Ελληνική Δημοκρατία
Υπουργείο Διοικητικής Ανασυγκρότησης

εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΥΠΟΕΡΓΟ 3 «ΔΡΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΠΟΙΟΤΗΤΑΣ ΕΠΙΜΟΡΦΩΤΙΚΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ»

Της Πράξης «ΔΡΑΣΕΙΣ ΣΥΝΕΧΙΖΟΜΕΝΗΣ ΚΑΤΑΡΤΙΣΗΣ 2014-2018»
Κωδ. ΟΠΣ 5000245

ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ:
«ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΒΑΣΙΚΗ ΕΚΠΑΙΔΕΥΣΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΥΡΓΕΙΟΥ ΟΙΚΟΝΟΜΙΚΩΝ»

ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΛΙΚΟ

Κωδικός εκπαιδευτικού υλικού:

Κωδικός Πιστοποίησης Προγράμματος: 606

Ευρωπαϊκή Ένωση
Ευρωπαϊκά Διαρθρωτικά και Επενδυτικά Ταμεία
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΥΠΟΕΡΓΟ 3 «ΔΡΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΠΟΙΟΤΗΤΑΣ ΕΠΙΜΟΡΦΩΤΙΚΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ»

ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ:
«ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΒΑΣΙΚΗ ΕΚΠΑΙΔΕΥΣΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΥΡΓΕΙΟΥ ΟΙΚΟΝΟΜΙΚΩΝ»

ΜΕΛΗ ΟΜΑΔΑΣ

Συντονιστής: **ΓΕΩΡΓΙΟΣ ΚΑΤΣΙΚΑΤΣΟΣ** (κωδ. ΟΠΣ 021274), Υπεύθυνος Σπουδών και Έρευνας Ε.Κ.Δ.Δ.Α.

Συντάκτες:
ΑΝΔΡΕΑΣ ΠΙΠΗΣ (κωδ. ΟΠΣ 018509), Προϊστάμενος Γενικής Διεύθυνσης Ανάπτυξης και Παραγωγικής Λειτουργίας Πληροφοριακών Συστημάτων, Γενική Γραμματεία Πληροφοριακών Συστημάτων, Υπουργείο Οικονομικών
ΓΕΩΡΓΙΟΣ ΚΩΤΣΑΚΗΣ (κωδ. ΟΠΣ 016180), Προϊστάμενος Αυτοτελούς Τμήματος Ασφάλειας, Γενική Γραμματεία Πληροφοριακών Συστημάτων, Υπουργείο Οικονομικών
ΒΑΣΙΛΙΚΗ ΤΖΟΒΛΑ (κωδ. ΟΠΣ 007693), Προϊσταμένη Τμήματος Β'- Διαχείρισης Διαδικτυακών Υπηρεσιών, Εφαρμογών και Βάσεων Δεδομένων της Διεύθυνσης Διαχείρισης Υπολογιστικών Υποδομών, Γενικής Γραμματείας Πληροφοριακών Συστημάτων, Υπουργείο Οικονομικών
ΜΑΡΙΑΝΘΗ ΨΩΜΑ (κωδ. ΟΠΣ 019907), Προϊσταμένη Τμήματος Γ΄- Διαχείρισης Περιφερειακού Τερματικού Εξοπλισμού & Λογισμικού, Διεύθυνση Διαχείρισης Υπολογιστικών Υποδομών και Κυβερνητικού Νέφους, Γενική Γραμματεία Πληροφοριακών Συστημάτων, Υπουργείο Οικονομικών

Αξιολογητές:

ΓΕΩΡΓΙΟΣ ΠΑΠΑΜΙΧΑΗΛ (κωδ. ΟΠΣ 001770), Προϊστάμενος Τμήματος ΣΥΝΤΟΝΙΣΜΟΥ ΙΝ.ΕΠ./ Ε.Κ.Δ.Δ.Α.

ΙΩΑΝΝΗΣ ΜΑΤΖΑΒΑΚΗΣ (κωδ. ΟΠΣ 018261), Υπεύθυνος Σπουδών και Έρευνας Ε.Κ.Δ.Δ.Α.

Ευρωπαϊκή Ένωση
Ευρωπαϊκά Διαρθρωτικά και Επενδυτικά Ταμεία
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Περιεχόμενα

1 Εισαγωγή στην Ασφάλεια 1
1.1 Τι είναι η Ασφάλεια Πληροφοριών; 1
1.2 Σε ποιους απευθύνεται το σεμινάριο 2
1.3 Τι θα έχετε μάθει στο τέλος του σεμιναρίου 2
1.4 Ιστορική αναδρομή – που είμαστε τώρα; 2
1.4.1 Γιατί η ΓΓΠΣ μπορεί και φιλοξενεί άλλους φορείς; 4
1.5 Η αναγκαιότητα της ασφάλειας 5
1.5.1 Τι μας οδήγησε εδώ; 5
1.5.2 Αλήθεια, τι συμβαίνει όταν δεν έχουμε ασφάλεια; 5
1.6 Η εκπαίδευση ασφάλειας 6
1.6.1 Η αναγκαιότητα της εκπαίδευσης ασφάλειας 6
1.6.2 Γιατί η εκπαίδευση πρέπει να επαναλαμβάνεται; 6
1.7 Παραπομπές 7
2 Το Εφαρμοστέο Νομικό Πλαίσιο 9
2.1 Προστασία Υπηρεσιακών Δεδομένων 9
2.2 Προστασία Φορολογικών Δεδομένων 9
2.2.1 Η ΠΟΛ 1154/2018 9
2.3 Προστασία Δεδομένων Προσωπικού Χαρακτήρα 10
2.3.1 Τι είναι προσωπικά δεδομένα; 10
2.3.2 Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Ε.Ε.) 2016/679 11
2.3.3 Ο ρόλος μας ως προς τον ΓΚΠΔ 11
2.4 Προστασία Δεδομένων που προέρχονται από ΑΕΟΙ 12
2.5 Εσωτερικό Πλαίσιο Ασφάλειας 12
2.6 Παραπομπές 13
3 Βασικοί Ορισμοί Ασφάλειας 15
3.1 Η βασική τριάδα της ασφάλειας 15
3.2 Διαχείριση Πρόσβασης – Λογοδοσία 15
3.3 Επίσημοι ορισμοί από το Πλαίσιο Ασφάλειας 16
3.4 Παραπομπές 18
4 Επιτελικοί Στόχοι Ασφάλειας 19
4.1 Επιτελικοί ρόλοι και αρμοδιότητες 19
4.2 Στρατηγική Ασφάλειας 20
4.3 Το Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων 20
4.3.1 Καλυπτόμενες απαιτήσεις ασφάλειας 20

4.3.2 Εφαρμοζόμενο νομικό πλαίσιο 21
4.3.3 Διεθνείς Βέλτιστες Πρακτικές 21
4.3.4 Διεθνείς Συμφωνίες 21
4.3.5 Οι πολιτικές ασφαλείας που συνθέτουν το ΠΑΠΣ-ΥΠΟΙΚ 22
5 Κανόνες Ασφάλειας 25
5.1 Η πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών (ΠΟΧΣΠ) 25
5.2 Γενικές απαιτήσεις 25
5.3 Χρήση κωδικών πρόσβασης 26
5.4 Εμπιστευτικότητα υπηρεσιακής πληροφορίας 27
5.4.1 Κανόνες Ασφάλειας των υπηρεσιακών δεδομένων 27
5.5 Χρήση Διαδικτύου / Ηλεκτρονικού Ταχυδρομείου 28
5.6 Αναφορά περιστατικών 29
5.7 Συμμόρφωση 29
5.8 Οδηγίες Ασφάλειας 29
6 Απειλές 31
6.1 Είδη Απειλών 31
6.2 Το Ανθρώπινο Πληροφοριακό Αγαθό 32
6.3 Ανάλυση Εξωτερικών Απειλών 34
6.3.1 Ψάρεμα 34
6.3.2 Κακόβουλο Λογισμικό 36
6.3.3 Η εξέλιξη του κακόβουλου λογισμικού 38
6.3.4 Κακόβουλο λογισμικό τύπου Ransomware (λυτρισμικό) 38
6.4 Ενδείξεις ώστε να καταλάβουμε ότι «κάτι έχουμε κολλήσει» 39
6.5 Τι κάνουμε αν πέσουμε θύματα κακόβολου λογισμικού; 40
6.6 Μέτρα προστασίας 40
7 Κωδικοί Πρόσβασης 43
7.1 Γενικά 43
7.2 Ορισμός Ταυτότητας 43
7.2.1 Όνομα χρήστη και κωδικός πρόσβασης 44
7.2.2 Πιστοποιητικά 44
7.2.3 Βιομετρία 44
7.2.4 Έλεγχος ταυτότητας πολλαπλών παραγόντων (Multi-Factor Authentication) 45
7.3 Γιατί χρειάζεται η Ηλεκτρονική Ταυτότητα 45
7.4 Η σημασία των μυστικών κωδικών 45
7.5 Ισχυροί Κωδικοί 46
7.6 Χρήση Μυστικών Κωδικών 48
7.7 Παραπομπές 49
8 Εμπιστευτικότητα Υπηρεσιακών Πληροφοριών 51

8.1 Η έννοια της ασφάλειας πληροφοριακών συστημάτων 51
8.2 Στρατηγική Ασφάλειας – Δέσμευση Εμπιστευτικότητας του Υπουργείου 52
8.3 Εμπιστευτικότητα 52
8.4 Διαβάθμιση Πληροφορίας 52
8.5 Κανόνες για την Προστασία της Εμπιστευτικότητας 53
8.6 Εξουσιοδοτημένη/ Μη Εξουσιοδοτημένη Πρόσβαση 54
8.7 Οδηγίες για Προστασία Πληροφορίας Περιορισμένης Χρήσης 55
9 Καθαρή Επιφάνεια Εργασίας (Clean Desk Policy) 57
9.1 Γενικά 57
9.2 Κανόνες 57
9.3 Kensington Lock 58
9.4 Κλείδωμα Επιφάνειας Εργασίας 59
9.5 Έλεγχος από το Αυτοτελές Τμήμα Ασφαλείας 59
10 Προστασία Ηλεκτρονικής Πληροφορίας με Κρυπτογράφηση 61
10.1 Κρυπτογράφηση – Αποκρυπτογράφηση 61
10.2 Κρυπτογραφία (Cryptography) - Κρυπτανάλυση (Cryptanalysis) – Κρυπτολογία (Cryptology) 62
10.3 Η Κρυπτογράφηση δεν αποτελεί πρόσφατη επινόηση 63
10.3.1 Σπαρτιάτες στρατηγοί 63
10.3.2 Enigma Κρυπτομηχανή 63
10.4 Είδη Κρυπτογράφησης 64
10.4.1 Συμμετρική Κρυπτογράφηση (Symmetric Cryptography) 64
10.4.2 Μη Συμμετρική (Asymmetric Cryptography) Κρυπτογράφηση ή Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Cryptography) 72
10.4.3 Διαφορές Συμμετρικής και Μη Συμμετρικής Κρυπτογράφησης 73
10.4.4 Pretty Good Privacy (PGP) 74
10.5 Εφαρμογές Κρυπτογράφησης 75
10.6 Ενδεδειγμένες Χρήσεις Κρυπτογράφησης στο Υπουργείο Οικονομικών 76
10.6.1 Ανταλλαγή πληροφοριών (αρχείων) με άλλες υπηρεσίες 76
10.6.2 Τακτική ασφαλής ανταλλαγή αρχείων με τρίτους φορείς 76
10.6.3 Ασφαλής εφεδρική αποθήκευση ευαίσθητης πληροφορίας σε φορητό μέσο αποθήκευσης 77
10.7 Ψηφιακή Υπογραφή 77
10.7.1 Ηλεκτρονική Διακίνηση Εγγράφων και Ψηφιακή Υπογραφή 77
10.7.2 Ορισμός Ψηφιακής Υπογραφής 78
10.7.3 Ψηφιακό Πιστοποιητικό 78
10.7.4 Δημιουργία Ψηφιακής Υπογραφής 79
10.8 Ψηφιακή Υπογραφή - Κρυπτογράφηση 80

10.9 Υπάρχουν Ασφαλή Συστήματα; 81
10.10 Παραπομπές 81
11 Ασφάλεια Συστημάτων και Πληροφοριών 83
11.1 Γενικά 83
11.2 Ασφαλής Χρήση Διαδικτύου 83
11.3 Ασφαλής Χρήση Ηλεκτρονικού Ταχυδρομείου 84
11.4 Ασφαλής Χρήση Φορητών Αποθηκευτικών Μέσων 84
11.4.1 Πολιτική Ορθής Χρήσης Πληροφοριακών Συστημάτων και Τρόποι Προστασίας των Φορητών Αποθηκευτικών Μέσων 85
11.4.2 Κίνδυνοι από χρήση φορητών μέσων αποθήκευσης 86
11.4.3 Πρακτικές Οδηγίες Ασφάλειας Φορητών Μέσων 86
11.4.4 Προστασία πληροφοριών σε φορητά μέσα με χρήση κρυπτογράφησης 88
11.5 Παραπομπές 89
12 Συμβάντα – Περιστατικά Ασφαλείας 91
12.1 Πολιτική και Διαδικασία Διαχείρισης Περιστατικών Ασφαλείας 92
12.2 Αξιολόγηση της Αποτελεσματικότητας Διαχείρισης Περιστατικών 94
12.3 Νομικά Θέματα και Πειθαρχικές Διαδικασίες 94

ΧΡΗΣΙΜΕΣ ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΠΑ	Πληροφορικό Αγαθό
ΙΠΑ	Ιδιοκτήτης Πληροφορικού Αγαθού
ΓΓΠΣΔΥ	Γενική Γραμματεία Πληροφοριακών Συστημάτων & Διοικητικής Υποστήριξης
ΓΓ-ΓΓΠΣΔΥ	Γενικός Γραμματέας ΓΓΠΣΔΥ
ΑΤΑ	Αυτοτελές Τμήμα Ασφαλείας του Υπουργείου Οικονομικών
ΜΕΕ	Μονάδα Εσωτερικού Ελέγχου του Υπουργείου Οικονομικών
ΟΜΑ-Φ	Οργανική Μονάδα Ασφάλειας Οργανισμού «Φ» στον οποίο παρέχονται υπηρεσίες φιλοξενίας Πληροφοριακού Συστήματος από τις Κεντρικές Υπολογιστικές Υποδομές του Υπουργείου
ΟΜΕΣΕΛ-Φ	Οργανική Μονάδα Εσωτερικών Ελέγχων Οργανισμού «Φ» στον οποίο παρέχονται υπηρεσίες φιλοξενίας Πληροφοριακού Συστήματος από τις Κεντρικές Υπολογιστικές Υποδομές του Υπουργείου
ΟΜΕΣΥΠ-Φ	Οργανική Μονάδα Εσωτερικών Υποθέσεων Οργανισμού «Φ» στον οποίο παρέχονται υπηρεσίες φιλοξενίας Πληροφοριακού Συστήματος από τις Κεντρικές Υπολογιστικές Υποδομές του Υπουργείου
ΟΜΣΑΕ	Οργανική Μονάδα Σχεδίασης και Ανάπτυξης Εφαρμογών ενός Οργανισμού
ΠΣ	Πληροφοριακό Σύστημα
ΠΑΠΣ-ΥΠΟΙΚ	Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών
ΣΔΑΠ-ΥΠΟΙΚ	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών του Υπουργείου Οικονομικών

1 Εισαγωγή στην Ασφάλεια

1.1 Τι είναι η Ασφάλεια Πληροφοριών;

Για να καταλάβουμε ποιο ακριβώς είναι το πρόβλημα με το οποίο ασχολείται η ασφάλεια πληροφοριών, θα ήταν χρήσιμο να έχουμε στο μυαλό μας ως ένα «φυσικό ανάλογο», την ασφάλεια άλλων πιο καθημερινών αγαθών, όπως είναι τα χρήματα και διάφορα άλλα περιουσιακά στοιχεία. Διαφορετικά αν το δούμε ως κάτι καινούργιο και ξεκομμένο από τον υπόλοιπο πραγματικό κόσμο μας, θα μας δημιουργήσει μεγάλη δυσκολία στην κατανόηση.

Από τον τίτλο «Ασφάλεια Πληροφοριών» και μόνο αντιλαμβανόμαστε ότι μας απασχολεί η προστασία των πληροφοριών, δηλαδή η προστασία αυτών των «αγαθών». Ωστόσο, το πρόβλημα της ασφάλειας των πληροφοριών είναι σύνθετο, αφού οι πληροφορίες είναι πλέον αντικείμενο επεξεργασίας σύνθετων τεχνολογικών και διοικητικών μηχανισμών, ειδικά με την εξάπλωση των διαδικτυακών εφαρμογών και την παροχή όλο και περισσότερων ηλεκτρονικών υπηρεσιών.

Κατά συνέπεια, μιλάμε για Ασφάλεια Πληροφοριακών Συστημάτων, διότι στην προσπάθειά μας να προστατέψουμε τις πληροφορίες, αναγκαζόμαστε να ασχοληθούμε ουσιαστικά με την ασφάλεια ολόκληρων συστημάτων, στα οποία συμμετέχουν **άνθρωποι**, **διαδικασίες**, **οργανισμοί, τεχνολογίες, δίκτυα** κλπ. Επομένως, μπορούμε να πούμε ότι στην περίπτωσή μας οι όροι Ασφάλεια Πληροφοριών και Ασφάλεια Πληροφοριακών Συστημάτων είναι ταυτόσημοι.

Μια πιο πρακτική θεώρηση της ασφάλειας πληροφοριών, με πολλές αναλογίες με την καθημερινότητά μας, είναι να τη δούμε ως μια διαδικασία που αποτελείται από τρία διακριτά βήματα:

Εικόνα 1-1: Τα τρία (3) στάδια της Ασφάλειας Πληροφοριών.

Με βάση το μοντέλο αυτό, δεν αρκεί μόνο να λάβουμε προληπτικά μέτρα, αλλά και να είμαστε σε θέση να ανιχνεύουμε πιθανές καταστάσεις, στις οποίες απειλείται η ασφάλεια των πληροφοριών, και κατ' επέκταση να αντιδρούμε το δυνατόν αμεσότερα ώστε να μειώσουμε τις επιπτώσεις και να ελαχιστοποιήσουμε την πιθανότητα επανεμφάνισης των καταστάσεων αυτών.

Η επίτευξη των στόχων ενός οργανισμού εξαρτάται σε μεγάλο βαθμό από τη δυνατότητά του να προστατεύσει τις υποδομές που είναι απαραίτητες για την αποτελεσματική λειτουργία του. Στους σύγχρονους οργανισμούς, οι Τεχνολογίες Πληροφορικής και Επικοινωνιών (Information and Communication Technologies) αξιοποιούνται, για τις περισσότερες από τις ενδοεπιχειρησιακές λειτουργίες και κυρίως για εκείνες που αφορούν τη λήψη αποφάσεων και το συντονισμό των μονάδων τους. Με βάση αυτή τη διαπίστωση προκύπτει ότι το Πληροφοριακό Σύστημα ενός οργανισμού αποτελεί κρίσιμο στοιχείο της υποδομής του και η αποτελεσματική λειτουργία του συνδέεται άρρηκτα με την αποτελεσματική λειτουργία του ίδιου του οργανισμού.

Η ασφάλεια ενός πληροφοριακού συστήματος χαρακτηρίζεται από το πλήθος και την ποικιλομορφία των παραγόντων που πρέπει να ληφθούν υπόψη. Οι παράγοντες αυτοί είναι

τόσο τεχνικοί όσο και διοικητικοί-οργανωτικοί. Για το λόγο αυτό, κάθε προσπάθεια προστασίας ενός Π.Σ. θα πρέπει να λαμβάνει υπόψη τις εξής γενικές διαπιστώσεις:

- Η ασφάλεια των Π.Σ. εξαρτάται από πολλούς παράγοντες και δεν είναι ούτε αποκλειστικά ούτε πρωτίστως τεχνικό ζήτημα.
- Η επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος.
- Για κάθε επίπεδο ασφάλειας υπάρχει ένα αντίστοιχο κόστος που θα πρέπει να καταβληθεί για την επίτευξή του.
- Στο πλαίσιο της γενικής αρχής της αναλογικότητας, τα μέτρα προστασίας που θα ληφθούν θα πρέπει να αντιστοιχούν στο επίπεδο και τη φύση των πραγματικών κινδύνων που αντιμετωπίζει το Π.Σ.

1.2 Σε ποιους απευθύνεται το σεμινάριο

Το σεμινάριο απευθύνεται σε όλους τους υπαλλήλους του Υπουργείου Οικονομικών και εν γένει οποιουδήποτε Οργανισμού υιοθετεί και εφαρμόζει το Πλαίσιο Ασφάλειας του Υπουργείου Οικονομικών, όπως για παράδειγμα:

- Η Ανεξάρτητη Αρχή Δημοσίων Εσόδων (ΑΑΔΕ)
- Η Ειδική Γραμματεία Διαχείρισης Ιδιωτικού Χρέους (ΕΓΔΙΧ)

1.3 Τι θα έχετε μάθει στο τέλος του σεμιναρίου

Το συγκεκριμένο σεμινάριο αποσκοπεί:

Στην ευαισθητοποίηση των εκπαιδευομένων ως προς την ασφάλεια πληροφοριών και συγκεκριμένα:

- Στην αναγκαιότητα της ασφάλειας.
- Στο πραγματικό μέγεθος των επιπτώσεων που έχει για τον οργανισμό αλλά και για τον υπάλληλο η ύπαρξη καταστάσεων μη-ασφάλειας.
- Στην παρουσίαση πραγματικών περιστατικών ασφαλείας και στα όσα μάθαμε από αυτά.
- Στην ανάδειξη της σημασίας της ενδεδειγμένης συμπεριφοράς όλων των υπαλλήλων.

Στην εκπαίδευσή των εκπαιδευομένων σε βασικά θέματα ασφάλειας πληροφοριών και συγκεκριμένα:

- Στους βασικούς ορισμούς και ορολογία που χρησιμοποιούνται στην ασφάλεια.
- Στο ισχύον θεσμικό πλαίσιο που αφορά στην ασφάλεια.
- Στις θέσεις και τις ενέργειες της Διοίκησης του Υπουργείου ως προς την ασφάλεια.
- Στους ισχύοντες κανόνες ασφάλειας που πρέπει να εφαρμόζονται καθώς και στον ενδεδειγμένο τρόπο εφαρμογής τους.
- Στα είδη των πιο συχνών απειλών, στο πως αντιμετωπίζονται στην πράξη και στην εκπαίδευση για την αντιμετώπισή τους.
- Στη χρήση ενδεδειγμένων εργαλείων κρυπτογράφησης.

1.4 Ιστορική αναδρομή – που είμαστε τώρα;

Αναφορικά με την εξέλιξη της ασφάλειας πληροφοριών στο Υπουργείο Οικονομικών υπάρχουν τα ακόλουθα καθοριστικά χρονικά σημεία:

- 1997: Πρόβλεψη για θέσεις Ειδικού Επιστημονικού Προσωπικού στην ασφάλεια πληροφοριακών συστημάτων. Προσλαμβάνονται 2 υπάλληλοι μέσω ΑΣΕΠ για την κάλυψη της ως άνω ανάγκης το 2004.
- 1999-2010: Διεξάγονται Μελέτες ασφάλειας που έχουν σαν σκοπό την ανάδειξη κενών ασφαλείας στις κεντρικές υπολογιστικές υποδομές της ΓΓΠΣ. Οι μελέτες αυτές χωρίζονται σε δυο κατηγορίες:
    - Συνολικές μελέτες που καλύπτουν όλα τα συστήματα, οι οποίες σε πολλές περιπτώσεις περιλαμβάνουν και τεχνικές δοκιμές ασφάλειας. Οι μελέτες κατέδειξαν με τον πιο κατηγορηματικό τρόπο την ανάγκη για: (α) απαιτούμενες οργανωτικές αλλαγές, (β) αναβάθμιση τόσο του προσωπικού όσο και των πληροφοριακών συστημάτων.
    - Μελέτες ασφάλειας στο πλαίσιο έργων ανάπτυξης νέων πληροφοριακών συστημάτων, όπως: Taxisnet, Icisnet. Κοινό αποτέλεσμα των μελετών αυτών ήταν η ανάγκη ύπαρξης οργανωτικών μονάδων για τη διαχείριση της ασφάλειας καθώς και διενέργειας εσωτερικών ελέγχων συμμόρφωσης.
- 2011: Ιδρύεται το «Αυτοτελές Γραφείο Ασφάλειας της ΓΓΠΣ» (ΑΓΑ)
- 2011-2012: Τίθεται σε ισχύ
    - (α) η «Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων της ΓΓΠΣ» και
    - (β) η «Πολιτική Δεοντολογίας - Ορθής Χρήσης Πληροφοριακών Συστημάτων της ΓΓΠΣ»
- 2011-2014: Τίθενται σε ισχύ και εφαρμόζονται επιτυχώς μια σειρά από βασικές απαραίτητες διαδικασίες/οδηγίες ασφάλειας, όπως:
    - Διαδικασία πρόσβασης στην Κεντρική Βάση Δεδομένων,
    - Οδηγίες Ασφαλούς Αποστολής Δεδομένων,
    - Διαδικασία Αυτοματοποιημένης Παρακολούθησης συναλλαγών κρίσιμων πινάκων στην κεντρική βάση δεδομένων,
    - Διαδικασία έγκρισης αλλαγών στα πληροφοριακά συστήματα
    - Συμμετοχή του ΑΓΑ σε όλες τις κρίσιμες διεργασίες του Υπουργείου σχετικά με την ανάπτυξη / συντήρηση πληροφοριακών συστημάτων με σκοπό να τεθούν οι απαραίτητες απαιτήσεις ασφάλειας έγκαιρα.
- 2013: Αντιμετωπίζεται ένα σοβαρό περιστατικό ασφαλείας μαζικής διαρροής φορολογικών δεδομένων και στη συνέχεια διεξάγεται διοικητικός έλεγχος από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Το πόρισμα του ελέγχου επιβάλλει μια σειρά από οργανωτικές αλλαγές, καθώς και υιοθέτηση βέλτιστων πρακτικών ασφάλειας και τεχνικών μέτρων. Αξιοσημείωτο είναι ότι επιβάλλεται διοικητικό πρόστιμο ύψους 150,000 ευρώ, για το οποίο ασκήθηκε έφεση από τη ΓΓΠΣ.
- 2013-2014: Η ΓΓΠΣ προσλαμβάνει ειδικό σύμβουλο ασφάλειας με σκοπό να καθοριστούν οι κατάλληλες άμεσες / μεσοπρόθεσμες / μακροπρόθεσμες δράσεις. Οι δράσεις περιλαμβάνουν: οργανωτικά, τεχνικά και διοικητικά μέτρα καθώς και έργα προμήθειας υπηρεσιών και υποδομών ασφάλειας.
- 2014: Σημαντικές αλλαγές στο οργανόγραμμα του Υπουργείου:

- Η «Μονάδα Εσωτερικού Ελέγχου» αποκτά αρμοδιότητα ελέγχου πληροφοριακών συστημάτων ως προς τη συμμόρφωση σύμφωνα με τις κείμενες διατάξεις, συμπεριλαμβανομένων και εκείνων της ασφάλειας.
- Παράλληλα η οργανική μονάδα «Εσωτερικών Υποθέσεων» ελέγχει και τη συμμόρφωση των υπαλλήλων ως προς τις κείμενες διατάξεις ασφάλειας.
- Ιδρύεται για πρώτη φορά «Αυτοτελές Τμήμα Ασφάλειας» με αρμοδιότητες για όλο το Υπουργείο Οικονομικών

- 2014-2015: Στο πλαίσιο πολιτικής συμφωνίας ανταλλαγής φορολογικών δεδομένων με τις ΗΠΑ (νόμος «FATCA» των ΗΠΑ), προκύπτει η απαίτηση άμεσης αναβάθμισης της ασφάλειας πληροφοριών του Υπουργείου, προϊόν της οποίας είναι η δημιουργία μιας ξεχωριστής ασφαλούς υπολογιστικής υποδομής, η οποία θα μπορεί να φιλοξενεί πληροφοριακά συστήματα αντίστοιχων απαιτήσεων ασφάλειας.
- 2015: Τίθεται σε ισχύ νέο «Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων ΑΕΟΙ» για πληροφοριακά συστήματα υψηλών προδιαγραφών ασφάλειας.
- 2015: Διαμορφώνεται «Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών» με σκοπό να ενισχυθεί η ασφάλεια και στα συστήματα εκτός ΑΕΟΙ.
- 2017: Στο πλαίσιο αναδιοργάνωσης του Υπουργείου Οικονομικών σε ένα πελατοκεντρικό Οργανισμό, ο οποίος πέραν της ΑΑΔΕ θα φιλοξενεί και άλλους οργανισμούς:
  - Δημιουργείται ένα πρότυπο Συμφωνίας Επιπέδου Εξυπηρέτησης με την ΑΑΔΕ, καθώς και με οποιονδήποτε φιλοξενούμενο φορέα, το οποίο περιλαμβάνει ειδικό κεφάλαιο διαχείρισης ασφάλειας.
  - Αναθεωρείται το «Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών» έτσι ώστε να εφαρμόζεται και από τους φιλοξενούμενους φορείς

1.4.1 Γιατί η ΓΓΠΣ μπορεί και φιλοξενεί άλλους φορείς;

Η στροφή της ΓΓΠΣ προς ένα πελατοκεντρικό φορέα, με αφορμή την ανεξαρτητοποίηση της ΑΑΔΕ ενισχύεται από τους εξής σημαντικούς παράγοντες:

- Διαθέτει κτίριο:

- υψηλών προδιαγραφών φυσικής ασφάλειας,
- με τεράστιες ηλεκτρομηχανολογικές εγκαταστάσεις,
- με εγκατεστημένες σύγχρονες δικτυακές υποδομές υψηλών ταχυτήτων,
- με σύγχρονες υπολογιστικές υποδομές νέφους, μεγάλης χωρητικότητας και με ικανότητα εξυπηρέτησης πολύ υψηλού επιπέδου όγκου συναλλαγών.

