρηση αυξάνεται όλο και περισσότερο. Με βάση τη σύγχρονη βιβλιογραφία απαρτίζουν ως «τη σπονδυλική στήλη της διοίκησης», καθώς συγκροτούν το στοιχείο, το οποίο ενώνει τη φυσική μέθοδο παραγωγής με τη μέθοδο της λήψης αποφάσεων. Βασικός χειρισμός των πληροφοριακών συστημάτων αποτελεί η αλλαγή των στοιχείων που υφίστανται στο φυσικό μοντέλο παραγωγής σε γνώσεις (στοιχεία), οι οποίες προϋποθέτουν τις δραστηριότητες της μεθόδου λήψης αποφάσεων.

Ωστόσο και αντιθέτως, μεταβιβάζει τα στοιχεία που παράγει το μοντέλο διοίκησης σε αρμόζουσα στοιχεία για το φυσικό σύστημα παραγωγής. Παρόλο τους προαναφερθέντες βασικούς χειρισμούς, ένα ολοκληρωμένο πληροφοριακό σύστημα δύναται να παρέχει και περαιτέρω ικανότητες όσον αφορά (Wallace, 2014):

- Την ενίσχυση των διοικητικών μελών όλων των επιπέδων για τη λήψη έγκαιρων και ορθών κρίσεων για κέρδος της επιχείρησης.
- Την ενίσχυση της επίβλεψης της καθημερινής διαδικασίας της επιχείρησης.
- Την καθοδήγηση της διαδικασίας της εταιρείας
- Την ενίσχυση στη μελέτη και το σχηματισμό της στρατηγικής εξάπλωσης της εταιρείας.
- Τη συμβολή στο σχηματισμό μεταβολών, προκειμένου η εταιρεία να μπορεί να εναρμονίζεται όλο και πιο πολύ στο χώρο του. Ένα ακέραιο πληροφοριακό σύστημα επιβάλλεται να είναι ευκίνητο και σύμφωνο, προκειμένου να εισακούει στις μετατροπές και στις διαφορετικές υποχρεώσεις διαφόρων συνόλων μελών.

Οι χειρισμοί αυτοί πραγματοποιούνται μέσω της ολοκληρωμένης επεξεργασίας των στοιχείων μιας εταιρείας μέσω της οποίας προκύπτουν τα αναγκαία στοιχεία που προστατεύουν όλους τους κλάδους της επιχείρησης, οδηγώντας τη στη λήψη ορθών κρίσεων.

2.2 Ορισμός και λειτουργία πληροφοριακών συστημάτων

Πληροφοριακό σύστημα ορίζεται μια ολότητα από αλληλοσχετιζόμενα δεδομένα, τα οποία δύνανται να συγκεντρώνουν, να εξετάζουν και να συσσωρεύουν πληροφορίες. Τα συστήματα αυτά εντείνουν, προκειμένου να δέχονται τις αρμόζουσες γνωματεύσεις με επιδίωξη την πραγματοποίηση της ορθής ενότητας της εταιρείας. Επιπροσθέτως, τα πληροφοριακά συστήματα προσφέρουν σημαντικές λύσεις σε πολύπλοκα ζητήματα καθώς και ενισχύουν στην εξάπλωση καινούριων αποτελεσμάτων (Kenneth C. Laudon & Jane P. Laudon 2005).

Οι πρωταρχικές διαδικασίες των πληροφοριακών συστημάτων θεωρούνται οι εισροές και οι εκροές. Συγκεκριμένα, το πληροφοριακό σύστημα λαμβάνει τις εισροές, όπου αποτελούν ακατέργαστα στοιχεία, τα οποία εντοπίζονται από τον χρήστη είτε εντός της εταιρείας είτε εκτός και με αυτό τον τρόπο εισχωρούν στο πληροφοριακό σύστημα. Έπειτα, ανακύπτουν οι εκροές, όπου είναι ολοκληρωμένα δεδομένα, τα οποία κρίνονται μέσω μιας διαδικασίας ανατροφοδότησης που συντελείται στο μοντέλο, ώστε η διαδικασία να λογίζεται φερέγγυα και εποικοδομητική. Η τελική φάση θεωρούνται τα δεδομένα, τα οποία πρέπει να είναι σε θέση να χρησιμοποιηθούν από τον τελικό χρήστη στη λήψη κρίσεων όπως διασαφηνίζεται στη παρακάτω εικόνα.



Εικόνα 1: Πληροφοριακό σύστημα (Πηγή: Φωλίνας, 2007)

Ένα πληροφοριακό σύστημα θεωρείται μια ολότητα από λειτουργίες που συγκεντρώνει, εξετάζει, συσσωρεύει και γνωστοποιεί γνώσεις με επιδίωξη την

ενίσχυση λήψης αποφάσεων και της εξέτασης. Στα πιο πολλά ενδεχόμενα, τα συστήματα πληροφοριών θεωρούνται σοβαρά συστήματα βασιζόμενα σε υπολογιστικά μοντέλα, τα οποία και διεξάγουν αξιόλογο ρόλο στις εταιρείες. Λόγω του ότι πολλά συστήματα πληροφοριών βασίζονται σε υπολογιστικά μοντέλα θεωρείται δηλωτικό να σημειωθεί πως κάθε υπολογιστικό μοντέλο ή λογισμικό δεν είναι αναγκαία μια οργάνωση πληροφοριών. Οι ηλεκτρονικοί υπολογιστές και τα συναρτώμενα σχέδια λογισμικού απαρτίζουν το τεχνικό θεμέλιο, τα βοηθήματα και το υλικό για τα νεωτεριστικά συστήματα πληροφοριών (Γκαζούνη, 2016).

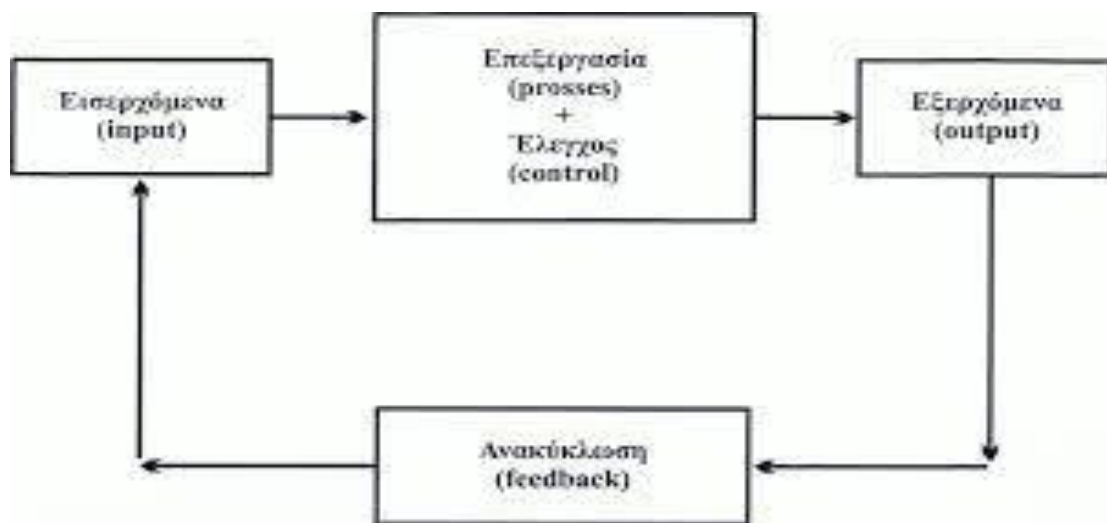
Για την αφομοίωση, όμως, των πληροφοριακών συστημάτων, χρειάζεται να κατανοηθούν ορισμένα ζητήματα, τα οποία δημιουργήθηκαν για να αντιμετωπίσουν τις αρχιτεκτονικές και σχεδιαστικές λύσεις τους, καθώς και τις λειτουργίες μιας εταιρείας, οι οποίες φέρνουν αυτές τις λύσεις. Θεωρείται σημαίνον να αποσαφηνιστεί ότι το κάθε πληροφοριακό σύστημα είναι αποκλειστικά μελετημένο ομόγνωμα με τις καθορισμένες προϋποθέσεις της εταιρείας για τις οποίες δημιουργήθηκε. Κάθε εταιρεία για να επιβληθεί και να διευθύνει τη μεγάλη ποσότητα στοιχείων που συναθροίζονται καθημερινώς, πρέπει να έχει ένα μοντέλο που να εισακούει στα ζητήματα που αντιμετωπίζονται απευθείας με ενεργητικό τρόπο.

Τοιουτοτρόπως, με το αναγκαίο προσωπικό που θα είναι ορθώς ειδικευμένο και με το αρμόζον πληροφοριακό σύστημα, η διαχείριση και η κατεργασία των δεδομένων γίνεται πιο απλή και γόνιμη. Ως σύστημα ορίζεται μια ολότητα από συνιστώσες, οι οποίες αλληλεπιδρούν μεταξύ τους προκειμένου να πραγματοποιήσουν ένα στόχο. Οι συνιστώσες αυτές ενδέχεται να είναι:

- Οντότητες
- Υλικά
- Αντιλήψεις
- Αξίες

Τα διαφορετικά τμήματα ενός μοντέλου θεωρούνται με τη σειρά τους μοντέλα με πιο μικρή κλίμακα, τα οποία απαρτίζουν υπό-μοντέλα του βασικού. Συνεπώς, κάθε μοντέλο θεωρείται υπέρ-μοντέλο ορισμένων μοντέλων, αλλά συγκροτεί ταυτόχρονα και υπό-μοντέλο κάποιου άλλου. Όλα τα μοντέλα εμπεριέχονται από το περιβάλλον τους, δηλαδή με κάθε ύπαρξη που έγκειται έξω από τα όρια (Yusuf, 2004).

Σε κάθε οργάνωση εισχωρούν στοιχεία από το χώρο, μετατρέπονται σε νέα στοιχεία και τέλος εξάγονται προς το περιβάλλον. Κατ' ακολουθία, κάθε μοντέλο έχει μια είσοδο, μια επεξεργασία, και μια έξοδο. Ως στοιχεία ορίζονται τα συμβάντα ή αξίες ορισμένων γνωρισμάτων, τα οποία υπάγονται σε υπάρξεις και για να είναι απαραίτητα αξίζει να έχουν πιστότητα, απαρτία, σχετικότητα και αποπομπή. Καταληκτικά, λοιπόν, πληροφοριακό σύστημα, θεωρείται μια ολότητα αλληλοσυνδεόμενων τμημάτων, τα οποία αλληλοβοηθούνται για τη συγκέντρωση, επεξεργασία, αποθήκευση και περίσσεια πληροφοριών στοχεύοντας στην ενίσχυση της λήψης κρίσεων, της ενότητας, του ελέγχου και της ερμηνείας στοιχείων μιας εταιρείας (H., P., & Manson, 2005).



Εικόνα 2: Σχηματική αναπαράσταση ενός μοντέλου (Πηγή: Γιαννακόπουλος & Παπουτσής, 1995)

2.3 Πλεονεκτήματα και μειονεκτήματα πληροφοριακών συστημάτων

Τα πλεονεκτήματα των πληροφοριακών συστημάτων σε μια νεωτεριστική εταιρεία θεωρούνται πολλά και τεράστιας σπουδαιότητας. Οι εταιρείες μεγάλου μεγέθους χρησιμοποιούν τα συστήματα ενδοεπιχειρησιακού σχεδιασμού (ERP), τα οποία προσφέρουν ευχέρεια για τη διαμόρφωση μιας κοινής κουλτούρας στην εταιρεία (Laudon & Laudon, 2004). Ένα ολοκληρωμένο ERP και ορθά εγκατεστημένο προσδίδει στην εταιρεία εξαιρετικά πλεονεκτήματα εξαιτίας της γοργής και εποικοδομητικής εξυπηρέτησης των πελατών της.

Η εποικοδομητική, ταχεία και ορθή λειτουργία όλων των υπηρεσιών της εταιρείας φέρνει την ευαρέσκεια των πελατών έχοντας ως απόρροια την τήρηση αυτών στην εταιρεία πολλαπλασιάζοντας, έτσι, τα κέρδη της.

Αναμφίβολα, από την ορθή λειτουργία της εταιρείας ανακύπτουν αρκετά και αξιόλογα πλεονεκτήματα που ωφελούν στην εξάπλωσή της απώτερα. Τα ουσιαστικότερα προτερήματα είναι τα εξής (Φιτσιλής, 2015):

1. Συσσώρευση χρόνου και χρηματικών δίδων, ώστε η λειτουργία της εταιρείας να θεωρείται πιο εποικοδομητική.
2. Μέσω του ERP πραγματοποιείται απλοποίηση και πιο ορθή συστηματοποίηση των υπηρεσιών, με επακόλουθο την ελάττωση της αξίας και την αύξηση της ευχέρειας στην εφαρμογή των υπηρεσιών.
3. Τα ERP ωφελούν αξιόλογα στο να γίνει ευκολότερος προγραμματισμός, μετριάζοντας σημαντικά τα σφάλματα κατά τη λειτουργία της κατανάλωσης των προϊόντων.
4. Περιορίζεται ο χρόνος που χρειάζεται για το σχηματισμό των προϊόντων μέχρι τη διάθεσή τους στο εμπόρευμα.
5. Η εταιρεία δύναται να δέχεται με άμεσο τρόπο όλα τα στοιχεία που έχει ανάγκη, προκειμένου να λαμβάνει τις ορθές κρίσεις.
6. Αποκρούεται η επανάληψη και διπλό μεταγραφής των υπηρεσιών.
7. Ελαχιστοποιείται σημαντική η τιμή των υπηρεσιών, καθώς και ο χρόνος που χρειάζεται για να πραγματοποιηθούν.
8. Τα ERP ωφελούν, προκειμένου η εταιρεία να κατακτήσει κοινή μόρφωση.
9. Τα στοιχεία των υπηρεσιών καταγράφονται στο σύστημα μόνο μία φορά, αλλά δύνανται να χρησιμοποιηθούν αρκετές φορές και από πολλές εφαρμογές.
10. Τα συστήματα ERP έχουν το σημαντικό προτέρημα της σβελτάδας και της πιστότητας στην ερμηνεία και την λειτουργία των εργασιών της εταιρείας. Το συμπαγές αυτό σύστημα εξετάζει και διευθύνει τα στοιχεία στην ολότητα της εταιρείας και αυτό έχει ως επακόλουθο εφόσον όλοι κάνουν χρήση το ίδιο αδιαίρετο σύστημα η χρήση να λογίζεται πιο πιστευτή.
11. Μέσω των ERP τα στοιχεία είναι πιο αλάνθαστα και υφίσταται βελτιωμένη και πιο εποικοδομητική εξέταση του μοντέλου (Φωλίνας, 2007).

Τα θεμελιώδη προνόμια των ERP είναι τα παρακάτω (Αμπλιανίτη, 2019):

1. Η εποικοδομητική συμμετοχή των λειτουργιών της παραγωγής και η ορθή ενότητα αυτής έχει ως απόρροια τα προϊόντα να προσεγγίζουν με άμεσο τρόπο τους τελικούς πελάτες. Αυτό ενισχύει την εταιρεία στο να κατέχει πρωτύτερα τις ανάγκες της για τα πρώτα υλικά, προκειμένου να αποφεύγεται η κοσμοσυρροή και οι μεγάλες ποσότητες παραγωγής και πρώτες ύλες που συχνά δεν ωφελούν την εταιρεία, αλλά αυξάνουν σημαντικά το κέρδος της.
2. Η εταιρεία μέσω των ERP ενδέχεται να προσεγγίζει με απλούστατο τρόπο το παρελθόν των καταναλωτών της, καθώς έτσι η εταιρεία δύναται να ερευνήσει τις επιχειρηματικές τις δοσοληψίες καθώς και να ομαδοποιήσει το πελατολόγιό της, με βάση τα κέρδη που παρέχει ο κάθε καταναλωτής στην εταιρεία.
3. Προμηθεύει τα αρμόζοντα βοηθήματα στους προμηθευτές αλλά και στην ίδια την εταιρεία, προκειμένου να έχουν βελτιωμένη εικόνα για τις ανάγκες της, με επακόλουθο να περιορίζεται το κέρδος εγκρίνοντας στην εταιρεία να επενδύει τους διόδους που υποκλέπτει σε άλλες δραστηριότητές της.

Υπερισχύει η άποψη ότι τα πληροφοριακά συστήματα δίνουν λύσεις σε όλα τα επιχειρησιακά προβλήματα, αντίληψη λανθασμένη, διότι η χρήση τους πολλές φορές ενέχει πολλούς κινδύνους και πολλά μειονεκτήματα τα κυριότερα από αυτά είναι:

1. Η υψηλή αξία θεωρείται ένα από τα πρωταρχικά μειονεκτήματα, η οποία σχετίζεται τόσο στην τοποθέτηση, τη διαδικασία καθώς και στην παραμετροποίηση, ώστε να ταιριάζει στις ανάγκες της κάθε εταιρείας.
2. Οι χρήστες πρέπει να εκπαιδευτούν, έτσι ώστε να αφομοιώνουν να χειρίζονται με σωστό τρόπο τα πληροφοριακά συστήματα. Παρόλα αυτά, η εκπαίδευση θεωρείται αρκετά δυσεπίλυτη, γιατί θα πρέπει οι υπάλληλοι να ασκηθούν σε έναν διαφορετικό τρόπο ενασχόλησης από αυτόν που διατελούσε πριν την εισαγωγή των πληροφοριακών συστημάτων στην εταιρεία.
3. Τα πληροφοριακά συστήματα έχουν έναν δεσμευτικό τρόπο ενώπιον των εταιρειών για μεγάλο χρονικό διάστημα, διότι πολλές φορές οι εταιρείες αναγκάζονται να εναρμονίσουν όλες τις διαδικασίες, ούτως ώστε να

συνδέονται με τις λειτουργίες των πληροφοριακών συστημάτων έχοντας ως απόληξη την αναμόρφωση όλης της εταιρείας.

1. Τα πληροφοριακά συστήματα μπορεί να αποκλίνουν από την επιδίωξή τους, όχι γιατί δεν έχει παραχθεί ορθή τοποθέτηση του συστήματος ή υφίσταται κάποιο παράπτωμα αλλά επειδή οι υπάλληλοι δεν δέχονται να ενταχθούν στα νέα πράγματα και στις μεταβολές με επιπτώσεις την όχι και τόσο ωφέλιμη λειτουργία τους.
2. Τα πληροφοριακά συστήματα εκδηλώνονται από διαδικασίες, οι οποίες δεν μεταβάλλονται και λογίζονται ως δύσκαμπτες και ορισμένες από εκείνες δεν ταυτίζονται με την γενική οργάνωση της εταιρείας, με απόρροια τα θέματα που παράγονται συχνά να είναι μείζονα από τα κέρδη που παρέχουν (Lambert & Stock, 2001).
3. Η εταιρεία συναρτάται σε σημαντικό βαθμό από την εταιρία που παρέχει το πληροφοριακό σύστημα.
4. Η αξία που παράγεται από την χρήση εξωτερικών μελών για την τοποθέτηση και την παραμετροποίηση που χρειάζεται, όπως επιπλέον και για την διατήρησή τους θεωρείται αρκετά υψηλή.
5. Το πληροφοριακό σύστημα συχνά έχει περισσότερες ικανότητες σε αλληλεξάρτηση με τις ανάγκες της εταιρείας και αυτό έχει ως επίπτωση η αξία για ορισμένες εταιρείες μικρότερου μεγέθους να θεωρείται τεράστια.
6. Συχνά, ένα πληροφοριακό σύστημα ενδέχεται να μην είναι χρηστικό για μέλη που δεν είναι τόσο μαθημένοι με την τεχνολογία, με επακόλουθο να αγανακτούν και να μην καταφέρνουν να το χρησιμοποιήσουν με παραγωγικό τρόπο.
7. Ένα πληροφοριακό σύστημα, αν έχει ελλείψεις, ενδέχεται να αποδώσει ανώφελα δεδομένα και ενδεχομένως δεν μπορέσει να φέρει εις πέρας τις κύριες ανάγκες του χρήστη. Αυτό γίνεται κατά κανόνα όταν θεωρείται δυσεπίλυτη η οριοθέτηση των ουσιαστικών υποχρεώσεων μιας εταιρείας καθώς παράγεται το πληροφοριακό σύστημα.
8. Οι αδιάλειπτες μετατροπές και βελτιώσεις στο λογισμικό είναι πιθανόν να έχουν μεγάλο οικονομικό κόστος στην εταιρεία, ώστε το λογισμικό της να θεωρείται όσο πιο σύγχρονο.

9. Η διατήρηση ενός ολόκληρου πληροφοριακού συστήματος πρέπει να ελέγχεται διαρκώς και να αναβαθμίζεται σε εξοπλισμό, να έχει ένα κατάλληλο και ειδικευμένο προσωπικό για άμεση εξασφάλιση τυχών σφαλμάτων, προκειμένου να αποφευχθούν μεγαλύτερες δυσκολίες.

2.4 Βασικές λειτουργίες πληροφοριακών συστημάτων

Με βάση τις λειτουργίες μιας εταιρείας τα πληροφοριακά συστήματα μπορούν να κατηγοριοποιηθούν ως εξής: (Laudon & Laudon, 2014):

1. Συστήματα Marketing και Πωλήσεων – Sales and Marketing Systems.

Τα συστήματα αυτά σχετίζονται με τη διαχείριση των πωλήσεων και την προβολή των αγαθών μιας εταιρείας. Επιδίδονται, επίσης, με τη σκιαγράφηση και τη σχηματισμό νέων αγαθών, καθώς και με την τιμολόγησή τους.

2. Συστήματα Ενίσχυσης Παραγωγής – Manufacturing and Production Systems.

Αυτά τα συστήματα συνδέονται αποκλειστικά με το τμήμα της κατανάλωσης, οτιδήποτε σχετίζεται με την παράδοση και παραλαβή υλικών και αγαθών. Σχετίζεται, επίσης, και με τα μηχανικά κομμάτια της κατανάλωσης καθώς και με τα συστήματα που αφορούν με την ποιοτική εξέταση.

3. Συστήματα Χρηματοοικονομικών και Λογιστικής – Financing and Accounting Systems.

Οι βασικές λειτουργίες αυτών των συστημάτων εμπεριέχουν όλες τις λογιστικές διαδικασίες μιας εταιρείας, καθώς επίσης και τους προϋπολογισμούς.

4. Συστήματα Ανθρωπίνων Πόρων – Human Resource Systems.

Αυτά τα συστήματα σχετίζονται με τη διαχείριση του ανθρώπινου δυναμικού. Οι πρωταρχικές λειτουργίες τους εμπερικλείουν τη μισθοδοσία, τα συστήματα μόρφωσης του δυναμικού, καθώς και τη διαχείριση των δεδομένων των υπαλλήλων της εταιρείας (Πολλάλης & Βοζίκης 2012).



Εικόνα 3: Βασικές Λειτουργίες Πληροφοριακών Συστημάτων
(Πηγή: <https://insightsolutionsglobal.com/what-is-erp-enterprise-resource-planning/>)

2.5 Κατηγορίες πληροφοριακών συστημάτων

Υπάρχουν τρεις πρωταρχικές κατηγορίες πληροφοριακών συστημάτων, οι οποίες ωφελούνται από τα διαφορετικά τμήματα μιας επιχείρησης (Αμπλιανίτη, 2019):

1. **Λειτουργικού επιπέδου συστήματα:** Τα συστήματα αυτά ενισχύουν τους ομόλογους διευθυντές διατηρώντας δεδομένα για τις πρωταρχικές δοσοληψίες της εταιρείας. Ο βασικός στόχος των συστημάτων του συγκεκριμένου επιπέδου, είναι η απόκριση των ερωτημάτων της καθημερινότητας και ο έλεγχος των δοσοληψιών της εταιρείας.
2. **Διοικητικού επιπέδου συστήματα:** Τα συστήματα αυτά ευνοούν την συμμετοχή, την εξέταση, τη λήψη αποφάσεων και τις διαχειριστικές δράσεις των διευθυντών μεσαίου επιπέδου.
3. **Στρατηγικού επιπέδου συστήματα:** Τα συστήματα στρατηγικού επιπέδου εγκρίνουν στην ανώτερη διοίκηση να αντεπεξέρχεται και να προσδιορίζει στρατηγικά ζητήματα και μακροχρόνιες διαθέσεις, τόσο μέσα στην εταιρεία όσο και έξω από εκείνη. Για κάθε επίπεδο διοίκησης, η εταιρεία κατέχει τα ομόλογα μοντέλα για την εξασφάλιση των αναγκών της.

1. Συστήματα Επεξεργασίας Συναλλαγών – Transaction Processing Systems (TPS)

Τα συστήματα αυτά χρησιμοποιούνται από το λειτουργικό ανθρώπινο δυναμικό για την απλοποίηση των τακτικών τους υπηρεσιών και εμπεριέχουν συμβάντα και δοσοληψίες που σχετίζονται με την επιχείρηση. Ζητήσεις, σκοπούς, τιμολογήσεις, δοσοληψία είναι ορισμένα από τα καθήκοντά τους. Τα συστήματα αυτά παρέχουν συγκεκριμένες συσχετίσεις για την πληροφόρηση των μελών τους.

2. Πληροφοριακά Συστήματα Διοίκησης – Management Information Systems (MIS)

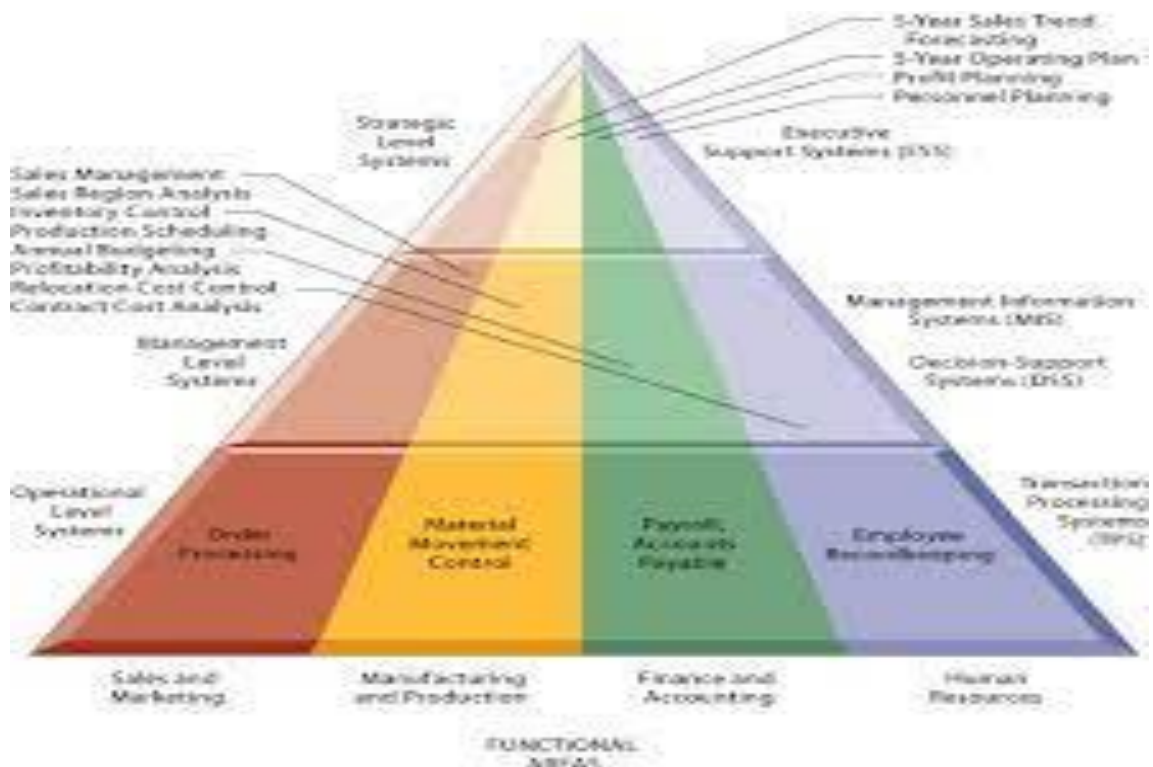
Τα συστήματα αυτά έχουν πρόσβαση σε μεγάλη ποσότητα δεδομένων από πολλούς κλάδους της εταιρείας παρέχοντας στα μεσαία διοικητικά στελέχη συγκεκριμένες συσχετίσεις, οι οποίες παράγονται με χρήση απλών μοντέλων διοίκησης όπως κατατάξεις και περιλήψεις.

3. Συστήματα Υποστήριξης Αποφάσεων – Decision Support Systems (DSS)

Τα μέλη τους υπάγονται επίσης στα μεσαία διοικητικά στελέχη και εγκρίνουν την αδιάλειπτη αλληλεπίδραση με το κάθε στέλεχος, χρησιμοποιώντας στοιχεία από τα συστήματα επεξεργασίας συναλλαγών, από τα πληροφοριακά συστήματα διοίκησης καθώς και από εξωτερικές πηγές, ενισχύοντας στην λήψη ορθών αποφάσεων. Κατέχουν συγκεκριμένα πρότυπα και περίπλοκα όργανα ερμηνείας στοιχείων για την εξαγωγή επακόλουθων.

4. Συστήματα Υποστήριξης Επιτελικών Στελεχών – Executive Support Systems (ESS)

Τα συστήματα αυτά προσαγορεύονται να αποκριθούν στις ερωτήσεις των επιτελικών διοικητικών μελών. Επιδεικνύουν συγκεντρωτικές συνδέσεις από τους επιμέρους κλάδους της εταιρείας, εμφανίζουν μακρόχρονες ροπές του εμπορεύματος και ενισχύουν στην απώτερη μελέτη της στρατηγικής της εταιρείας. Στην παρακάτω εικόνα αποσαφηνίζεται μια προσκόμιση των διαφορετικών συστημάτων μιας εταιρείας. Η εταιρεία κατέχει συστήματα ενίσχυσης επιτελικών μελών (ESS) για το στρατηγικό επίπεδο, πληροφοριακά συστήματα διοίκησης (MIS) και συστήματα ενίσχυσης κρίσεων (DSS) για το διοικητικό επίπεδο και τέλος συστήματα επεξεργασίας συναλλαγών (TPS) για το λειτουργικό επίπεδο.



Εικόνα 4: Προσκόμιση συστημάτων μιας εταιρείας

2.6 Είδη πληροφοριακών συστημάτων

Τα βασικά είδη πληροφοριακών συστημάτων είναι τα εξής:

1. Συστήματα επεξεργασίας συναλλαγών

Τα συστήματα επεξεργασίας συναλλαγών απαρτίζουν πρωταρχικά συστήματα για την ενίσχυση της ορθής βάσης της εταιρείας. Βασικός χειρισμός αυτών των συστημάτων είναι η τακτική καταμέτρηση όλων των διαδικασιών της εταιρείας, καθώς και η επεξεργασία όλων των δοσοληψιών που συντελούνται εντός της εταιρείας, όπως οι λειτουργίες για τη δοσοληψία του ανθρώπινου δυναμικού, η κατάταξη τιμολογίων, η πληροφόρηση των μεταφορών της αποθήκης, η κατάταξη ρουτίνας των εσόδων και των εξόδων της εταιρείας. Η λειτουργία της συγκέντρωσης και της επεξεργασίας αυτών των στοιχείων δέχεται από τα υψηλόβαθμα μέλη, τα οποία προσδιορίζουν το πώς γίνεται η όλη διαδικασία (Αναστασιάδης, 2001).

2. Πληροφοριακά συστήματα διοίκησης

Τα συστήματα αυτά σχετίζονται με το διοικητικό κομμάτι της εταιρείας πραγματοποιώντας διαδικασίες λήψης αποφάσεων και μελέτης. Έχουν την ικανότητα να παραχωρούν στοιχεία στα μέλη αναφορικά με την απονομή του κάθε κλάδου αλλά και τα ιστορικά δεδομένα που συνδέονται με την εταιρεία, και πραγματοποιούν κινήσεις σχετιζόμενες με την εταιρεία. Τα πληροφοριακά συστήματα αυτής της ομοταξίας προμηθεύουν στα ανώτατα διευθυντικά μέλη συνδέσεις που πηγάζουν από τους κατώτερους κλάδους της εταιρείας. Τέλος αυτά τα συστήματα αποπειρώνται να παραχωρήσουν καθολική εικόνα για την εταιρεία και επινοούν τεχνικές, προκειμένου να αντιμετωπίζουν τα σύντομα ζητήματα που ενδέχεται να εμφανιστούν (Kenneth, Laudon & Jane, Laudon, 2005).

3. Συστήματα υποστήριξης αποφάσεων

Τα συστήματα σχετίζονται και αυτά με το διοικητικό κομμάτι της εταιρείας και κατέχουν στοιχεία με βάση κάποια προηγμένα πρότυπα, προκειμένου να λαμβάνουν σωστά δομημένες αποφάσεις. Αυτά τα πληροφοριακά συστήματα θεωρούνται πολύ χρήσιμα βοηθήματα για τα διοικητικά μέλη, αφού τους ενισχύουν προκειμένου να δέχονται ωφέλιμες γνωματεύσεις για ενδεχόμενα εξαιρετικά δύσκολα και πολύπλοκα. Τα στοιχεία που χρησιμοποιούν πιθανόν να πηγάζουν και από άλλα κατεστημένα της εταιρείας όπως αυτά της επεξεργασίας συναλλαγών ή των πληροφοριακών συστημάτων διοίκησης. Τα μέλη των συστημάτων αυτών είναι σημαντικά ευέλικτα, αφού έχουν την ικανότητα να αναμειχτούν στην οργάνωση και να μεταποιήσουν τα στοιχεία χρησιμοποιώντας πολλούς συντελεστές για να επιχειρήσουν πολλές και διαφορετικές υποθέσεις.