- Διαθέτει έμπειρο και εξειδικευμένο προσωπικό στις Τεχνολογίες Πληροφορικής
- Διαθέτει σημαντική εμπειρία στη σχεδίαση και λειτουργία υπολογιστικών υποδομών

1.5 Η αναγκαιότητα της ασφάλειας

1.5.1 Τι μας οδήγησε εδώ;

Διαβάζοντας κανείς το ιστορικό της ασφάλειας στο Υπουργείο Οικονομικών, καταλαβαίνει ότι οι λόγοι που μας οδήγησαν στην ενίσχυση της ασφάλειας ήταν πολλοί και αφορούσαν στην:

- Αντιμετώπιση μεταβαλλόμενων και αυξανόμενων απειλών.
- Εξυπηρέτηση σημαντικών απαιτήσεων που τίθενται από το σχετικό θεσμικό πλαίσιο και αφορούν σε:
  - υπηρεσιακά δεδομένα
  - προσωπικά δεδομένα
  - φορολογικά δεδομένα
  - δεδομένα από ανταλλαγή με άλλα κράτη (AEOI).
- Εξυπηρέτηση σημαντικών απαιτήσεων που προκύπτουν από Συμφωνίες Επιπέδου Εξυπηρέτησης (SLA) με φιλοξενούμενους φορείς και από Διακρατικές Συμφωνίες (AEOI).
- Εφαρμογή διεθνών βέλτιστων πρακτικών και προτύπων ασφάλειας Πληροφοριακών Συστημάτων, τα οποία στις μέρες μας έχουν εξελιχθεί σημαντικά και εφαρμόζονται ευρέως, προσδίδοντας κύρος στις προσφερόμενες υπηρεσίες.
- Ανάγκη για δημιουργία κλίματος εμπιστοσύνης στις κρατικές δομές από τους πολίτες και τους φιλοξενούμενους φορείς.

1.5.2 Αλήθεια, τι συμβαίνει όταν δεν έχουμε ασφάλεια;

Η απουσία συστηματικής προσέγγισης της ασφάλειας έχει αποδεδειγμένα καταστρεπτικά αποτελέσματα για τον Οργανισμό, όπως:

- Σοβαρά περιστατικά ασφαλείας (π.χ. διαρροή εμπιστευτικών δεδομένων, απώλεια ή αλλοίωση κρίσιμων δεδομένων, διακοπή κρίσιμων λειτουργειών του οργανισμού λόγω μη διαθεσιμότητας, κτλ.)
- Παραβίαση θεσμικού πλαισίου με σοβαρά επακόλουθα: διοικητικές κυρώσεις λόγω παραβίασης θεσμικού πλαισίου, προσφυγές/μηνύσεις, επιπτώσεις στη φήμη του οργανισμού.
- Παραβίαση Συμφωνιών με άλλους φορείς και Κράτη με σοβαρές επιπτώσεις: διακοπή συμφωνιών, ποινικές ρήτρες, υποβάθμιση του οργανισμού.
- Μειωμένη αποδοτικότητα / αποτελεσματικότητα λόγω μη χρήσης σύγχρονων βέλτιστων πρακτικών.

- Απώλεια εμπιστοσύνης απέναντι σε πολίτες και συνεργαζόμενους φορείς.

1.6 Η εκπαίδευση ασφάλειας

1.6.1 Η αναγκαιότητα της εκπαίδευσης ασφάλειας

Η ευαισθητοποίηση και εκπαίδευση ασφάλειας αποτελεί ένα από τα πιο αποδοτικά και αναγκαία μέτρα, προκειμένου να βελτιωθεί γρήγορα και σημαντικά το επίπεδο ασφάλειας κάθε οργανισμού. Σύμφωνα με διεθνή πρότυπα ασφάλειας, όπως το ISO 27001, η εκπαίδευση ασφάλειας του προσωπικού θα πρέπει να διαφοροποιείται ανάλογα με τα καθήκοντα και τις αρμοδιότητες του.

Το παρόν πρόγραμμα καλύπτει το πρώτο επίπεδο εκπαίδευσης που αφορά όλο το προσωπικό, ανεξάρτητα από αρμοδιότητες και βαθμίδες, στοχεύοντας στην επίτευξη ενός ενιαίου οριζόντιου επιπέδου ευαισθητοποίησης και βασικής εκπαίδευση ασφάλειας.

Στο πρόγραμμα «ΕΚΠΑΙΔΕΥΣΗ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ ΠΛΑΙΣΙΟΥ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΟΙΚΟΝΟΜΙΚΩΝ», το οποίο αποτελεί το επόμενο επίπεδο εκπαίδευσης, πραγματοποιείται μια πιο εξειδικευμένη εκπαίδευση στην εφαρμογή του Πλαισίου Ασφάλειας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών και αφορά συγκεκριμένους υπαλλήλους με συγκεκριμένες αρμοδιότητες.

Εκτός από την ανάγκη εφαρμογής διεθνών βέλτιστων πρακτικών, υπήρξε μια σειρά από υψηλού επιπέδου συμφωνίες, η υλοποίηση των οποίων προέβλεπε ρητά την πιστοποιημένη και συστηματική ευαισθητοποίηση και εκπαίδευση ασφάλειας του προσωπικού. Ενδεικτικά επισημαίνονται:

- Η Διακυβερνητική Συμφωνία της 19ης Ιανουαρίου 2017 με τις Ηνωμένες Πολιτείες Αμερικής, με αντικείμενο την αυτόματη ανταλλαγή φορολογικών δεδομένων πολιτών των δύο χωρών στο πλαίσιο ελέγχου της κίνησης κεφαλαίων με αντικείμενο τη φορολογική συμμόρφωση.
- Η πολυμερής συμφωνία των Κρατών-Μελών του ΟΟΣΑ με αντικείμενο την Αυτόματη Ανταλλαγή Πληροφοριών Χρηματοοικονομικών Λογαριασμών, η οποία επικυρώθηκε με τον Νόμο 4428 της 13ης Οκτωβρίου 2016.
- Η Οδηγία 16/2011 της 15ης Φεβρουαρίου, 2011 για τη συνεργασία Κρατών-Μελών της ΕΕ σχετικά με τη διοικητική συνεργασία στον τομέα της φορολογίας.
- Η συμφωνία Επιπέδου Εξυπηρέτησης (Service Level Agreement – S.L.A.) μεταξύ του Υπουργείου Οικονομικών και των Γενικών Γραμματειών της Γ.Γ.Π.Σ. & Δ.Υ. και της Γ.Γ.Δ.Ε. του ίδιου Υπουργείου (σημείωση: η Γ.Γ.Δ.Ε. έγινε Ανεξάρτητη Αρχή Δημοσίων Εσόδων (ΑΑΔΕ) από την 1-1-2017), σύμφωνα με τις διατάξεις της παραγράφου 11 άρθρου 41 του Νόμου 4389/2016, ειδικότερα του άρθρου 6 «ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ», δημιούργησε νέες σοβαρές απαιτήσεις παροχής υπηρεσιών ασφάλειας, οι οποίες περιλαμβάνουν, μεταξύ άλλων, την περιοδική ευαισθητοποίηση και εκπαίδευση στην ασφάλεια του προσωπικού του ίδιου του Υπουργείου αλλά και της Ανεξάρτητης Αρχής Δημοσίων Εσόδων.

Τέλος, ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), ο οποίος έχει τεθεί σε ισχύ από 25/5/2018, προβλέπει ρητά την ύπαρξη συστηματικής εκπαίδευσης και ευαισθητοποίησης ασφάλειας για όλο το προσωπικό.

1.6.2 Γιατί η εκπαίδευση πρέπει να επαναλαμβάνεται;

Η απλή λογική θα έλεγε ότι δεν υπάρχει ανάγκη κάποιος που έχει ήδη εκπαιδευτεί να παρακολουθήσει το συγκεκριμένο πρόγραμμα. Ωστόσο, υπάρχουν σοβαροί λόγοι που επιβάλλουν την τακτική επανάληψη της εκπαίδευσης:

- Επικαιροποίηση και ενημέρωση του υλικού εκπαίδευσης λόγω σοβαρών οργανωτικών / θεσμικών αλλαγών (π.χ. ανεξαρτητοποίηση της Γ.Γ.Δ.Ε. και δημιουργία της ΑΑΔΕ, αλλαγή οργανογράμματος του Υπουργείου Οικονομικών, έναρξη ισχύος νέων συμφωνιών μεταξύ φορέων, Κανονισμός Προστασίας Προσωπικών Δεδομένων GDPR κοκ).
- Προσαρμογή του υλικού εκπαίδευσης στο νέο Κανονιστικό Πλαίσιο Ασφάλειας (πολιτικές, διαδικασίες, οδηγίες).
- Εκπαίδευση σε αντιμετώπιση των νέων εξελιγμένων τεχνολογικών απειλών (π.χ. wannacry, νέοι τύποι phishing.
- Επανεκπαίδευση με έμφαση στα «μαθήματα» που μας διδάσκουν τα σημειωθέντα περιστατικά ασφαλείας με ταυτόχρονη αξιολόγηση των διαδικασιών και πολιτικών ασφαλείας στο πρότυπο ενός κύκλου διαρκούς βελτίωσης

1.7 Παραπομπές

1. https://el.wikipedia.org/wiki/Ασφάλεια_πληροφοριακών_συστημάτων
2. https://en.wikipedia.org/wiki/Security_awareness
3. https://en.wikipedia.org/wiki/Computer_security

2 Το Εφαρμοστέο Νομικό Πλαίσιο

Όπως αναφέραμε και στην εισαγωγή, ένας από τους σημαντικότερους, αν όχι ο σημαντικότερος, παράγοντας που δημιουργεί την αναγκαιότητα για ασφάλεια πληροφοριακών συστημάτων είναι το εφαρμοστέο θεσμικό πλαίσιο προστασίας δεδομένων. Στο παρόν κεφάλαιο θα αναλύσουμε τις απαιτήσεις ασφάλειας που δημιουργούνται από το πλαίσιο αυτό.

2.1 Προστασία Υπηρεσιακών Δεδομένων

Η προστασία των υπηρεσιακών δεδομένων προβλέπεται από τον Δημοσιοϋπαλληλικό Κώδικα και συγκεκριμένα από το Άρθρο 26 περί εχεμύθειας. Συγκεκριμένα:

Ο υπάλληλος οφείλει να τηρεί εχεμύθεια:

- για θέματα που χαρακτηρίζονται ως απόρρητα από τις κείμενες διατάξεις (Νομικό Πλαίσιο)
- σε κάθε περίπτωση που αυτό επιβάλλεται από την κοινή πείρα και λογική, για γεγονότα ή πληροφορίες των οποίων λαμβάνει γνώση κατά την εκτέλεση των καθηκόντων του ή επ' ευκαιρία αυτών

Μαρτυρία ή πραγματογνωμοσύνη για θέματα απόρρητα επιτρέπεται μόνο με άδεια του οικείου Υπουργού.

2.2 Προστασία Φορολογικών Δεδομένων

Η βασική νομική πρόβλεψη για την προστασία των φορολογικών δεδομένων προβλέπεται από το Νόμο υπ' αριθμ. Ν. 4174 - Α' 170 - 26/7/2013 και συγκεκριμένα από το Άρθρο 17 «Διαφύλαξη πληροφοριών - απόρρητο». Ακολουθούν κάποια αποσπάσματα από το εν λόγω άρθρο:

- «Πρόσωπα που είναι ή έχουν διατελέσει υπάλληλοι της Φορολογικής Διοίκησης και εν γένει του Υπουργείου Οικονομικών ή συνδέονται ή συνδέονταν με οποιαδήποτε σχέση εργασίας ή έργου με αυτά, καθώς και οποιοδήποτε πρόσωπο, στο οποίο έχουν ή είχαν ανατεθεί αρμοδιότητες ή καθήκοντα της Φορολογικής Διοίκησης οφείλουν να τηρούν ως απόρρητα όλα τα στοιχεία και πληροφορίες φορολογουμένων, τα οποία περιήλθαν σε γνώση τους κατά την άσκηση των καθηκόντων τους».
- «Δύνανται να αποκαλύπτονται» μόνο σε ρητά προβλεπόμενες περιπτώσεις.
- Ακόμα και στις περιπτώσεις αυτές ο παραλήπτης των πληροφοριών έχει την υποχρέωση τήρησης του απορρήτου: «Τα πρόσωπα, τα οποία λαμβάνουν γνώση απόρρητων στοιχείων ή πληροφοριών, σύμφωνα με την παράγραφο 1, οφείλουν να τηρούν το απόρρητο, σύμφωνα με τις διατάξεις του παρόντος άρθρου. Η χρήση των πληροφοριών και στοιχείων γίνεται αποκλειστικά και μόνο για την επίτευξη του σκοπού, για τον οποίο χορηγήθηκαν».

2.2.1 Η ΠΟΛ 1154/2018

Επισημαίνεται ότι οι λεπτομερείς διαδικασίες και οι συγκεκριμένοι μηχανισμοί χορήγησης των δεδομένων στις περιπτώσεις όπου αυτό προβλέπεται από το Άρθρο 17 του Ν. 4174/201 , καθορίζονται πλέον με σαφείς οδηγίες από την ΠΟΛ 1154/2018.

2.3 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

2.3.1 Τι είναι προσωπικά δεδομένα;

Δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αναφέρεται στο "υποκείμενο των δεδομένων".

Υποκείμενο δεδομένων: Κάθε Φυσικό Πρόσωπο – η ταυτότητα του οποίου είναι προσδιορισμένη ή μπορεί να προσδιοριστεί βάσει ενδεικτικά απαριθμούμενων χαρακτηριστικών –στοιχείων.

Δεν λογίζονται ως δεδομένα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα.

Στοιχεία προσδιορισμού ταυτότητας με βάση τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ άρθρο 4):

- ….επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας (online identifiers), τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων…
- ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα

Κατηγορίες Προσωπικών Δεδομένων (ΠΔ):

- Περιγραφικά
- Αξιολογικά
- Σχέσεις προς πρόσωπα/πράγματα
- Συμπεριλαμβάνονται
- δεδομένα ήχου-εικόνας
- Βιομετρικά δεδομένα : βιολογικά/συμπεριφορικά
- Στοιχεία ψηφιακής ταυτότητας

Ευαίσθητα ΠΔ:

- φυλετική ή εθνοτική καταγωγή
- τα πολιτικά φρονήματα
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- συμμετοχή σε συνδικαλιστική οργάνωση
- γενετικά δεδομένα, βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου
- υγεία
- σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό
- Ποινικές καταδίκες και αδικήματα

Νέες ειδικές κατηγορίες δεδομένων:

- Βιομετρικά δεδομένα: προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα

- Γενετικά δεδομένα: γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου,

2.3.2 Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Ε.Ε.) 2016/679

Αφορά την «επεξεργασία» ΠΔ:

- Ευρύς και Τεχνολογικά ουδέτερος ορισμός
- Κάθε εργασία – Ενδεικτική απαρίθμηση στο νόμο
- Από τη Συλλογή έως την Καταστροφή
- Ανωνυμοποίηση / Ψευδωνυμοποίηση ως μορφές επεξεργασίας
- Με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων
- Που εφαρμόζεται σε δεδομένα
- Ο ΓΚΠΔ αναφέρεται (άρθρο 4) σε «δεδομένα» και σε «σύνολα δεδομένων»

Το πεδίο εφαρμογής περιλαμβάνει:

- Κάθε επεξεργασία αυτοματοποιημένη και μη
- Δημόσιες αρχές με εξαίρεση την επεξεργασία για σκοπούς πρόληψης, διερεύνησης κλπ. εγκλημάτων και δημόσιας ασφάλειας
- Δικαστήρια με εξαίρεση την άσκηση δικαιοδοτικής αρμοδιότητας
- Δεν περιλαμβάνεται η επεξεργασία για αποκλειστικά προσωπικούς/οικιακούς σκοπούς

Υπεύθυνος και Εκτελών

- Υπεύθυνος επεξεργασίας: οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο της επεξεργασίας.
  - Ευθύνη για εφαρμογή νόμου – κυρώσεις
  - Οδηγίες σε εκτελούντα
- Εκτελών την επεξεργασία: οποιοσδήποτε επεξεργάζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας.
  - εκτελών στον ΓΚΠΔ επιφορτίζεται με πολύ περισσότερες υποχρεώσεις
  - Ευθύνη για εφαρμογή νόμου (ιδίως μέσω τήρησης οδηγιών υπεύθυνου/ ασφάλεια – εμπιστευτικότητα

2.3.3 Ο ρόλος μας ως προς τον ΓΚΠΔ

Εφόσον είμαστε υπάλληλοι με εξαρτημένη εργασία ενός Οργανισμού[1], μας έχουν ανατεθεί είτε από τον Υπεύθυνο είτε από τον Εκτελούντα την Επεξεργασία, συγκεκριμένα καθήκοντα τα οποία πιθανώς να έχουν σχέση με εργασίες επεξεργασίας ΠΔ.

Επομένως δεν είμαστε εμείς οι ίδιοι ούτε ο Υπεύθυνος ούτε ο Εκτελών, εκτός και αν υπάρχει ισχυρό νομικό έγγραφο εξουσιοδότησης που μας ορίζει.

[1] Σύμβαση εξαρτημένης εργασίας είναι η συμφωνία με την οποία ο εργαζόμενος αναλαμβάνει την υποχρέωση να παρέχει την εργασία του για ορισμένο ή αόριστο χρονικό διάστημα στον εργοδότη, κάτω από τις οδηγίες και τον έλεγχο του οποίου εργάζεται έναντι παροχής μισθού.

- Δεν επιτρέπεται η επεξεργασία / χρήση των ΠΔ για σκοπό πέραν του υπηρεσιακού, ακριβώς όπως μας έχει ανατεθεί είτε από το Οργανόγραμμα του Οργανισμού μας, είτε από τα επισήμως προβλεπόμενα καθήκοντά μας και τις υποθέσεις που μας αναθέτουν γραπτώς οι υπηρεσιακοί μας προϊστάμενοι.

2.4 Προστασία Δεδομένων που προέρχονται από ΑΕΟΙ

Τα δεδομένα που προέρχονται από αυτοματοποιημένη ανταλλαγή με άλλους οργανισμούς (κυρίως άλλες Χώρες), προστατεύονται από ειδικές διατάξεις που προβλέπονται μέσα στις Συμφωνίες Ανταλλαγής τις οποίες έχει υπογράψει είτε ο Οργανισμός είτε η Χώρα μας. Τα δεδομένα αυτά θα πρέπει να προστατεύονται με πρόσθετα μέτρα σε σχέση με τα Προσωπικά, Φορολογικά Δεδομένα, όπως:

- Εμφανής σήμανση ότι τα δεδομένα προέρχονται από Ανταλλαγή στο πλαίσιο Συμφωνίας και ότι απαγορεύεται η επεξεργασία τους για περιπτώσεις που δεν προβλέπονται από την Συμφωνία αυτή
- Ειδικά μέτρα φυσικής, λογικής, διοικητικής και δικτυακής προστασίας, συμπεριλαμβανομένων ενδεικτικά:
  - Ειδικές διαδικασίες χορήγησης και επεξεργασίας
  - Κρυπτογράφηση
  - Απομόνωση από άλλα δεδομένα του οργανισμού

2.5 Εσωτερικό Πλαίσιο Ασφάλειας

Το εσωτερικό Πλαίσιο Ασφάλειας (Πληροφοριακών Συστημάτων), για το οποίο θα μιλήσουμε σε επόμενη ενότητα δεν είναι τίποτα άλλο από το σύνολο των κανόνων ασφαλείας που θα πρέπει να τηρούν οι υπάλληλοι κατά τη χρήση, διαχείριση και επεξεργασία συστημάτων και πληροφοριών.

Οι κανόνες αυτές είναι συνήθως με τη μορφή Αποφάσεων του ανώτατου διοικητή του Οργανισμού και αποτελούν αυτομάτως υπηρεσιακές υποχρεώσεις όλου του προσωπικού, η παραβίαση των οποίων επιφέρει σοβαρές πειθαρχικές ευθύνες.

Σημειωτέων ότι οι κανόνες αυτοί έχουν διαμορφωθεί ώστε να καλύπτουν κυρίως τις εξής συνθήκες:

- Λαμβάνουν υπόψη τους το προαναφερόμενο νομικό πλαίσιο προστασίας δεδομένων
- Λαμβάνουν υπόψη τους το οργανόγραμμα του Οργανισμού
- Λαμβάνουν υπόψη τους το είδος των δεδομένων που επεξεργάζεται ο Οργανισμός

Οι κανόνες αυτοί έχουν την εξής μορφή:

- Έγγραφα σχετικά με ασφάλεια που θεσμοθετούνται με Αποφάσεις της Διοίκησης ή με έγγραφα των αρμοδίων Οργανικών Μονάδων Ασφάλειας.
- Πολιτικές Ασφαλείας: Νόμοι, Κανόνες
- Διαδικασίες Ασφαλείας: Τρόπος Εφαρμογής των Πολιτικών
- Οδηγίες Ασφαλείας: Οδηγίες που διευκρινίζουν την εφαρμογή των κανόνων από τους υπόχρεους

<u>Σημαντικά έγγραφα που πρέπει να γνωρίζετε και να εφαρμόζετε:</u>

- Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών.

- Στρατηγική Ασφάλειας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών.
- Ανακοινώσεις / Οδηγίες ασφάλειας που κοινοποιούνται από την αρμόδια Οργανική Μονάδα Ασφάλειας.

2.6 Παραπομπές

1. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
2. https://en.wikipedia.org/wiki/ISO/IEC_27001

3 Βασικοί Ορισμοί Ασφάλειας

3.1 Η βασική τριάδα της ασφάλειας

Η τριάδα της ασφάλειας αποτελείται από τρεις βασικές αρχές:

Εμπιστευτικότητα (Confidentiality):

Αποφυγή αποκάλυψης πληροφοριών σε μη- εξουσιοδοτημένες οντότητες.

Ακεραιότητα (Integrity):

Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

Διαθεσιμότητα (Availability):

Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας ή των υπολογιστικών πόρων σε νόμιμα εξουσιοδοτημένους χρήστες.

Εικόνα 2: Η βασική τριάδα της ασφάλειας

Πρόσθετα υπάρχουν και οι εξής συμπληρωματικές αρχές:

«Ελάχιστη Πρόσβαση»

Είναι μια από τις θεμελιώδεις αρχές της ασφάλειας σύμφωνα με την οποία δεν πρέπει να δίδονται περισσότερα δικαιώματα από αυτά που πραγματικά χρειάζονται στο πλαίσιο εξυπηρέτησης μιας ανάγκης.

«Ανάγκη Χρήσης»

Είναι μια από τις θεμελιώδεις αρχές της ασφάλειας σύμφωνα με την οποία επιτρέπεται η χρήση ενός Αγαθού μόνο στην περίπτωση που αυτό είναι αναγκαίο.

3.2 Διαχείριση Πρόσβασης – Λογοδοσία

Η διαχείριση πρόσβασης είναι απαραίτητη για να αποκτούν πρόσβαση σε πληροφορίες (και κατ' επέκταση πληροφοριακά αγαθά) μόνο οι εξουσιοδοτημένοι υπάλληλοι.