Τα πληροφοριακά συστήματα κατηγοριοποιούνται σε ενεργητικά, παθητικά και σε συνεργατικά. Το ενεργητικό σύστημα κρίσεων έχει την ικανότητα να υποβάλλει μια πρόταση αλλά όχι τη απάντηση για ένα καθορισμένο ζήτημα. Το παθητικό σύστημα ενδέχεται εύκολα να λάβει μια απόφαση αλλά δεν ενδέχεται να υποβάλλει την απάντηση. Τέλος το συνεργατικό σύστημα δοσοληψιών δίνει την ικανότητα στον χρήστη να μεταποιήσει τις κρίσεις που ήδη διατελούν στο σύστημα και έπειτα να τις διαβιβάσει για έγκριση. Τα πληροφοριακά συστήματα αυτής της κατηγορίας θεωρούνται σημαντικά απαραίτητα όργανα για την εταιρεία, αφού επιτελούν έναν βελτιωμένο έλεγχο, αναβαθμίζοντας αξιόλογα την συνεννόηση και ωφελούν στην επικοινωνιακή και ορθή συλλογική ενασχόληση, ανταποκρινόμενα με σβελτάδα και τελεσφόρηση στα θέματα που ενδέχεται να εμφανιστούν (Υψηλάντης, 2001).

4. Πληροφοριακά συστήματα υποστήριξης

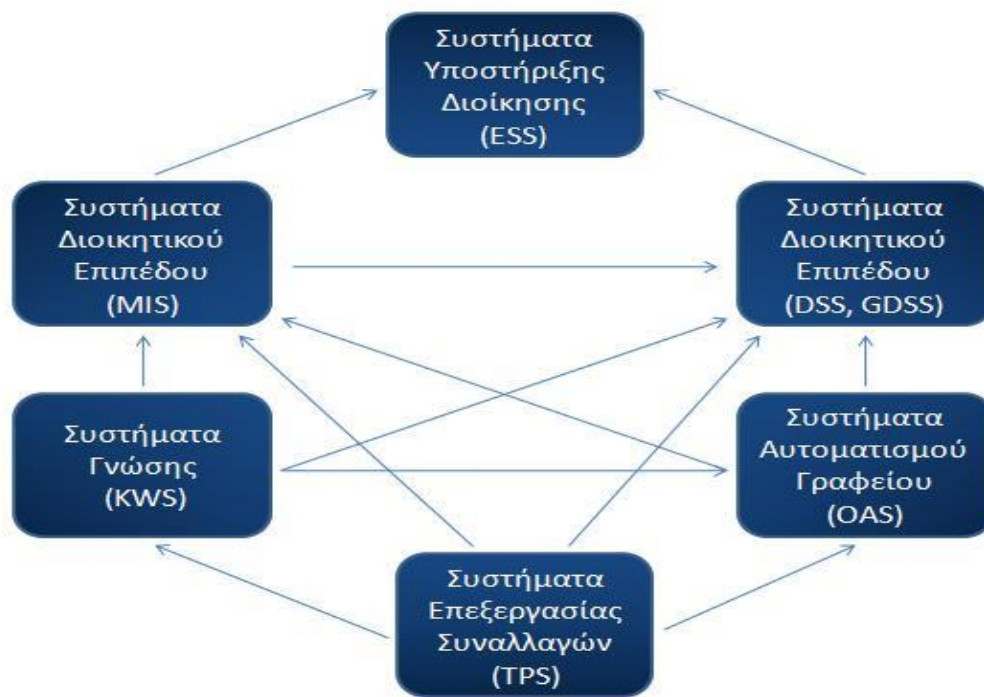
Τα πληροφοριακά συστήματα αυτής της κατηγορίας ενισχύουν τις εταιρείες, προκειμένου να είναι σε θέση να αντεπεξέρχονται περιστάσεις που απαιτείται να ληφθεί κάποια εκτός προγράμματος κρίση ή που θα πρέπει το μέλος να εκμεταλλευτεί την άποψή του ή την διαίσθησή του. Τα συστήματα αυτά δέχονται στοιχεία από τον εξωτερικό περίγυρο, π.χ. από εθνικές βάσεις δεδομένων, από μελέτες εμπορευμάτων. Τα στοιχεία που δέχεται το εξωτερικό περιβάλλον τέμνουν με εκείνα που ενδημούν εντός της εταιρείας. Τα συστήματα αυτά χρησιμοποιούνται με απλό τρόπο από εργαζόμενους που δεν είναι τόσο εξοικειωμένοι με τα πληροφοριακά συστήματα.

Ένα σημαντικό προτέρημα αυτών των συστημάτων αποτελεί η συνθετική ερμηνεία, ο προβιβασμός του προσανατολισμού που πρέπει να ακολουθήσει η εταιρεία, όπως και η σημαντική ευελιξία που παρέχουν στα μέλη τους ωφελεί, προκειμένου να διαχειρίζονται το ζήτημα οριοθετώντας τα προσωπικά τους στοιχεία και συντελεστές για να αναπτύσσουν έτσι τον δικό τους τρόπο συλλογισμού. Τέλος, η αδυναμία αυτών των συστημάτων αποτελεί η πολυδάπανη συντήρησή τους και ο μεγάλος αριθμός υπαλλήλων που χρειάζεται για να λειτουργήσουν (Αναστασιάδης, 2001).

5. Πληροφοριακά συστήματα αυτοματισμού γραφείου

Τα πληροφοριακά συστήματα αυτοματισμού γραφείου υπάγονται στον οργανωτικό κλάδο της εταιρείας και ωφελούν τους εργαζόμενους που δεν έχουν ειδικές πληροφορίες. Τα συστήματα αυτά εργάζονται ως διεργασίες, τα οποία διαβιβάζουν ενημερώσεις και επινοούν διάυλο συνεννόησης ανάμεσα στους πελάτες και στους προμηθευτές. Θεωρούνται εύχρηστα βοηθήματα, γιατί χρησιμοποιούνται από μέλη που διαμένουν σε μακρινές πόλεις και τους ευνοούν, ούτως ώστε να συντονίζονται μεταξύ τους.

Ορισμένες από τις λειτουργίες αυτών των συστημάτων είναι: η διαχείριση των στοιχείων, η διαχείριση καθήκοντος, η επεξεργασία κειμένου, η ψηφιακή αρχειοθέτηση. Ένα επιπλέον προτέρημα θεωρείται πως παραχωρεί στα μέλη την ικανότητα, προκειμένου να καταφέρνουν να εποπτεύουν τη ροή των ενημερώσεων που υφίσταται είτε μεταξύ του συνόλου, είτε για όλο το άθροισμα της εταιρείας. Τέλος, συμβάλλουν προκειμένου να εκτείνονται οι ενημερώσεις νωρίς στους αποδέκτες, αλλά συντελούν και στην βελτιωμένη καταβολή των πόρων (Δημητριάδης, 2007).



Εικόνα 5: Σχέση διαφόρων τύπων Πληροφοριακών Συστημάτων (Πηγή: τροποποιημένο Laudon K. C., Laudon J. P., 2002)

2.7 Ασφάλεια των πληροφοριακών συστημάτων

Οι εταιρείες πριν την εγκατάσταση των πληροφοριακών συστημάτων αναμφίβολα αντεπεξέρχονταν ελάχιστες απειλές αναφορικά με το τμήμα της ασφάλειας σε αναλογία με την νεωτεριστική εποχή όπου όλες περίπου οι εταιρείες κατέχουν στο ενεργητικό τους ένα είδος πληροφοριακό σύστημα. Η έννοια ασφάλεια άπτεται (Στεφάνου & Μπιάλας, 2017):

- Στα συστήματα που χρησιμοποιούνται από πολλά μέλη και στα στοιχεία που έχουν αποθηκευτεί σε αυτά, τα οποία συχνά θεωρούνται επισφαλή στη κακομεταχείριση, και περισσότερο επισφαλή σε ζητήματα ασφάλειας.
- Στην προφύλαξη από φυσικές πανωλεθρίες και διαρρήξεις. Έτσι, για κάθε εγκατάσταση ενός πληροφοριακού συστήματος θα πρέπει η εταιρεία να δέχεται όλους εκείνους τους κανόνες που θα έχει ανάγκη, προκειμένου να προσέχουν από φυσικές συμφορές.
- Στο σχηματισμό ενός συστήματος κρυπτογράφησης, το οποίο δίνει την ικανότητα στο σύστημα να αντιλαμβάνεται εμπιστευτικές ενημερώσεις με μείζονα ασφάλεια. Αυτό το σύστημα δίνει την ικανότητα, προκειμένου

να μετασχηματίζει το κείμενο σε θωριά μη ευνόητη από τα μέλη, τα οποία δεν κατέχουν αυτό το σύστημα.

- Στην χρησιμοποίηση των εφαρμογών των συστημάτων από μέλη που είναι εξουσιοδοτημένοι. Αυτό το μέσο δύναται να πραγματοποιηθεί από την εισαγωγή κωδικών ασφαλείας, που θα εγκρίνουν την εισαγωγή μόνο σε μέλη που τους ξέρουν. Επιπλέον, για την ορθή λειτουργία των κωδικών αυτών αξίζει ανά τακτά χρονικά διαστήματα να μεταβάλλουν για μείζονα προστασία.

Η ασφάλεια πληροφοριακών συστημάτων και βάσεων σχετίζεται με υπάρξεις και αντικείμενα που πρέπει να φυλαχθούν. Οτιδήποτε πρέπει να προστατευθεί καλείται αγαθό και πρέπει να προστατευθούν λόγω του ότι έχουν υπόληψη. Η υπόληψή τους ενδέχεται να συρρικνωθεί αν υπάρξουν απώλειες. Τα αγαθά χρειάζονται προάσπιση μόνο αν υπάρχουν διακινδυνεύσεις που ενδέχεται να τους προξενήσουν απώλεια.

Ο κάτοχος ενός προστατευόμενου αγαθού κατέχει μέσα προφύλαξης είτε για να περιορίσει την απειλή προξενώντας απώλεια στο αγαθό, είτε για να ελαχιστοποιήσει τις συνέπειές της. Τα μέσα προφύλαξης επιφέρουν κέρδος, λόγω του ότι δεν δύνανται να εγγυηθούν πλήρη εγγύηση, και έτσι το κέρδος τους πρέπει να αντιστοιχεί με την επισφάλεια του αγαθού αυτού. Ο κάτοχος θεωρείται εκείνος που θα αξιολογεί, όταν θέτει το σκοπό ασφαλείας, για το ποια είναι η πιο ωφέλιμη σταθεροποίηση μεταξύ του κόστους, της επισφάλειας και τις κυρώσεις. Ακόμη, ενδέχεται, ο ίδιος να ερευνήσει αποκατάσταση πως ο σκοπός του θα πραγματοποιηθεί μέσω των μέσων προφύλαξης που θα χρησιμοποιήσει.

Εφόσον, τα προϊόντα υφίστανται για να αξιοποιούνται, σημαντικό θεωρείται η σημασία τόσο του μέλους όσο και του κατόχου τους. Κάθε προϊόν έχει γνωρίσματα που αξίζει να φυλαχθούν. Οι απώλειες ενδέχεται να εμφανιστούν από ρίσκα και σχετίζονται με πλήγματα και προϊόντα, και όχι με τα γνωρίσματά τους (Γκρίτζαλης, 2004).

2.8 Επιθέσεις στα πληροφοριακά συστήματα ασφαλείας

Η ασφάλεια των πληροφοριακών συστημάτων δεν σχετίζεται αποκλειστικά με μια μεθοδολογία προφύλαξης, αλλά σχετίζεται με μια ολότητα εμποδίων, τα οποία διαφεντεύουν τα στοιχεία του κάθε μοντέλου με πολλά διαφορετικά μέσα. Ακόμα και αν ένα μέσο δεν ευδοκιμήσει στην προάσπιση του μοντέλου, τα υπόλοιπα συνεχίζουν να δουλεύουν, προκειμένου να διαφυλάσσεται από ορισμένες επιθέσεις. Δεν υφίσταται κάποιο σύστημα ασφαλείας που να έχει

εγκατασταθεί και, έτσι τα συστήματα κινδυνεύουν μέσω της χρήσης και της επίθεσης από ορισμένα μη εξουσιοδοτημένα μέλη. Επιπλέον, απειλούνται με διακοπή λειτουργίας του δικτύου, με διακοπή εξυπηρετήσεων έχοντας προφανή τη διάρρηξη και την εκμετάλλευση ιδιωτικών επιχειρηματικών αλλά και προσωπικών στοιχείων και, τέλος, υπάρχει το ενδεχόμενο νομικής αγωγής.

Για την απόκτηση πρόσβασης στα δεδομένα, υφίστανται δύο μέσα. Το πρώτο είναι να υπάρχει φυσική προσέγγιση στη συσκευή και το δεύτερο είναι να συνδέσει κάποιος το μηχάνημα με απομακρυσμένο τρόπο. Η φυσική προσέγγιση φαίνεται να είναι πιο εύκολη, προκειμένου να μπορέσει κάποιος να υποκλέψει στοιχεία από έναν υπολογιστή, χωρίς να έχει την εξουσιοδότηση. Σε αυτό το μέσο δύναται κανείς και να ανοίξει το κουτί της συσκευής, να ανοίξει το σκληρό δίσκο και με ευχέρεια να υποκλέψει τα στοιχεία. Με τον όρο βέβαια πως τα στοιχεία δεν έχουν αποκρυπτογραφηθεί, συνεπώς και το εμπόδιο μεγαλώνει αντίστοιχα με τον αλγόριθμο αποκρυπτογράφησης (GrayHat4Life, 2020).

Το δεύτερο μέσο που σχετίζεται με την απομακρυσμένη προσέγγιση σε έναν υπολογιστή θεωρείται η εναλλακτική λύση. Γίνεται φανερό ότι προκειμένου να πραγματοποιηθεί μια απομακρυσμένη επίθεση σε ένα μοντέλο, πρέπει αυτό να έχει συνδεθεί στο διαδίκτυο ή σε ένα δίκτυο που θα μπορεί ο επιτιθέμενος να εγκρίνει τη σύνδεση μέσω αυτού του δικτύου σε άλλα μέλη, ειδάλλως δεν είναι εφικτή η πρόσβαση σε αυτό. Έτσι, θεωρείται αρκετά ευχερές να βρεθεί ο επιτιθέμενος.

Οι υπολογιστές συγκαταλέγουν όλα τα συμβάντα που γίνονται σε «logs» και εάν ο επιτιθέμενος δεν το έχει ήδη σκεφτεί, επομένως υπάρχουν επαληθεύσεις για την επίθεσή του. Υπάρχουν αναμφίβολα λύσεις σε αυτή τη δυσκολία για να μη γίνονται καθορισμένοι μηχανισμοί προστασίας και, έτσι, να καλύπτεται η ταυτότητα «έλεγχος διεισδυτικότητας και εκτίμηση τρωτότητας» μέσω του Metasploit Framework του επιτιθέμενου. Τέλος, ένα σημαντικό ελάττωμα της μεθοδολογίας αυτής είναι πως λόγω της μεσολάβησης του δικτύου οι λειτουργίες γίνονται πιο αργές.

ΚΕΦΑΛΑΙΟ 3: Αυθεντικοποίηση χρηστών

3.1 Έλεγχος αυθεντικότητας και διατήρησης δεδομένων

Στη συστηματοποιημένη γνώση των υπολογιστών, η επαλήθευση της φυσιογνωμίας ενός μέλους πολλές φορές χρειάζεται για να εγκριθεί η πρόσβαση σε εμπιστευτικά στοιχεία ή μοντέλα. Το πρώτο είδος αυθεντικοποίησης θεωρείται η παραδοχή αποδεικτικών στοιχείων ενός δελτίου ταυτότητας που λαμβάνονται από ένα φερέγγυο πρόσωπο, το οποίο έχει δεδομένα ότι το δελτίο αυτό είναι πράγματι γνήσιο.

Για παράδειγμα, όταν χρειάζεται αυθεντικοποίηση για ορισμένα έργα καλλιτεχνίας ή φυσικά αντικείμενα, το τεκμήριο ενδέχεται να είναι ένας γνωστός, ένα πρόσωπο της οικογένειας ή του στενού περιγύρου ή ένας εταίρος που να επισημοποιούν την προέλευση του αντικειμένου, ενδεχομένως με το να είχαν παρατηρήσει το αντικείμενο πράγματι στη κυριότητα του δημιουργού του. Επιπλέον, κεντρικοποιημένες συμπλέξεις πεποίθησης συναρτώμενες σε βεβαιώσεις θεωρούνται πιο σίγουρες συζεύξεις διαδικτύου με αναγνωρισμένες αφετηρίες επικύρωσης. Οι μη – κεντρικοποιημένες συζεύξεις πίστης ανάμεσα σε χρήστες, επιπλέον θεωρούνται διακεκριμένες ως web of trust, και μετέχουν για ιδιαίτερες εργασίες, όπως email ή αρχεία (GNU Privacy Guard) και η αξιοπιστία επικυρώνεται από γνώριμα πρόσωπα, τα οποία διαβεβαιώνουν το καθένα για τα κρυπτογραφικά κλειδιά τους, π.χ. σε key signing parties (Κακούρης, 2018).