Αποτελείται από τρία διακριτά στάδια:

Αναγνώριση προσώπου (Identification): Στη φάση αυτή το φυσικό πρόσωπο αναγνωρίζεται με κάποιο τρόπο (πχ μέσω φυσικής παρουσίας και ΑΔΤ) και του αποδίδονται

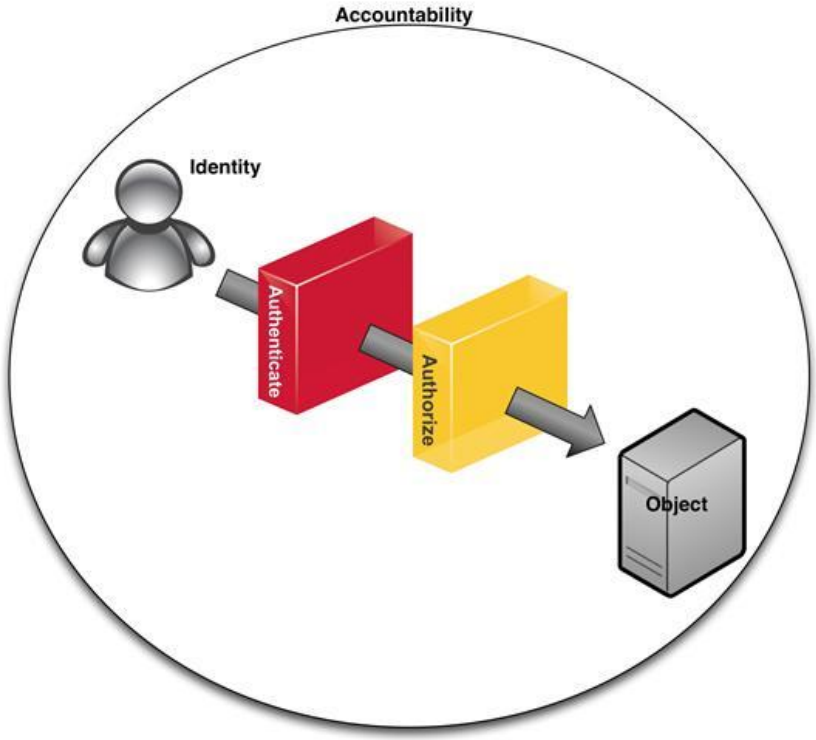
διαπιστευτήρια πρόσβασης στο σύστημα (συνήθως username / password). Η διαδικασία γίνεται μόνο μια φορά και δημιουργείται ο λεγόμενος 'λογαριασμός' στο σύστημα.

Έλεγχος ηλεκτρονικής ταυτότητας (Authentication): Στη φάση αυτή το πρόσωπο εισάγει τα διαπιστευτήρια στο πληροφοριακό σύστημα και το σύστημα ελέγχει αν υπάρχει ο σχετικός λογαριασμός. Αυτή η διαδικασία γίνεται κάθε φορά που το πρόσωπο θέλει να εισέλθει στο σύστημα.

Ισχυρή ταυτοποίηση (strong authentication): Εννοούμε τον έλεγχο ηλεκτρονικής ταυτότητας που βασίζεται σε συνδυασμό διαπιστευτηρίων. Π.χ. επιπλέον του username / password, απαιτείται και ένας κωδικός που στέλνεται από το σύστημα μέσω sms.

Εξουσιοδότηση (Authentication): Στη φάση αυτή, αφού έχει γίνει επιτυχώς ο έλεγχος ηλεκτρονικής ταυτότητας, ελέγχεται αν χρήστης έχει δικαίωμα πρόσβασης στις υπηρεσίες του συστήματος τις οποίες αιτήθηκε.

Η **λογοδοσία** διασφαλίζεται εφόσον το σύστημα γνωρίζοντας σε ποιο φυσικό πρόσωπο ανήκει ο λογαριασμός, μπορεί να του αποδώσει όλες τις ενέργειες που καταγράφονται από αυτό.



Εικόνα 3: Λογοδοσία

3.3 Επίσημοι ορισμοί από το Πλαίσιο Ασφάλειας

Κρίσιμες Πληροφορίες ή Κρίσιμα Δεδομένα

Πληροφορίες ή δεδομένα τα οποία χρήζουν προστασίας είτε λόγω εφαρμογής ισχύοντος θεσμικού πλαισίου είτε λόγω σοβαρών επιπτώσεων που προκύπτουν για ένα Οργανισμό σε περίπτωση μη εξουσιοδοτημένης πρόσβασης, μεταβολής ή καταστροφής.

Πληροφοριακό Αγαθό ή Αγαθό

Κάθε μονάδα υλικού εξοπλισμού, λογισμικού, έντυπου ή ηλεκτρονικού αρχείου που αξιοποιείται ως μέρος διεργασιών συλλογής, επεξεργασίας και μετάδοσης Κρίσιμων Πληροφοριών, και ως συνέπεια έχει κάποια αξία για ένα Οργανισμό (εξ ου και ο όρος 'Αγαθό') .

Πληροφοριακό Σύστημα (ΠΣ) ή Ολοκληρωμένο Πληροφοριακό Σύστημα

Είναι ένα ενιαίο σύνολο που περιλαμβάνει Πληροφοριακά Αγαθά, Διοικητική Οργάνωση, Ανθρώπινο Δυναμικό, προκειμένου να υπηρετείται ένας αυτοτελής Υπηρεσιακός σκοπός μέσω της συλλογής, επεξεργασίας και μετάδοσης ευαίσθητων πληροφοριών .

Ασφάλεια ΠΣ

Η προστασία των Κρίσιμων Πληροφοριών και κατ' επέκταση η προστασία των εμπλεκομένων Αγαθών ενός ΠΣ από μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη μεταβολή και μη εξουσιοδοτημένη απώλεια διαθεσιμότητας ή καταστροφή.

Μέτρο Ασφάλειας ή Μέτρο

Οποιοδήποτε φυσικό, τεχνολογικό, διοικητικό, νομικό ή διαδικαστικό μέτρο βελτιώνει την Ασφάλεια ΠΣ .

Ιδιοκτήτης Πληροφοριακού Αγαθού ή Ιδιοκτήτης Αγαθού

Ο προϊστάμενος της Διεύθυνσης που έχει την ευθύνη διαχείρισης του Πληροφοριακού Αγαθού όπως προκύπτει από τις επίσημες αρμοδιότητες του Οργανισμού στον οποίο υπάγεται η ως άνω Διεύθυνση. Εφόσον εντός της εν λόγω Διεύθυνσης υπάρχει διακριτή αρμοδιότητα διαχείρισης του Αγαθού από συγκεκριμένο τμήμα, τότε ο προϊστάμενος του τμήματος ορίζεται ως συν-Ιδιοκτήτης του Αγαθού.

Εξουσιοδότηση (σε Πληροφοριακό Αγαθό)

Η απόδοση δικαιωμάτων χρήσης ή διαχείρισης ενός Αγαθού είτε μέσω εφαρμογής του ισχύοντος θεσμικού πλαισίου είτε μέσω ρητής έγκρισης από τον Ιδιοκτήτη του Αγαθού.

Εγκεκριμένος Διαχειριστής Αγαθού

Κατάλληλα εξουσιοδοτημένος από τον Ιδιοκτήτη Αγαθού υπάλληλος, που καλύπτει τις ανάγκες διαχείρισης του Αγαθού .

Εσωτερικός Χρήστης Αγαθού

Κατάλληλα εξουσιοδοτημένος υπάλληλος ο οποίος κατόπιν αιτήματος του προϊσταμένου του και στο πλαίσιο άσκησης των καθηκόντων κάνει χρήση ενός Αγαθού .

Εξωτερικός Χρήστης Αγαθού

Φυσικό πρόσωπο ή φορέας που δεν ανήκει στον Οργανισμό ο οποίος κάνει χρήση ενός Αγαθού.

Πλαίσιο Ασφάλειας

Ένα σαφώς ορισμένο σύνολο κανόνων ασφαλείας ή ένα σύνολο πολιτικών ασφαλείας με το οποίο συμμορφώνεται ένας Οργανισμός.

Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Ένα σύνολο από πολιτικές, διαδικασίες, οδηγίες, τεχνικά πρότυπα μέσω του οποίου ένας Οργανισμός διαχειρίζεται την ασφάλεια.

3.4 Παραπομπές

1. https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
2. https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems
3. https://danielmiessler.com/blog/security-identification-authentication-and-authorization/

4 Επιτελικοί Στόχοι Ασφάλειας

4.1 Επιτελικοί ρόλοι και αρμοδιότητες

Στο πλαίσιο εφαρμογής του Πλαισίου Ασφάλειας Πληροφοριακών Συστημάτων του Υπ. Οικονομικών (ΠΑΠΣ-ΥΠΟΙΚ) προβλέπονται οι εξής αρμοδιότητες:

Υπουργός Οικονομικών:

1. Έχει την ευθύνη της τελικής έγκρισης των εγγράφων που απαρτίζουν το ΠΑΠΣ-ΥΠΟΙΚ με διακριτές Διοικητικές Αποφάσεις.

2. Έχει τη συνολική ευθύνη εφαρμογής του ΠΑΠΣ-ΥΠΟΙΚ στα Πληροφοριακά Αγαθά ιδιοκτησίας του Υπουργείου η οποία κατανέμεται στους υφισταμένους του σύμφωνα με ισχύον οργανωτικό του πλαίσιο.

3. Λαμβάνει τις απαραίτητες αποφάσεις για ζητήματα ασφάλειας που αφορούν Πληροφοριακά Αγαθά ιδιοκτησίας του Υπουργείου.

Διοικητικός Προϊστάμενος Οργανισμού «Φ» ο οποίος αποδέχεται επίσημα την εφαρμογή του ΠΑΠΣ-ΥΠΟΙΚ:

1. Έχει την ευθύνη της αναδιαμόρφωσης εγγράφων που απαρτίζουν το ΠΑΠΣ-ΥΠΟΙΚ τα οποία αφορούν κανόνες ασφάλειας Πληροφοριακών Αγαθών ιδιοκτησίας του Οργανισμού «Φ» .

2. Έχει τη συνολική ευθύνη εφαρμογής του ΠΑΠΣ-ΥΠΟΙΚ στα Πληροφοριακά Αγαθά ιδιοκτησίας του Οργανισμού «Φ», η οποία κατανέμεται στους υφισταμένους του σύμφωνα με ισχύον οργανωτικό πλαίσιο του εν λόγω Οργανισμού.

3. Λαμβάνει τις απαραίτητες αποφάσεις για ζητήματα ασφάλειας που αφορούν Πληροφοριακά Αγαθά ιδιοκτησίας του Οργανισμού «Φ».

Υπάλληλος με θέση ευθύνης (προϊστάμενοι οργανικών μονάδων ή υπεύθυνοι έργων που εφαρμόζουν το ΠΑΠΣ-ΥΠΟΙΚ):

1. Έχει την ευθύνη της συμμόρφωσης με το ΠΑΠΣ-ΥΠΟΙΚ κατ' αρμοδιότητα .

2. Αποτελεί μοναδικό σημείο επικοινωνίας με το ΑΤΑ σε περιπτώσεις που κριθεί αναγκαίο.

Ιδιοκτήτης Πληροφοριακού Αγαθού (ΙΠΑ):

1. Έχει την ευθύνη της συμμόρφωσης με το ΠΑΠΣ-ΥΠΟΙΚ κατ' αρμοδιότητα.

2. Έχει την ευθύνη εφαρμογής κανόνων του ΠΑΠΣ-ΥΠΟΙΚ στο Αγαθό.

3. Συνδράμει το ΑΤΑ ή τις ΟΜΑ-Φ για τη διαμόρφωση κανόνων, διαδικασιών, τεχνικών προτύπων και οδηγιών που απαιτούνται για την εφαρμογή του ΠΑΠΣ-ΥΠΟΙΚ και σχετίζονται με τις αρμοδιότητες του.

Αυτοτελές Τμήμα Ασφαλείας και Οργανική Μονάδα Ασφάλειας Οργανισμού «Φ» (ΑΤΑ και ΟΜΑ-Φ):

Έχουν τις αρμοδιότητες που προβλέπονται το οργανωτικό θεσμικό πλαίσιο (οργανόγραμμα), οι οποίες περιλαμβάνουν κατ' ελάχιστον τα εξής:

1. Εισήγηση εγγράφων του ΠΑΠΣ-ΥΠΟΙΚ.

2. Καθοδήγηση άλλων οργανικών μονάδων στην εφαρμογή του ΠΑΠΣ-ΥΠΟΙΚ.

3. Διαχείριση περιστατικών ασφαλείας.

4. Παρακολούθηση δράσεων ασφαλείας και εισηγήσεις προς το Διοικητικό τους Προϊστάμενο για λήψη αποφάσεων ασφαλείας.

Μονάδα Εσωτερικού Ελέγχου (ΜΕΕ), Οργανική Μονάδα Εσωτερικών Ελέγχων Οργανισμού «Φ» (ΟΜΕΣΕΛ-Φ) και Οργανική Μονάδα Εσωτερικών Υποθέσεων Οργανισμού «Φ» (ΟΜΕΣΥΠ-Φ):

Έχουν τις αρμοδιότητες που προβλέπονται από το οργανωτικό θεσμικό πλαίσιο (οργανόγραμμα) σε σχέση με τον έλεγχο ασφάλειας Πληροφοριακών Συστημάτων, οι οποίες περιλαμβάνουν τον έλεγχο συμμόρφωσης με το ισχύον ΠΑΠΣ-ΥΠΟΙΚ.

Οργανική Μονάδα Σχεδίασης και Ανάπτυξης Εφαρμογών (ΟΜΣΑΕ):

Έχει την ευθύνη της συμμόρφωσης με το ΠΑΠΣ-ΥΠΟΙΚ στο πλαίσιο σχεδίασης ανάπτυξης νέων εφαρμογών και συστημάτων.

4.2 Στρατηγική Ασφάλειας

Αποτελεί το κεντρικό και αναπόσπαστο έγγραφο του Πλαισίου Ασφάλειας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών (ΠΑΠΣ-ΥΠΟΙΚ), και περιλαμβάνει τα εξής:

(α) Τον ορισμό του ΠΑΠΣ-ΥΠΟΙΚ και τη δομή του.

(β) Το πεδίο εφαρμογής του ΠΑΠΣ-ΥΠΟΙΚ.

(β) Τις απαιτήσεις ασφάλειας που λαμβάνονται υπόψη για τη διαμόρφωση του ΠΑΠΣ-ΥΠΟΙΚ.

(γ) Τις Δεσμεύσεις και τους στόχους του Υπουργείου ως προς την ασφάλεια.

(δ) Την οργανωτική δομή και τις σχετικές αρμοδιότητες ως προς την ασφάλεια.

- Ως μια βασική δέσμευση της Στρατηγικής Ασφάλειας είναι η συμμόρφωση με το πρότυπο ISO 27001.

4.3 Το Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων

Το Πλαίσιο Ασφαλείας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών (ΠΑΠΣ-ΥΠΟΙΚ) είναι το σύνολο των κανόνων που καλύπτουν κάθε πτυχή ασφαλείας ενός Πληροφοριακού Συστήματος που φιλοξενείται στις Κεντρικές Υπολογιστικές Υποδομές του Υπουργείου.

Για λόγους καλύτερης κατανόησης και αποδοτικότερης εφαρμογής από τους αρμόδιους, το ΠΑΠΣ-ΥΠΟΙΚ διαιρείται σε ένα σύνολο ανεξάρτητων (επιμέρους) Πολιτικών Ασφαλείας. Η κάθε πολιτική καλύπτει μια συγκεκριμένη θεματική περιοχή του προτύπου ISO 27001:2013, ενώ το σύνολο των πολιτικών αυτών καλύπτει πλήρως όλες τις περιοχές του προτύπου.

4.3.1 Καλυπτόμενες απαιτήσεις ασφάλειας

Λαμβάνονται υπόψη οι εξής απαιτήσεις ασφαλείας:

(α) οι απαιτήσεις που προκύπτουν από το εφαρμοζόμενο νομικό πλαίσιο

(β) οι απαιτήσεις που προκύπτουν από τις Συμφωνίες Επιπέδου Εξυπηρέτησης που έχει συνάψει το Υπουργείο Οικονομικών με άλλους Οργανισμούς των οποίων τα Πληροφοριακά Συστήματα φιλοξενούνται στις Κεντρικές Υπολογιστικές Υποδομές του Υπουργείου

(γ) οι απαιτήσεις που προκύπτουν βάσει ακολουθούμενων διεθνών βέλτιστων πρακτικών ασφάλειας

(δ) οι απαιτήσεις που προκύπτουν από τις Διακρατικές Συμφωνίες Αυτοματοποιημένης Ανταλλαγής Πληροφοριών στις οποίες συμμετέχει το Υπουργείο Οικονομικών.

4.3.2 Εφαρμοζόμενο νομικό πλαίσιο

Λαμβάνονται υπόψη τα εξής:

- Διαχείριση ασφάλειας δεδομένων της Ανεξάρτητης Αρχής Δημοσίων Εσόδων:

(α) Νόμος 4389/2016 «Επείγουσες διατάξεις για την εφαρμογή της συμφωνίας δημοσιονομικών στόχων και διαρθρωτικών μεταρρυθμίσεων και άλλες διατάξεις», ιδίως άρθρο 37 «Διαχείριση δεδομένων και συστημάτων» και

(β) Συμφωνία Επιπέδου Εξυπηρέτησης (Service Level Agreement – S.L.A.) μεταξύ του Υπουργείου Οικονομικών και των Γενικών Γραμματειών της Γ.Γ.Π.Σ. & Δ.Υ. και της Γ.Γ.Δ.Ε. του ίδιου Υπουργείου σύμφωνα με τις διατάξεις της παραγράφου 11 άρθρου 41 του Νόμου 4389/2016, ειδικότερα του άρθρου 6 «ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ»

- Φορολογικό Απόρρητο: Νόμος 4174/2013 «Φορολογικές διαδικασίες και άλλες διατάξεις», άρθρο 17 Διαφύλαξη πληροφοριών – απόρρητο, όπως έχει τροποποιηθεί και ισχύει
- Προστασία Δεδομένων Προσωπικού Χαρακτήρα:

(α) Νόμος 2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» όπως έχει τροποποιηθεί και ισχύει, και

(β) Κανονισμός 2016/679 της ΕΕ «Κανονισμός για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ»

4.3.3 Διεθνείς Βέλτιστες Πρακτικές

- Το ΠΑΠΣ-ΥΠΟΙΚ ακολουθεί το πρότυπο ISO 27001:2013
- Το ΠΑΠΣ-ΥΠΟΙΚ συμμορφώνεται με τις απαιτήσεις του Βιβλίου Εργασίας για την εφαρμογή της ρύθμισης FATCA (FATCA Workbook)
- Το ΠΑΠΣ-ΥΠΟΙΚ συμμορφώνεται με τις απαιτήσεις του Κοινού Πρότυπου Αναφοράς (Common Reporting Standard) του ΟΟΣΑ

- Για την εφαρμογή του ΠΑΠΣ-ΥΠΟΙΚ, ακολουθούνται πρακτικές που προτείνονται από τη σειρά προτύπων ISO 2700X:2013 (X>=2) καθώς και από τον Οργανισμό NIST

4.3.4 Διεθνείς Συμφωνίες

Λαμβάνονται υπόψη οι απαιτήσεις ασφάλειας που επιβάλλονται από τις εξής συμφωνίες:

- Διμερής Διακρατική Συμφωνία FATCA μεταξύ Ελλάδας και ΗΠΑ (ημερομηνία υπογραφής 19/1/2017)
- Πολυμερής Συμφωνία Αρμόδιων Αρχών του ΟΟΣΑ για την Αυτόματη Ανταλλαγή Χρηματοοικονομικών Πληροφοριών, σύμφωνα με το Κοινό Πρότυπο Αναφοράς (Common Reporting Standard) που κυρώθηκε με το Νόμο 4428/2016 (ημερομηνία υπογραφής 13/10/2016)
- Διοικητική συνεργασία Μελών της ΕΕ στον τομέα της Φορολογίας, σύμφωνα με τις Οδηγίες ΕΕ 16/2011 (DAC), 107/2014 (DAC2), 2376/2015 (DAC3) και 881/2016 (DAC4).

4.3.5 Οι πολιτικές ασφαλείας που συνθέτουν το ΠΑΠΣ-ΥΠΟΙΚ

α/α	Όνομα εγγράφου	Κωδικός εγγράφου	Αρμόδιοι (ενδεικτικά)
1.	Στρατηγική Ασφάλειας Πληροφοριακών Συστημάτων (το παρόν έγγραφο)	GR.MOF.INFOSEC.POL.**01**-ΑΕ[2]	Υπάλληλοι με θέση ευθύνης (και υπεύθυνοι έργων), κοινοποίηση προς όλους τους υπαλλήλους
2.	Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών	GR.MOF.INFOSEC.POL.**02**-ΑΕ	Όλο το προσωπικό
3.	Πολιτική Διαχείρισης Πληροφοριακών Αγαθών	GR.MOF.INFOSEC.POL.**03**-ΑΕ	ΙΠΑ και αρμόδιοι Εγκεκριμένοι Διαχειριστές
4.	Πολιτική Αξιολόγησης Ασφαλείας Πληροφοριών και Κινδύνων	GR.MOF.INFOSEC.POL.**04**-ΑΕ	ΑΤΑ, ΟΜΑ-Φ, ΜΕΕ, ΟΜΕΣΕΛ-Φ
5.	Πολιτική Διαχείρισης Απειλών και Ευπαθειών	GR.MOF.INFOSEC.POL.**05**-ΑΕ	ΑΤΑ, ΟΜΑ-Φ
6.	Πολιτική Διαχείρισης Αρχείων Καταγραφής Ασφαλείας	GR.MOF.INFOSEC.POL.**06**-ΑΕ	ΟΜΣΑΕ, ΙΠΑ, αρμόδιοι Εγκεκριμένοι Διαχειριστές, ΑΤΑ, ΟΜΑ-Φ
7.	Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας	GR.MOF.INFOSEC.POL.**07**-ΑΕ	ΙΠΑ φυσικών υποδομών, αρμόδιοι Εγκεκριμένοι Διαχειριστές, ΑΤΑ
8.	Πολιτική Αποδεκτής Χρήσης Κρυπτογράφησης	GR.MOF.INFOSEC.POL.**08**-ΑΕ	ΑΤΑ, ΟΜΑ-Φ
9.	Πολιτική Διαχείρισης Πρόσβασης	GR.MOF.INFOSEC.POL.**09**-ΑΕ	Υπάλληλοι με θέση ευθύνης (και Υπεύθυνοι Έργων), ΙΠΑ, και αρμόδιοι Εγκεκριμένοι Διαχειριστές λογαριασμών

[2] ΑΕ: αριθμός έκδοσης της μορφής 01, 02, …

10.	Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης	GR.MOF.INFOSEC.POL.**10**-ΑΕ	ΙΠΑ, αρμόδιοι Εγκεκριμένοι Διαχειριστές, ΑΤΑ, ΟΜΑ-Φ
11.	Πολιτική Διαχείρισης Περιστατικών Ασφαλείας	GR.MOF.INFOSEC.POL.**11**-ΑΕ	ΑΤΑ, ΟΜΑ-Φ, ΙΠΑ, Εγκεκριμένοι Διαχειριστές
12.	Πολιτική Διαχείρισης Επιχειρησιακής Συνέχειας	GR.MOF.INFOSEC.POL.**12**-ΑΕ	ΙΠΑ, αρμόδιοι Εγκεκριμένοι Διαχειριστές, ΑΤΑ, ΟΜΑ-Φ
13.	Πολιτική Ανάπτυξης, Λειτουργίας και Συντήρησης Πληροφοριακού Συστήματος	GR.MOF.INFOSEC.POL.**13**-ΑΕ	ΑΤΑ, ΟΜΑ-Φ, ΟΜΣΑΕ
14.	Πολιτική Ευαισθητοποίησης και Εκπαίδευσης Ασφάλειας	GR.MOF.INFOSEC.POL.**14**-ΑΕ	ΑΤΑ, ΟΜΑ-Φ
15.	Πολιτική Ασφάλειας Προσωπικού	GR.MOF.INFOSEC.POL.**15**-ΑΕ	Υπάλληλοι με θέση ευθύνης (και Υπεύθυνοι Έργων)
16.	Πολιτική Προστασίας Επικοινωνιών και Δικτύου	GR.MOF.INFOSEC.POL.**16**-ΑΕ	ΙΠΑ δικτυακών ΠΑ, αρμόδιοι Εγκεκριμένοι Διαχειριστές δικτύων

5 Κανόνες Ασφάλειας

5.1 Η πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών (ΠΟΧΣΠ)

Αποτελεί το βασικό σύνολο κανόνων που πρέπει να ακολουθεί όλο το προσωπικό του οργανισμού το οποίο κάνει χρήση διαφόρων υπηρεσιακών αγαθών στο πλαίσιο άσκησης των καθηκόντων του.

Οι κατευθυντήριες αρχές της ΠΟΧΣΠ εφαρμόζονται υποχρεωτικά από οποιονδήποτε Οργανισμό αποδέχεται επισήμως και εφαρμόζει το ως άνω Πλαίσιο, συμπεριλαμβανομένου του ίδιου του Υπουργείου Οικονομικών.

Σκοπός της ΠΟΧΣΠ είναι να ευαισθητοποιήσει το προσωπικό του Οργανισμού ως προς τις ευθύνες του και τη συνεισφορά του (ανάλογα με τον ειδικό του υπηρεσιακό ρόλο) στην ασφάλεια των Πληροφοριών και των Πληροφοριακών Συστημάτων με σκοπό την ελαχιστοποίηση των κινδύνων από αμέλεια ή από κακόβουλη χρήση.

5.2 Γενικές απαιτήσεις

Κάθε Χρήστης, πρέπει να τηρεί τους ακόλουθους γενικούς κανόνες:

1. **Γνώση και συμμόρφωση**: Να έχει διαβάσει και κατανοήσει την παρούσα πολιτική. Σε περίπτωση μη κατανόησης θα πρέπει να συμβουλεύεται τον άμεσο αρμόδιο Υπεύθυνο Χρηστών. Εφόσον ο Υπεύθυνος Χρηστών προϊστάμενος δεν κατανοεί την πολιτική θα πρέπει να επικοινωνεί με την αρμόδια Οργανική Μονάδα Ασφάλειας του Οργανισμού του για διευκρινίσεις.
2. **Συμπεριφορά**: Να ενεργεί με ακεραιότητα και ειλικρίνεια, τηρώντας το νόμο, τις εντολές και οδηγίες, σεβόμενος/η τις αξίες, τη φήμη και την αποστολή του Οργανισμού του. Να αποφεύγει ενέργειες ή συμπεριφορές που δύναται να θέσουν σε διακινδύνευση τους πληροφοριακούς όρους π.χ. κάπνισμα σε μη ενδεδειγμένους χώρους, ακραίες συμπεριφορές.
3. **Ρόλος**: να γνωρίζει επακριβώς ποιες είναι οι αρμοδιότητές του, και εάν έχει δυσκολία στην κατανόησή τους να συμβουλευτεί τον άμεσο αρμόδιο Υπεύθυνο Χρηστών.
4. **Αναφορά συμβάντων ασφαλείας**: Σε περίπτωση υποψιών ή διαπίστωσης συμβάντος που πιθανώς παραβιάζουν την παρούσα πολιτική ή γενικότερα μπορεί να αποτελούν κίνδυνο για τα συστήματα ή τις εμπιστευτικές πληροφορίες του Οργανισμού, να ειδοποιεί άμεσα τον αρμόδιο Υπεύθυνο Χρηστών ή και την αρμόδια Οργανική Μονάδα Ασφάλειας, όπως περιγράφεται στην ενότητα (4.7) «Αναφορά περιστατικών».
5. **Γνώση παρακολούθησης/ελέγχου**: Να γνωρίζει ότι ο Οργανισμός εφαρμόζει μια σειρά από αναγκαία μέτρα ασφάλειας τα οποία πιθανώς περιλαμβάνουν την καταγραφή και παρακολούθηση ενεργειών των Χρηστών, με σκοπό τη διαπίστωση και τεκμηρίωση συμβάντων παραβίασης του Πλαισίου Ασφαλείας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών.
6. **Χρήση υπηρεσιακού εξοπλισμού**: Ο εξοπλισμός που έχει διατεθεί για τα υπηρεσιακά καθήκοντα δεν πρέπει να χρησιμοποιείται για προσωπικούς λόγους και ούτε να παραχωρείται σε τρίτους.
7. **Χρήση προσωπικού εξοπλισμού**: Δεν επιτρέπεται να χρησιμοποιούνται προσωπικές συσκευές όπως φορητά αποθηκευτικά μέσα, υπολογιστές, ταμπλέτες, έξυπνα κινητά τηλέφωνα, κάμερες κ.λπ. για την αποθήκευση υπηρεσιακών πληροφοριών, χωρίς άδεια από τον άμεσο αρμόδιο Υπεύθυνο Χρηστών, και μόνο βάσει υπηρεσιακής ανάγκης με την τήρηση των κανόνων

εμπιστευτικότητας της παραγράφου 4.3. Σε περίπτωση αποχώρησης ή μη ύπαρξης πλέον της ανάγκης θα πρέπει να διαγράφεται οποιαδήποτε υπηρεσιακή πληροφορία από προσωπικό εξοπλισμό.

8. **Σύνδεση εξοπλισμού**: Η σύνδεση εξοπλισμού στις δικτυακές πληροφοριακές υποδομές, επιτρέπεται μόνο μετά από έγκριση από την αρμόδια Διεύθυνση Διαχείρισης Υπολογιστικών Υποδομών και μόνο με δικαιολογημένο αίτημα εξυπηρέτησης υπηρεσιακής ανάγκης.
9. **Χρήση Λογισμικού**: (α) Δεν επιτρέπεται χρήση λογισμικού πέραν αυτού που παρέχεται κεντρικά από την αρμόδια Διεύθυνση Διαχείρισης Υπολογιστικών Υποδομών. Σε περίπτωση που χρειάζεται μια πρόσθετη λειτουργία, θα πρέπει να ζητηθεί εγγράφως από τον άμεσο αρμόδιο Υπεύθυνο Χρηστών δικαιολογώντας επαρκώς το αίτημα και μόνο βάσει υπηρεσιακής ανάγκης. Το αίτημα αυτό θα πρέπει υποχρεωτικά να εγκρίνεται από την ως άνω Διεύθυνση Διαχείρισης Υπολογιστικών Υποδομών. (β) Απαγορεύεται η απεγκατάσταση λογισμικού που είναι ήδη εγκατεστημένο χωρίς έγκριση από την ως άνω Διεύθυνση Διαχείρισης Υπολογιστικών Υποδομών, συμπεριλαμβανομένου του λογισμικού προστασίας από κακόβουλο λογισμικό.
10. **Εκμετάλλευση αδυναμιών**: Απαγορεύεται ρητά: (α) η εκμετάλλευση πιθανών κενών ασφάλειας του τηλεπικοινωνιακού εξοπλισμού, των συστημάτων, των υπηρεσιών και εφαρμογών του Οργανισμού, (β) η διατάραξη της ομαλής λειτουργίας των δικτύων και των υπηρεσιών του Οργανισμού καθώς και η εκτέλεση οποιουδήποτε κακόβουλου λογισμικού δύναται να θέσει σε κίνδυνο ή να υποβαθμίσει το επίπεδο ασφάλειας του Οργανισμού
11. **Κλείδωμα οθόνης υπολογιστή**: να κλειδώνει με μυστικό προσωπικό κωδικό την επιφάνεια εργασίας του προσωπικού του υπολογιστή όταν απουσιάζει/απομακρύνεται από το γραφείο του.
12. **Χρήση υπηρεσιακών φορητών υπολογιστών**: Απαιτείται ιδιαίτερη προσοχή ως προς τη φυσική ασφάλεια φορητών υπολογιστών και άλλων συσκευών με δυνατότητα αποθήκευσης, που πιθανώς περιέχουν ευαίσθητα υπηρεσιακά δεδομένα, ιδίως κατά τη μεταφορά εκτός υπηρεσιακών χώρων . Η περίπτωση κλοπής αποτελεί σημαντικό συμβάν ασφάλειας το οποίο πρέπει να αναφέρεται άμεσα σύμφωνα με την προηγούμενη παράγραφο 4.

5.3 Χρήση κωδικών πρόσβασης

Οι Χρήστες θα πρέπει να είναι ιδιαίτερα προσεκτικοί ως προς τη διαχείριση μυστικών κωδικών πρόσβασης σε συστήματα και μέσα του Οργανισμού. Κατ' ελάχιστον θα πρέπει να ισχύουν οι ακόλουθοι κανόνες:

1. Να επιλέγονται **ισχυροί κωδικοί πρόσβασης,** ακόμη και αν δεν υπάρχουν τα τεχνικά μέσα για τον αυτόματο έλεγχο της συμμόρφωσης. Ένας κωδικός θεωρείται ισχυρός εάν ικανοποιούνται οι ακόλουθοι περιορισμοί:
   - Έχει μήκος τουλάχιστον 8 χαρακτήρες
   - Περιέχει ένα τουλάχιστον πεζό γράμμα (λατινικοί χαρακτήρες)
   - Περιέχει ένα τουλάχιστον κεφαλαίο γράμμα (λατινικοί χαρακτήρες)
   - Περιέχει ένα τουλάχιστον αριθμό
2. Οι κωδικοί πρόσβασης είναι **προσωπικοί** και πρέπει να παραμένουν **μυστικοί**. Δεν επιτρέπεται η αποκάλυψή τους σε συναδέλφους ή τρίτους. Η αποκάλυψη μπορεί να επιτραπεί μόνο για συγκεκριμένο δικαιολογημένο χρονικό διάστημα, μετά από έγγραφη ανάθεση από άμεσο αρμόδιο Υπεύθυνο Χρηστών και μόνο στο πλαίσιο επείγουσας υπηρεσιακής ανάγκης. Στις περιπτώσεις αυτές ο Χρήστης πρέπει να αλλάζει το δυνατόν αμεσότερα τον προσωπικό του κωδικό, εφόσον ολοκληρώθηκε η απαιτούμενη ενέργεια.

3. Οι κωδικοί πρόσβασης θεωρούνται εν γένει ως η κορυφαία εμπιστευτική πληροφορία και σε περίπτωση που είναι αποτυπωμένη με έντυπο ή ηλεκτρονικό τρόπο, θα πρέπει να προστατεύεται ως τέτοια είτε με χρήση κρυπτογράφησης ή μέσω επαρκούς φυσικής ασφάλειας. Ιδιαίτερη προσοχή πρέπει να δίδεται κατά την αποστολή ή κοινοποίηση τέτοιας πληροφορίας ώστε να μην είναι δυνατόν να διαρρεύσει σε μη εξουσιοδοτημένα άτομα.
4. Αν υπάρχει υποψία ότι ο προσωπικός κωδικός πρόσβασης έχει υποκλαπεί, θα πρέπει να αλλάζεται άμεσα και σε περίπτωση που αυτό δεν είναι εφικτό να ειδοποιείται ο αρμόδιος Διαχειριστής. .
5. Θα πρέπει να αλλάζονται περιοδικά οι κωδικοί πρόσβασης ώστε να ελαχιστοποιηθεί η πιθανότητα μη εξουσιοδοτημένης χρήσης τους.
6. Απαγορεύεται η χρήση των ίδιων κωδικών πρόσβασης στις υπηρεσίες και συστήματα του Οργανισμού με προσωπικούς κωδικούς πρόσβασης που χρησιμοποιεί ο εκάστοτε χρήσης στη χρήση Διαδικτύου ή Ηλεκτρονικού Ταχυδρομείου.

5.4 Εμπιστευτικότητα υπηρεσιακής πληροφορίας

Οι υπάλληλοι του Οργανισμού και σε ορισμένες περιπτώσεις και οι εξωτερικοί συνεργάτες, στο πλαίσιο των καθηκόντων τους χειρίζονται μια σειρά από υπηρεσιακές πληροφορίες οι οποίες είναι πολύ πιθανό να διαβαθμίζονται ως «ΕΜΠΙΣΤΕΥΤΙΚΟ». Ως «εμπιστευτικές» θεωρούνται οι πληροφορίες, η γνωστοποίηση των οποίων σε μη εξουσιοδοτημένα πρόσωπα παραβιάζει την νόμιμη ή συμβατική υποχρέωση τήρησης απορρήτου ή ενδέχεται να βλάψει την ασφάλεια των πληροφορικών συστημάτων. Οι πληροφορίες αυτές μπορεί να βρίσκονται σε οποιαδήποτε μορφή, όπως ηλεκτρονικά αρχεία, υπηρεσιακά έγγραφα, εκτυπώσεις, οπτικά μέσα αποθήκευση (CD/DVD/Blu-ray), εξωτερικοί σκληροί δίσκοι, σκληροί δίσκοι, αφαιρούμενα μέσα (USB sticks), ακόμα και σε προφορική μορφή.

«**Εμπιστευτικές**» χαρακτηρίζονται ιδίως οι ακόλουθες υπηρεσιακές πληροφορίες:

- Φορολογικά δεδομένα φυσικών/νομικών προσώπων
- Προσωπικά δεδομένα πολιτών ή υπαλλήλων
- Δεδομένα που έχουν περιέλθει στην υπηρεσία στα πλαίσια ανταλλαγής δεδομένων με διεθνείς φορείς (με αυτόματο ή μη τρόπο)
- Ευαίσθητες τεχνικές πληροφορίες υπολογιστικών υποδομών που θα βοηθούσαν έναν κακόβουλο να βλάψει τα συστήματα
- Διοικητικά και λοιπά ηλεκτρονικά και μη έγγραφα με ένδειξη εμπιστευτικότητας (π.χ. ΕΜΠΙΣΤΕΥΤΙΚΟ, ΑΠΟΡΡΗΤΟ, ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ)

5.4.1 Κανόνες Ασφάλειας των υπηρεσιακών δεδομένων

1. **Τήρηση εχεμύθειας**: Τα υπηρεσιακά δεδομένα θα πρέπει να μην αποκαλύπτονται σε πρόσωπα ή οντότητες που δεν διαθέτουν ρητή εξουσιοδότηση/άδεια.
2. **Ανάγκη χρήσης / ανάγκη γνώσης**: Δεν επιτρέπεται η πρόσβαση/χρήση σε υπηρεσιακές πληροφορίες και συστήματα, παρά μόνο στα πλαίσια υπηρεσιακών υποθέσεων και καθηκόντων.
3. **Διακίνηση υπηρεσιακής πληροφορίας** (με συμβατική ή ηλεκτρονική αλληλογραφία): Δεν επιτρέπεται διακίνηση υπηρεσιακής πληροφορίας με μεθόδους που ενδέχεται να οδηγήσουν σε απώλεια εμπιστευτικότητας σε μη έχοντες εξουσιοδότηση ή σε μη γνήσιους παραλήπτες.
4. **Απαγόρευση καταγραφής**: Απαγορεύεται ρητά η καταγραφή ήχου, εικόνας ή βίντεο εντός των χώρων του Οργανισμού, χωρίς την έγκριση της αρμόδιας Οργανικής Μονάδας Ασφαλείας και μόνο κατόπιν υπηρεσιακής ανάγκης.

5. **Χρήση φορητών αποθηκευτικών μέσων**: Σε περίπτωση που χρησιμοποιούνται φορητά μέσα αποθήκευσης βάσει υπηρεσιακής ανάγκης (βλέπε και ενότητα 4.1, σημείο 7 «Χρήση προσωπικού εξοπλισμού»), θα πρέπει να δίδεται ιδιαίτερη προσοχή στο χειρισμό των μέσων αυτών ώστε να αποφευχθεί ο κίνδυνος κλοπής ή αποκάλυψης. Τα μέσα αυτά θα πρέπει είτε να παραμένουν κλειδωμένα σε ντουλάπια εντός γραφείων είτε να κρυπτογραφούνται με μεθόδους που προτείνονται από το Αυτοτελές Τμήμα Ασφάλειας (πχ αρχείο zip με password).
6. **Καθαρή Επιφάνεια Εργασίας** (Clean Desk Policy): Δεν επιτρέπεται η ανεξέλεγκτη έκθεση εντύπων, φακέλων ή φορητών αποθηκευτικών μέσων που πιθανώς φέρουν εμπιστευτικές πληροφορίες σε μη προστατευμένα σημεία όπως θέσεις εργασίας, εκτυπωτικά μηχανήματα, φωτοαντιγραφικά μηχανήματα, αίθουσες συναντήσεων, καλάθια αχρήστων. Θα πρέπει κατ' ελάχιστον να τηρούνται οι εξής κανόνες:
   - με το τέλος της εργάσιμης μέρας, όλα τα έντυπα, φάκελοι και αποθηκευτικά μέσα στα οποία ενδέχεται να υπάρχει εμπιστευτική πληροφορία, να απομακρύνονται από μη προστατευμένους χώρους και να κλειδώνονται σε ντουλάπια ή συρταριέρες ή να καταστρέφονται εφόσον δεν θα επαναχρησιμοποιηθούν.
   - εφόσον τα μέσα αυτά δεν απαιτούνται για άμεση χρήση να παραμένουν κλειδωμένα σε ντουλάπια. Σε κάθε περίπτωση, εάν δεν απαιτείται πλέον το υλικό αυτό, θα πρέπει να καταστρέφεται ασφαλώς.
   - Τις εργάσιμες ώρες θα πρέπει να κλειδώνεται με κωδικό η επιφάνεια εργασίας του προσωπικού υπολογιστή για διάστημα αδράνειας το μέγιστο 10 λεπτών.
   - Σε μη εργάσιμες ώρες, ο προσωπικός υπολογιστής θα πρέπει να είναι απενεργοποιημένος. Εξαιρούνται περιπτώσεις που υπάρχει δικαιολογημένη υπηρεσιακή ανάγκη μετά από γραπτή έγκριση του αρμόδιου Υπεύθυνου Χρηστών.
7. **Ρήτρα Εμπιστευτικότητας**: Σε περίπτωση που μετά από ανάλυση κινδύνου κριθεί αναγκαίο από την αρμόδια Οργανική Μονάδα Ασφάλειας του Οργανισμού, θα πρέπει πέραν της αποδοχής της παρούσας πολιτικής, να υπογράφεται από το Χρήστη η «ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΠΡΟΣΒΑΣΗΣ ΥΠΑΛΛΗΛΟΥ ΜΕ ΡΗΤΡΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ» σύμφωνα με το Παράρτημα του παρόντος εγγράφου, αφού διαμορφωθεί κατάλληλα από τον αρμόδιο Υπεύθυνο Χρηστών.

5.5 Χρήση Διαδικτύου / Ηλεκτρονικού Ταχυδρομείου

Το διαδίκτυο και το ηλεκτρονικό ταχυδρομείο αποτελούν χώρους ύπαρξης σημαντικών απειλών, όπως η διακίνηση κακόβουλου λογισμικού. Επίσης αποτελούν πεδίο δράσης hackers με μεγάλους κινδύνους για τα Πληροφοριακά Συστήματα αλλά και την έξωθεν εικόνα του Οργανισμού. Θα πρέπει να τηρούνται οι εξής κανόνες:

1. Απαγορεύεται η χρήση προσωπικού ηλεκτρονικού ταχυδρομείου (gmail, yahoo, κλπ) καθώς και χρήση προσωπικών υπηρεσιών νέφους (google drive, ms cloud, κλπ) για αποστολή και αποθήκευση υπηρεσιακών πληροφοριών. Μπορεί να επιτραπεί μόνο μετά από έγγραφη άδεια του αρμόδιου Υπεύθυνου Χρηστών βάσει δικαιολογημένης υπηρεσιακής ανάγκης και μόνο με χρήση κατάλληλων μεθόδων κρυπτογράφησης , σύμφωνα με σχετικές οδηγίες της αρμόδιας Οργανικής Μονάδας Ασφάλειας.
2. Δεν επιτρέπεται χρήση του διαδικτύου και του υπηρεσιακού ηλεκτρονικού ταχυδρομείου με τρόπο που να αντιβαίνει τον υπηρεσιακό σκοπό και προσβάλλει το κύρος του Οργανισμού. Κάθε Χρήστης πρέπει να είναι προσεκτικός ως προς τη διατύπωση, το περιεχόμενο και τη μορφοποίηση του κειμένου και κυρίως τους αποδέκτες των ηλεκτρονικών μηνυμάτων που αποστέλλει.
3. Δεν επιτρέπεται το άνοιγμα ύποπτων συνδέσμων ή επισυναπτόμενων αρχείων χωρίς να έχει ελεγχθεί η γνησιότητα του αποστολέα.

4. Απαγορεύεται η διακίνηση μηνυμάτων με παράνομο ή άσεμνο περιεχόμενο και με κακόβουλο/ιομορφικό λογισμικό, συμπεριλαμβανομένων ανεπιθύμητων ηλεκτρονικών μηνυμάτων (unsolicited mails ή junk mails) ή άλλου διαφημιστικού ή προωθητικού περιεχομένου (spams).
5. Εφόσον ο παραλήπτης είναι εκτός του Οργανισμού και πρέπει να διακινηθεί υπηρεσιακή πληροφορία, θα πρέπει να γίνεται μόνο με χρήση κατάλληλων μεθόδων κρυπτογράφησης .
6. Απαγορεύεται ρητά η αυτόματη προώθηση ηλεκτρονικού ταχυδρομείου σε μη υπηρεσιακούς λογαριασμούς, τόσο σε επίπεδο προσωπικού υπολογιστή όσο και σε επίπεδο mail server του Οργανισμού. Αν υπάρχει υπηρεσιακή ανάγκη, θα υλοποιείται το αίτημα με γραπτή έγκριση από τον αρμόδιο Υπεύθυνο Χρηστών.
7. Πρέπει να αποφεύγεται η αποστολή ιδιωτικών δεδομένων/αρχείων (μη υπηρεσιακών) μέσω του υπηρεσιακού ηλεκτρονικού ταχυδρομείου.
8. Πρέπει να δίδεται ιδιαίτερη προσοχή όσον αφορά τη χρήση ιστοτόπων κοινωνικής δικτύωσης, όπου σε καμία περίπτωση δεν θα πρέπει να αναφέρονται υπηρεσιακές εμπιστευτικές πληροφορίες.
9. Δεν επιτρέπεται στο Χρήστη η αποστολή email σε παραλήπτες εκτός του Οργανισμού, χωρίς την γνώση και έγκριση του αρμόδιου Υπεύθυνου Χρηστών, σε περιπτώσεις που αυτό από την κοινή λογική θα είχε πιθανές σοβαρές επιπτώσεις. Προκειμένου να ελαχιστοποιηθεί η πιθανότητα εμφάνισης τέτοιων φαινομένων θα πρέπει να ελέγχεται με προσοχή η λίστα των παραληπτών πριν την εκτέλεση της εντολής «Αποστολή».

5.6 Αναφορά περιστατικών

Κάθε Χρήστης είναι υποχρεωμένος να αναφέρει οποιοδήποτε συμβάν σχετικά με ενδεχόμενη παραβίαση της παρούσας πολιτικής, ή με παραβίαση του Πλαισίου Ασφάλειας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών ή με ενδεχόμενο κίνδυνο της ασφάλειας συστημάτων και πληροφοριών. Η αναφορά αυτή θα πρέπει να γίνεται μόνο στον άμεσο αρμόδιο Υπεύθυνο Χρηστών, ο οποίος θα πρέπει με τη σειρά του να αναφέρει το συμβάν μόνο στην αρμόδια Οργανική Μονάδα Ασφάλειας. Σε εξαιρετικές περιπτώσεις που υπάρχει υποψία παραβίασης από τον αρμόδιο Υπεύθυνο Χρηστών, ο Χρήστης θα πρέπει να αναφέρει το συμβάν απευθείας στην αρμόδια Οργανική Μονάδα Ασφάλειας, σύμφωνα με τα επίσημα στοιχεία επικοινωνίας αυτής.

Απαγορεύεται η κοινοποίηση συμβάντων ασφαλείας σε άτομα εκτός του άμεσου αρμόδιου Υπεύθυνου Χρηστών ή της αρμόδιας Οργανικής Μονάδας Ασφάλειας

5.7 Συμμόρφωση

Η χρήση υπηρεσιακών συστημάτων, μέσων και πληροφοριών του Οργανισμού επιτρέπεται, μόνο σε Χρήστες που αποδέχονται με ενυπόγραφη γνώση την παρούσα Πολιτική.

Σε περίπτωση διαπίστωσης μη συμμόρφωσης με την παρούσα Πολιτική, είναι δυνατόν να αναστέλλονται τα δικαιώματα πρόσβασης του Χρήστη, κατόπιν σχετικής σύστασης της αρμόδιας Οργανικής Μονάδας Ασφάλειας. Επιπλέον, για τους Χρήστες που τεκμηριωμένα παραβίασαν την πολιτική αυτή θα πρέπει να αναλόγως της σοβαρότητας των επιπτώσεων, να εξετάζεται η εκκίνηση πειθαρχικής ή και ποινικής διαδικασίας απο τα αρμόδια Πειθαρχικά Όργανα, σύμφωνα με το ισχύον Θεσμικό Πλαίσιο .

5.8 Οδηγίες Ασφάλειας

Στο πλαίσιο εφαρμογής της ΠΟΧΣΠ, έχουν ήδη κοινοποιηθεί στο προσωπικό οι ακόλουθες οδηγίες:

- Ασφαλής λήψη εφεδρικών αντιγράφων (αρχείο «ΛΗΨΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ.PDF») https://testintranet.ggps.gsis/browserInstall.htm

- Αντιμετώπιση κυβερνοεπιθέσων (αρχείο «ΑΝΤΙΜΕΤΩΠΙΣΗ ΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ.zip»)
- Αποστολή αρχείων με χρήση κρυπτογράφησης (αρχείο «Οδηγίες Αποστολής Αρχείων με χρήση κρυπτογράφησης.pdf»)
- Γενικές οδηγίες σχετικά με την ασφαλή χρήση ηλεκτρονικού ταχυδρομείου και την πλοήγηση στο διαδίκτυο διαδικτύου (αρχείο «Γενικές οδηγίες σχετικά με την ασφαλή χρήση ηλεκτρονικού ταχυδρομείου και την πλοήγηση στο διαδίκτυο διαδικτύου.pdf»)

6 Απειλές

Στα θέματα ασφαλείας Πληροφοριακών Συστημάτων και Προσωπικών Υπολογιστών υπερισχύει ο κανόνας: ***Δεν υπάρχει απόλυτη ασφάλεια!***

Είναι γεγονός ότι ένα πληροφοριακό σύστημα δέχεται συνεχώς απειλές. Με δεδομένη την απειλή προς την ασφάλεια ενός συστήματος θα πρέπει να υπάρχει διαρκής πρόβλεψη για λήψη μέτρων, ενημέρωση ως προς τη σωστή χρήση των συστημάτων, ευαισθητοποίηση και συνεχής επαγρύπνηση για την αποτροπή των κινδύνων.

Θα πρέπει να είμαστε συνεχώς σε εγρήγορση αναφορικά με τους σοβαρούς κινδύνους που διατρέχουμε καθώς χρησιμοποιούμε συνηθισμένες εφαρμογές διαδικτύου, όπως το email και ο φυλλομετρητής διαδικτύου (browser). Θα πρέπει, επίσης, να έχουμε υπόψη ότι με τις τελευταίες τεχνολογικές εξελίξεις, είναι πολύ πιθανό οι επιπτώσεις να μην περιοριστούν μόνο στο δικό μας προσωπικό υπολογιστή αλλά να επεκταθούν ραγδαία σε κοινόχρηστα αρχεία καθώς και στους υπολογιστές συναδέλφων που βρίσκονται στο ίδιο τοπικό δίκτυο.

Η εύλογη ερώτηση που θα μπορούσε να τεθεί από κάποιον είναι «γιατί να δεχτώ επίθεση αφού δεν υπάρχει κάτι με σημαντική αξία στον υπολογιστή μου;»

Για να δοθεί απάντηση στο πιο πάνω ερώτημα, θα πρέπει να αντιληφθούμε την «αξία» ενός αγαθού (ενός προσωπικού υπολογιστή, μιας πληροφορίας, ενός κωδικού, κτλ.) για έναν κακόβουλο χρήστη. Ο υπολογιστής μας αποτελεί στόχο κακόβουλων χρηστών με πρόθεση να χρησιμοποιηθεί σε κάποιου είδους παράνομη δραστηριότητα. Η σύγχρονη ανάγκη για επικοινωνία επιβάλλει τη χρήση δικτυακών συσκευών, όπως υπολογιστών, tablets, κινητών και συνέπεια αυτού είναι να διακινείται καθημερινά πληθώρα ψηφιακών πληροφοριών που αφορούν εμάς προσωπικά, την εργασία μας, την οικογένειά μας και τις συνήθειές μας. Οι πληροφορίες αυτές όπως και ο ίδιος υπολογιστής ενδέχεται να έχουν μεγάλη «αξία» για έναν εισβολέα.

Στο σημείο αυτό υπεισέρχεται η έννοια της απειλής (threat) που αναφέρεται σε οποιοδήποτε γεγονός προκαλεί, άμεσα ή έμμεσα αρνητικές συνέπειες, σε ένα πληροφοριακό αγαθό.