Το δεύτερο είδος αυθεντικοποίησης θεωρείται η αντιπαραβολή των γνωρισμάτων του αντικειμένου με τα χαρακτηριστικά της απαρχής του αντικειμένου. Για παράδειγμα, ένας γνώστης ενδέχεται να διερευνά τις ομολογίες στο τρόπο σχεδιασμού, να επικυρώσει τον τόπο και τη θωριά της μονογραφής ή να αντιπαραβάλλει το αντικείμενο με μια περασμένη φωτογραφία. Ένας αρχαιολόγος, πιθανόν να μεταχειριστεί τη χρονολογία του άνθρακα για να επαληθεύσει το έτος ενός αντικειμένου ή να κάνει χημική και στερεοσκοπική ερμηνεία των υλικών που μεταχειρίζονται. Επίσης, ο ήχος και το φως συγκρίνοντάς τα με ένα γνώριμο φυσικό χώρο, υπάρχει πιθανότητα να χρησιμοποιηθεί η αυθεντικοποίηση για να ελεγχθεί η ποιότητα καταχωρήσεων ήχου, φωτογραφιών ή βίντεο.

Το τρίτο είδος αυθεντικοποίησης συναρτάται σε τεκμήρια με αρχεία ή με άλλες εξωτερικές επικυρώσεις. Στα δικαστήρια, για παράδειγμα, οι νόμοι αποδεικτικών τεκμηρίων πολλές φορές προϋποθέτουν την θέσπιση της αλληλουχίας μέριμνας των αποδεικτικών που εμφανίζονται. Αυτό δύναται να πραγματοποιηθεί με ένα χειρόγραφο έγγραφο καταγραφής αποδεικτικών

δεδομένων, ή μια μαρτυρία από μέλη της αστυνομίας και προσωπικό ιατροδικαστών που το χρησιμοποίησαν. Στην εμπειρική γνώση των υπολογιστών, σε ένα μέλος ενδέχεται να του παραχωρηθεί πρόσβαση σε ασφαλή μοντέλα με βάση ορισμένα δεδομένα που υπονοούν αυθεντικότητα. Ένας επιμελητής ενδέχεται να παραχωρήσει ένα κωδικό σε ένα μέλος, ή να προμηθεύει στον χρήστη μια εξειδικευμένη κάρτα ή άλλο μηχανήμα που θα του εγκρίνει την πρόσβαση στο μοντέλο. Σε αυτό το ενδεχόμενο η αυθεντικότητα δηλώνεται αλλά δεν επιτυγχάνεται.

3.2 Συντελεστές και είδη αυθεντικοποίησης

Τα μέσα με τα οποία ενδέχεται να πραγματοποιηθεί η αυθεντικοποίηση διασπώνται σε τρεις ομοταξίες, συναρτώμενες στους, όπως είναι αναγνωρισμένες, συντελεστές της αυθεντικοποίησης: οτιδήποτε που ο χρήστης επίσταται, οτιδήποτε που ο χρήστης κατέχει, οτιδήποτε που ο χρήστης θεωρείται. Κάθε συντελεστής αυθεντικοποίησης συγκαλύπτει μια ευρεία γκάμα δεδομένων που κάνουν χρήση προκειμένου να αυθεντικοποιήσουν ή να τεκμηριώσουν το δελτίο ταυτότητας ενός προσώπου. Μελέτη εγγύησης έχει προσδιορίσει πως για μια ευμενή αυθεντικοποίηση, δεδομένα από έστω δυο, και ακόμη βελτιωμένα από όλους τους τρεις συντελεστές αυθεντικοποίησης, αξίζει να διαπιστώνονται.

Οι τρεις συντελεστές και ορισμένα δεδομένα από κάθε συντελεστή είναι:

1. **Οι συντελεστές γνώσεις:** Οτιδήποτε που ο χρήστης επίσταται (π.χ. ένας κωδικός, μια πρόταση, ένα PIN, μια ανταπάντηση πειρασμού, ένα ερώτημα εγγύησης)
2. **Οι συντελεστές ιδιοκτησίας:** Οτιδήποτε που ο χρήστης κατέχει (π.χ. μια κάρτα, ένα ειδικευμένο βραχιόλι, ένα security token, ένα κινητό με ενσωματωμένο λογισμικό token)
3. **Οι σύμφυτοι συντελεστές:** Οτιδήποτε που ο χρήστης θεωρείται ή πραγματοποιεί (π.χ. δακτυλικό ίχνος, επωδός αμφιβληστροειδούς, ειρμός DNA, μονογραφή, πρόσωπο, φωνή, πληκτρολόγηση, κουνήσεις ποντικιού, και άλλα βιομετρικά συστατικά)

1. Αυθεντικοποίηση ενός συντελεστή

Θεωρείται ο πιο ανίσχυρος τομέας αυθεντικοποίησης, μόνο ένα αποκλειστικό στοιχείο από μια από τις τρεις ομοταξίες συντελεστών μεταχειρίζεται για την αυθεντικοποίηση ενός μέλους. Η χρησιμοποίηση απλώς ενός συντελεστή δεν

παρέχει ικανοποιητική προάσπιση από μια μοχθηρή επιδρομή. Αυτός ο τομέας αυθεντικοποίησης δεν συνιστάται για φειδωλές δοσοληψίες ή για διανομή διαφόρων εύθικτων ιδιαίτερων ενημερώσεων.

2. Αυθεντικοποίηση δυο συντελεστών

Όταν δεδομένα που περιγράφουν δυο συντελεστές επιθυμούν αυθεντικοποίηση, η έννοια αυθεντικοποίηση δυο συντελεστών μεταχειρίζεται, για παράδειγμα για μια τραπεζική κάρτα (οτιδήποτε που ο χρήστης κατέχει) και ένα PIN (οτιδήποτε που ο χρήστης επίσταται). Πολλές φορές, ιστοσελίδες στο διαδίκτυο παρέχουν στα μέλη τους την ικανότητα να διαλέξουν αυθεντικοποίηση δυο συντελεστών για την συσχέτισή τους με το μοντέλο, και ως ακολούθως, κατά τη συνοχή πρέπει αρχικά να πληκτρολογείται ο κωδικός του μέλους (κάτι που επίσταται) και στη συνέχεια, να πληκτρολογεί ένα PIN, που να δύναται να αποθηκεύσει σε μια συσκευή (κάτι που κατέχει).

3. Αυθεντικοποίηση πολλών συντελεστών

Αντί να χρησιμοποιηθούν δυο συντελεστές, πολλοί συντελεστές μεταχειρίζονται για να πολλαπλασιάσουν την εγγύηση μιας δοσοληψίας.

4. Συνεχής Αυθεντικοποίηση

Τα τυποποιημένα υπολογιστικά μοντέλα αυθεντικοποιούν τα μέλη τους αποκλειστικά κατά τη συσχέτισή τους στην αφετηρία μιας συνεδρίας (log – in), πράγμα που σημαίνει πως ενδέχεται να συσταίνει δηλωτικό μειονέκτημα εγγύησης. Για την επίλυση αυτού του ζητήματος, τα μοντέλα απαιτούν μεθοδολογίες αδιάλειπτης αυθεντικοποίησης που όλο και περισσότερο αντιλαμβάνονται και αυθεντικοποιούν τα μέλη με βάση ορισμένα βιομετρικά στοιχεία.

3.3 Χρηστικότητα των μεθόδων αυθεντικοποίησης

Η προστασία και η χρηστικότητα απαρτίζουν πρωταρχικές αρχές στην υλοποίηση της διαδικασίας εξέτασης ενός δελτίου ταυτότητας. Όμως, οι συνεχώς αύξουσες προϋποθέσεις σε ότι σχετίζεται με το αίτημα ενός σημαντικού επιπέδου προστασίας, συγχρόνως με την αξίωση για τη τήρηση της χρηστικότητας της εφαρμογής κατά την επαφή με τα μέλη, πολλές φορές ανατίθενται μεταξύ τους. Η ιδανική υπόθεση, εμπεριέχει την ανακάλυψη μιας απάντησης, στην οποία να τηρείται η ομοιόσταση ανάμεσα σε ασφάλεια και χρηστικότητα για το ίδιο χρονικό διάστημα. Αξίζει πρώτα να ληφθεί υπόψη το ζήτημα πως η επιβεβαίωση ταυτότητας θεωρείται μια περίπλοκη άποψη και το

ίδιο χρονικό διάστημα, τα δεδομένα αναφορικά με τη λειτουργία εξέτασης ταυτότητας ενδείκνυται να εμφανίζονται με επιγραμματικό και καταληπτό τρόπο στα μέλη.

Ένα πρότυπο καθημερινό μέλος δεν γνωρίζει σε υπερβολικό βαθμό τις πληροφορίες σχετικά με την ασφάλεια και το περιβάλλον επαφής του κάθε μέλους, όπως για παράδειγμα η μέθοδος περιήγησης στο διαδίκτυο, η οποία έχει προγραμματιστεί για να κρύβει τις λειτουργίες εξέτασης ενός δελτίου ταυτότητας, παρέχοντας τα στοιχειώδη δεδομένα για το τι γίνεται κάθε φορά στο θεμέλιο. Αυτό το συμβάν πιθανόν να απαρτίζει μια ορθή διαδικασία, σχετικά τη γενική άποψη της χρησιμότητας προς τα μέλη, εφόσον τους παραχωρεί να δώσουν βαρύτητα και να επιδοθούν ιδίως με την εργασία που θέλουν να επιτελέσουν.

Έτσι, συγκεντρώνονται ορισμένα ελαττώματα και αντιπαραθέσεις με την άποψη της σημαντικής και ικανής επαλήθευσης του δελτίου ταυτότητας. Το εκάστοτε κατεστημένο δεν μπορεί να επίσταται την ονομασία της κάθε οντότητας με την οποία το μέλος επιθυμεί να συνεννοηθεί και κατ' ακολουθία δεν δύναται να αξιολογεί τα επακόλουθα της διαδικασίας επιβεβαίωσης του δελτίου ταυτότητας. Μια κοινή άποψη μελέτης των κατεστημένων αυθεντικοποίησης αναμφίβολα είναι να πραγματοποιήσει την όλη διαδικασία επαλήθευσης της πρωτοτυπίας του δελτίου ταυτότητας του κάθε μέλους όσο το δυνατόν πιο διαυγές, ώστε να συρρικνωθεί η νοερή επίπτωση του μέλους και έτσι να προσδιορίσει το κατεστημένο δύσχρηστο.

Η εξέταση ενός δελτίου ταυτότητας ενδέχεται να πραγματοποιηθεί κάνοντας χρήση διαφορετικές λειτουργίες και αν αυτές καταλήγουν τελείως κρυφές από το μέλος, τότε εκείνος δεν θα μπορεί να εξαγάγει αν καταληκτικά είναι αποτελεσματικές ή όχι. Αυτή η διαδικασία αναμφίβολα εγκρίνει προκειμένου να διαμείνουν ακαθόριστες οι επιτυχημένες εφορμήσεις και, έτσι, τελικά να γίνεται το κατεστημένο ανασφαλές. Συγχρόνως, η ικανότητα του προσώπου να προσέχει πολλές και διάφορες λειτουργίες και γεγονότα το ίδιο χρονικό διάστημα, θεωρείται καθορισμένη και αν εμφανιστούν ποίκιλλα δεδομένα στην ίδια χρονική στιγμή, στις περισσότερες φορές είτε θα εξοργιστεί είτε απλά θα παραλύσει.

Κάτι τέτοιο θα μπορούσε να συγκατατεθεί στην υπόσταση πολλών και διαφορετικών ατυχών αγώνων εξέτασης του δελτίου ταυτότητας, ακόμη και αν έχουν εμφανιστεί στο μέλος δεδομένα για την λεπτομερή αστοχία. Το γεγονός αυτό επινοεί το παρακάτω δίλημμα στους προγραμματιστές: Πολλά στοιχεία το ίδιο χρονικό διάστημα είναι πιθανοφανές να επινοήσουν τις ίδιες δυσκολίες όσες και οι στοιχειώδεις γνώσεις. Βέβαια, δεν υπάρχει πιθανότητα να υπάρχουν

πολλά στοιχεία από ότι το μέλος να μπορεί να αντιληφθεί και να διαχειριστεί, αλλά συγχρόνως αξίζει να είναι ικανό για τον απαιτούμενο τομέα προστασίας της εφαρμογής. Ο πειρασμός είναι να ενονομασθούν τα πιο κατάλληλα δεδομένα και να εμφανισθούν με τρόπο ευνόητο στο κάθε μέλος.

3.4 Συστήματα κρυπτογράφησης δεδομένων

Στην καθημερινότητα πολλοί χρήστες επικοινωνούν με μηνύματα μέσω ηλεκτρονικού ταχυδρομείου (e-mail) χρησιμοποιώντας το κινητό τους τηλέφωνο. Η ουσία των μηνυμάτων είναι ότι εμπεριέχει οποιαδήποτε ενημέρωση, η οποία συχνά ενδέχεται να είναι εύθικτη. Από την αρχή της ανακάλυψης του διαδικτύου έως και σήμερα, το μέσο ανταλλαγής ηλεκτρονικών μηνυμάτων δεν έχει μεταβληθεί. Ο πομπός συγκροτεί ένα μήνυμα χρησιμοποιώντας μια μέθοδο από τον υπολογιστή ή / και κινητό του και το αποστέλλει στον εξυπηρετητή του παρόχου της εργασίας όπου και το κρατάει. Ο δέκτης χρησιμοποιώντας ένα παρόμοιο πρόγραμμα, αποκρίνεται στον εξυπηρετητή αν υφίσταται κάποιο μήνυμα για εκείνον και στο ενδεχόμενο καταφατικής απόκρισής του προσπελαύνει το μήνυμα.

Οι στρατηγικές απορρήτου των Google, Microsoft και Yahoo των οργανισμών, δηλαδή, που παρέχουν τις παραπάνω υπηρεσίες ηλεκτρονικού ταχυδρομείου, επισημαίνουν πως οι οργανισμοί αυτοί συγκεντρώνουν στοιχεία που σχετίζονται με τον χρήστη. Τα στοιχεία αυτά είναι εκείνα που παρέδωσε ο ίδιος ο χρήστης όταν εγγράφηκε για πρώτη φορά στην υπηρεσία όπως για παράδειγμα ονοματεπώνυμο, τηλέφωνο, διεύθυνση) αλλά και στοιχεία που συγκεντρώνονται χρησιμοποιώντας την υπηρεσία, όπως για παράδειγμα πληροφορίες συσκευής, τοποθεσία.

Οι αιτίες συγκέντρωσης αυτών των στοιχείων μεταβάλλονται συνεχώς και εμπερικλείουν τη διατήρηση της βάσης της εργασίας, προφύλαξη των χρηστών από εφορμήσεις, για παράδειγμα το Gmail αποστέλλει μήνυμα στο χρήστη αν εισαχθεί στην εφαρμογή από κάποιο άλλο τόπο ή άλλη συσκευή εκτός της γνωστής, αναβάθμιση της υπάρχουσας εφαρμογής. Αναφορικά με την κοινή χρήση της πληροφορίας με τρίτα άτομα, όλοι οι ανωτέρω οργανισμοί επισημαίνουν πως έχουν την άδεια να μοιραστούν τα στοιχεία με διάφορες μονάδες για την κατεργασία των γεγονότων αλλά και για νομικές αιτίες.

Η Google επισημαίνει πως θα δώσει στοιχεία σε τρίτα άτομα μόνο με την εξουσιοδότηση του ατόμου. Η αποκλειστική σύνδεση στο περιεχόμενο των ηλεκτρονικών μηνυμάτων υφίσταται από τη Microsoft, δηλώνοντας ότι δεν το μεταχειρίζεται για διαφημιστικές επιδιώξεις. Αξίζει να υπογραμμιστεί πως κανένας οργανισμός δεν επισημαίνει το χρονικό διάστημα αποθήκευσης των

ενημερώσεων. Η αποστολή και λήψη των μηνυμάτων ανάμεσα στις συσκευές και στα άτομα στις περισσότερες περιπτώσεις είναι κρυπτογραφημένη. Παρόλα αυτά, στον διαχειριστή και τις συσκευές τα μηνύματα διαβάζονται. Όπως αναφέρθηκε και από τις δηλώσεις απορρήτου, είναι στη διακριτική άνεση του κάθε οργανισμού το αν και σε ποιους θα δώσει προσέγγιση σε αυτά τα στοιχεία. Εκτός από την εκούσια ειδοποίηση των στοιχείων, η προσέγγιση ενδέχεται να γίνει και με ηλεκτρονική εφόρμηση στους εξυπηρετητές του οργανισμού, συνεπώς τα στοιχεία θα εντοπισθούν στα χέρια τρίτων με άνομες διαδικασίες.

Για την αποφυγή υποκλοπής των στοιχείων, ενδημούν πολλοί πάροχοι οι οποίοι παρέχουν υπηρεσίες ηλεκτρονικού ταχυδρομείου με κρυπτογράφηση. Ο πιο αναγνωρισμένος είναι ο ProtonMail. Ο συγκεκριμένος πάροχος κρυπτογραφεί τα μηνύματα του χρήστη με ένα ιδιωτικό κλειδί που βρίσκεται στον εξυπηρετητή του, προκειμένου να μπορεί το άτομο να αποκρυπτογραφεί τα μηνύματά του οπουδήποτε και αν συνδεθεί. Για την αποκρυπτογράφηση απαιτείται και ένας κωδικός που κατέχει μόνο το άτομο. Κατ' ακολουθία, αν κάποιος εισαχθεί στα μηνύματα και στο κλειδί του ατόμου (είτε έκνομα είτε άνομα) δεν μπορεί να τα αποκρυπτογραφήσει. Όπως αναφέρεται από την πολιτική απορρήτου, τα στοιχεία που συγκεντρώνονται είναι στοιχειώδη σε αναλογία με τους άλλους οργανισμούς. Άλλοι πάροχοι που παρέχουν κρυπτογράφηση θεωρούνται οι Disroot, Tutanota, Mailbox.org. (Χατζηγεωργίου, 2017).