6.1 Είδη Απειλών

Οι απειλές σε ένα σύστημα διακρίνονται σε:

- **Εσωτερικές,** δηλαδή απειλές που προέρχονται από το εσωτερικό περιβάλλον – π.χ. εντός του Οργανισμού: «Νόμιμοι» χρήστες του συστήματος προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε πόρους του συστήματος.
- **Εξωτερικές,** δηλαδή απειλές που προέρχονται από το εξωτερικό περιβάλλον – π.χ. εκτός του Οργανισμού: Γεγονότα, καταστάσεις ή οντότητες που δρουν ή εκτυλίσσονται στο εξωτερικό περιβάλλον και απειλούν την ασφάλεια του συστήματος.

Οι εσωτερικές απειλές προέρχονται από εσωτερικούς χρήστες. Πρόκειται ουσιαστικά για άτομα που γνωρίζουν πληροφορίες λόγω εγγύτητας με τον οργανισμό, που έχουν φυσική/λογική πρόσβαση και παραβιάζουν σκοπούμενα ή από άγνοια κανόνες ασφαλείας πληροφοριών. Τέτοια παραδείγματα θα μπορούσε να είναι εν ενεργεία υπάλληλοι ή πρώην υπάλληλοι ή υπάλληλοι σε άδεια/απόσπαση, προσωπικό εξωτερικού συνεργάτη/αναδόχου που έχουν πρόσβαση σε χώρους, δίκτυα, συστήματα, εφαρμογές, δεδομένα κλπ.

Οι Εξωτερικές απειλές διακρίνονται σε :

- Εξωτερικούς εισβολείς : Hachers / Crackers κλπ όπου με διάφορες τεχνικές προσπαθούν να εκμεταλλευτούν αδυναμίες των συστημάτων και λογισμικών ώστε να παρακάμψουν τα συστήματα ασφαλείας και να αποκτήσουν πρόσβαση στα πληροφοριακά αγαθά και πόρους του οργανισμού.
- Κακόβουλο λογισμικό : ιοί, σκουλήκια, δούρειοι ίπποι κλπ. Ειδικό λογισμικό που ενεργοποιείται και διαδίδεται «εν αγνοία» του χρήστη με σκοπό την υποκλοπή πληροφοριών.
- Κοινωνική μηχανική (social engineering) που αφορά σε εξωτερικούς χρήστες που εκμεταλλεύονται τον ανθρώπινο παράγοντα ώστε να αποκτήσουν την κατάλληλη πληροφόρηση και να παρακάμψουν μηχανισμούς ασφαλείας προκειμένου να επιτύχουν μη εξουσιοδοτημένη πρόσβαση στα συστήματα.

Παραδείγματα απειλών είναι :

- Κακή χρήση ηλεκτρονικού ταχυδρομείου, διαδικτύου
- Προσβολή συστημάτων από κακόβουλο λογισμικό
- Κατάχρηση δικαιωμάτων (διαχειριστικών ή και απλού χρήστη)
- Κακή χρήση εφαρμογών (π.χ. πρόσβαση «νόμιμη» σε δεδομένα για εξυπηρέτηση όμως που δεν άπτεται υπηρεσιακής ανάγκης – για φίλους, συγγενείς κλπ)
- Κακή χρήση δεδομένων (αποθήκευση τους σε μέσα και μεταφορά χωρίς προφυλάξεις)
- Κλοπή δεδομένων και εμπορική εκμετάλλευση τους

Όλες οι πιο πάνω ενέργειες γίνονται είτε σκόπιμα είτε από άγνοια.

Οι σκοπούμενες ενέργειες έχουν ως κίνητρα :

- Δολιοφθορά λόγω προσωπικών / επαγγελματικών / πολιτικών διαφορών
- Κλοπή πνευματικών δικαιωμάτων
- Κατασκοπεία
- Απάτη για οικονομικό / πολιτικό όφελος
- Απλή περιέργεια

Οι ενέργειες από άγνοια γίνονται χωρίς να υπάρχει δόλος από τον χρήστη και οφείλονται σε :

- Ανθρώπινα λάθη / κακή κρίση / μη ορθή τήρηση διαδικασιών
- Ψάρεμα (phishing)
- Προσβολή από κακόβουλο λογισμικό

6.2 Το Ανθρώπινο Πληροφοριακό Αγαθό

Τόσο στην περίπτωση ενεργειών που γίνονται σκόπιμα όσο και στην περίπτωση που γίνονται από άγνοια, σημαντικό ρόλο παίζει ο **ανθρώπινος παράγοντας**. Στην περίπτωση άγνοιας ο άνθρωπος χρήστης ενός Πληροφορικού αγαθού πέφτει θύμα συνήθως κακόβουλων ενεργειών που έχουν δημιουργηθεί από άλλους (κακόβουλα) με σκοπό να υποκλέψουν χρήσιμες πληροφορίες ή να δημιουργήσουν δολιοφθορές και ταυτόχρονα να ενοχοποιήσουν τον χρήστη θύμα. Στην περίπτωση δόλου, ο χρήστης εκμεταλλεύεται

εσκεμμένα τυχόν αδυναμίες του συστήματος ή παραβιάζει διαδικασίες με σκοπό να δημιουργήσει μη επιθυμητές καταστάσεις.

Επομένως σε ένα οργανισμό ο ανθρώπινος παράγοντας θα πρέπει να αντιμετωπίζεται ως ένα «πληροφοριακό αγαθό», του οποίου η συνεισφορά συμβάλει στην ορθή ή μη λειτουργία των Πληροφοριακών Συστημάτων.

Ως «Πληροφοριακό αγαθό» ο ανθρώπινος παράγοντας :

- Είναι απαραίτητος για την διαθεσιμότητα και ορθή λειτουργία των Πληροφοριακών Συστημάτων. Απαιτείται ο διαχωρισμός του σε ρόλους (Προϊστάμενοι, Εσωτερικοί χρήστες, διαχειριστές Εφαρμογών, Διαχειριστές Συστημάτων κλπ)
- Επειδή δεν «αυτοματοποιείται» παρουσιάζει εγγενείς ευπάθειες που οφείλονται στην περιέργεια, πλεονεξία, άγνοια και γενικότερα στα συναισθήματα.
- Αποτελεί τον πιο «αδύναμο κρίκο» στη λειτουργία ενός συστήματος.
- Θεωρείται ως η πιο δύσκολη απειλή τόσο ως προς την ανίχνευση της όσο και ως προς την προστασία από αυτή.

Διάφορες έρευνες έχουν αναδείξει τη σημασία του κινδύνου από το ανθρώπινο Πληροφοριακό αγαθό :

- Σύμφωνα με το «Enisa Threat landscape report – January 2017”, ανάμεσα στα κυριότερα τέσσερα περιστατικά συγκαταλέγονται περιπτώσεις :
  - Κατάχρησης προνομιακών δικαιωμάτων
  - Κακής διαχείρισης δεδομένων
  - Χρήσης μη επιτρεπτών συσκευών
  - Χρήσης μη επιτρεπτού λογισμικού
  - Κατάχρησης δικαιωμάτων πρόσβασης

  με κύριο λόγο την εμπορική εκμετάλλευση
- Σύμφωνα με την Accenture («The state of cyberscecurity and digital trust 2016»):
  - το 69% των οργανισμών αντιμετώπισαν σοβαρό περιστατικό ασφαλείας τους τελευταίους 12 μήνες που οφειλόταν σε εσωτερική απειλή και 57% των οργανισμών σε εξωτερική απειλή.
  - το 62% των χρηστών θεωρούν ότι έχουν πρόσβαση σε δεδομένα που κατά την γνώμη τους δεν θα έπρεπε να έχουν
  - Ως προς την ταχύτητα ανίχνευσης από τους οργανισμούς των υπαλλήλων που έχουν πρόσβαση σε δεδομένα στα οποία δεν έχουν εξουσιοδότηση, 24% μόνο ανιχνεύονται εντός 24 ωρών ενώ 14% σε περισσότερο από 1 χρόνο !
  - Ως προς την τεχνική δυνατότητα ανίχνευσης εσωτερικής επίθεσης το 31.9% δήλωσε ότι δεν την διαθέτει !

Για τον περιορισμό της εκ των έσω απειλής απαιτούνται τόσο τεχνικά όσο και διοικητικά μέτρα. Ως ελάχιστα τεχνικά μέτρα είναι :

- Εφαρμογή τεχνικών ασφάλειας εφαρμογών / δεδομένων :

- Ανωνυμοποίηση (κυρίως σε test δεδομένα, αλλά και σε περιπτώσεις στατιστικής επεξεργασίας)
- Μηνύματα ασφαλείας
- Τεχνικές Κρυπτογράφησης

➢ Εφαρμογή τεχνικών ελέγχου πρόσβασης ώστε να διασφαλίζονται οι αρχές της «ελάχιστης πρόσβασης» και της «ανάγκης γνώσης – ανάγκης χρήσης»

➢ Καταγραφή ενεργειών

- Χρήση SIEM εργαλείων για καταγραφή και παρακολούθηση συμπεριφορών χρηστών και αυτόματης ανίχνευσης και αποτροπής τους.

Ως ελάχιστα διοικητικά μέτρα είναι :

➢ Θέσπιση πολιτικών και διαδικασιών ασφαλείας

➢ Ανάθεση ρόλων και διαχωρισμός αρμοδιοτήτων

➢ Έλεγχος συμμόρφωσης με κανόνες και απόδοση ευθυνών

➢ Ταχεία αναγνώριση και διερεύνηση περιστατικών και απόδοση ευθυνών

➢ Συνεχής εκπαίδευση και ενημέρωση.

Στο Υπουργείο Οικονομικών έχουν γίνει οι ακόλουθες ενέργειες:

➢ Έχει τεθεί σε ισχύ η Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών ΠΟΧΣΠ

➢ Έχει ενεργοποιηθεί δράση ευαισθητοποίησης του προσωπικού μέσω πιστοποιημένων σεμιναρίων

➢ Εφαρμόζεται η αρχή του διαχωρισμού αρμοδιοτήτων

➢ Έχει βελτιστοποιηθεί η διαδικασία αναφοράς και διερεύνησης συμβάντων

➢ Γίνονται αποτελεσματικοί εσωτερικοί έλεγχοι

6.3 Ανάλυση Εξωτερικών Απειλών

Οι εξωτερικές απειλές ουσιαστικά χωρίζονται σε 2 κατηγορίες

1. Ψάρεμα – phishing
2. Κακόβουλο λογισμικό – malware

6.3.1 Ψάρεμα

Σύμφωνα με τον Κεβιν Μίτνικ, έναν από τους μεγαλύτερους χάκερ της εποχής μας, «Είναι πολύ ευκολότερο να ξεγελάσεις κάποιον να σου δώσει έναν κωδικό πρόσβασης για ένα σύστημα από το να προσπαθήσεις να τον σπάσεις»

Το ψάρεμα που στα Αγγλικά γράφεται «phishing» είναι μία τεχνική ευρέως διαδεδομένη που σκοπό έχει να παραπλανήσει τον χρήστη και να του αποσπάσει χρήσιμες πληροφορίες με σκοπό την περαιτέρω αξιοποίηση τους με δόλιο σκοπό.

Τέτοιες πληροφορίες μπορεί να είναι τα οι κωδικοί πρόσβασης σε ένα σύστημα αλλά και προσωπικές πληροφορίες όπως αριθμοί πιστωτικών καρτών κλπ

“Ψάρεμα” είναι στην ουσία μια ηλεκτρονική παγίδα που κάποιος κακόβουλος έχει στήσει με σκοπό να αποσπάσει τα προσωπικά σου δεδομένα ή και τους μυστικούς σου κωδικούς.

Ο τρόπος που το επιτυγχάνει είναι συνήθως με τη αποστολή ανεπιθύμητης αλληλογραφίας (spam email) στο οποίο ο κακόβουλος αποστολέας ισχυρίζεται ψευδώς ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.) με σκοπό την παραπλάνηση και την παγίδευση, μέσω συνδέσμου, σε σύστημα που βρίσκεται υπό τον πλήρη έλεγχο του εγκέφαλου της απάτης.

Π.χ. ο χρήστης ενημερώνεται μέσω email από την φερόμενη «*Τράπεζά*» του ότι υπήρξε μια επίθεση και για λόγους ασφαλείας θα πρέπει να αλλάξει άμεσα τους κωδικούς του. Για «διευκόλυνσή» του υποδεικνύεται σύνδεσμος που παρουσιάζεται ως έγκυρος.[3] Σε ορισμένες μάλιστα περιπτώσεις, στα κακόβουλα μηνύματα αναφέρεται εκβιαστικά ότι εάν ο χρήστης δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων κλπ.) άμεσα, ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός είναι ο εξαναγκασμός του χρήστη στην αποκάλυψη πληροφοριών χωρίς να εξετάσει την γνησιότητα του μηνύματος.

Αν ο χρήστης παραπλανηθεί, τότε θα μεταφερθεί ηλεκτρονικά, μέσω του παγιδευμένου συνδέσμου, σε πλαστούς ιστοτόπους, πειστικά αντίγραφα υπαρκτών ιστοτόπων οργανισμών, οι οποίοι βρίσκονται υπό τον έλεγχο του κακόβουλου. Η προσωπικών δεδομένων είναι πλέον γεγονός, εφόσον ο χρήστης τα αποστείλει στην κακόβουλη ιστοσελίδα. Τέτοιου τύπου απόπειρες ψαρέματος έχουν παρατηρηθεί για τους χρήστες του taxisnet!

Χρειάζεται ιδιαίτερη προσοχή, ώστε ο παραλήπτης ενός τέτοιου μηνύματος να αποφύγει την εξαπάτηση μέσω Phishing. Υπογραμμίζεται ότι τα κακόβουλα email συντάσσονται αρκετά πειστικά και οι πλαστές σελίδες τις περισσότερες φορές είναι πανομοιότυπες με τις πραγματικές, αφού δημιουργούνται με αντιγραφή του HTML κώδικά

Οι τρόποι εξαπάτησης είναι πολλοί και πρέπει πάντα ο χρήστης να βρίσκεται σε εγρήγορση.

6.3.1.1 Τρόποι προφύλαξης από το Phishing

Πρέπει να είμαστε γενικά καχύποπτοι και να μην απαντάμε σε μηνύματα ηλεκτρονικού ταχυδρομείου που ζητούν να αποκαλύψουμε αξιοποιήσιμα προσωπικά στοιχεία οικονομικού χαρακτήρα. Οι αξιόπιστες εταιρείες δεν συνηθίζουν να ζητούν από τους πελάτες τους να ενημερώσουν ή να επαληθεύσουν τέτοια απόρρητα στοιχεία με ένα απλό email.

Ακόμη και σε περιπτώσεις που όλα δείχνουν ότι το μήνυμα είναι γνήσιο, είναι προτιμότερο να επικοινωνήσουμε με την εταιρία που παρουσιάζεται ως αποστολέας, για να επιβεβαιωθεί ότι πράγματι αυτή έστειλε το μήνυμα και ότι δεν πρόκειται για περίπτωση απάτης. Τονίζεται ότι η επικοινωνία με την εν λόγω εταιρεία επιβάλλεται να πραγματοποιηθεί με τον προβλεπόμενο καθιερωμένο τρόπο και όχι σύμφωνα με τις φερόμενες οδηγίες που περιέχει το κακόβουλο email.

Πριν προβούμε στην παραχώρηση ευαίσθητων προσωπικών πληροφοριών μέσω του διαδικτύου προσέχουμε την ηλεκτρονική διεύθυνση στην οποία βρισκόμαστε: Αντί για το απλό «http://», θα πρέπει να αρχίζει με «**https://».** Έτσι διασφαλίζεται η χρήση ασφαλούς σύνδεσης Web (http secure).

Επίσης, χρειάζεται μεγάλη προσοχή σε ηλεκτρονικά μηνύματα που λαμβάνουμε από άγνωστες πηγές και κατά συνέπεια συστήνεται η αποφυγή συμπλήρωσης ηλεκτρονικών φορμών οι οποίες παραλαμβάνονται μέσω ηλεκτρονικού ταχυδρομείου.

---

3 Για την προστασία του χρήστη, επισημαίνεται ότι η πραγματική διεύθυνση στην οποία ανακατευθύνει ο παγιδευμένος σύνδεσμος αποκαλύπτεται με ένα απλό πέρασμα του ποντικιού πάνω από τον τελευταίο.

Πολλά μηνύματα Phising οδηγούν σε διαδικτυακές τοποθεσίες με σκοπό την εγκατάσταση στον υπολογιστή του θύματος κατασκοπευτικό λογισμικό (spywares), το οποίο καταγράφει κάθε πληροφορία που εισάγει ο χρήστης (όπως αριθμούς λογαριασμών, πιστωτικών καρτών και κωδικούς πρόσβασης). Η καταγραφή πιθανότατα συνεχίζεται για πολύ καιρό μετά την αποχώρηση του χρήστη από τον συγκεκριμένο διαδικτυακό τόπο. Παρόλο που τα προγράμματα κατά των ηλεκτρονικών ιών (antivirus) δεν μπορούν να αποτρέψουν το άνοιγμα ενός πλαστού ηλεκτρονικού μηνύματος, μπορούν εντούτοις να προστατεύσουν από ιούς ή λογισμικά υποκλοπής (spyware) που θα προέλθουν από τέτοιες ενέργειες. Συστήνεται η εγκατάσταση ενημερωμένου λογισμικού προστασίας από ιούς (antivirus) στον σταθμό εργασίας του χρήστη.

6.3.2 Κακόβουλο Λογισμικό

Πρόκειται για προγράμματα (κώδικας) τα οποία αποσκοπούν σε παραβίαση μίας ή περισσοτέρων εκ των αρχών ασφαλείας και συγκεκριμένα της Εμπιστευτικότητα, της Ακεραιότητα και της Διαθεσιμότητας των πληροφοριακών συστημάτων. Οι επιθέσεις αυτές προέρχονται από τρίτους με σκοπό την υποκλοπή ή καταστροφή των δεδομένων και σε πολλές περιπτώσεις την χρήση του υπολογιστή ως βάσης για περαιτέρω επιθέσεις σε άλλους υπολογιστές στο ίδιο δίκτυο. Οι επιτιθέμενοι εκμεταλλεύονται διάφορα μικρά ή μεγάλα κενά ασφαλείας για την εκτέλεση του κακόβουλου λογισμικού τους.

Για την εγκατάσταση (μόλυνση) ενός κακόβουλου λογισμικού σε έναν Η/Υ, συνήθως απαιτείται η ανθρώπινη συμμετοχή: άμεση (π.χ. ανταλλαγή αρχείων, άνοιγμα συνημμένων ή προεπισκόπηση μηνυμάτων αλληλογραφίας αμφιβόλου προέλευσης) ή έμμεση (ανεπαρκής προστασία του υπολογιστή, μη λήψη ενημερωμένων εκδόσεων – updates του λογισμικού ασφαλείας και των προγραμμάτων).

Εκτός από τις παρενέργειες, το κακόβουλο λογισμικό περιλαμβάνει επιπλέον κώδικα με σκοπό την:

- Αναπαραγωγή του: Εξάπλωση του στο σύστημα που προσβάλλει («μόλυνση» από πρόγραμμα σε πρόγραμμα).
- Μετάδοση του: Εξάπλωση του από το σύστημα που μολύνθηκε σε άλλο/άλλα συστήματα (π.χ. από Η/Υ σε Η/Υ).

Όλα τα είδη κακόβουλου λογισμικού έχουν ορισμένα κοινά χαρακτηριστικά. Για παράδειγμα, ένα κακόβουλο λογισμικό συνήθως προσπαθεί:

1. Να εγκατασταθεί στην κατάλληλη περιοχή, ώστε να εκτελείται μια φορά, συχνά ή πάντα. Η πλέον συνήθης τακτική είναι η δημιουργία μιας εγγραφής στο μητρώο του συστήματος, π.χ. στη θέση HKLM\Software\Microsoft\Windows\CurrentVersion\Run
2. Να εγκατασταθεί στην κατάλληλη περιοχή ώστε η εκτέλεση του να μην είναι ανιχνεύσιμή,
3. Να εγκατασταθεί στην κατάλληλη περιοχή ώστε η αφαίρεση του να είναι δύσκολη.

6.3.2.1 Κατηγοριοποίηση & Παρενέργειες Κακόβουλων Προγραμμάτων

Τα κακόβουλα λογισμικά κατηγοριοποιούνται ως ακολούθως:

- **Ιός** (virus). Κακόβουλο λογισμικό το οποίο αφού μολύνει έναν Η/Υ και έχει την ικανότητα να αναπαράγεται και να μολύνει άλλα προγράμματα στον Η/Υ-ξενιστή. Η μετάδοση του σε άλλους Η/Υ μπορεί να γίνεται αυτόματα (να έχει δηλαδή τα χαρακτηριστικά ενός Σκουληκιού – Worm) ή να απαιτεί ανθρώπινη παρέμβαση

(π.χ.αντιγραφή ενός αρχείου σε USB flash disk και άνοιγμα του αρχείου σε κάποιον Η/Υ).

- **Σκουλήκι** (Worm). Κακόβουλο λογισμικό το οποίο, αφού μολύνει έναν Η/Υ, έχει την ικανότητα να μεταδίδεται αυτόματα, κάνοντας χρήση της υπάρχουσας δικτυακής υποδομής (π.χ. τοπικά δίκτυα - δίκτυα WAN) ή/και των υπηρεσιών του Internet (IRC chat, e-mail, newsgroups, κ.λ.π).

- **Δούρειοι Ίπποι (Trojan Horses)**. Κακόβουλο λογισμικό στο οποίο είναι εγγενές το στοιχείο της παραπλάνησης, καθώς συνήθως μεταμφιέζεται σε μια (καθ' όλα) χρήσιμη εφαρμογή, η οποία όμως περιέχει κακόβουλο κώδικα. Στην πιο κλασσική των περιπτώσεων, ένα Trojan δημιουργεί μια *κερκόπορτα* (backdoor) στο σύστημα, στην οποία ο επιτιθέμενος θα μπορέσει αργότερα να συνδεθεί ώστε να διαχειριστεί εξ' αποστάσεως το σύστημα. Τις περισσότερες φορές τα trojans δεν έχουν μολυσματικό χαρακτήρα, δηλαδή δεν αναπαράγονται και για αυτό το λόγο δεν χαρακτηρίζονται επισήμως ως ιοί.

- **Spyware – Adware**. Κακόβουλο λογισμικό με χαρακτηριστικά προσομοιάζουν αυτά ενός Δούρειου Ίππου (κυρίως ως προς τον τρόπο μόλυνσης), με σκοπό την παρακολούθηση - υποκλοπή ευαίσθητων δεδομένων (spyware), ή την αποστολή ανεπιθύμητων διαφημιστικών μηνυμάτων (adware). Αναφέρονται ως μέλη της ίδιας κατηγορίας, καθώς συνήθως συνεργάζονται για να πετύχουν τον σκοπό τους (π.χ. παρακολούθηση της αγοραστικής συμπεριφοράς κατά την περιήγηση στο Web και στη συνέχεια αποστολή-εμφάνιση διαφημιστικών μηνυμάτων).

- **Rootkits**. Όπως φαίνεται από την ονομασία τους, ένα rootkit είναι κακόβουλο λογισμικό το οποίο λειτουργεί σε πολύ χαμηλό επίπεδο στο λειτουργικό σύστημα, και συνήθως ενσωματώνει *λειτουργίες απόκρυψης* ώστε να παρακάμπτει τους μηχανισμούς πρόληψης και ανίχνευσης, όπως firewalls και antivirus. Ένα λογισμικό rootkit μπορεί να ανήκει σε οποιαδήποτε από τις ως άνω κατηγορίες, ωστόσο συνήθως ανοίγει κερκόπορτες (backdoors) που θα επιτρέψουν τη μετέπειτα απομακρυσμένη διαχείριση του ξενιστή από κάποιον τρίτο.

- **Bots – zombies**. Κακόβουλο λογισμικό που προσβάλλει Η/Υ καθιστώντας τους μέλη ενός δικτύου Η/Υ (botnet) που ελέγχεται εξ' αποστάσεως από τρίτους, με σκοπό την πραγματοποίηση *Κατανεμημένων Επιθέσεων Άρνησης Εξυπηρέτησης* (DDOS attacks), δηλαδή επιθέσεων κατά τις οποίες ένας (συνήθως μεγάλος) αριθμός μολυσμένων υπολογιστών προσπαθεί να συνδεθεί στον Η/Υ-στόχο μέσω δικτύου. Ένας Η/Υ που έχει μολυνθεί από ένα bot συχνά αναφέρεται ως «*zombie*». Οι Η/Υ – zombies μπορεί να χρησιμοποιηθούν για επιθέσεις DOS σε εξυπηρετητές Web, για την αποστολή μηνυμάτων spam, για την πραγματοποίηση επιθέσεων παραπλάνησης (phishing) κ.λπ.

6.3.2.2 Πως μεταδίδεται το κακόβουλο λογισμικό

Οι κυριότεροι τρόποι μετάδοσης κακόβουλου λογισμικού, με σειρά κρισιμότητας, είναι:

- μέσω της ηλεκτρονικής αλληλογραφίας **email**,
- μέσω επίσκεψης σε «περίεργους» συνδέσμους **διαδικτύου**,
- μέσω χρήσης μη έμπιστων **φορητών μέσων αποθήκευσης**

Η πιο συνηθισμένη και πιο επικίνδυνη περίπτωση είναι η λήψη **email** από ένα άγνωστο ή «περίεργο» αποστολέα, η οποία αναφέρει οδηγίες όπως: «παρακαλώ βρείτε συνημμένο το τιμολόγιο για την παραγγελία σας», «ανοίξτε το συνημμένο να δείτε το ταξίδι που κερδίσατε» κοκ. Το επισυναπτόμενο αρχείο μπορεί να είναι σε μορφή συμπιεσμένου

αρχείου (zip) είτε σε μορφή αρχείου κειμένου word ή pdf. Η βιασύνη ή η απλή περιέργεια του χρήστη, τον οδηγούν αρκετές φορές στο άνοιγμα του επισυναπτόμενου αρχείου με συνέπεια την εκτέλεση του κακόβουλου λογισμικού, το οποίο δύναται να μην εντοπιστεί από το αντιιικό λογισμικό του υπολογιστή.

Μια ακόμα συνήθης τακτική είναι η ενθάρρυνση, από πλευράς του κακόβουλου, ο αποστολέας να ανοίξει μια «περίεργη» ιστοσελίδα μέσω παγιδευμένου συνδέσμου. Η προβολή (άνοιγμα) της ιστοσελίδας από τον φυλλομετρητή (browser) στον υπολογιστή του θύματος έχει ως συνέπεια την εκτέλεση κακόβουλου λογισμικού. Αυτό συμβαίνει κυρίως γιατί ο επιτιθέμενος έχει ανακαλύψει μια «τρύπα» στο λογισμικό του φυλλομετρητή από όπου εκτελεί λογισμικό του.