Στις εφαρμογές Viber και WhatsApp υπάρχει ενεργοποιημένη η δυνατότητα κρυπτογράφησης από άκρο σε άκρο και μάλιστα για το Viber εξηγούν και την υλοποίησή της. Οι άλλες δύο εφαρμογές αρκούνται στην κρυπτογράφηση της επικοινωνίας μεταξύ εφαρμογής και εξυπηρετητή με το Facebook Messenger να έχει τη δυνατότητα ενεργοποίησης της κρυπτογράφησης από άκρο σε άκρο αν το θέλει ο χρήστης και μόνο για συγκεκριμένες συνομιλίες. Αξίζει να σημειωθεί ότι οι εφαρμογές που δεν υποστηρίζουν από προεπιλογή κρυπτογράφηση από άκρο σε άκρο είναι αυτές που στη δήλωση απορρήτου δεν κάνουν αναφορά στα μηνύματα.

Η εφαρμογή Viber έχει ακόμα δύο σημαντικά χαρακτηριστικά τα οποία βοηθάνε στην προστασία της ιδιωτικότητας. Το πρώτο είναι οι κρυφές συζητήσεις στις οποίες τα μηνύματα έχουν χρόνο αυτοκαταστροφής, προστατεύονται από προώθηση σε άλλους χρήστες και είτε απαγορεύουν τη λήψη στιγμιότυπου της οθόνης είτε προειδοποιούν τον άλλο χρήστη ότι ελήφθη κάποιο στιγμιότυπο. Το δεύτερο χαρακτηριστικό είναι η προστασία κάποιας συζήτησης με έναν τετραψήφιο κωδικό. Ορίζοντας κάποιο κωδικό, η συζήτηση δεν είναι πλέον ορατή στη λίστα με τις συζητήσεις και για την εμφάνισή της

απαιτείται η εισαγωγή του κωδικού. Η μόνη άλλη εφαρμογή που περιλαμβάνει χρόνο αυτοκαταστροφής των μηνυμάτων είναι η Facebook Messenger.

Μία εναλλακτική πλατφόρμα άμεσων μηνυμάτων η οποία δίνει βάση στην προστασία της ιδιωτικότητας και της ασφάλειας είναι η Signal η οποία συνίσταται και από τη διεθνή αμνηστία (Amnesty, 2016). Η πλατφόρμα συλλέγει και αποθηκεύει όσες πληροφορίες είναι απαραίτητες για τη λειτουργία της. Οι πληροφορίες αυτές δε μοιράζονται με τρίτους εκτός αν υπάρχει συγκατάθεση του χρήστη ή αν απαιτείται νομικά (Open, 2017). Αυτό έχει άλλωστε αποδειχθεί, όταν η υπεύθυνη εταιρία για την πλατφόρμα είχε κλητευθεί από το δικαστήριο να μοιραστεί πληροφορίες σχετικές με έναν τηλεφωνικό αριθμό και το μόνο που μοιράστηκε ήταν τότε έκανε εγγραφή ο χρήστης στην πλατφόρμα και τότε την χρησιμοποίησε τελευταία φορά (Perlroth & Benner, 2016). Για την κρυπτογράφηση από άκρο σε άκρο χρησιμοποιεί το πρωτόκολλο Signal, ένα ανοιχτό πρωτόκολλο ανεπτυγμένο από την ίδια εταιρία το οποίο χρησιμοποιούν και οι πλατφόρμες που αναφέρθηκαν προηγουμένως για τον ίδιο λόγο.

3.5 Κωδικοποίηση tokens

Τα αναγνωριστικά σύμβολα (χαρακτήρες αντικατάστασης ή ενδείξεις) εκπροσωπούν προγραμματιζόμενα δεδομένα ή άδειες προσέγγισης, τα οποία διευθύνει ένα ευφρές συμβόλαιο και ένα υποκείμενο μοιρασμένο καθολικά. Θεωρούνται προσβάσιμα μόνο από το πρόσωπο που κατέχει το ιδιωτικό κλειδί για αυτήν τη διεύθυνση και ενδέχεται να υπογραφεί μόνο με αυτό το ιδιωτικό κλειδί. Τα tokens είναι πιθανόν να επιδράσουν προς τον οικονομικό κόσμο με το ίδιο μέσο όπως το ηλεκτρονικό ταχυδρομείο επενέργησε το ταχυδρομικό κατεστημένο. Τα tokens, πατροπαράδοτα, δύνανται να εκπροσωπούν οποιαδήποτε θωριά οικονομικής αξίας. Για παράδειγμα, μάρκες καζίνο, κουπόνια, πιστοποιητικά μετοχών, ομόλογα, κρατήσεις, συνδρομές και πολλά άλλα. Πολλά tokens έχουν ορισμένα ενσωματωμένα μέσα κατά της παραποίησης, που ενδέχεται να είναι παραπάνω ή πιο λίγο αλάνθαστα, ώστε να αποτραπεί η απάτη του κατεστημένου.

Τα χαρτονομίσματα ή τα κέρματα θεωρούνται επίσης tokens. Τα tokens χρησιμοποιούνται στο χώρο των υπολογιστών, όπου μπορούν να εκπροσωπούν την άδεια εφαρμογής ορισμένης λειτουργίας ή χρήσης δικαιωμάτων προσέγγισης. Τα κρυπτογραφικά tokens στο Blockchain δύνανται να εναρμονίσουν και τις δύο σημασίες:

1. Αξιώσεις προσέγγισης σε κάποια υποκείμενη οικονομική τιμή (κυριότητα)

2. Άδεια προσέγγισης στην κυριότητα ή τις προσφορές οποιουδήποτε άλλου ή ομαδικού αγαθού.

Αυτή η κυριότητα ή η εργασία ενδέχεται να είναι κοινή ή ιδιωτική. Θεωρείται αξιόλογο να υπογραμμιστεί πως η έννοια «token» είναι απλώς μια μετάφραση. Ένα token άπτεται σε δεδομένα ενεργού ή και άδειες προσέγγισης που διευθύνουν ομαδικώς από ένα δίκτυο υπολογιστών, ένα δίκτυο blockchain ή άλλο μοιρασμένο καθολικά. Ένα μοιρασμένο καθολικά προμηθεύει ένα επίπεδο ειδικής κατάστασης, μια δημόσια βάση με τη θωριά διαμοιρασμένου αρχείου συναλλαγών που αντιλαμβάνεται ποια διεύθυνση πορτοφολιού είναι ο ιδιοκτήτης του διακριτικού.

Τα κρυπτογραφικά tokens αποτελούν μια ενότητα νόμων, που κωδικοποιούνται σε ευφυή συμβόλαια – τη σύμβαση tokens. Κάθε διακριτικό υπάγεται σε μια διεύθυνση blockchain. Αυτά τα διακριτικά θεωρούνται προσβάσιμα με ένα ειδικευμένο πορτοφόλι, προκειμένου να συγκοινωνεί με το blockchain και διευθύνει το ζευγάρι κοινού ιδιωτικού κλειδιού που συνδέεται με τη διεύθυνση blockchain.

Μονάχα το πρόσωπο που κατέχει το ιδιωτικό κλειδί για αυτήν τη διεύθυνση ενδέχεται να έχει πρόσβαση στα ομόλογα token. Αυτό το πρόσωπο ενδέχεται, ως εκ τούτου, να λογισθεί ο ιδιοκτήτης ή ο θεματοφύλακας αυτού του διακριτικού. Αν το token εκπροσωπεί ένα συστατικό, ο ιδιοκτήτης δύναται να κινήσει τη μετακίνηση των διακριτικών υπογράφοντας με το ιδιωτικό κλειδί του, το οποίο με τη σειρά του κατασκευάζει ψηφιακό δακτυλικό αποτύπωμα ή ψηφιακή υπογραφή.

Αν το διακριτικό αποτελεί δικαίωμα προσέγγισης σε κάτι που διακατέχει κάποιος άλλος, ο ιδιοκτήτης αυτού του διακριτικού υπάρχει πιθανότητα να κινήσει την πρόσβαση υπογράφοντας με το ιδιωτικό κλειδί του, δημιουργώντας έτσι ένα ψηφιακό δακτυλικό αποτύπωμα. Αν το διακριτικό αποτελεί ψήφο, ο ιδιοκτήτης αυτού του διακριτικού δύναται να ψηφοφορήσει υπογράφοντας με το ιδιωτικό κλειδί του, κατασκευάζοντας μια ψηφιακή υπογραφή (Βαβαδάκης, 2020).



Εικόνα 6: Εφαρμογές των Tokens (Πηγή: Voshmgir, 2019)

Τα εμβλήματα εγγύησης έχουν παρεμφερή τεχνοτροπία με τις επικουρικές ιδιότητες, αλλά χρησιμοποιούνται πολλές φορές στη διαδικασία της χρηματοδότησης ενός νέου κρυπτονομίσματος ή ενός έργου blockchain. Ένα έμβλημα εγγύησης εκπροσωπεί μια μερίδα στο έργο και τακτικά συνοδεύεται από προσμονή απολαβής μελλοντικά. Οι ιδιοκτήτες tokens δύνανται να λάβουν ωφέλειες όπως δικαίωμα ψήφου, χρηματικοί τίτλοι κέρδους και μερίδια. Λόγω αυτού, τα εμβλήματα προστασίας εξαρτώνται σε καθορισμένους ομοσπονδιακούς κανόνες εγγύησης.

Τα επικουρικά εμβλήματα θεωρούνται ψηφιακά εμβλήματα που χρησιμοποιούνται για ένα προϊόν ή υπηρεσία βασιζόμενη σε blockchain. Τρέχουν σε μια πλατφόρμα blockchain, ή απαρτίζουν κομμάτι μιας οικονομίας Blockchain. Τα πιο πολλά tokens ωφελιμότητας είναι εμβλήματα ERC20 που γίνονται στο Ethereum blockchain, αλλά με τη συνεχιζόμενη διακίνηση άλλων πλατφορμών blockchain. Έχουν επίσης παρουσιαστεί και άλλα είδη εμβλημάτων, όπως TRC10 και TRC20.

3.6 Πρότυπα χρηστικότητας αυθεντικοποίησης

Στις δυνητικές διαμάχες ανάμεσα στην εγγύηση και στη χρηστικότητα, ενδέχεται να μετριαστούν κάνοντας χρήση ορισμένες γενικές αρχές σκιαγράφησης, όπως ο μετριασμός του αγώνα της εισαγωγής ενός μέλους,

λήψη αποφάσεων στο όνομα του χρήστη, πληροφόρηση του μέλους για τις επιδράσεις που υλοποιήθηκαν για λογαριασμό του και την ικανότητα να αναιρέσει αυτές τις επιδράσεις όταν είναι άξιο και αν όχι να μετριάσει την απήχυσή τους. Παρόλα αυτά θεωρείται αξιόλογο να ληφθεί πραγματικά υπόψη ότι δεν υφίσταται ορισμένη και εγνωσμένη αρχή χρηστικότητας και υποδείγματα για τις μεθοδολογίες εξέτασης ταυτότητας (Καλκουτσή & Μαρινέρα, 2018).

Οι μελετητές μέσω της έρευνας που πραγματοποίησαν συμπεραίνουν πως για καθορισμένες επενεργήσεις στις διαδικασίες επιβεβαίωσης ταυτότητας βασίζονται οι διαφορετικοί ανθρώπινοι συντελεστές. Αυτοί οι ερευνητές (Rosenberger & Schwartzmann, 2014) έδωσαν μια έρευνα που βασίστηκαν και σε προγενέστερες, σχετικά με την επιβολή που έχουν στην χρηστικότητα και παραγωγικότητα ενός μοντέλου στα διαφορετικά γνωρίσματα των μελών.

Μέσω της ανασκόπησης βιβλιογραφίας (Cranor & Buchler, 2014 & Fischer, Sadeghi, & Winandy, 2009) αναφορικά με τη χρηστικότητα των μοντέλων, ορισμένοι από τους βασικούς συντελεστές χρηστικότητας, δίνονται παρακάτω:

1. Χρόνος εκμάθησης

Ο χρόνος εκμάθησης επιδρά τόσο στο κέρδος εγκατάστασης και τοποθέτησης του μοντέλου όσο και στην παραδοχή του από τα μέλη. Εάν ο χρόνος μάθησης προϋποθέτει πολύ χρόνο και ανεκτικότητα, δεν είναι αναμφίβολο ότι τα μέλη, πολλές φορές εργαζόμενοι, θα θεωρούνται τελικά τόσο καλοδιάθετοι να κάνουν χρήση του συστήματος. Αυτό θα θεωρήσει την χρήση του σχετικά ανούσια και συγχρόνως πολυδάπανη σε χρόνο και κέρδος. Ο αγώνας σχετίζεται στενά με την κατανάλωση χρόνου, και η προσπάθεια που χρειάζεται ξεχωρίζει αντίστοιχα με το κάθε μέλος.

2. Ταχύτητα απόδοσης

Η ταχύτητα απόδοσης σχετίζεται άρρηκτα με την σημασία του δεκτού χρόνου χρησιμοποίησης. Τα μέλη ρέπουν να δυσφορούν στη διαχείριση ενός μοντέλου εάν απαιτείται πολύς χρόνος και αγώνας.

3. Υποκειμενική ευχαρίστηση

Τα πιο δηλωτικά στοιχεία συναρτώμενα με τη χρηστικότητα του μοντέλου αυθεντικοποίησης είναι οι κριτικές και το σχόλιο από το κάθε μέλος. Οι υποκειμενικές πεποιθήσεις των μελών θεωρούνται ευεργετικές αλλά κάπως δυσεπίτευκτο να αξιολογηθούν. Είναι, συνεπώς, αξιόλογο να μεταχειρίζεται

μια συγκεκριμένη κλίμακα κάθε φορά που ζητείται από τα μέλη η άποψή τους αναφορικά με το μοντέλο.

4. Ποσοστό παραπτωμάτων από τα μέλη

Αν ένα μοντέλο ελέγχου ταυτότητας πρόκειται να μπει σε χρήση και να μεταχειριστεί, θεωρείται πολύ αξιόλογο το ποσοστό των παραπτωμάτων που προξενούνται από το μοντέλο να είναι ελάχιστο ή μηδενικό. Ικανοποιητικός αριθμός ελέγχων αξίζει να γίνει με στόχο να ανακλύψουν όσο το δυνατόν πιο θετικά επακόλουθα, ώστε να αποφευχθούν σφάλματα ύστερα από τη διάθεση του μοντέλου στα μέλη.

5. Ευρωστία

Η εγγύηση ενός μοντέλου δεν θα πρέπει να είναι χρονοβόρα ή φανερό και αυτό γιατί αυτό προξενεί δυσανασχέτηση στο κάθε μέλος, που ενδεχομένως να κλείσει την ιδιότητα ασφαλείας προκειμένου να αποσοβήσει την φορτική πίεσή του (Cranor & Buchler, 2014). Υπογραμμίζεται πως η διάρκεια υπομονής του μέλους σε μια ιδιότητα προστασίας θεωρείται ελάχιστη λόγω του ότι εισακούμε στα αρνητικά σε μοντέλα που βιώνει ότι του δαπανούν το χρόνο του δίχως φανερά αποτέλεσμα. Διερευνώντας την σημασία της ευχέρειας, λοιπόν, για ένα μοντέλο εξέτασης ταυτότητας, λαμβάνεται υπόψη ο χρόνος που δαπανάται για την υλοποίηση μιας εξέτασης ταυτότητας ή αλλαγής και καταχώρησης ενός μέλους (Fischer, Sadeghi, & Winandy, 2009). Ο χρόνος εξέτασης ταυτότητας άπτεται στον χρόνο που επιζεί καθώς το μέλος επιχειρεί να καθιερώνει τα ιδιαίτερά του δεδομένα ώστε να έχει πρόσβαση σε ένα μοντέλο. Ο χρόνος υποκατάστασης θεωρείται ο χρόνος ανάκτησης των δεδομένων εξέτασης ταυτότητας για ένα μέλος όταν δεν είναι πλέον δραστήριος.

6. Αφομοίωση

Η δεξιοσύνη των μελών ενός μοντέλου να αντιλαμβάνονται τα γνωρίσματα ασφαλείας παρουσιάζει την έκταση της χρηστικότητας αυτού του μοντέλου (Cranor & Buchler, 2014). Μια από τις αφετηρίες της μελέτης περιβάλλοντος διεπαφής χρήστη, είναι πως το μέλος αξίζει να είναι σε θέση να αποδεχτεί αντί να χρειάζεται να αναθυμηθεί το γνώρισμα μιας αναλυτικής διαδικασίας.

7. Σύσταση

Δεδομένου ότι η χρήση της τεχνολογίας δεν είναι θεληματική αλλά πιθανόν κάτι που πρέπει να μεταχειρίζονται τα μέλη, η μελέτη του περιβάλλοντος διεπαφής χρήστη πρέπει να μπορεί να περιλαμβάνει διάφορους τύπους μελών

(Mihajlov, Jerman – Blazic, & Josimovsk, 2011 & Reed & Monk, 2011). Αυτό επιτυγχάνει ότι κάθε μέλος, αυθυπόστατα από το πόσο κατανοεί τις δεξιότητες και τις γνώσεις του, μπορεί να μεταχειριστεί ένα μοντέλο με γνωρίσματα εξέτασης ταυτότητας. Αυτό το κριτήριο ποσοτικοποιείται με εκτίμηση του εμπλουτισμού μελών σε κατατάξεις αρτιμέλειας. Τα μέλη αξίζει να δέχονται εναργή βεβαίωση για το τι πρέπει να τελούν σε όποιο επίπεδο και αν βρίσκονται.

8. Δυναμικότητα – Επιδεξιότητα

Δίνει άδεια στα μέλη να δαπανούν τα στοιχειώδη δυνατά ποσά πόρων (π.χ. MB) σε αναλογία με την τελεσφόρηση που υλοποιείται.

9. Τελεσφόρηση

Η δεξιосύνη της εφαρμογής εγκρίνει στα μέλη να πραγματοποιούν καθορισμένες ενασχολήσεις με πιστότητα και απαρτία.

10. Αποδοτικότητα

Το επίπεδο τελεσφόρησης που πραγματοποιείται σε αναλογία με τους πόρους που καταναλώνουν τα μέλη και το μοντέλο. Οι γόνιμες ενέργειες χρήστη θεωρούνται εκείνες που βοηθούν στην κατανάλωση των εργασιών. Ως εκ τούτου, η σημασία της αποδοτικότητας ελέγχει τους γόνιμους πόρους που καταναλώνονται για την ικανοποίηση των υποχρεώσεων των μελών.

11. Ευαρέσκεια

Άπτεται στις υποκειμενικές αποκρίσεις των μελών αναφορικά με τα αισθήματά τους κατά τη χρησιμοποίηση ενός λογισμικού.

12. Ευχέρεια Μάθησης

Η ευχέρεια με την οποία δύνανται να κυριαρχήσουν τα γνωρίσματα που χρειάζονται για το επίτευγμα καθορισμένων σκοπών. Είναι η ικανότητα του δημιουργήματος λογισμικού να εγκρίνει στα μέλη να νιώθουν πως είναι ικανοί να χρησιμοποιούν γόνιμα το προϊόν λογισμικού μόλις αφομοιώσουν και άλλες καινούργιες λειτουργίες.

13. Εγγύηση

Σχετίζεται το αν ένα προϊόν λογισμικού μετριάζει το ρίσκο φθοράς σε πρόσωπα ή άλλους πόρους, όπως υλικό ή αποθηκευμένα στοιχεία. Η λειτουργική εγγύηση επισημαίνεται στην δεξιοσύνη του προϊόντος λογισμικού να χαροποιεί τις προϋποθέσεις του μέλους κατά την κανονική λειτουργία χωρίς να ζημιώνει άλλους πόρους και τον περίγυρο. Τα κριτήρια που αξίζει να ληφθούν υπόψη κατά την εκτίμηση της λειτουργικής εγγύησης εμπεριέχουν τη σύνδεση, την πιστότητα, την απαρτία, την προστασία και την σιγουριά. Η εγγύηση σε ενδεχόμενο έκτακτης ανάγκης σχετίζεται με την επιτηδειότητα του προϊόντος λογισμικού να υπηρετεί εκτός της κανονικής λειτουργίας του, αλλά συνεχίζει να απομακρύνει τις απειλές. Τα κριτήρια για την εγγύηση έκτακτης ανάγκης εμπεριέχουν υπομονή παραπτώματος και εγγύηση των πόρων.

14. Προσβασιμότητα

Η δεξιοσύνη ενός προϊόντος λογισμικού να κάνει χρήση από πρόσωπα με κάποιον τύπο χωλότητας (π.χ. οπτική, ακοή, ψυχοκινητική) (Mieczakowski & Clarkson, 2013). Ο οργανισμός World Wide Web (Caldwell et al., 2004) υπέβαλλε διάφορες κατευθυντήριες γραμμές σχεδίασης για το σχηματισμό ιστοσελίδων πιο οικονομικών σε πρόσωπα με αναπηρίες.

15. Καθολικότητα

Κατά πόσον ένα προϊόν λογισμικού υποδέχεται πολλά μέλη με διαφορετικό πολιτισμικό θεμέλιο.

16. Ωφελιμότητα

Αν ένα προϊόν λογισμικού εγκρίνει στα μέλη να επιλύσουν ουσιαστικά ζητήματα με δεκτό τρόπο. Η ωφελιμότητα τεκμαίρεται ότι ένα προϊόν λογισμικού θεωρείται πρακτικό, αντικατοπτρίζοντας το πόσο στενά το προϊόν υποβαστάζει το πρότυπο εργασίας του χρήστη. Η ωφελιμότητα συναρτάται προφανώς από τα γνώρισμα και τη λειτουργικότητα που παρέχει το προϊόν λογισμικού. Αντανακλά, επίσης, την ενημέρωση και το επίπεδο ικανοτήτων των μελών κατά την εφαρμογή καθορισμένων ενασχολήσεων.

17. Φορητότητα

Η δεξιοσύνη ενός μοντέλου να παρουσιάζεται σε διαφορετικές πλατφόρμες.

Φυσικά οι συντελεστές που μόλις περιγράφηκαν δεν θεωρούνται ότι είναι αυθυπόστατοι. Στο ηλεκτρονικό εμπόριο, για παράδειγμα, οι ηλεκτρονικοί πελάτες είναι πιθανόν να εκμυστηρεύονται έναν ιστότοπο μόνο εάν αρχικά

νιώθουν σίγουροι, όμως την ίδια στιγμή πλήρεις από την πλοήγηση, την παρουσίαση, την ευχερή αναζήτηση όταν τον χρησιμοποιούν. Είναι φανερό πως τα ποιοτικά κριτήρια χρηστικότητας και εγγύησης δεν δύνανται να συζητηθούν ανεπηρέαστα. Είναι επιβεβλημένο να ελεγχθούν μαζί ενώ σχεδιάζεται το περιβάλλον επαφής μέλους. Αυτό θα παρακωλύει τους προγραμματιστές από το να εφεύρουν και να επινοήσουν ένα μοντέλο στο οποίο όλες οι διαδικασίες εγγύησης να διαμένουν αφανέρωτες, να γίνονται αυτόματα δίχως το κάθε μέλος να αντιλαμβάνεται πραγματικά τα γνωρίσματα εγγύησης του μοντέλου. Μια βελτιωμένη επίλυση θα ήταν να κατέχουν τα μέλη τα αντικείμενα που τελούν καθώς και τις συνέπειες που ενδέχεται να προξενηθούν λόγω των επιδράσεών τους.

Υφίσταται η γενική γνώμη πως η εγγύηση και η χρηστικότητα θεωρούνται ασυμβίβαστοι όροι όταν πρόκειται για μελέτη που εμπεριέχει την συμπλοκή μέλους. Η χρηστικότητα και η εγγύηση αξίζει να ελεγχθούν κατά τέτοιο τρόπο που να εγκρίνει στα μέλη να κάνουν προτάσεις στους προγραμματιστές για τη μελέτη των περιβαλλόντων χρήστη που βρίσκουν άνετα προκειμένου να δύναται να ωφελούνται και, συγχρόνως, να χρησιμοποιούν με εγγύηση τα πληροφοριακά συστήματα.

Με την παρουσίαση της χρήσης υπηρεσιών διαδικτύου που καθιστά τη ζωή πολύ πιο ευχερή και άνετη για τα μέλη, τίθεται το ερώτημα αναφορικά με την χρηστικότητα και την εγγύηση του μοντέλου που χρησιμοποιούν. Το πρόβλημα της χρηστικότητας σχετίζεται με το να τονίζεται πιο πολύ με νέα μέσα που κατασταλάζουν στην πρόοδο της μελέτης της ανθρώπινης αλληλεπίδρασης με το μοντέλο, με στοιχειώδη λόγια για την εγγύηση.

3.7 Κωδικοποίηση one time password (OTP)

Μια κραταιή μεθοδολογία εξέτασης ταυτότητας είναι ο κωδικός (OTP), ο οποίος εντάσσεται στις εφαρμογές SaaS. Αυτό εγκρίνει μια ισχυρότερη εξέταση ταυτότητας από μονάχα κωδικούς πρόσβασης. Οι πάροχοι SaaS κατά κανόνα δεν ισχυρίζονται διαφορετικές λύσεις ελέγχου ταυτότητας, εκτός από την απλή εισαγωγή με ένα όνομα χρήστη και κωδικό πρόσβασης. Ο πιο αυστηρός έλεγχος ταυτότητας προϋποθέτει τη χρήση διακριτικού υλικού ή δυνατότητας OTP δίχως κωδικούς για μέλη που επιθυμούν να λάβουν ένα μήνυμα.

Με ποικίλες εφαρμογές OTP, ο επιμελητής ή ο διαχειριστής συγκαταλέγει τις χρήσεις SaaS στο διαδίκτυο. Μόλις εισαχθεί μια εφαρμογή SaaS στην εφαρμογή, θα ληφθεί ένα αναγνωριστικό αίτησης. Υπάρχει πιθανότητα χρήσης για πραγματοποίηση εισόδου δίχως κωδικό πρόσβασης ή δοσοληψίες υψηλής ιδιοσυστασίας στην εφαρμογή SaaS. Με ένα API, η εφαρμογή SaaS ενδέχεται

πλέον να αποστέλλει έναν κωδικό μιας χρήσης μέσω μηνυμάτων. Από εκείνη τη στιγμή και μετά, τα μέλη δύνανται να μετέρχονται την εφαρμογή εξέτασης ταυτότητας ή τα μαλακά διακριτικά (Hoogenraad, 2019).

Τα μέλη που δεν δύνανται να λάβουν μηνύματα εξαιτίας μιας κακής αποδοχής δύνανται να επινοήσουν με μη αυτόματο τρόπο μάρκες. Επιπροσθέτως, χρησιμοποιώντας το API για την επαλήθευση αυτών των διακριτικών και για τη διαβεβαίωση ότι το κάθε μέλος έχει πραγματικά πρόσβαση στον σωστό αριθμό τηλεφώνου. Ο κωδικός μιας χρήσης παρέχει μια σημαντική ασφαλή λύση 2FA, εναρμονίζοντας μια χρηστική εφαρμογή για κινητά με έναν μη προαιρετικό κωδικό PIN και περαιτέρω σχηματίσεις ασφαλείας, όπως μια ερώτηση ασφαλείας. Αυτές οι επιλύσεις προμηθεύουν άτεγκτα μέτρα προστασίας, τόσο από την πλευρά του διαχειριστή όσο και από την πλευρά της εφαρμογής για κινητά (Hoogenraad, 2019).

Ο κωδικός πρόσβασης ενός χρόνου με βάση το χρόνο (TOTP ή OTP) είναι μια σειρά δυναμικών ψηφίων κώδικα, η μεταβολή των οποίων βασίζεται στην ώρα. Συχνά, αυτοί παρουσιάζονται ως αριθμοί sic – digit που αναπαράγονται κάθε 30 δευτερόλεπτα. Τα TOTP πηγάζουν από έναν μυστικό κωδικό πρόσβασης που δίνεται κατά την εγγραφή χρήστη με τη εμφάνιση κωδικού QR ή σε απλό κείμενο. Τα TOTP εμφανίζονται είτε σε διακριτικά ασφαλείας λογισμικού είτε ως soft tokens, που έχουν να κάνουν με εφαρμογές για κινητές συσκευές που παρουσιάζουν τους αριθμούς. (HYPR, 2015).

Ένας τέτοιος κωδικός πρόσβασης (OTP) είναι μια αριθμητική ή αλφαριθμητική συμβολοσειρά χαρακτήρων που παράγεται με αυτόματο τρόπο και διαβεβαιώνει τον χρήστη για μία μόνο συναλλαγή ή συνεδρία σύνδεσης. Ένα OTP είναι πιο αλάνθαστο από έναν στατικό κωδικό πρόσβασης, ειδικά έναν κωδικό πρόσβασης που παρήχθη από χρήστη, ο οποίος μπορεί να είναι ανίσχυρος ή και να επαναχρησιμοποιηθεί σε πολλούς λογαριασμούς. Τα OTP μπορούν να υποκαταστήσουν τις πληροφορίες σύνδεσης ταυτότητας ή μπορούν να χρησιμοποιηθούν επιπλέον σε αυτές για να προσθέσουν ένα άλλο επίπεδο ασφάλειας (Richards & Wigmore, 2019).

Είναι ένας κωδικός πρόσβασης που μπορεί να χρησιμοποιηθεί μία φορά και μετά λήγει. Οι κωδικοί μίας χρήσης αναφέρονται συχνά με τη συντομογραφία OTP και μερικές φορές ονομάζονται, επίσης, κωδικοί OTP. Ένας εφάπαξ κωδικός πρόσβασης συνήθως αποτελείται από έναν αλφαριθμητικό κωδικό OTP (γράμματα και αριθμούς) και δημιουργείται για μία συνεδρία σύνδεσης. Μόλις συνδεθείτε με έναν εφάπαξ κωδικό πρόσβασης, λήγει και δεν μπορεί να χρησιμοποιηθεί για την επόμενη περίοδο σύνδεσης (IONOS, 2020).

Στις μεθόδους ελέγχου ταυτότητας που βασίζονται τα OTP, η εφαρμογή OTP του χρήστη και ο διακομιστής ελέγχου ταυτότητας συναρτώνται σε δημόσια μυστικά. Οι τιμές για OTP κωδικούς παράγονται κάνοντας χρήση τον αλγόριθμο Hashed Message Authentication Code (HMAC) και έναν κινούμενο συντελεστή, όπως στοιχείο βάσει χρόνου (TOTP) ή μετρητή γεγονότων (HOTP). Οι τιμές OTP έχουν λεπτά ή δευτερόλεπτα, χρονικά σήματα για μεγαλύτερη εγγύηση. Ο OTP κωδικός πρόσβασης μπορεί να δοθεί σε έναν χρήστη μέσω διαφόρων καναλιών, συμπεριλαμβανομένου ενός μηνύματος κειμένου που βασίζεται σε SMS, ενός email ή μιας ειδικής εφαρμογής σε τελικό σημείο (Richards & Wigmore, 2019).

Οι επαγγελματίες ασφαλείας αγωνιούν εδώ και πολύ καιρό ότι η παραποίηση μηνυμάτων SMS και οι επιθέσεις man – in – the – middle (MITM) μπορούν να χρησιμοποιηθούν για να σπάσουν τα συστήματα 2FA που βασίζονται σε εφάπαξ κωδικούς πρόσβασης. Ωστόσο, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) γνωστοποίησε σχέδια για κατάργηση της χρήσης SMS για κωδικούς πρόσβασης 2FA και OTP, καθώς η μέθοδος είναι ευάλωτη σε μια ποικιλία επιθέσεων που θα μπορούσαν να θέσουν σε κίνδυνο αυτούς τους κωδικούς πρόσβασης. Ως αποτέλεσμα, οι επιχειρήσεις που σκέφτονται να αναπτύξουν κωδικούς μίας χρήσης θα πρέπει να διερευνήσουν άλλες μεθόδους παράδοσης εκτός από SMS (Richards & Wigmore, 2019).

Ο OTP κωδικός πρόσβασης αποφεύγει τις κοινές παγίδες που αντιμετωπίζουν οι διαχειριστές πληροφορικής και οι διαχειριστές ασφαλείας με προστασία του κωδικού πρόσβασης. Δεν χρειάζεται να ανησυχούν για τους κανόνες σύνθεσης, τους γνωστούς και τους αδύναμους κωδικούς πρόσβασης, την κοινή χρήση διαπιστευτηρίων ή την επαναχρησιμοποίηση του ίδιου κωδικού πρόσβασης σε πολλούς λογαριασμούς και συστήματα. Ένα άλλο πλεονέκτημα των OTP κωδικών πρόσβασης είναι ότι καθίστανται άκυροι σε λίγα λεπτά, γεγονός που εμποδίζει τους εισβολείς να αποκτήσουν τους μυστικούς κωδικούς και να τους ξαναχρησιμοποιήσουν (Richards & Wigmore, 2019).