Τέλος ένα ακόμα σενάριο μετάδοσης είναι να συνδέσουμε στον υπολογιστή μας **φορητό μέσο αποθήκευσης** από μη έμπιστη πηγή και να εκτελεστεί κακόβουλο λογισμικό που είναι «κρυμμένο» στο μέσο αυτό, χωρίς να γίνει αντιληπτό από το αντιιικό λογισμικό του υπολογιστή σου.

6.3.3 Η εξέλιξη του κακόβουλου λογισμικού

Όταν το κακόβουλο λογισμικό εμφανίστηκε για πρώτη φορά, εξυπηρέτησε έναν απλό σκοπό να προκαλέσει βλάβη χωρίς οικονομικό όφελος: η διαγραφή των αρχείων, η μετονομασία των δεδομένων ή η διαγραφή δεδομένων από τα μέσα αποθήκευσης («κυβερνο-βανδαλισμός»). Αν και οι ιοί εκτελούνται κρυφά, το θύμα μπορεί μερικές φορές να τους «αισθανθεί», καθώς ο υπολογιστής γίνεται πιο αργός ή σύνδεση στο διαδίκτυο γίνεται πιο αργή ή «κολλάει».

Σήμερα, η συντριπτική πλειοψηφία του κακόβουλου λογισμικού έχει δημιουργηθεί για την αποκόμιση παράνομου χρήματα, συχνά με τη συλλογή εμπιστευτικών δεδομένων από τον υπολογιστή του θύματος. Το κακόβουλο λογισμικό έχει σχεδιαστεί να εγκαθίσταται όσο πιο διακριτικά γίνεται και να εκτελείται χωρίς να διαταράσσει τη λειτουργία του μηχανήματος του θύματος. Ένα κατεστραμμένο μηχάνημα δεν έχει καμία αξία για τους εγκληματίες του κυβερνοχώρου, αλλά ένα μολυσμένο μηχάνημα αποτελεί ένα ισχυρό εργαλείο που είναι σε θέση να εκτελεί διάφορες εργασίες χωρίς να το γνωρίζει ο χρήστης.

Ο παράνομος χαρακτήρας των δραστηριοτήτων του εγκλήματος στον κυβερνοχώρο καθιστά αδύνατη την απόκτηση μιας ακριβούς εικόνας για το πόσα χρήματα αποκομίζονται από αυτές τις δραστηριότητες, υπάρχουν, όμως, διάφορες εκτιμήσεις που κυμαίνονται από εκατομμύρια σε εκατοντάδες δισεκατομμύρια ευρώ. Σίγουρο είναι ότι ο αυξανόμενος όγκος των επιθέσεων καθιστά σαφές ότι η «σκοτεινή αγορά» του εγκλήματος στον κυβερνοχώρο είναι εξαιρετικά επικερδής.

Εδώ και μια δεκαετία γίνονται τυχαίες, κερδοσκοπικές επιθέσεις σε όποιον έχει την ατυχία να μολυνθεί. Ωστόσο, ο αριθμός των στοχευμένων επιθέσεων αυξάνεται. Τέτοιες επιθέσεις συνήθως στοχεύουν σε επιχειρήσεις.

6.3.4 Κακόβουλο λογισμικό τύπου Ransomware (λυτρισμικό)

Το κακόβουλο λογισμικό τύπου ransomware (CTB-locker, CryptoWall, Wannacry κ.λπ.) κρυπτογραφεί τα αρχεία του χρήστη, ώστε το θύμα να εξαναγκαστεί στην καταβολή λύτρων στον θύτη για την αποκρυπτογράφηση και την εκ νέου πρόσβαση στα αρχεία του. Αποτελεί αυτή τη στιγμή *την πιο επικίνδυνη* και την πιο διαδεδομένη μορφή κακόβουλου λογισμικού.

Το πιο συνηθισμένο σενάριο είναι το ακόλουθο: εμφανίζεται απροσδόκητα ένα παράθυρο στην οθόνη του χρήστη, όπου τον ενημερώνει ότι τα αρχεία του είναι κλειδωμένα και ότι για να παραλάβει τον κωδικό ξεκλειδώματος πρέπει να πληρώσει κάποιο χρηματικό ποσό! Αυτό που κατά πάσα πιθανότητα έχει συμβεί είναι ότι με κάποιο τρόπο έχει εγκατασταθεί

κακόβουλο λογισμικό το οποίο ψάχνει σε όλους τους δίσκους του υπολογιστή μας - ακόμα και τους κοινόχρηστους δικτυακούς! - να βρει αρχεία με κατάληξη doc, xls, jpg, ppt καθώς και τα email, και τα κρυπτογραφεί με κωδικό που μόνο ο επιτιθέμενος γνωρίζει. Στην πραγματικότητα, το θύμα αν δε διαθέτει εφεδρικό αντίγραφο των αρχείων του σε κάποιο εξωτερικό αποθηκευτικό μέσο, έχει χάσει όλα τα αρχεία του! Πρέπει να σημειωθεί, ότι και σε περίπτωση καταβολής του ζητηθέντος ποσού, δεν παρέχεται σε καμία περίπτωση ουσιαστική εγγύηση για την πλήρη αποκατάσταση των αρχείων.

Το σημαντικότερο μέτρο πρόληψης για αυτόν τον κίνδυνο είναι **η λήψη αντιγράφου ασφαλείας** των σημαντικών αρχείων του υπολογιστή **ανά τακτά χρονικά διαστήματα** σε εξωτερικό αποθηκευτικό μέσο σύμφωνα με τις οδηγίες που έχουν δοθεί με επίσημο σχετικό έγγραφο της Διεύθυνσης Διαχείρισης Υπολογιστικών Υποδομών (https://testintranet.ggps.gsis/browserInstall.htm).

ΠΡΟΣΟΧΗ: Σύμφωνα με την Πολιτική Ορθής Χρήσης (βλέπε 4.3.2 Κανόνες Ασφάλειας), αντιγραφή υπηρεσιακών δεδομένων σε εξωτερικό αποθηκευτικό μέσο επιτρέπεται ΜΟΝΟ με χρήση κρυπτογραφημένων αρχείων zip με password.

6.3.4.1 Παρενέργειες

Οι παρενέργειες εκτέλεσης ενός κακόβουλου λογισμικού ποικίλλουν, ενδεικτικά αναφέρουμε τα εξής :

• Ενοχλητικά μηνύματα, διαφημίσεις κ.λπ. (σχετική κατηγορία: adware)

• Επιθέσεις Διακοπής, Αλλοίωσης, Εισαγωγής (σχετικές κατηγορίες: Ιοί, worms)

- διαγραφή ή αλλοίωση δεδομένων, εφαρμογών και αρχείων συστήματος
- αντιγραφή αρχείων στο τοπικό δίκτυο (μετάδοση μέσω κοινής χρήσης αρχείων) ή στο Internet (για μετάδοση μέσω των προγραμμάτων P2P)
- αναστολή λειτουργίας ή δυσλειτουργία του λειτουργικού συστήματος
- Καταστροφή των τομέων εκκίνησης (boot sectors)

• Δημιουργία «κερκόπορτας» (back door) με σκοπό την σε δεύτερο χρόνο παραβίαση της ασφάλειας του συστήματος (σχετικές κατηγορίες: trojans, rootikits, zombies)

• Επιθέσεις εναντίον της διαθεσιμότητας συστημάτων (σχετικές κατηγορίες: worms, bots- zombies)

- Κατανάλωση υπολογιστικών πόρων (κύρια μνήμη, αποθηκευτικός χώρος)
- Κατανάλωση της χωρητικότητας (bandwidth) του δικτύου
- Χρήση των ξενιστών για συγχρονισμένη επίθεση σε κάποιον τρίτο, στα πλαίσια μιας επίθεσης DDOS (Distributed DOS).

6.4 Ενδείξεις ώστε να καταλάβουμε ότι «κάτι έχουμε κολλήσει»

Στις μέρες μας δυστυχώς δεν είναι εύκολα αντιληπτό αυτό, κυρίως λόγω της εξέλιξης των κακόβουλων λογισμικών. Συνήθως το καταλαβαίνουμε ενώ είναι πλέον αργά. Σε πολλές περιπτώσεις όμως ένας εκπαιδευμένος και ευαισθητοποιημένος χρήστης μπορεί να καταλάβει ότι κάτι δε πάει καλά, όπως για παράδειγμα:

- Ο υπολογιστής κάνει υπερβολικά πολύ ώρα να ανοίξει.
- Ο υπολογιστής έχει γίνει ασυνήθιστα αργός παρόλο που δεν τρέχουν πολλές εφαρμογές ή πολλά παράθυρα φυλλομετρητή.

- Τα αρχεία (έγγραφα, εικόνες) εμφανίζονται με διαφορετικό εικονίδιο από το συνηθισμένο είτε δεν εμφανίζονται καν είτε φαίνονται με «κινέζικους» χαρακτήρες.
- Έχει εμφανιστεί μια περίεργη ειδοποίηση ότι τα αρχεία είναι κλειδωμένα και ότι για να ανοίξουν πρέπει να επισκεφτούμε μια ιστοσελίδα (πολύ αργά ίσως για τα αρχεία μας!).

6.5 Τι κάνουμε αν πέσουμε θύματα κακόβολου λογισμικού;

Λόγω του ότι τέτοια λογισμικά είναι καθαρά θέμα χρόνου να κάνουν οποιαδήποτε ζημιά και επιπλέον να εξαπλωθούν γρήγορα και σε άλλους διασυνδεδεμένους υπολογιστές εκτός του δικού μας, είναι πολύ σημαντικό να αντιδράσουμε άμεσα, κάνοντας τα εξής:

1. Κλείνουμε τον υπολογιστή - κατά προτίμηση κρατάμε το κουμπί έναρξης (power) πατημένο μέχρι να σβήσει.
2. Αποσυνδέουμε το καλώδιο δικτύου του υπολογιστή.
3. Αν εμφανίζεται μήνυμα ότι τα αρχεία έχουν κρυπτογραφηθεί (βλέπε την πιο πάνω εικόνα), καλούμε άμεσα στο **2104803218**. Σε κάθε περίπτωση και για λόγους καταγραφής του συμβάντος στέλνουμε email στη διεύθυνση virusalert@gsis.gr αναφέροντας οποιαδήποτε πληροφορία σχετικά με το πρόβλημα και απαραίτητα τα στοιχεία επικοινωνίας καθώς και την οργανική μονάδα μας (πιθανώς να χρειαστεί η βοήθεια συναδέλφου εφόσον ο υπολογιστής μας θα είναι αποσυνδεδεμένος).

Σημείωση: Σε πολλές περιπτώσεις η άμεση αναφορά και αντιμετώπιση του προβλήματος μπορεί να προλάβει την καταστροφή των δεδομένων. Υπάρχουν για παράδειγμα και περιπτώσεις που έχει ανακαλυφθεί τρόπος αποκρυπτογράφησης με χρήση εξειδικευμένων εργαλείων.

6.6 Μέτρα προστασίας

Η υπηρεσία μεριμνά ώστε να εγκαθίστανται στον υπολογιστή μας οι τελευταίες ενημερώσεις λογισμικού (BIOS updates, OS patches, application patches) του υπολογιστή, καθώς και στο εγκατεστημένο αντιικό σύστημα να είναι εγκατεστημένες οι τελευταίες διαθέσιμες ενημερώσεις, ώστε να προλάβει πολλές από τις επιθέσεις αυτές. Δυστυχώς δεν είναι πάντα εφικτό να προστατευτεί κάποιος μόνο επειδή διαθέτει ενημερωμένο σύστημα με ενημερωμένο αντιικό λογισμικό, για αυτό και χρειάζεται εγρήγορση και προσοχή!

Από την πλευρά μας ως χρήστες ηλεκτρονικών υπολογιστών και υπηρεσιών (mail, internet κ.λπ.), ο μόνος σίγουρος τρόπος προστασίας είναι η πιστή εφαρμογή των οριζόμενων στην ισχύουσα Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών, ιδίως της παραγράφου «**4.4 Χρήση Διαδικτύου / Ηλεκτρονικού Ταχυδρομείου**».

Με άλλα λόγια:

- ✓ Δεν ανοίγουμε email από άγνωστο αποστολέα ή με ύποπτο ή «περίεργο» τίτλο ή σε περίπτωση που δε μας αφορά προσωπικά / υπηρεσιακά.
- ✓ Δεν ανοίγουμε ύποπτα συνημμένα αρχεία ιδίως αν έχουν ύποπτα ονόματα (πχ τιμολόγιο, invoice, voucher, ticket) και «φαίνεται» να είναι γνωστών τύπων zip, pdf, jpg, doc, xls.
- ✓ Δεν ενεργοποιούμε τις μακροεντολές (macro) σε αρχεία office (doc, xls) από μη έμπιστες πηγές (εκτός υπηρεσίας), εκτός και αν είμαστε απόλυτα σίγουροι για τον αποστολέα τους.

- ✓ Δεν ανοίγουμε ύποπτους συνδέσμους (link) και σε καμία περίπτωση δεν εισάγουμε προσωπικά δεδομένα σε ύποπτες ιστοσελίδες. Συστήνεται να πληκτρολογούνται οι διευθύνσεις των ιστοσελίδων (URL) στον φυλλομετρητή (browser), αντί να χρησιμοποιούνται υπερ- σύνδεσμοι (links).
- ✓ Δίνουμε αυξημένη προσοχή στις περιπτώσεις σύνδεσης εξωτερικών φορητών μέσων αποθήκευσης στον υπολογιστή. Αν δεν υπάρχει διαβεβαίωση προέλευσης δεν τα συνδέουμε σε καμία περίπτωση.
- ✓ Σε καμία περίπτωση δεν κάνουμε οποιαδήποτε απόπειρα απεγκατάστασης του αντιικού λογισμικού του υπολογιστή.
- ✓ Δεν εγκαθιστούμε λογισμικό πέραν του προεγκατεστημένου στον υπολογιστή, παρά μόνο με την έγκριση της Διεύθυνσης Διαχείρισης Υπολογιστικών Υποδομών.
- ✓ Εφόσον υπάρχουν κρίσιμα αρχεία στον υπολογιστή μας, φροντίζουμε για την ασφαλή αποθήκευσή τους σε φορητά αποθηκευτικά μέσα ή συμβουλευόμαστε τον προϊστάμενό μας για εξεύρεση άλλης εγκεκριμένης λύσης.
- ✓ Σε περίπτωση υποψίας ότι συμβαίνει κάτι περίεργο στον υπολογιστή μας, το αναφέρουμε άμεσα, έτσι προστατεύουμε και τους συναδέλφους και το υπηρεσιακό δίκτυο από εξάπλωση.

7 Κωδικοί Πρόσβασης

7.1 Γενικά

Οι έλεγχοι πρόσβασης βοηθούν στο να περιορίσουμε την πρόσβαση σε πληροφοριακά συστήματα και δεδομένα και γενικότερα να ελέγξουμε το είδος της πρόσβασησ που ο κάθε χρήστης έχει στους πληροφοριακούς πόρους.

Οι έλεγχοι πρόσβασης διαθέτουν τέσσερις γενικές λειτουργίες:

- επαλήθευση ταυτότητας (identity verification),
- έλεγχο ταυτότητας (authentication),
- εξουσιοδότηση (authorization) και
- λογοδοσία/ευθύνη (accountability).

Οι προαναφερόμενες διαδικασίες λειτουργούν από κοινού για να παρέχουν ασφαλή πρόσβαση στους πόρους και να καθορίζουν τι μπορεί να κάνει ο χρήστης με αυτούς.

Η διαχείριση ταυτότητας (Identity Management) αποτελείται από μία ή περισσότερες διαδικασίες που στοχεύουν στην επαλήθευση της ταυτότητας ενός ατόμου που επιχειρεί να αποκτήσει πρόσβαση σε ένα πληροφοριακό αγαθό. Η διαχείριση ταυτότητας και ο έλεγχος ταυτότητας είναι αδιαχώριστα:

- Η διαχείριση ταυτότητας περιλαμβάνει την εκχώρηση και τη διαχείριση της ταυτότητας ενός ατόμου.
- Ο έλεγχος ταυτότητας είναι η διαδικασία επαλήθευσης της ταυτότητας ενός ατόμου κατά τη πρόσβαση σε κάποιο αγαθό/πόρο.

7.2 Ορισμός Ταυτότητας

Ένα από τα βασικά εργαλεία επικοινωνίας στον ψηφιακό κόσμο είναι η ταυτότητα κατ' αντιστοιχία με το φυσικό κόσμο.

Ταυτότητα στο φυσικό κόσμο μπορούν να αποτελέσουν:

- Η αστυνομική ταυτότητα (γενική χρήση)
- Το διαβατήριο (για ταξίδια στο εξωτερικό)
- Η κάρτα Ανάληψης (πρόσβαση σε τραπεζικό λογαριασμό)
- Η άδεια Οδήγησης (οδήγηση)

Ταυτότητα στον ηλεκτρονικό κόσμο μπορούν να αποτελέσουν:

- Το **Όνομα Χρήστη** (username) και ο **Κωδικός Πρόσβασης** (password)
- Το **Ψηφιακό Πιστοποιητικό** (digital certificate)
- Το **Βιομετρικό Σύστημα** (biometrics)
- Ο **Συνδυασμός** δύο ή περισσοτέρων από τα παραπάνω (multi-factor authentication)

Μια καλή ηλεκτρονική ταυτότητα είναι κάτι που είναι επαληθεύσιμο, δύσκολο να αναπαραχθεί και εύκολο στη χρήση (μια δύσκολη στη χρήση ταυτότητα είναι σχεδόν βέβαιο ότι δεν θα χρησιμοποιηθεί).

7.2.1 Όνομα χρήστη και κωδικός πρόσβασης

Η πρόσβαση σε ένα σύστημα περιλαμβάνει τη χρήση ενός **ονόματος χρήστη** και ενός **κωδικού πρόσβασης**, τα οποία, αν εισαχθούν σωστά, θα επιτραπεί η πρόσβαση στο σύστημα. Για πολλά χρόνια, αυτή ήταν η κύρια μέθοδος ελέγχου ταυτότητας. Ωστόσο:

- Η συγκεκριμένη μορφή επαλήθευσης αποτελεί μια ασθενή μορφή επαλήθευσης αν η μεταφορά του κωδικού πρόσβασης γίνει από ένα μη κρυπτογραφημένο κανάλι. Η **μη κρυπτογραφημένη** μορφή επιτρέπει σε κάποιον που παρακολουθεί τη σύνδεση, χρησιμοποιώντας τεχνολογία **sniffing**, να **υποκλέψει** εύκολα το όνομα χρήστη και το κωδικό πρόσβασης και στη συνέχεια να τα χρησιμοποιήσει για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα.
- Ένας εύκολος στη χρήση κωδικός πρόσβασης δύναται να γίνει εύκολος και στην αναπαραγωγή. Οποιαδήποτε πληροφορία που μπορεί εύκολα κάποιος να μαντέψει ή να κλέψει δεν είναι επαρκώς ασφαλής.

Ακόμη και με τη κρυπτογράφηση, η προσέγγιση χρήσης ονόματος χρήστη και κωδικού πρόσβασης για τον έλεγχο ταυτότητας έχει πολλές εγγενείς αδυναμίες:

- **ταυτοποιεί** μόνο το λογαριασμό και δεν κάνει τίποτα για να επαληθεύσει ότι το άτομο που χρησιμοποιεί το λογαριασμό είναι εξουσιοδοτημένος χρήστης. Ως εκ τούτου, αν το όνομα χρήστη και ο κωδικός πρόσβασης πέσουν σε λάθος χέρια ο έλεγχος ταυτότητας δεν θα έχει κανέναν τρόπο να γνωρίζει ότι λάθος άτομο έχει αποκτήσει πρόσβαση (*πολλοί χρήστες έχουν το όνομα χρήστη και το κωδικό τους γραμμένο σε ένα κομμάτι χαρτί κολλημένο στην οθόνη τους*).
- η ασφάλεια ονόματος χρήστη και κωδικού πρόσβασης σχετίζεται με την **επιλογή** του κωδικού πρόσβασης. Υπάρχει αυξημένη πιθανότητα ένα σύστημα που χρησιμοποιεί **password cracking technology** να «**μαντέψει**» έναν ασθενή κωδικό πρόσβασης. Το συγκεκριμένο πρόβλημα μετριάζεται μέσω της εφαρμογής αυστηρών κανόνων για τους κωδικούς πρόσβασης, με τους οποίους οι χρήστες εμποδίζονται να δημιουργούν αδύναμους κωδικούς πρόσβασης, καθώς και με την απενεργοποίηση/κλείδωμα ενός λογαριασμού μετά από έναν καθορισμένο αριθμό προσπαθειών εισαγωγής μη έγκυρου κωδικού πρόσβασης.

Καθώς, οι κωδικοί πρόσβασης θεωρούνται αδύναμες μορφές διαχείρισης ταυτότητας είναι ακατάλληλοι/ανεπαρκείς όταν η πρόσβαση αφορά σ' ευαίσθητες πληροφορίες.

7.2.2 Πιστοποιητικά

Η ασφάλεια πιστοποιητικού παρέχει ένα μηχανισμό για την επίτευξη κρυπτογραφημένων επικοινωνιών μέσω μη ασφαλών δικτύων και βασίζεται στην υποδομή δημόσιου κλειδιού (Public Key Infrastructure). Τα πιστοποιητικά χρησιμοποιούν ασύμμετρη κρυπτογράφηση, με την οποία χρησιμοποιούνται διαφορετικά κλειδιά για τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης (βλ. Κεφάλαιο Δέκατο). Πιο συγκεκριμένα, κατά την κρυπτογράφηση δημόσιου κλειδιού απαιτούνται δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό, τα οποία ένας χρήστης αποκτά μέσω μιας Αρχής Πιστοποίησης (CA) –αξιόπιστο τρίτο μέρος.

7.2.3 Βιομετρία

Παλαιοτέρα η βιομετρία περιοριζόταν στις κατασκοπευτικές ταινίες του 1970, όπου το δάχτυλο ή ο αμφιβληστροειδής ενός ατυχούς κυβερνητικού υπαλλήλου χρησιμοποιείτο από κακούς κατασκόπους για να σαρωθεί και να επιτραπεί η πρόσβαση σε μια ασφαλή περιοχή. Πλέον η βιομετρία είναι πραγματικότητα.

Η βιομετρία περιλαμβάνει τη χρήση μέρους του σώματος ενός ατόμου ως μορφή αναγνώρισης. Οι πιο συνηθισμένες συσκευές για το σκοπό αυτό είναι οι σαρωτές

δακτυλικών αποτυπωμάτων (περιλαμβάνονται ακόμη και σε ορισμένα μοντέλα φορητών υπολογιστών), οι οποίοι αρνούνται την πρόσβαση σε ένα σύστημα μέχρι να σαρωθεί το κατάλληλο δακτυλικό αποτύπωμα. Άλλες πιθανές δυνατότητες βιομετρικής αναγνώρισης περιλαμβάνουν σαρώσεις αμφιβληστροειδούς και αναγνώριση φωνής.

7.2.4 Έλεγχος ταυτότητας πολλαπλών παραγόντων (Multi-Factor Authentication)

Η συγκεκριμένη μέθοδος ελέγχου (MFA) χρησιμοποιεί:

- Κάτι που ο χρήστης **ξέρει**
- Κάτι που ο χρήστης **έχει**
- Κάτι που ο χρήστης **είναι**

Στα παραδείγματα για «κάτι που ο χρήστης ξέρει» περιλαμβάνονται οι κωδικοί πρόσβασης και το PIN. Στα παραδείγματα για «κάτι που ο χρήστης έχει» περιλαμβάνονται η έξυπνη κάρτα και το πιστοποιητικό που έχει εκδοθεί από αξιόπιστο τρίτο μέρος. Τέλος, τα βιομετρικά στοιχεία (δακτυλικά αποτυπώματα, χαρακτηριστικά προσώπου, μοτίβα φλεβών, κλπ.) παρέχουν πληροφορίες για «κάτι που ο χρήστης είναι». Χρησιμοποιώντας δύο από τους προαναφερόμενους παράγοντες ελέγχου αυξάνεται σημαντικά η πιθανότητα σωστής επαλήθευσης ταυτότητας.

7.3 Γιατί χρειάζεται η Ηλεκτρονική Ταυτότητα

Η χρήση της ηλεκτρονικής ταυτότητας είναι απαραίτητη για να προστατεύσει τα Πληροφοριακά Αγαθά.

Αναλυτικότερα , με τη χρήση της ηλεκτρονικής ταυτότητας το Πληροφοριακό Αγαθό πρέπει:

- Να μπορεί να αναγνωρίζει τον χρήστη.
- Να επιτρέπει πρόσβαση σε δεδομένα που δικαιούται ο χρήστης να δει, να μεταβάλλει, να συλλέξει και να επεξεργαστεί.
- Να προστατεύει από μη εξουσιοδοτημένα άτομα.
- Να προστατεύει τα δεδομένα-υποθέσεις-ενέργειες του χρήστη από άλλους χρήστες.
- Να μπορεί να καταγράφει τις ενέργειές του χρήστη για λόγους ασφάλειας (εντοπισμός λαθών, παραβίαση ή απόπειρα παραβίασης, απόδοση ευθυνών).

Η ηλεκτρονική ταυτότητα πρέπει να είναι εύχρηστη και αντίστοιχης πολυπλοκότητας με το αγαθό το οποίο προστατεύει. Μια λύση που παρέχει σχεδόν απόλυτη ασφάλεια αναφορικά με την ταυτοποίηση ενός υποκειμένου, αλλά είναι εξαιρετικά δύσχρηστη και πολύ κοστοβόρα δεν ενδείκνυται.

Για παράδειγμα, ένας συνδυασμός προσωπικού πιστοποιητικού (certificate), κωδικού μιας χρήσης που παράγεται από έξυπνη κάρτα (token), κωδικού πρόσβασης (password) και φωνητικής αναγνώρισης για πρόσβαση σε μια εφαρμογή που αφορά οικονομικά στοιχεία είναι σπατάλη πόρων. Το **κόστος** και η **πολυπλοκότητα της διαδικασίας επαλήθευσης** της ταυτότητας θα πρέπει **να αντικατοπτρίζουν τον κίνδυνο** που συνδέεται με τη μη εξουσιοδοτημένη πρόσβαση και εξακολουθεί να έχει νόημα κατά την ολοκλήρωση μιας ανάλυσης κόστους-οφέλους.

7.4 Η σημασία των μυστικών κωδικών

Η Ηλεκτρονική Ταυτότητα δίνει πρόσβαση σε κάποιο Πληροφοριακό Αγαθό/Σύστημα και όσο υψηλότερη είναι η αξία του Πληροφοριακού Αγαθού (προσωπικά δεδομένα, φορολογικά δεδομένα, δεδομένα από Διεθνείς Συμφωνίες) τόσο μεγαλύτερη είναι η

σημασία της ηλεκτρονικής ταυτότητας και η ασφάλεια που αυτή πρέπει να παρέχει. Ο χειρισμός της δεν πρέπει να διαφέρει από το χειρισμό της φυσικής ταυτότητας.

Ο κωδικός πρόσβασης (password), όταν επιλέγεται να χρησιμοποιείται για την προστασία συστημάτων και πληροφοριών, θα πρέπει να είναι προσωπικός και παραμένει ιδιωτικός/μυστικός:

- Μόνο ο κάτοχος του να τον ορίζει
- Μόνο ο κάτοχος του να τον γνωρίζει
- Μόνο ο κάτοχος του να τον χρησιμοποιεί

Ακριβώς όπως δεν δίνουμε την ταυτότητά μας και την κάρτα ανάληψης χρημάτων του προσωπικού μας λογαριασμού σε κάποιο άλλο πρόσωπο, για τους ίδιους λόγους δεν μοιραζόμαστε την ηλεκτρονική μας ταυτότητα. Η ηλεκτρονική ταυτότητα αποτελεί ένα πολύτιμο στοιχείο ισοδύναμο του PIN της κάρτας πρόσβασης ή της υπογραφής μας. Όπως δεν θα δίναμε την υπογραφή μας σε κάποιον άλλον με την ίδια λογική δεν αποκαλύπτουμε τον κωδικό πρόσβασής μας σε κανέναν.

Αντίστοιχης μοναδικότητας με την υπογραφή αποτελεί και το δακτυλικό αποτύπωμα. Αυτό, εκτός του ότι δεν είναι δυνατό να μεταφερθεί σε κάποιον άλλον, αποτελεί διαφορετικό στοιχείο σε κάθε άνθρωπο. Με ανάλογο τρόπο θα πρέπει να σκεφτόμαστε για την ηλεκτρονική ταυτότητα όσον αφορά στη μοναδικότητά της, την αποκλειστική της χρήση και τη σωστή προστασία της.

Αν κάποιος κλέψει το μυστικό κωδικό ενός χρήστη, πιθανώς να διαπράξει κακόβουλες ενέργειες εναντίον του ή εναντίον των Πληροφοριακών Αγαθών που ο κωδικός του χρήστη δίνει πρόσβαση. Με αυτό τον τρόπο θα ενοχοποιηθεί ένα αθώο πρόσωπο, και θα θεωρηθεί υπεύθυνο για όλες τις ενέργειες σαν να έγιναν από εκείνον. Το ίδιο ισχύει αν δώσουμε το μυστικό μας κωδικό σε άλλο άτομο. Όλες οι ενέργειές του, ακόμα και τα ακούσια λάθη του, θα αποδοθούν στον κάτοχο του κωδικού.

Συμπερασματικά, οι **μυστικοί κωδικοί** πρέπει να παραμένουν **αυστηρά προσωπικοί**, για να προστατεύουν τον κάτοχο τους και τα πληροφοριακά αγαθά, στα οποία επιτρέπουν πρόσβαση.

7.5 Ισχυροί Κωδικοί

Οι χρήστες πρέπει να είναι ιδιαίτερα προσεκτικοί όχι μόνο ως προς τη χρήση των μυστικών κωδικών αλλά και ως προς τη επιλογή τους.

Ισχυροί κωδικοί θα πρέπει να επιλέγονται ανεξάρτητα αν υπάρχουν τα τεχνικά μέσα για τον αυτόματο έλεγχο της συμμόρφωσης. Ενδέχεται, δηλαδή, το ίδιο το πληροφοριακό σύστημα να αναγκάζει το χρήστη στην επιλογή ενός ισχυρού κωδικού απορρίπτοντας αδύναμους κωδικούς που αυτός επιλέγει. Ακόμα, όμως, κι όταν αυτό δεν γίνεται θα πρέπει ο χρήστης από μόνος του να γνωρίζει ότι η επιλογή ισχυρού κωδικού είναι δική του ευθύνη.

Η επιλογή του κωδικού πρόσβασης δεν θα πρέπει να είναι τυχαία, να στηρίζεται σε γνωστές για τον κάτοχο του λέξεις ή φράσεις ώστε να μην μπορεί να προβλεφθεί εύκολα. Οι κωδικοί θα πρέπει να δημιουργούνται με βάση στους παρακάτω κανόνες:

- Να έχουν ελάχιστο μήκος 8 χαρακτήρες.
- Να περιέχουν :
    - Ένα τουλάχιστον πεζό γράμμα (λατινικοί χαρακτήρες).
    - Ένα τουλάχιστον κεφαλαίο γράμμα (λατινικοί χαρακτήρες).
    - Έναν τουλάχιστον αριθμό.

- Έναν τουλάχιστον ειδικό χαρακτήρα (μη υποχρεωτικό αλλά ενισχύει πολύ την ασφάλεια): ! @ # $ % ^ & * ? < >

Ωστόσο, ο κωδικός που επιλέγεται θα πρέπει να απομνημονεύεται εύκολα από το κάτοχο του, διαφορετικά γίνεται αναποτελεσματικός, δύσχρηστος και κινδυνεύει να βρεθεί γραμμένος σε κάποιο εμφανές σημείο (για λόγους υπενθύμισης) και άρα να εκτεθεί στον κακόβουλο χρήστη.

Ακολούθως, αναγράφονται μερικοί πρακτικοί κανόνες επιλογής κωδικού:

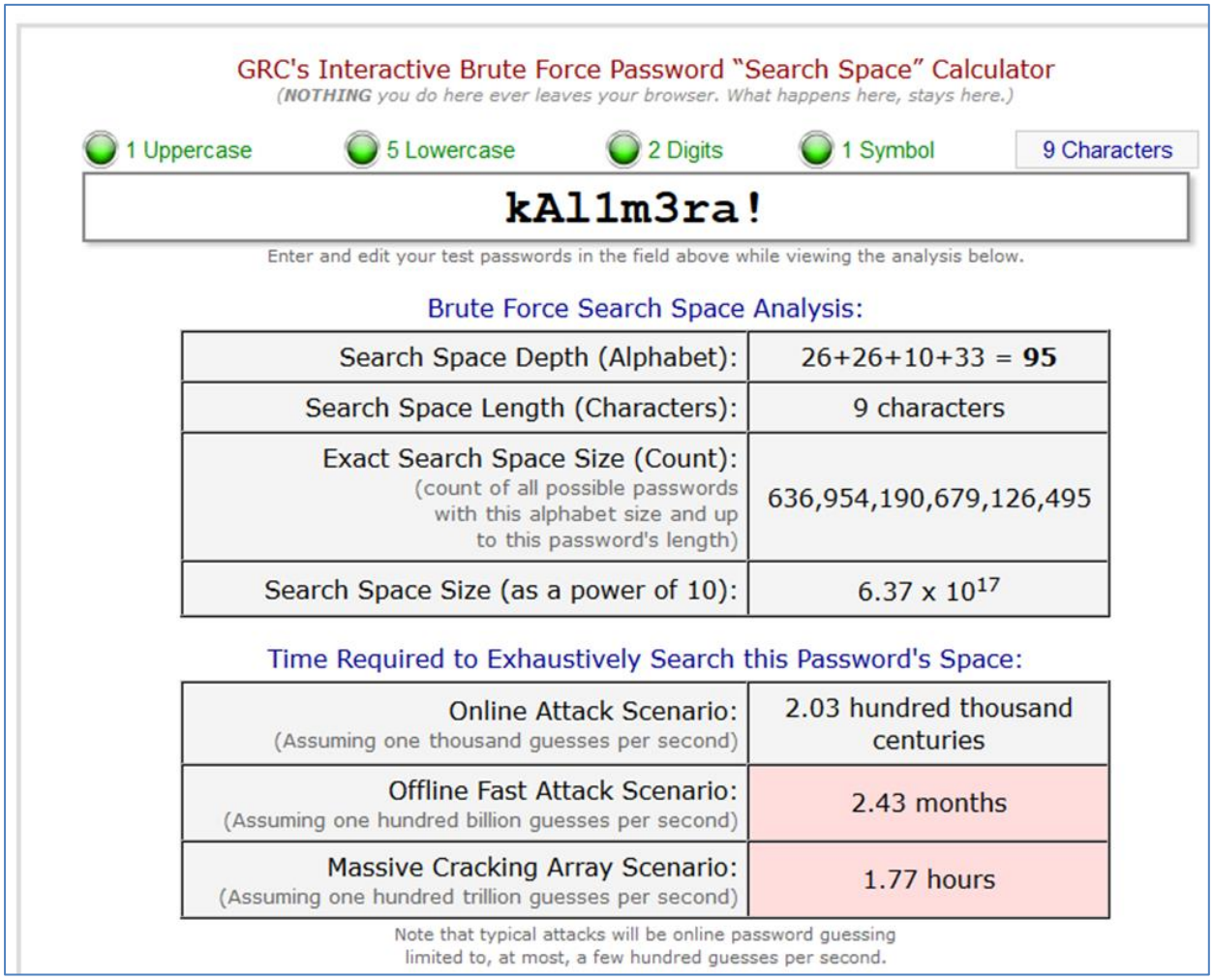
1. Με λίγη φαντασία κοιτώντας το πληκτρολόγιο παρατηρούμε κάποιες αντιστοιχίσεις γραμμάτων και αριθμών, οι οποίες μπορούν να χρησιμοποιηθούν και τις οποίες μπορούμε να θυμόμαστε εύκολα. Για παράδειγμα:
   - l,i → 1, !
   - a → @
   - o →0 (προσοχή όμως στο να διαχωρίζουμε το μηδέν από το κεφαλαίο Όμικρον)
   - b → 8
   - e → 3
   - z → 7

   Με τον ίδιο τρόπο μπορούμε να ανακαλύψουμε και άλλους δικούς μας συσχετισμούς και να μετατρέψουμε αγαπημένες μας λέξεις ή φράσεις σε δύσκολους αλλά εύχρηστους προσωπικούς μας κωδικούς.
2. Επιλέγοντας μία γνωστή λέξη και τροποποιώντας την:
   - Επιλέγουμε τη λέξη «καλημέρα»
   - Μετατρέπουμε τη λέξη σε λατινικούς χαρακτήρες : kalimera
   - Αντικαθιστούμε κάποιους χαρακτήρες με κεφαλαία, αριθμό ή ειδικό χαρακτήρα που μοιάζει οπτικά: kAl1m3ra
   - Προσθέτουμε στην αρχή ή το τέλος ένα ειδικό χαρακτήρα [!%^&*?]: kAl1m3ra!

   Παρατηρούμε ότι ο κωδικός μας είναι ισχυρός καθώς αποτελείται συνολικά από 9 χαρακτήρες και περιέχει κεφαλαίο γράμμα, αριθμό και ειδικό χαρακτήρα.
3. Επιλέγοντας μια φράση και προσαρμόζοντας την:
   - Επιλέγουμε τη φράση: «Σήμερα μαθαίνω για τους μυστικούς κωδικούς στην αίθουσα του εκδδα».
   - Μετατρέπουμε τη φράση σε λατινικούς χαρακτήρες «Shmera mathaino gia tous mistikous kodikous stin aithousa tou ekdda»
   - Μετασχηματίζουμε σε συμβολική λέξη χρησιμοποιώντας τα αρχικά των λέξεων: smgtmksate
   - Αντικαθιστούμε κάποιους χαρακτήρες με κεφαλαίο, αριθμό ή ειδικό χαρακτήρα: sMgtmks@t3

   Παρατηρούμε ότι ότι ο κωδικός μας είναι ισχυρός καθώς αποτελείται συνολικά από 10 χαρακτήρες και περιέχει κεφαλαίο γράμμα, αριθμό και ειδικό χαρακτήρα.

Στον ιστότοπο GRC Brute Force Calculator http://www.grc.com/haystack.htm παρέχεται ένα εργαλείο, με το οποίο μπορούμε να ελέγξουμε πόσο ισχυρός είναι ο κωδικός που επιλέξαμε:



Εικόνα 7-4: Εργαλείο GRC Brute Force Calculator για έλεγχο ισχυρών κωδικών

Παρατηρώντας το αποτέλεσμα της διερεύνησης για την «επιτυχία» του κωδικού που επιλέξαμε αναλύουμε τους χρόνους που χρειάζεται ένα cracking scenario για να ανακαλύψει (μαντέψει) τον κωδικό μας:

1. Απαιτείται **1,77 της ώρας** όταν εκτελούνται 100 τρισεκατομμύρια εναλλακτικά σενάρια για διαφορετικούς κωδικούς το δευτερόλεπτο.
2. Απαιτούνται **2,43 μήνες** όταν εκτελούνται 100 δισεκατομμύρια εναλλακτικά σενάρια κωδικών το δευτερόλεπτο.
3. Απαιτούνται **2,03 εκατοντάδες χιλιάδες αιώνες** όταν εκτελούνται 1000 εναλλακτικά σενάρια κωδικών το δευτερόλεπτο.

Έχοντας υπόψη ότι μια τυπική επίθεση πραγματοποιείται από κάποιο κακόβουλο hacker, ο οποίος κάνει το πολύ κάποιες εκατοντάδες προσπάθειες εναλλακτικού σεναρίου κωδικού το δευτερόλεπτο, καταλήγουμε στο συμπέρασμα ότι ο κωδικός που επιλέξαμε είναι αρκετά ισχυρός.

7.6 Χρήση Μυστικών Κωδικών

Οι κωδικοί πρόσβασης είναι **προσωπικοί** και πρέπει να παραμένουν **μυστικοί:**

- Δεν επιτρέπεται η αποκάλυψή τους σε συναδέλφους ή τρίτους.

- Θα πρέπει να μην δίδονται σε κανέναν. Αν ζητηθούν θα πρέπει να γίνεται επίκληση της Πολιτικής Ορθής Χρήσης Συστημάτων και Πληροφοριών (ΠΟΧΣΠ) με άμεση ειδοποίηση του Υπεύθυνου Χρηστών.

Οι κωδικοί πρόσβασης θεωρούνται εμπιστευτική πληροφορία και σε περίπτωση που είναι αποτυπωμένη με έντυπο ή ηλεκτρονικό τρόπο, θα πρέπει να προστατεύεται επαρκώς ως εμπιστευτική.

Αξίζει να προσέξουμε τα παρακάτω που αφορούν στην αποκάλυψη των κωδικών πρόσβασης:

- ✓ Σύμφωνα με την Πολιτική Ορθής Χρήσης (ΠΟΧΣΠ) μπορεί να επιτραπεί η χρήση των κωδικών ενός χρήστη από άλλον μετά από δικαιολογημένη υπηρεσιακή ανάγκη και μόνο **για συγκεκριμένο δικαιολογημένο χρονικό διάστημα μετά από έγγραφη ανάθεση** από τον αρμόδιο Υπεύθυνο των Χρηστών. Αυτό μπορεί να συμβεί μόνο στα πλαίσια επείγουσας υπηρεσιακής ανάγκης. Στις περιπτώσεις αυτές ο χρήστης θα πρέπει να αλλάζει τον κωδικό του άμεσα, όταν ολοκληρωθεί η απαιτούμενη ενέργεια.
- ✓ Δεν γράφουμε τον κωδικό μας σε χαρτάκια που είναι εκτεθειμένα, δεν τον αποκαλύπτουμε στο email μας ούτε στα μέσα κοινωνικής δικτύωσης (facebook).
- ✓ Αν υπάρχει υποψία ότι ο προσωπικός κωδικός έχει υποκλαπεί, θα πρέπει να αλλάζεται άμεσα και σε περίπτωση που αυτό δεν είναι εφικτό να ειδοποιείται ο αρμόδιος Διαχειριστής.

Επιπλέον σε ότι αφορά τη διαχείριση των κωδικών πρόσβασης ισχύουν τα παρακάτω:

- Να μην αποστέλλονται ή αποθηκεύονται χωρίς να λαμβάνονται επαρκή μέτρα. Ωστόσο αν υπάρχει ανάγκη να αποσταλούν αυτό θα πρέπει να γίνει σε σφραγισμένο φάκελο με συστημένη επίδοση ή σε κρυπτογραφημένο αρχείο.
- Να αλλάζονται περιοδικά ώστε να ελαχιστοποιηθεί η πιθανότητα μη εξουσιοδοτημένης χρήσης τους γιατί με την πάροδο του χρόνου αυξάνεται ο κίνδυνος κάποιος να δει / μαντέψει τον κωδικό μου.

Απαγορεύεται η χρήση των ίδιων κωδικών πρόσβασης στις υπηρεσίες και συστήματα του Υπουργείου Οικονομικών/Ανεξάρτητης Αρχής Δημοσίων Εσόδων με προσωπικούς κωδικούς πρόσβασης που χρησιμοποιεί ο εκάστοτε χρήσης για χρήση Διαδικτύου ή προσωπικού Ηλεκτρονικού Ταχυδρομείου. Για παράδειγμα ο κωδικός πρόσβασης στο facebook θα πρέπει να είναι διαφορετικός από τον κωδικό πρόσβασης στο Σύστημα TAXIS!

Σε κάθε περίπτωση οποιοδήποτε συμβάν κλοπής, απώλειας, ή/και επιλεκτικής αποκάλυψης του κωδικού απαιτεί άμεση αντίδραση και αντιμετώπιση.

7.7 Παραπομπές

1. Πολιτική Ορθής Χρήσης Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών
2. http://www.grc.com/haystack.htm

8 Εμπιστευτικότητα Υπηρεσιακών Πληροφοριών

8.1 Η έννοια της ασφάλειας πληροφοριακών συστημάτων

Η Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών αφορά οντότητες και αντικείμενα που αξίζει να προστατευθούν. Ότι αξίζει να προστατευθεί ονομάζεται Αγαθό (Asset).

Αγαθό είναι κάθε μονάδα υλικού εξοπλισμού, λογισμικού, έντυπου ή ηλεκτρονικού αρχείου που αξιοποιείται ως μέρος διεργασιών συλλογής, επεξεργασίας και μετάδοσης κρίσιμων πληροφοριών και ως συνέπεια έχει κάποια αξία για ένα Οργανισμό.

Τα Αγαθά αξίζει να προστατευθούν επειδή έχουν Αξία, η οποία μπορεί να μειωθεί αν υποστούν ζημιά:

Αναλυτικότερα μείωση της αξίας του Αγαθού προκύπτει:

- αν υπάρξει απώλεια εμπιστευτικότητας του Αγαθού, δηλαδή αν πραγματοποιηθεί αποκάλυψή του χωρίς την άδεια του ιδιοκτήτη του (Confidentiality),
- αν υπάρξει απώλεια ακεραιότητας για το Αγαθό, δηλαδή αν πραγματοποιηθεί μη εξουσιοδοτημένη τροποποίησή του (Integrity),
- αν υπάρξει απώλεια διαθεσιμότητας ή καταστροφή του Αγαθού (Availability).

Ιδιοκτήτης του Πληροφοριακού Αγαθού είναι ο Προϊστάμενος της Διεύθυνσης που έχει την ευθύνη διαχείρισης του Πληροφοριακού Αγαθού όπως προκύπτει από τις επίσημες αρμοδιότητες του Οργανισμού στον οποίο υπάγεται η ως άνω Διεύθυνση. Εφόσον, εντός της εν λόγω Διεύθυνσης, υπάρχει διακριτή αρμοδιότητα διαχείρισης του Αγαθού από συγκεκριμένο τμήμα, τότε ο Προϊστάμενος του τμήματος ορίζεται ως συν-Ιδιοκτήτης του Αγαθού.

Ο Ιδιοκτήτης (Owner) ενός προστατευόμενου Αγαθού χρησιμοποιεί μέσα προστασίας είτε για να μειώσει τον Κίνδυνο να προξενηθεί Ζημιά στο Αγαθό είτε για να μειώσει τις συνέπειές της.

Παραδείγματα Πληροφοριακών Αγαθών είναι:

- το έντυπο υλικό,
- ο Εξυπηρετητής Εφαρμογής,
- το Λογισμικό Εφαρμογής,
- η Βάση Δεδομένων,
- οι Συσκευές Δικτύου,
- τα Φορητά μέσα αποθήκευσης,
- τα Ηλεκτρονικά Αρχεία.

Μια πληροφορία (Αγαθό) που μεταφέρεται, αποθηκεύεται και επεξεργάζεται από ένα Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) είναι ασφαλής όταν ισχύει η τριάδα CIA:

- Προστατεύεται από μη εξουσιοδοτημένη πρόσβαση (Confidentiality)
- Προστατεύεται από μη εξουσιοδοτημένη μεταβολή (Integrity)
- Προστατεύεται από μη εξουσιοδοτημένη απώλεια ή καταστροφή (Availability)

Η προσπάθεια για την προστασία ενός αγαθού στηρίζεται σε δύο (2) βασικές αρχές Ασφάλειας Πληροφοριών:

- «Ελάχιστη πρόσβαση»
  - Απαιτεί να δίδονται τα ελάχιστα απαιτούμενα δικαιώματα πρόσβασης σε ένα πληροφοριακό αγαθό που επιτρέπουν την άσκηση υπηρεσιακών καθηκόντων.
- «Ανάγκη γνώσης / χρήσης»
  - Απαιτεί η χρήση ενός πληροφοριακού αγαθού να επιτρέπεται μόνο εφόσον είναι αναγκαία για την άσκηση υπηρεσιακών καθηκόντων.

8.2 Στρατηγική Ασφάλειας – Δέσμευση Εμπιστευτικότητας του Υπουργείου

Το Υπουργείο Οικονομικών αξιοποιεί τις Τεχνολογίες της Πληροφορικής και των Επικοινωνιών (ΤΠΕ) για την επίτευξη των επιχειρησιακών του στόχων και της αποστολής του. Η ανάπτυξη και λειτουργία Πληροφοριακών Συστημάτων (ΠΣ) αποτελεί σημαντική οικονομική επένδυση και αποσκοπεί, αφενός, στη βελτίωση της αποτελεσματικότητας της λειτουργίας του Υπουργείου και αφετέρου, στην παροχή υψηλής στάθμης υπηρεσιών προς τους πολίτες, επιχειρήσεις, φορείς του Δημόσιου και Ιδιωτικού Τομέα καθώς και σε άλλα Κράτη στο πλαίσιο διεθνών συμφωνιών και συνεργασιών.

Παράλληλα το Υπουργείο, αναγνωρίζοντας τις πολύπλευρες απαιτήσεις ασφαλείας που προκύπτουν τόσο από το εφαρμοζόμενο θεσμικό πλαίσιο, όσο και από τους αποδέκτες των υπηρεσιών του, θέτει ως πρώτη προτεραιότητα τη συστηματική και αποδοτική αντιμετώπιση της ασφάλειας των πληροφοριακών συστημάτων του.

Το Υπουργείο Οικονομικών δεσμεύεται ως προς τη συμμόρφωση με το εφαρμοστέο Νομικό Πλαίσιο (απόρρητο φορολογικών δεδομένων, προστασία προσωπικών δεδομένων).

Το Υπουργείο Οικονομικών δεσμεύεται γενικά για την προστασία εμπιστευτικών πληροφοριών.

8.3 Εμπιστευτικότητα

Οι υπάλληλοι του Οργανισμού και σε ορισμένες περιπτώσεις και οι εξωτερικοί συνεργάτες, στο πλαίσιο των καθηκόντων τους, χειρίζονται μια σειρά από υπηρεσιακές πληροφορίες, οι οποίες είναι πολύ πιθανό να διαβαθμίζονται ως «ΕΜΠΙΣΤΕΥΤΙΚΕΣ». Εμπιστευτικές θεωρούνται οι πληροφορίες, η γνωστοποίηση των οποίων σε μη εξουσιοδοτημένα πρόσωπα παραβιάζει τη νόμιμη ή συμβατική υποχρέωση τήρησης απορρήτου ή ενδέχεται να βλάψει την ασφάλεια των πληροφοριακών συστημάτων.

8.4 Διαβάθμιση Πληροφορίας

Οι πληροφορίες αυτές διαβαθμίζονται, ανάλογα με το είδος τους, ως προς την προστασία που πρέπει να τους εφαρμόσουμε:

- <u>Δημόσιες Πληροφορίες</u>:
  Η αποκάλυψή τους σε οποιαδήποτε πρόσωπα:
  - δεν παραβιάζει καμία νομική ή συμβατική υποχρέωση του Υπουργείου Οικονομικών,
  - δεν προκαλεί οποιαδήποτε ζημιά στο Υπουργείο Οικονομικών,
  - δεν έχει κάποια επίπτωση στην ασφάλεια των ΟΠΣ.

  Παραδείγματα: ανακοινώσεις, αποφάσεις, νομικό πλαίσιο.
- <u>Περιορισμένης Χρήσης Πληροφορίες</u>:

- Προορίζονται για χρήση μόνο για συγκεκριμένο σκοπό και από συγκεκριμένα άτομα για τα οποία ισχύει η αρχή της «ανάγκης γνώσης».
- Η αποκάλυψη τέτοιας πληροφορίας σε μη εξουσιοδοτημένα πρόσωπα δεν παραβιάζει νομικές ή συμβατικές υποχρεώσεις του Υπουργείου Οικονομικών.
- Η αποκάλυψή τους μπορεί να προκαλέσει μέτρια ζημιά στο Υπουργείο Οικονομικών, κυρίως ως προς το κύρος του, χωρίς σοβαρές επιπτώσεις ως προς την ασφάλεια των ΟΠΣ.

Παραδείγματα: εσωτερικές διαδικασίες, τεχνικές προδιαγραφές, πρακτικά συναντήσεων, πρακτικά συνεδριάσεων κλπ.

- Εμπιστευτικές Πληροφορίες:
«Εμπιστευτικές» θεωρούνται οι πληροφορίες, η γνωστοποίηση των οποίων σε μη εξουσιοδοτημένα πρόσωπα παραβιάζει τη νόμιμη ή συμβατική υποχρέωση τήρησης απορρήτου ή/και ενδέχεται να βλάψει σοβαρά την ασφάλεια των ΟΠΣ.
Οι πληροφορίες αυτές μπορεί να βρίσκονται σε οποιεσδήποτε μορφές:
  - Ηλεκτρονικά αρχεία
  - Υπηρεσιακά έγγραφα
  - Εκτυπώσεις
  - Οπτικά μέσα αποθήκευση (CD/DVD/Blu-ray)
  - Εξωτερικοί σκληροί δίσκοι, σκληροί δίσκοι
  - Αφαιρούμενα μέσα (USB sticks)
  - Ακόμα και σε προφορική μορφή

  Παραδείγματα:
  - ✓ Φορολογικά δεδομένα φυσικών/νομικών προσώπων
  - ✓ Προσωπικά δεδομένα πολιτών ή υπαλλήλων
  - ✓ Δεδομένα που έχουν περιέλθει στην υπηρεσία στα πλαίσια ανταλλαγής δεδομένων με διεθνείς φορείς (FATCA, AEOI, OECD)
  - ✓ Τεχνικές πληροφορίες υπολογιστικών υποδομών
  - ✓ Διοικητικά και λοιπά ηλεκτρονικά και μη έγγραφα με ένδειξη εμπιστευτικότητας (π.χ. ΕΜΠΙΣΤΕΥΤΙΚΟ, ΑΠΟΡΡΗΤΟ, ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ).