Οι κωδικοί μίας χρήσης χρησιμοποιούνται συχνά για έλεγχο ταυτότητας δύο συντελεστών σε ειδικότητες όπως οι διαδικτυακές τραπεζικές συναλλαγές, αλλά στις μέρες μας χρησιμοποιούνται όλο και περισσότερο από οργανισμούς. Σε πρώτο βήμα, εισάγονται τα συνηθισμένα διαπιστευτήρια σύνδεσης. Στη συνέχεια, δημιουργείται ένας δυναμικός κωδικός μίας χρήσης, ο οποίος απαιτείται επίσης για έλεγχο ταυτότητας OTP, χρησιμοποιώντας ένα εργαλείο όπως ένα διακριτικό ασφαλείας. Αυτό το επιπλέον βήμα εξασφαλίζει πολύ μεγαλύτερη ασφάλεια. Εάν οι μη εξουσιοδοτημένοι χρήστες αποκτήσουν πρόσβαση στον συνηθισμένο κωδικό πρόσβασης κατά τη διάρκεια αυτής της διαδικασίας, εξακολουθούν να μην έχουν αυτόν τον κωδικό, ο οποίος

παράγεται μόνο όταν απαιτείται για σύνδεση. Για αυτόν τον λόγο, όλο και περισσότερες διαδικτυακές υπηρεσίες αρχίζουν να χρησιμοποιούν έλεγχο ταυτότητας δύο παραγόντων, ειδικά όταν πρόκειται για ευαίσθητα δεδομένα.

Η χρήση ενός OTP όχι μόνο μπορεί να εξοικονομήσει πολλά έξοδα, αλλά και να προσφέρει στους πελάτες γαλήνη, γνωρίζοντας ότι τα διαπιστευτήριά τους είναι ασφαλή. Εάν τα στοιχεία του λογαριασμού ενός πελάτη παραβιαστούν, η διαδικασία εξουσιοδότησης δεν θα ολοκληρωθεί χωρίς το σωστό OTP για να αποσταλεί στον εγγεγραμμένο λογαριασμό του. Σε περίπτωση που ένας πελάτης εισέλθει με λάθος OTP, μπορεί να ζητήσει νέο κωδικό (έως και τρεις φορές) για να αποκτήσει πρόσβαση.

Οι κωδικοί μίας χρήσης λειτουργούν μέσω τυχαίων αλγορίθμων δημιουργώντας έναν νέο και τυχαίο κωδικό με κάθε φορά να απαιτείται ένας νέος κωδικός πρόσβασης. Στη συνέχεια, ο κωδικός αυτός χρησιμεύει ως ο δεύτερος κωδικός πρόσβασης που διακρίνεται σε κάθε σύνδεση λογαριασμού και διαρκεί τρία έως πέντε λεπτά μετά τη λήψη του. Αυτό καθιστά ένα OTP ιδανικό για μερικές από τις πιο προνομιούχες και ευαίσθητες δραστηριότητες που εκτελούνται στο διαδίκτυο (Virgillito, 2019).

3.8 Πλεονεκτήματα και μειονεκτήματα των one time passwords

ΠΛΕΟΝΕΚΤΗΜΑΤΑ (Virgillito, 2019)

- **Είναι ασφαλή από επιθέσεις που επαναλαμβάνονται**

Το πιο σημαντικό πλεονέκτημα που παρέχουν τα OTP σε αντιπαράθεση με τους αυτόνομους κωδικούς πρόσβασης είναι πως είναι ασφαλή από επιθέσεις που επαναλαμβάνονται. Δηλαδή, ένας αντίπαλος που τα μεταχειρίζεται με παραπλανητικό τρόπο για να συλλάβει τον κωδικό OTP δεν μπορεί να το υλοποιήσει ξανά, καθώς δεν ισχύει πλέον για μελλοντικές συνδέσεις.

- **Επιτρέπει να διατηρούνται τα email ασφαλή**

Τα OTP λαμβάνονται γενικά σε κινητές συσκευές μέσω μηνυμάτων. Αυτό σημαίνει ότι δεν απαιτείται να υπάρχει πρόσβαση στο email. Ως εκ τούτου, αποφεύγεται η σύνδεση στο λογαριασμό email σε δημόσιους υπολογιστές ή ενώ υπάρχει σύνδεση σε ένα μη ασφαλές σημείο πρόσβασης με Wi-Fi.

- **Είναι εύχρηστο στη χρησιμοποίηση**

Πολλά άτομα έχουν κινητό τηλέφωνο και υπάρχει λειτουργικότητα μηνυμάτων σε κάθε συσκευή. Το μήνυμα σημαίνει ότι οι OTP κωδικοί πρόσβασης είναι πρακτικοί στη χρήση. Αυτό είναι επίσης ωφέλιμο για τους οργανισμούς που προμηθεύουν τα OTP, καθώς οι τελικοί χρήστες είναι ήδη μαθημένοι με τις συσκευές τους και δεν χρειάζονται άλλη συσκευή για να λάβουν τον κωδικό. Ως επακόλουθο, τα OTP εγκρίνουν στους οργανισμούς όχι μόνο να αναβαθμίσουν την εμπειρία του χρήστη αλλά και να ελαττώσουν το λειτουργικό τους κόστος.

ΜΕΙΟΝΕΚΤΗΜΑΤΑ (Virgillito, 2019)

- **Δεν είναι δυνατός ο συγχρονισμός**

Οι ηλεκτρονικοί κωδικοί έχουν πολλά προβλήματα. Τα OTP βασιζόμενα σε αλγόριθμο πρέπει να ανταπεξέλθουν τη μετατόπιση εκτός συγχρονισμού με τον διακομιστή ελέγχου ταυτότητας αν το μοντέλο απαιτεί το OTP να υποβληθεί εντός προθεσμίας. Παρόλα αυτά, το πρόβλημα μπορεί εύκολα να επιλυθεί κάνοντας χρήση ένα συγχρονισμένο σύστημα χρόνου. Αυτά τα μοντέλα απομακρύνουν τέτοια προβλήματα, διαφυλάσσοντας ένα χρονόμετρο σε ηλεκτρονικούς κωδικούς.

- **Μπορεί να κλειδώσει τον λογαριασμό**

Αν η συσκευή OTP κλαπεί ή χαθεί ούδέποτε, πολλές επιθέσεις για σύνδεση από τον εισβολέα μπορούν να κλειδώσουν οριστικά τον λογαριασμό. Αυτό ενδέχεται να είναι δυσάρεστο σε περίπτωση ταξιδιού, καθώς η επικοινωνία με τον πάροχο OTP είναι πιθανόν να προϋποθέτει διεθνή κλήση, με ακριβά τέλη περιαγωγής. Έτσι, εάν ο πάροχος δεν μετριάσει τον αριθμό των προσπαθειών σύζευξης, ο αντίπαλος ενδέχεται να συνεχίζει να μπλοκάρει τον λογαριασμό.

- **Ενδέχεται να είναι πολυδάπανο για τους παρόχους**

Για παρόχους OTP, το κόστος ενδέχεται να είναι πρόβλημα, ιδίως αν παρέχουν κωδικό OTP. Άλλα προβλήματα με συσκευές κωδικού είναι πως υπάρχει πιθανότητα κλοπής ή καταστροφής ή εξαφάνισης. Επιπροσθέτως, οι χρήστες θα πρέπει να περάσουν από την δοκιμασία της φόρτισης όταν τελειώσει η διάρκεια ζωής της μπαταρίας. Ο καλύτερος τρόπος για την αποφυγή αυτών των προβλημάτων είναι η αποστολή κωδικών πρόσβασης μιας χρήσης μέσω μηνυμάτων SMS.

Καταληκτικά, αν ληφθούν υπόψη στη χρήση, τα πλεονεκτήματα και τα μειονεκτήματα των OTP, κάθε χρήστης δύναται να αναβαθμίσει την προστασία του λογαριασμού του, αξιοποιώντας έναν μοναδικό κωδικό πρόσβασης για

κάθε συνοχή. Εφόσον ο πάροχος συγχρονίζεται βάσει χρόνου και έχοντας μαζί του το κινητό ή τον κωδικό OTP, δύναται να αποτραπούν οι συντελεστές απειλής για πλαστογράφηση διαπιστευτηρίων του λογαριασμού. Επιπλέον, υπάρχει η δυνατότητα αποφυγής σε δημόσιους υπολογιστές που είναι πιθανόν να υπάρχει εγκατεστημένο καταγραφικό πληκτρολόγησης και άλλο λογισμικό ή λογισμικό καταγραφής διακριτικών (Virgillito, 2019).

ΚΕΦΑΛΑΙΟ 4: Υλοποίηση Εφαρμογής Αυθεντικοποίησης 2 παραγόντων (two factor authentication)

4.1 Αυθεντικοποίηση 2 παραγόντων

Πρόκειται για ένα πρωτόκολλο, το οποίο προστατεύει τους χρήστες, ζητώντας τους να επιβεβαιώσουν την ταυτότητά τους χρησιμοποιώντας 2 μεθόδους αυθεντικοποίησης.

Την σημερινή εποχή, οι περισσότεροι οργανισμοί χρησιμοποιούν τέτοιου τύπου τεχνικές, προκειμένου να εξασφαλίσουν μεγαλύτερο επίπεδο ασφάλειας στα συστήματα τα οποία χρησιμοποιούν.

Η αυθεντικοποίηση 2 παραγόντων μπορεί να χρησιμοποιήσει κάποιους από τους ακόλουθους παράγοντες:

- Possession factor: Αυθεντικοποιεί χρήστες χρησιμοποιώντας μόνο κάτι το οποίο ο χρήστης κατέχει, όπως ταυτότητα, mobile εφαρμογή για την λήψη OTP, ή ένα security token.
- Biometric factor: Αυτός συνήθως απαιτεί από τους χρήστες να είναι φυσικά παρόντες κατά την διάρκεια της αυθεντικοποίησης. Χαρακτηριστικά παραδείγματα αποτελούν το δακτυλικό αποτύπωμα ή η αναγνώριση προσώπου.
- Location and time factors: Πρόκειται για περιπτώσεις στις οποίες χρησιμοποιείται η τρέχουσα τοποθεσία του χρήστη, χρησιμοποιώντας GPS ή VPN.

4.2 Πως λειτουργεί η αυθεντικοποίηση 2 παραγόντων

Η αυθεντικοποίηση 2 παραγόντων περιλαμβάνει την παρακάτω διαδικασία:

1. Ο χρήστης αυθεντικοποιείται χρησιμοποιώντας email και password.
2. Η πλατφόρμα επιβεβαιώνει τις πληροφορίες του χρήστη και ζητάει μια δεύτερη τεχνική αυθεντικοποίησης.
3. Η πλατφόρμα δημιουργεί ένα one-time-password (OTP) και το στέλνει στην συσκευή που μόνο ο χρήστης έχει πρόσβαση.

4. Ο χρήστης παρέχει το OTP που έλαβε προς την πλατφόρμα, η οποία πραγματοποιεί έλεγχο και αυθεντικοποιεί τον χρήστη.

Time – based One – Time Password (TOTP)

Το time – based One – Time Password (TOTP) είναι ένα αρκετά συνηθισμένος τρόπος για την υλοποίηση του 2FA. Λειτουργεί ζητώντας από τον χρήστη ένα token το οποίο συνήθως στέλνεται με SMS, email ή με μια μυστικά δημιουργημένη πρόσβαση στην συσκευή του χρήστη που έχει συγκεκριμένο χρονικό περιθώριο. Συγκρίνει το token που παρέχεται με το δημιουργημένο token, έτσι ώστε να μπορέσει να γίνει ο απαραίτητος έλεγχος.

Google Authenticator

Χρησιμοποιεί μια τεχνική, η οποία υλοποιεί το 2FA χρησιμοποιώντας TOTP και HMAC-based OTP για την αυθεντικοποίηση των χρηστών σε μία εφαρμογή. Αποτελεί ένα μέρος του Open Authentication (OATH).

4.3 Λεπτομέρειες Υλοποίησης

Η αυθεντικοποίηση 2 παραγόντων χρησιμοποιείται συχνά σε web εφαρμογές, έτσι ώστε να παρέχεται ένα επιπλέον επίπεδο ασφάλειας, όταν ο χρήστης χρησιμοποιεί έναν server. Έτσι λοιπόν, χρησιμοποιώντας την γλώσσα Python, δημιουργήσαμε μια Flask εφαρμογή, στην οποία προσθέσαμε ένα επιπλέον επίπεδο ασφάλειας χρησιμοποιώντας Google Authenticator.

Καταρχάς, έγινε εγκατάσταση του Flask web framework, του Flask – Bootstrap, και της βιβλιοθήκης PyOTP, που χρησιμοποιήθηκαν για την υλοποίηση κρίσιμων λειτουργιών.

Για την εγκατάστασή τους χρησιμοποιήθηκαν οι παρακάτω εντολές:

```
pip install flask  
pip install pyotp  
pip install flask-bootstrap4
```

4.4 Δημιουργία ενός απλού Flask Server

Ξεκινήσαμε την υλοποίηση της εφαρμογής με την δημιουργία ενός Flask Server. Το αρχείο το οποίο δημιουργήσαμε περιελάμβανε τον παρακάτω κώδικα:

```

from flask import *
from flask_bootstrap import Bootstrap

app = Flask(__name__)
app.config["SECRET_KEY"] = "APP_SECRET_KEY"
Bootstrap(app)

@app.route("/")
def index():
    return "<h1>Hello World!</h1>"

if __name__ == "__main__":
    app.run(debug=True)

```

Με τον τρόπο αυτό ελέγξαμε ότι ο Flask Server δημιουργήθηκε με επιτυχία.

4.5 Αυθεντικοποίηση ενός παράγοντα

Στην συνέχεια προστέθηκε στον κώδικα της εφαρμογής μας, η δυνατότητα αυθεντικοποίησης χρησιμοποιώντας username και password. Ο κώδικας ο οποίος χρησιμοποιήθηκε ήταν ο εξής:

```

@app.route("/login/")
def login():
    return render_template("login.html")

```

Επίσης δημιουργήθηκε, ένα αρχείο (login.html), το οποίο περιέχει την φόρμα για την εισαγωγή των στοιχείων εισόδου. Ο κώδικας του συγκεκριμένου αρχείου είναι ο εξής:

```

{% extends "bootstrap/base.html" %}

{% block content %}
<div class="container">
  <div class="row justify-content-center">
    <div class="col-lg-12">
      <div class="jumbotron text-center p-4">

```

```

    <h2>Flask + 2FA Demo</h2>
  </div>
</div>
<div class="col-lg-6">
  {% with messages = get_flashed_messages(with_categories=true) %}
  {% if messages %}
  {% for category, message in messages %}
  <div class="alert alert-{{ category }}" role="alert">
    {{ message }}
  </div>
  {% endfor %}
  {% endif %}
  {% endwith %}
  <form method="POST">
    <div class="form-group">
      <label for="username">Username</label>
      <input type="text" class="form-control" id="username" name="username"
required>
    </div>
    <div class="form-group">
      <label for="password">Password</label>
      <input type="password" class="form-control" id="password"
name="password" required>
    </div>
    <div class="text-center">
      <button type="submit" class="btn btn-primary">Authenticate User</button>
    </div>
  </form>
</div>
</div>
{% endblock %}

```

Παραθέτουμε screenshot από την συγκεκριμένη σελίδα:

Flask + 2FA Demo

Username

Password

Authenticate User

Εικόνα 7: Φόρμα εισαγωγής στοιχείων εισόδου

Στην συνέχεια, ο κώδικας που γράφτηκε έτσι ώστε να πραγματοποιεί την αυθεντικοποίηση του χρήστη:

```
@app.route("/login/", methods=["POST"])
def login_form():
    creds = {"username": "george", "password": "1234"}

    username = request.form.get("username")
    password = request.form.get("password")

    if username == creds["username"] and password == creds["password"]:

        flash("The credentials provided are valid", "success")
        return redirect(url_for("login"))
    else:

        flash("You have supplied invalid login credentials!", "danger")
        return redirect(url_for("login"))
```

Σε περίπτωση που ο χρήστης δώσει λανθασμένα στοιχεία εισόδου, εμφανίζεται το εξής:

Flask + 2FA Demo

You have supplied invalid login credentials!

Username

Password

Authenticate User

Εικόνα 8: Εισαγωγή λανθασμένων στοιχείων χρήστη και μήνυμα σφάλματος

Ενώ σε περίπτωση που ο χρήστης δώσει τα σωστά στοιχεία εισόδου, εμφανίζεται το μήνυμα της επιτυχούς αυθεντικοποίησης:

Flask + 2FA Demo

The credentials provided are valid

Username

Password

Authenticate User

Εικόνα 9: Εισαγωγή ορθών στοιχείων χρήστη και μήνυμα επιτυχούς αυθεντικοποίησης

4.6 Αυθεντικοποίηση 2 παραγόντων χρησιμοποιώντας TOTP

Συνεχίσαμε, με την προσθήκη του δεύτερου παράγοντα αυθεντικοποίησης. Για τον σκοπό αυτό χρησιμοποιήθηκε η βιβλιοθήκη PyOTP και πιο συγκεκριμένα η κλάση TOTP αυτής της βιβλιοθήκης:

```
import pyotp
totp = pyotp.TOTP("base32secret3232")
```

```
print(totp.now())
```

Η πιο βασική μέθοδος που χρησιμοποιείται στην συγκεκριμένη περίπτωση είναι η verify με τρόπο όπως φαίνεται παρακάτω:

```
import pyotp

# verifying TOTP codes with PyOTP
totp = pyotp.TOTP("base32secret3232")
print(totp.verify("492039"))
```

Επιπλέον, η βιβλιοθήκη PyTOP παρέχει την δυνατότητα δημιουργίας μυστικών κλειδιών (secret keys), έτσι ώστε να αρχικοποιούνται οι κλάσεις TOTP και HOTP, με τρόπο όπως φαίνεται παρακάτω:

```
import pyotp

print(pyyotp.random_base32())
```

Επιπλέον, οι χρήστες θα ανακατευθύνονται σε περίπτωση επιτυχούς αυθεντικοποίησης με το username και password) στην σελίδα login_2fa.html. Ο κώδικας που χρησιμοποιείται για την ανακατεύθυνση είναι ο εξής:

```
if username == creds["username"] and password == creds["password"]:
    return redirect(url_for("login_2fa"))
```

Επίσης, ο κώδικας που προστέθηκε στην εφαρμογή είναι ο εξής:

```
@app.route("/login/2fa/")
def login_2fa():
    secret = pyotp.random_base32()
    return render_template("login_2fa.html", secret=secret)
```

Και ο κώδικας του αρχείου login_2fa.html:

```
{% extends "bootstrap/base.html" %}

{% block content %}
<div class="container">
```

```

<div class="row justify-content-center">
  <div class="col-lg-12">
    <div class="jumbotron text-center p-4">
      <h2>Flask + 2FA Demo</h2>
      <h4>Setup and Authenticate 2FA</h4>
    </div>
  </div>
  <div class="col-lg-5">
    <form>
      <div>
        <h5>Instructions!</h5>
        <ul>
          <li>Download


```

```
{% endif %}
{% endwith %}
<form method="POST">
  <div class="form-group">
    <label for="otp">Generated OTP</label>
    <input type="hidden" name="secret" value="{{ secret }}" required>
    <input type="number" class="form-control" id="otp" name="otp" required>
  </div>
  <div class="text-center">
    <button type="submit" class="btn btn-primary">Authenticate User</button>
  </div>
</form>
</div>
</div>
</div>

<script>
function copySecret() {
  /* Get the text field */
  var copyText = document.getElementById("secret");

  /* Select the text field */
  copyText.select();
  copyText.setSelectionRange(0, 99999); /*For mobile devices*/

  /* Copy the text inside the text field */
  document.execCommand("copy");

  alert("Successfully copied TOTP secret token!");
}
</script>
{% endblock %}
```

Επομένως, η σελίδα η οποία δημιουργήθηκε είναι η εξής:

Flask + 2FA Demo

Setup and Authenticate 2FA

Instructions!

- Download [Google Authenticator](#) on your mobile.
- Create a new account with **setup key** method.
- Provide the required details (name, secret key).
- Select time-based authentication.
- Submit the generated key in the form.

Generated OTP

Authenticate User

Secret Token

NFW2PFCEBD5PB3ZZ

Copy Secret

Εικόνα 10: Οδηγίες εγκατάστασης και αυθεντικοποίησης Google Authenticator

Στην συγκεκριμένη σελίδα δίνονται σαφείς οδηγίες για την χρήση της εφαρμογής Google Authenticator:

- Ο χρήστης κατεβάζει την εφαρμογή
- Δημιουργεί έναν νέο λογαριασμό (χρήστη της μεθόδου setup key)
- Παρέχει τις κατάλληλες πληροφορίες (όνομα, secret key)
- Επιλέγει αυθεντικοποίηση time-based
- Παράγεται το token, το οποίο στην συνέχεια εισάγει στην σελίδα

Τέλος, προστέθηκε και ο παρακάτω κώδικας στον κώδικα της εφαρμογής για την υποστήριξη της απαιτούμενης λειτουργικότητας (έλεγχος του one time password):

```
@app.route("/login/2fa/", methods=["POST"])
def login_2fa_form():
    secret = request.form.get("secret")
    otp = int(request.form.get("otp"))

    if pyotp.TOTP(secret).verify(otp):
        flash("The TOTP 2FA token is valid", "success")
```

```
return redirect(url_for("login_2fa"))
else:
    flash("You have supplied an invalid 2FA token!", "danger")
    return redirect(url_for("login_2fa"))
```

Επομένως, ολοκληρώνοντας την παρουσίαση της εφαρμογής που υλοποιήθηκε, δείχνουμε περίπτωση στην οποία εισάγεται λανθασμένο token (το οποίο θα πρέπει να έχει παραχθεί από την εφαρμογή Google Authenticator):

Flask + 2FA Demo

Setup and Authenticate 2FA

Instructions!

- Download [Google Authenticator](#) on your mobile.
- Create a new account with **setup key** method.
- Provide the required details (name, secret key).
- Select time-based authentication.
- Submit the generated key in the form.

Secret Token

CWPF07VNYN6QZHR7

Copy Secret

You have supplied an invalid 2FA token!

Generated OTP

Authenticate User

Εικόνα 11: Περίπτωση εισαγωγής λανθασμένου token και μήνυμα σφάλματος

Και η περίπτωση στην οποία έχει εισαχθεί έγκυρο token:

Flask + 2FA Demo

Setup and Authenticate 2FA

Instructions!

- Download [Google Authenticator](#) on your mobile.
- Create a new account with **setup key** method.
- Provide the required details (name, secret key).
- Select time-based authentication.
- Submit the generated key in the form.

Secret Token

VOIUD076JZXUQMYQ

Copy Secret

The TOTP 2FA token is valid

Generated OTP

Authenticate User

Εικόνα 12: Περίπτωση εισαγωγής έγκυρου token και μήνυμα εγκυρότητας

Βιβλιογραφικές Αναφορές

Ξενόγλωσση Βιβλιογραφία

- [1]. Amnesty, I. (2016, Οκτωβρίου 21). *6 really practical ways to protect your privacy online*. Ανάκτηση από <https://www.amnesty.org/en/latest/campaigns/2016/10/really-practical-ways-to-protect-your-privacy-online/>.
- [2]. Cranor, L. F., & Buchler, N. (2014). Better together: Usability and security go hand in hand. *IEEE Security & Privacy*, 89-93.
- [3]. Downey, A. B. (2012). *Think Python: How to Think Like a Computer Scientist* (1.6.6 ed εκδ.).
- [4]. Fischer, T., Sadeghi, A.-R., & Winandy, M. (2009). *A pattern for secure graphical user interface systems*. doi:10.1109/DEXA.2009.76
- [5]. GitHub. (2019). *SpiderLabs/msfrpc*. Ανάκτηση από [msfrpc/python-msfrpc: https://github.com/SpiderLabs/msfrpc/tree/master/python-msfrpc](https://github.com/SpiderLabs/msfrpc/tree/master/python-msfrpc)
- [6]. GrayHat4Life. (2020, Νοεβρίου 3). *7 Types of Hackers You Should Know*. Ανάκτηση από [https://www.cybrary.it: https://www.cybrary.it/blog/0p3n/types-of-hackers/](https://www.cybrary.it/blog/0p3n/types-of-hackers/)
- [7]. Hoogenraad, W. (2019, Φεβρουαρίου 11). *Ο κωδικός One Time (OTP) για καλύτερη ασφάλεια*. Ανάκτηση από Πληροφορική Itpedia: <https://el.itpedia.nl/2019/02/11/uw-one-time-password-otp-voor-een-betere-security/>
- [8]. Kenneth, C. L., & Laudon, J. P. (2005). *Essentials of Management Information Systems: Managing the Digital Firm* (6th Edition εκδ.). Pearson Education Inc: Prentice Hall.
- [9]. Lambert, D., & Stock, J. (2001). *«Strategic Logistics Management* (4th Edition εκδ.). Boston: Mc Graw – Hill.
- [10]. Laudon, K. C., & Laudon, J. P. (2009). *Management Information Systems: Managing the Digital Firm* (11th Edition εκδ.). Upper Saddle River, United States: Pearson College Div.

- [11]. Laudon, K., & Laudon, J. (2004). *Management Information – System – Management the Digital Firms* (8th Edition εκδ.). Prentice Hall.
- [12]. Laudon, K., & Laudon, J. (2014). *Πληροφοριακά Συστήματα Διοίκησης*. Αθήνα: Κλειδάριθμος.
- [13]. Matthes, E. (2016). *Python Crash Course*.
- [14]. Mertz, D. (2015). *Picking a Python PDF version*. Sebastopol: CA:O'Reilly Media.
- [15]. Mieczakowski, L. P., & Clarkson, .. J. (2013). Investigating designers“ and users“ cognitive representations of products to assist inclusive interaction design. *Universal access in the information society*(12), 279-296. doi:10.1007/s10209-012-0278-8
- [16]. Mihajlov, M., Jerman-Blazic, B., & Josimovsk, S. (2011). *A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives*. doi:10.1109/ICNSS.2011.6060025
- [17]. Mouratidis, P., G., & Manson, G. (2005). When Security meets Software Engineering: A case of modelling secure information systems. *University of East London Institutional Repository*, 30(8), σσ. 609-629. doi:10.1016/j.is.2004.06.002
- [18]. Open, W. S. (2017). *Signal Privacy Policy*. Ανάκτηση από <https://signal.org/signal/privacy/>
- [19]. Perlroth, N., & Benner, K. (2016, Οκτωβρίου 4). *Subpoenas and Gag Orders Show Government Overreach*. Ανάκτηση από Tech Companies Argue: <https://www.nytimes.com/2016/10/05/technology/subpoenas-and-gag-orders-show-government-overreachttech-companies-argue.html>
- [20]. Reed, D., & Monk, A. (2011). Inclusive design: beyond capabilities towards context of use. *Universal Access in the Information Society*(10), 295-305. doi:10.1007/s10209-010-0206-8
- [21]. Rosenberger, C., & Schwartzmann, J. (2014). A Review on Authentication Methods - Syed Zulkarnain Syed Idrus^{1,2}, Estelle Cherrier². *Kangar, Malaysia*.

- [22]. Voshmgir, S. (2019). *Tokens, Cryptocurrencies & other Cryptoassets*. Ανάκτηση από Blockchain Hub Berlin: <https://blockchainhub.net/tokens/>
- [23]. Wallace, P. (2014). *Πληροφοριακά συστήματα διοίκησης: άνθρωποι, τεχνολογία, διαδικασίες*. Αθήνα: Κριτική.
- [24]. Yusuf, A. G. (2004). Enterprise information systems project implementation : A case study of ERP in Rolls-Royce. *International Journal of Production Economics*, 87(3), σσ. 251-266.

Ελληνόγλωσση Βιβλιογραφία

- [25]. Αμπλιανίτη, Ε. (2019). *Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗΝ ΑΠΟΔΟΣΗ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ, ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΓΡΟΤΙΚΩΝ ΠΡΟΪΟΝΤΩΝ ΚΑΙ ΤΡΟΦΙΜΩΝ*, Αργίνιο. Ανάκτηση από <https://nemertes.lis.upatras.gr/jspui/bitstream/10889/12784/1/%CE%94%CE%99%CE%A0%CE%9B%CE%A9%CE%9C%CE%91%CE%A4%CE%99%CE%9A%CE%97%20%CE%95%CE%A1%CE%93%CE%91%CE%A3%CE%99%CE%91%20%CE%91%CE%9C%CE%A0%CE%9B%CE%99%CE%91%CE%9D%CE%99%CE%A4%CE%97.pdf>
- [26]. Αναστασιάδης Σ, Π. (2001). *Τα Πληροφοριακά Συστήματα Διοίκησης στη Νέα Οικονομία – Η νέα Ψηφιακή Μεταμηχανογραφημένη Επιχείρηση*. Alfa Books Scientific Editions.
- [27]. Βαβαδάκης, Ε. (2020). *Επίδραση κοινωνικο-οικονομικών παραγόντων σε δείκτες αποδοχής του Bitcoin και κατ' επέκταση του Blockchain στις χώρες της Ευρωπαϊκής Ένωσης*. Διπλωματική Εργασία, Ε.Α.Π, Πάτρα. Ανάκτηση από https://193.108.160.200/bitstream/repo/47460/1/111514_VAVADAKIS_EIRINAIOS-ANTONIOS.pdf
- [28]. Γιαννακόπουλος, Δ., & Παπουτσής, Ι. (1995). *Πληροφοριακά Συστήματα Διοίκησης*. Αθήνα: Έλλην.
- [29]. Γκαζούνη, Α. (2016). *Ανάπτυξη, Συντήρηση και Βελτιστοποίηση Πληροφοριακού Συστήματος Καταγραφής Διαδικασιών*. ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ, ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ, Αθήνα. Ανάκτηση από

<http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/13174/1/D2016-0157.pdf>

- [30]. Γκρίτζαλης, Δ. (2004). Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση. Στο Δ. Γκρίτζαλης, *ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ* (σσ. 21-45). Αθήνα: Παπασωτηρίου. Ανάκτηση από https://newtech-pub.com/wp-content/uploads/2013/10/kef-asf.plhr_.sust_.pdf
- [31]. Δημητριάδης, Α. (2007). *Διοίκηση – Διαχείριση Πληροφοριακών Συστημάτων*. Αθήνα: Νέων Τεχνολογιών.
- [32]. Κακούρης, Α. (2018). *Συνεχής Αυθεντικοποίηση Χρήστη σε Διαδικτυακές Εφαρμογές βάσει Συμπεριφοράς*. Διπλωματική εργασία, Α.Π.Θ, Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών, ΘΕΣΣΑΛΟΝΙΚΗ.
- [33]. Καλκουτσή, Α., & Μαργέρα, Φ. (2018). *ΑΣΦΑΛΕΙΑ ΚΑΙ ΧΡΗΣΤΙΚΟΤΗΤΑ ΜΕΘΟΔΩΝ ΕΛΕΓΧΟΥ ΤΑΥΤΟΤΗΤΑΣ ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ: Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΑΣΦΑΛΟΥΣ ΓΡΗΓΟΡΗΣ ΑΞΙΟΠΙΣΤΗΣ ΣΥΝΔΕΣΗΣ (SQRL)*. Διπλωματική Εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ, ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, Σάμος. Ανάκτηση από <https://hellanicus.lib.aegean.gr/bitstream/handle/11610/21091/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%95%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1%20%20%CE%A4%CF%81%CE%BF%CF%80%CE%BF%CE%B9%20%CE%91%CF%85%CE%B8%CE%B5%CE%BD%CF%84>
- [34]. Πατραμάνης, Γ. (2019). *Εκμετάλλευση της αδυναμίας eternal blue με τη χρήση της Python και αρχείων*. Πρόγραμμα Μεταπτυχιακών Σπουδών, Πανεπιστήμιο Πειραιώς, Ψηφιακών Συστημάτων, Αθήνα. Ανάκτηση από <https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11927/%ce%94%ce%99%ce%a0%ce%9b%ce%a9%ce%9c%ce%91%ce%a4%ce%99%ce%9a%ce%97%20%ce%95%ce%a1%ce%93%ce%91%ce%a3%ce%99%ce%91%ce%a0%ce%91%ce%a4%ce%a1%ce%91%ce%9c%ce%91%ce%9d%ce%97%ce%a3%20%ce%93%ce%95%ce%a9>

- [35]. Στεφάνου, Κ., & Μπιάλας, Χ. (2017). *Σύγχρονα Επιχειρησιακά Συστήματα: Πληροφοριακά Συστήματα Διοίκησης και Συστήματα Επιχειρησιακών Πόρων (ERP)*. Θεσσαλονίκη: Αλτιντζή.
- [36]. Τερζίδου, Α., & Δασυγένης, Μ. (2016). *Python Programming*. Βιβλίο, Πανεπιστήμιος Μακεδονίας, Μηχανικών Πληροφορικής & Τηλεπικοινωνιών, Κοζάνη. Ανάκτηση από https://arch.ece.uowm.gr/docs/Python_Programming_Full_Book_Dasygenis_Terzidou.pdf
- [37]. Υψηλάντης, Π. (2001). *Πληροφοριακά Συστήματα Διοίκησης*. Αθήνα: Πατάκης.
- [38]. Φιτσιλής, Π. (2015). *Σύγχρονα Πληροφοριακά Συστήματα Επιχειρήσεων ERP-CRM-BPR*. (Δ. Καλλιάρης, Επιμ.) Ζωγράφου, Αττικής, Ελλάδα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Ανάκτηση από file:///C:/Users/user/Downloads/%CE%A3%CF%8D%CE%B3%CF%87%CF%81%CE%BF%CE%BD%CE%B1_%CE%A0%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CE%A3%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1_%CE%95%CF%80%CE%B9%CF%87%CE%B5%CE%B9%CF%81%CE%
- [39]. Φωλίνας, Δ. (2007). *«Ολοκληρωμένα Πληροφοριακά Συστήματα Διαχείρισης Επιχειρηματικών Πόρων*. Θεσσαλονίκη: Ανικούλα.
- [40]. Χατζηγεωργίου, Χ. (2017). *Αρχιτεκτονικές προστασίας ιδιωτικότητας για κινητό και φορητό υπολογισμό*. ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ, ΑΝΩΤΑΤΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ Τ.Τ., Ηλεκτρονικών Μηχανικών Τ.Ε., Αθήνα. Ανάκτηση από http://oceanis.lib2.uniwa.gr/xmlui/bitstream/handle/123456789/3974/MSC_IES_CHATZIGEORGIOU_CHRISTOS_0007_MSC_THESIS_final.pdf?sequence=1&isAllowed=y