8.5 Κανόνες για την Προστασία της Εμπιστευτικότητας

Για την προστασία της εμπιστευτικότητας των διαβαθμισμένων πληροφοριών, σύμφωνα με την Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών του Υπουργείου Οικονομικών, ισχύουν οι εξής κανόνες:

- Τήρηση εχεμύθειας: Τα υπηρεσιακά δεδομένα θα πρέπει να μην αποκαλύπτονται σε πρόσωπα ή οντότητες που δεν διαθέτουν ρητή εξουσιοδότηση/άδεια.
- Ανάγκη χρήσης / ανάγκη γνώσης: Δεν επιτρέπεται η πρόσβαση/χρήση σε υπηρεσιακές πληροφορίες και συστήματα, παρά μόνο στα πλαίσια υπηρεσιακών υποθέσεων και καθηκόντων.
- Διακίνηση υπηρεσιακής πληροφορίας (με συμβατική ή ηλεκτρονική αλληλογραφία): Δεν επιτρέπεται διακίνηση υπηρεσιακής πληροφορίας με

μεθόδους που ενδέχεται να οδηγήσουν σε απώλεια εμπιστευτικότητας σε μη έχοντες εξουσιοδότηση ή σε μη γνήσιους παραλήπτες.

- Απαγόρευση καταγραφής: Απαγορεύεται ρητά η καταγραφή ήχου, εικόνας ή βίντεο εντός των χώρων του Οργανισμού, χωρίς την έγκριση της αρμόδιας Οργανικής Μονάδας Ασφαλείας. Η έγκριση δίνεται αυστηρά και μόνο όταν υπάρχει υπηρεσιακή ανάγκη.
- Χρήση φορητών αποθηκευτικών μέσων: Σε περίπτωση που χρησιμοποιούνται φορητά μέσα αποθήκευσης βάσει υπηρεσιακής ανάγκης, θα πρέπει να δίδεται ιδιαίτερη προσοχή στο χειρισμό των μέσων αυτών ώστε να αποφευχθεί ο κίνδυνος κλοπής ή αποκάλυψης. Τα μέσα αυτά θα πρέπει είτε να παραμένουν κλειδωμένα σε ντουλάπια εντός γραφείων είτε να κρυπτογραφούνται με μεθόδους που προτείνονται από το Αυτοτελές Τμήμα Ασφάλειας (π.χ. συμπιεσμένο, κρυπτογραφημένο αρχείο προστατευμένο με κωδικό).
- Χρήση προσωπικού εξοπλισμού: Δεν επιτρέπεται να χρησιμοποιούνται προσωπικές συσκευές, όπως φορητά αποθηκευτικά μέσα, υπολογιστές, ταμπλέτες, έξυπνα κινητά τηλέφωνα, κάμερες κ.λπ. για την αποθήκευση υπηρεσιακών πληροφοριών, χωρίς άδεια από τον άμεσο αρμόδιο Υπεύθυνο Χρηστών. Η έγκριση δίνεται αυστηρά και μόνο όταν υπάρχει υπηρεσιακή ανάγκη εφαρμόζοντας τους κανόνες εμπιστευτικότητας. Σε περίπτωση αποχώρησης του υπαλλήλου, αλλαγή αρμοδιοτήτων ή μη ύπαρξης πλέον της ανάγκης θα πρέπει να διαγράφεται οποιαδήποτε υπηρεσιακή πληροφορία από προσωπικό εξοπλισμό.
- Ρήτρα Εμπιστευτικότητας: Σε περίπτωση που μετά από ανάλυση κινδύνου κριθεί αναγκαίο από την αρμόδια Οργανική Μονάδα Ασφάλειας του Οργανισμού, θα πρέπει, πέραν της αποδοχής της παρούσας πολιτικής, να υπογράφεται από το Χρήστη η «ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΠΡΟΣΒΑΣΗΣ ΥΠΑΛΛΗΛΟΥ ΜΕ ΡΗΤΡΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ» σύμφωνα με το ΠΑΡΑΡΤΗΜΑ της Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών του Υπουργείου Οικονομικών, αφού διαμορφωθεί κατάλληλα από τον αρμόδιο Υπεύθυνο Χρηστών

8.6 Εξουσιοδοτημένη/ Μη Εξουσιοδοτημένη Πρόσβαση

Για την προστασία της εμπιστευτικότητας των πληροφοριών, είναι απαραίτητη η τήρηση των θεσμοθετημένων πολιτικών και διαδικασιών σχετικά με την πρόσβαση σε αυτές μόνο από εξουσιοδοτημένους υπαλλήλους και πάντα εφαρμόζοντας τις αρχές της «Ελάχιστης πρόσβασης» και της «Ανάγκης γνώσης».

Για την έγκριση εξουσιοδότησης πρόσβασης σε Πληροφοριακό Αγαθό:

- Απαιτείται η (συνήθως γραπτή) συγκατάθεση Προϊσταμένου Οργανικής Μονάδας που είναι αρμόδια για την προστασία του.
- Εφαρμόζεται η αρχή της «ελάχιστης πρόσβασης».
- Παρέχεται πρόσβαση σε εμπιστευτική πληροφορία μόνο στο πλαίσιο:
  - άσκησης καθηκόντων τηρώντας την αρχή «ανάγκη γνώσης»,
  - υπηρεσιακής υπόθεσης μέσω «επίσημου καναλιού».

Επίσημο Κανάλι Επικοινωνίας Εξουσιοδοτημένης Πρόσβασης

Ως **Επίσημο Κανάλι** για εξουσιοδοτημένη πρόσβαση σε πληροφορίες θεωρείται καθένα από τα ακόλουθα:

- Ανάθεση εγγράφου γραπτώς ή ηλεκτρονικώς από Προϊστάμενο

- Λήψη εγγράφου από πολίτες / συναλλασσόμενους μέσω επίσημου υπηρεσιακού μέσου επικοινωνίας
  - Υπηρεσιακό τηλέφωνο
  - Υπηρεσιακό email
  - Υπηρεσιακή αλληλογραφία

Ως **μη Επίσημο Κανάλι** για πρόσβαση σε πληροφορίες θεωρείται καθένα από τα ακόλουθα:

- Ερώτηση συγγενικού ή γνωστού προσώπου για προσωπική του υπόθεση σε περιβάλλον εκτός εργασίας.
- Ερώτηση προσώπου μέσω μέσου κοινωνικής δικτύωσης.
- Ερώτηση συναδέλφου για προσωπική υπόθεση ή για υπόθεση άλλου προσώπου.

Παράδειγμα

Ο Προϊστάμενος του τμήματος Α εξουσιοδοτεί τον υπάλληλο Υ του τμήματος να έχει πρόσβαση σε ένα πληροφοριακό αγαθό αρμοδιότητας του τμήματός του (εφαρμογή, ΒΔ. κ.α.), προκειμένου να εκτελέσει τα υπηρεσιακά καθήκοντά του.

Περιπτώσεις μη νόμιμης πρόσβασης έχουμε όταν:

- Μη εξουσιοδοτημένος υπάλληλος εκμεταλλεύεται αδυναμίες του συστήματος και αποκτά πρόσβαση σε πληροφοριακό αγαθό για προσωπικό σκοπό ή περιέργεια.
- Εξουσιοδοτημένος υπάλληλος αποκτά πρόσβαση σε πληροφοριακό αγαθό για μη υπηρεσιακή χρήση ή για προσωπική υπόθεση ή από περιέργεια.
- Εξουσιοδοτημένος υπάλληλος, λόγω μη εφαρμογής της «ελάχιστης πρόσβασης», αποκτά πρόσβαση σε διάφορα πληροφοριακά αγαθά για προσωπική υπόθεση ή από περιέργεια.
- Εξουσιοδοτημένος υπάλληλος αποκτά πρόσβαση σε πληροφοριακό αγαθό για υπηρεσιακή χρήση που αφορά μη επίσημο κανάλι (συγγενικό, γνωστό πρόσωπο ή συνάδελφο).

Ιδιαίτερη προσοχή απαιτείται σε περιπτώσεις που η υπόθεση που ανατίθεται στον υπάλληλο αφορά γνωστά ή συγγενικά πρόσωπα. Στην περίπτωση αυτή θα πρέπει να ακολουθούνται οι παραπάνω κανόνες ώστε να μην προκύψει κατηγορία για διαφθορά.

8.7 Οδηγίες για Προστασία Πληροφορίας Περιορισμένης Χρήσης

Για την προστασία **Πληροφορίας Περιορισμένης Χρήσης**, θα πρέπει να ακολουθούμε τους εξής κανόνες:

- Πρέπει να υπάρχει η σήμανση «Περιορισμένης Χρήσης»
- Φροντίζουμε να ελέγχουμε τους παραλήπτες σε περίπτωση που την κοινοποιούμε μέσω μαζικού τρόπου επικοινωνίας
- Δίνουμε οδηγίες για το χειρισμό της πληροφορίας, αναφέροντας ότι «*δεν επιτρέπεται η κοινοποίησή της σε άτομα που δεν έχουν ανάγκη γνώσης της πληροφορίας στο πλαίσιο άσκησης των καθηκόντων τους*»

Για την προστασία **Εμπιστευτικής Πληροφορίας** θα πρέπει να ακολουθούμε τους εξής κανόνες:

- Πρέπει να υπάρχει η σήμανση «ΕΜΠΙΣΤΕΥΤΙΚΟ»

- Φροντίζουμε ώστε η πληροφορία να φτάσει ΜΟΝΟ στον αυθεντικό παραλήπτη
  - π.χ. με χρήση κρυπτογράφησης αρχείου και κοινοποίηση κωδικού μέσω τηλεφώνου ή φυσική παρουσία του παραλήπτη με επίδειξη εγγράφου ταυτότητας.
- Φροντίζουμε στο συνοδευτικό κείμενο να αναφέρουμε ότι «*η πληροφορία μπορεί να χρησιμοποιηθεί μόνο για το συγκεκριμένο σκοπό που ζητήθηκε και δεν μπορεί να χρησιμοποιηθεί για άλλο λόγο χωρίς την άδεια της Υπηρεσίας. Πιθανή παραβίαση του απορρήτου της πληροφορίας μπορεί να οδηγήσει σε σοβαρές διοικητικές και ποινικές κυρώσεις.*»
- Ιδιαιτέρως στην περίπτωση που η πληροφορία προέρχεται από ανταλλαγή φορολογικών δεδομένων με διεθνείς οργανισμούς, επισημαίνουμε επιπρόσθετα ότι «*η πληροφορία αποτελεί πληροφορία που προέρχεται από Διεθνή Συμφωνία και προστατεύεται από ισχυρές νομικές ασφαλιστικές δικλείδες».*

9 Καθαρή Επιφάνεια Εργασίας (Clean Desk Policy)

9.1 Γενικά

Οι υπάλληλοι του Οργανισμού, στο πλαίσιο εκτέλεσης των καθηκόντων τους, χειρίζονται μια σειρά από υπηρεσιακές πληροφορίες, οι οποίες διαβαθμίζονται ανάλογα. Οι πληροφορίες αυτές μπορεί να βρίσκονται σε οποιαδήποτε μορφή, όπως:

- υπηρεσιακά έγγραφα,
- εκτυπώσεις,
- ηλεκτρονικά αρχεία,
- οπτικά μέσα αποθήκευση (CD/DVD/Blu-ray),
- εξωτερικοί σκληροί δίσκοι,
- σκληροί δίσκοι,
- αφαιρούμενα μέσα (USB sticks),
- ακόμα και σε προφορική μορφή.

Όλοι οι υπάλληλοι πρέπει να είναι ευαισθητοποιημένοι για τις εμπιστευτικές πληροφορίες / αγαθά που είναι εκτεθειμένα στο χώρο εργασίας τους.

9.2 Κανόνες

Για την προστασία των διαβαθμισμένων πληροφοριών, σύμφωνα με την Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών του Υπουργείου Οικονομικών (Παρ. 4.3.2 Κανόνες Ασφαλείας, σημείο 6.), ισχύουν οι εξής κανόνες:

- Δεν επιτρέπεται η ανεξέλεγκτη έκθεση εντύπων, φακέλων ή φορητών αποθηκευτικών μέσων που πιθανώς φέρουν εμπιστευτικές πληροφορίες σε μη προστατευμένα σημεία όπως θέσεις εργασίας, εκτυπωτικά μηχανήματα, φωτοαντιγραφικά μηχανήματα, αίθουσες συναντήσεων, καλάθια αχρήστων.
- Στο τέλος της εργάσιμης μέρας, όλα τα έντυπα, φάκελοι και αποθηκευτικά μέσα στα οποία ενδέχεται να υπάρχει εμπιστευτική πληροφορία, να απομακρύνονται από μη προστατευμένους χώρους και να κλειδώνονται σε ντουλάπια ή συρταριέρες ή να καταστρέφονται εφόσον δεν θα επαναχρησιμοποιηθούν.
- Εφόσον τα μέσα αυτά δεν απαιτούνται για άμεση χρήση να παραμένουν κλειδωμένα σε ντουλάπια. Σε κάθε περίπτωση, εάν δεν απαιτείται πλέον, το υλικό αυτό θα πρέπει να καταστρέφεται ασφαλώς.
- Τις εργάσιμες ώρες θα πρέπει να κλειδώνεται με κωδικό η επιφάνεια εργασίας του προσωπικού υπολογιστή, με μέγιστο διάστημα αδράνειας τα 10 λεπτά.
- Στις μη εργάσιμες ώρες, ο προσωπικός υπολογιστής θα πρέπει να είναι απενεργοποιημένος, εξαιρώντας τις περιπτώσεις που υπάρχει δικαιολογημένη υπηρεσιακή ανάγκη μετά από γραπτή έγκριση του αρμόδιου Υπεύθυνου Χρηστών.
- Τα κλειδιά των ντουλαπιών / γραφείων φυλάσσονται σε χώρο υπό την ευθύνη προϊσταμένων (γραφεία γραμματείας).
- Τα κλειδιά των γραμματειών των τμημάτων / διευθύνσεων θα πρέπει να φυλάσσονται σε χώρο ευθύνης της Υπηρεσίας Ασφάλειας (Security) ή να φυλάσσονται από άτομα αυστηρά ορισμένα από τον προϊστάμενο.

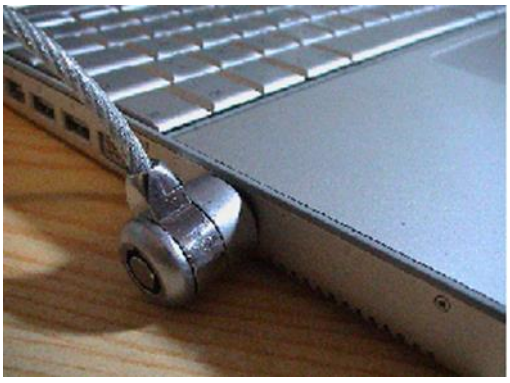
- Οι φορητοί υπολογιστές (laptop) πρέπει είναι «δεμένοι» με ειδική κλειδαριά Kensington lock (βλ. ενότητα 9.3 Kensington Lock), το οποίο αποτελεί μέρος συστήματος προστασίας από κλοπές.
- Οι εκτυπώσεις που στέλνονται σε κοινόχρηστους δικτυακούς εκτυπωτές θα πρέπει να μην παραμένουν στον εκτυπωτή ακόμα και αν στάλθηκαν από λάθος.
- Θα πρέπει να γίνεται ασφαλής καταστροφή εγγράφων που πλέον δεν χρησιμοποιούνται. Αν δεν υπάρχει διαθέσιμος στην υπηρεσία ειδικός αυτόματος καταστροφέας εγγράφων θα πρέπει να γίνεται «manual» - δηλαδή με το χέρι – καταστροφή έτσι ώστε να μην είναι δυνατόν ένας τρίτος να διαβάσει διαβαθμισμένο έγγραφο. Αυτή θεωρείται ασφαλής καταστροφή.

9.3 Kensington Lock

Το Kensington lock συνιστά σύστημα προστασίας από κλοπές, αποτελούμενο από μια μικρή οπή, ενισχυμένη με μέταλλα, που βρίσκεται συνήθως σε ηλεκτρονικό εξοπλισμό όπως φορητοί υπολογιστές, οθόνες υπολογιστών, επιτραπέζιοι υπολογιστές, κονσόλες παιχνιδιών και βιντεοπροβολείς.
Αποτελείται από:

- Μια μεταλλική άγκυρα στερεωμένη σε ασφαλισμένο μεταλλικό καλώδιο με κλείδωμα κλειδιού.
- Ένα καλώδιο, το άκρο του οποίου φέρει ένα μικρό βρόχο που επιτρέπει στο καλώδιο να περιστρέφεται γύρω από ένα μόνιμο αντικείμενο, όπως ένα βαρύ τραπέζι ή άλλο παρόμοιο εξοπλισμό.

Η υποδοχή Kensington ενδέχεται να έχει επισημανθεί στον φορητό εξοπλισμό που θέλουμε να προστατεύσουμε με ένα μικρό εικονίδιο που μοιάζει με λουκέτο ή/και με ένα κεφαλαίο "Κ" αλλά ενδέχεται και να μην έχει επισημανθεί.



Εικόνα 9-1: Kensington lock

Εικόνα 9-2: Καλώδιο Kensington lock

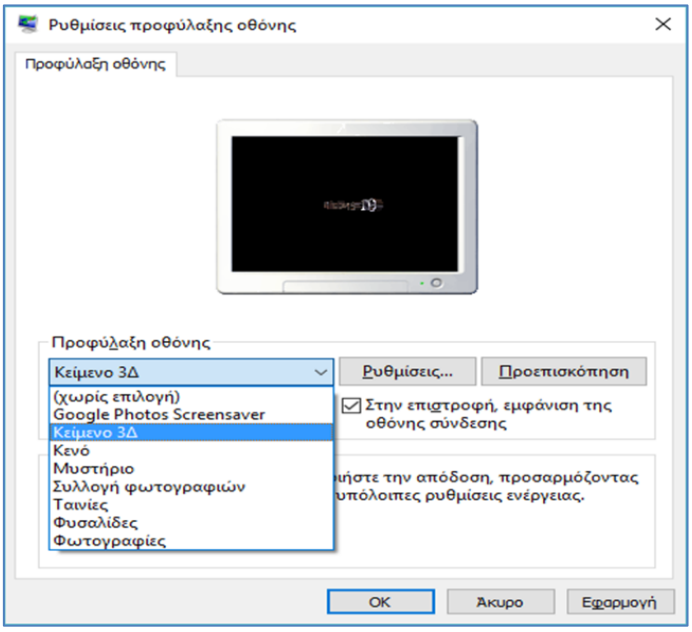
9.4 Κλείδωμα Επιφάνειας Εργασίας

Για την προστασία του προσωπικού του σταθμού εργασίας (Η/Υ) ο χρήστης οφείλει να κλειδώνει την επιφάνεια εργασίας του όταν απουσιάσει από το γραφείο του για περισσότερο από 10 λεπτά.

Η δυνατότητα κλειδώματος της επιφάνειας εργασίας του υπολογιστή υπάρχει σ' όλες τις εκδόσεις του λειτουργικού συστήματος Windows. Ωστόσο, τα ονόματα των «παραθύρων» και οι λεπτομέρειες για τις απαιτούμενες ρυθμίσεις που πρέπει να ακολουθήσει ο χρήστης ενδέχεται να διαφέρουν ανάλογα με την έκδοση του λειτουργικού συστήματος Windows.

Ακολουθούν ενδεικτικά τα βήματα:

- Δεξί κλικ στην Επιφάνεια Εργασίας του υπολογιστή.
- Επιλογή «Εξατομίκευση – Personalize».
- Επιλογή «Ρυθμίσεις προφύλαξης οθόνης – Lock Screen».
- Επιλογή προτιμούμενων ρυθμίσεων (εικόνα, χρόνος, ξεκλείδωμα, κτλ.).



Εικόνα 9-3: Ρυθμίσεις Προφύλαξης Οθόνης

9.5 Έλεγχος από το Αυτοτελές Τμήμα Ασφαλείας

Επισημαίνεται ότι το Αυτοτελές Τμήμα Ασφαλείας του Υπουργείου Οικονομικών καθώς και η Οργανική Μονάδα Ασφαλείας του Οργανισμού (ΟΜΑ) διατηρούν το δικαίωμα να κάνουν αιφνιδιαστικούς ελέγχους για τον έλεγχο συμμόρφωσης ως προς την καθαρή επιφάνεια στους χώρους εργασίας, ακόμα και σε μη εργάσιμες ημέρες και ώρες.

10 Προστασία Ηλεκτρονικής Πληροφορίας με Κρυπτογράφηση

10.1 Κρυπτογράφηση – Αποκρυπτογράφηση

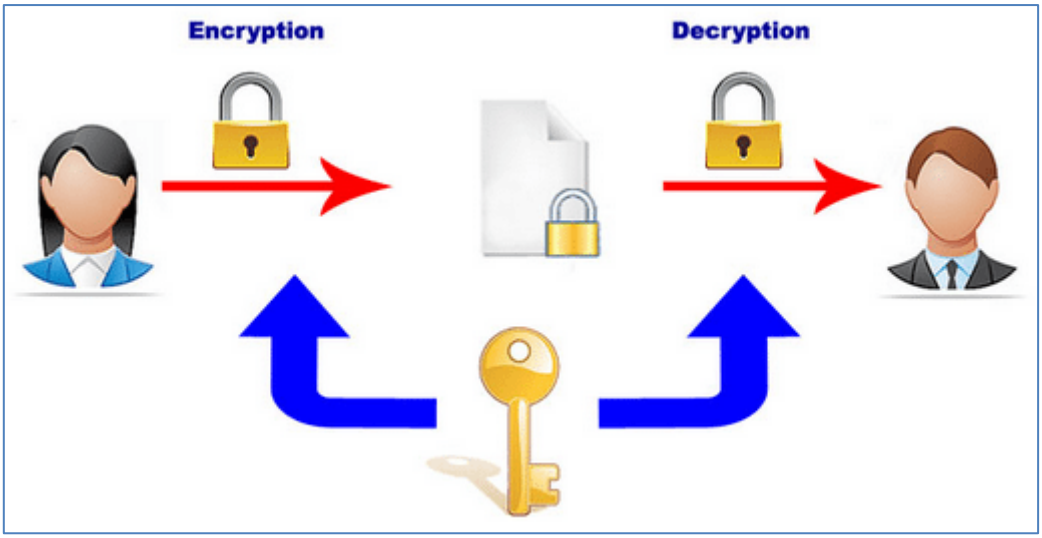
Ο αντικειμενικός σκοπός της διαδικασίας κρυπτογράφησης – αποκρυπτογράφησης είναι να δώσει τη δυνατότητα σε δύο άτομα να επικοινωνήσουν μέσα από ένα ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο, μη εξουσιοδοτημένο πρόσωπο, να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να υποκλέψει/αλλοιώσει το περιεχόμενο των μηνυμάτων που ανταλλάσουν τα δύο άτομα. Οι ορισμοί που ακολουθούν περιγράφουν με γενικό τρόπο τη συγκεκριμένη διαδικασία:

- **Κρυπτογράφηση (encryption)** είναι η διαδικασία **μετασχηματισμού ενός μηνύματος**/κειμένου **σε μία ακατανόητη μορφή** με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου, ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.
- **Αποκρυπτογράφηση (decryption) είναι η αντίστροφη διαδικασία** όπου το αρχικό κείμενο παράγεται από το κρυπτογραφημένο κείμενο.

Αναλυτικά:

- **Αρχικό κείμενο (plaintext):** πρόκειται για το μήνυμα/κείμενο το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- **Κρυπτογραφικός αλγόριθμος (cipher):** πρόκειται για τη **μέθοδο μετασχηματισμού** δεδομένων σε μία μορφή **που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη**. Ουσιαστικά αποτελεί μια πολύπλοκη μαθηματική συνάρτηση.
- **Κλειδί (key) Κρυπτογράφησης:** πρόκειται για μια **ακολουθία χαρακτήρων** που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.
- **Κρυπτογραφημένο κείμενο (ciphertext):** πρόκειται για το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Σχηματικά η διαδικασία της κρυπτογράφησης - αποκρυπτογράφησης παριστάνεται στο ακόλουθο σχήμα, όπου απεικονίζεται ότι μόνο όποιος έχει το "κλειδί" της κρυπτογράφησης μπορεί να διαβάσει την αρχική πληροφορία.



Εικόνα 10-4: Διαδικασία Κρυπτογράφησης - Αποκρυπτογράφησης

10.2 Κρυπτογραφία (Cryptography) - Κρυπτανάλυση (Cryptanalysis) – Κρυπτολογία (Cryptology)

Η **Κρυπτογραφία (cryptography)** είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση **τεχνικών κρυπτογράφησης και αποκρυπτογράφησης** με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η **Κρυπτανάλυση (cryptanalysis)** είναι η επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής, ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η Κρυπτογραφία και η Κρυπτανάλυση είναι οι δύο κλάδοι της **Κρυπτολογίας**, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Συνεπώς, η Κρυπτολογία από τη μία πλευρά ασχολείται με την **απόκρυψη** και από την άλλη με την **αποκάλυψη** του περιεχομένου ενός κωδικοποιημένου μηνύματος.

Σήμερα η Κρυπτολογία θεωρείται ένα διεπιστημονικό γνωστικό πεδίο, το οποίο μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης του ηλεκτρονικού μηχανικού. Η ρίζα της Κρυπτολογίας έγκειται στην προσπάθεια αποστολής μηνυμάτων, το περιεχόμενο των οποίων θα προστατεύεται, ώστε να αναγνωστεί μόνο από τον επιθυμητό παραλήπτη.

Η **Κρυπτογραφία** παρέχει τέσσερις βασικές λειτουργίες/ αντικειμενικούς σκοπούς:

1. ***Εμπιστευτικότητα***: Η πληροφορία προς μετάδοση είναι:
    - προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη,
    - ακατανόητη σε κάποιον τρίτο.
2. ***Ακεραιότητα***: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
3. ***Μη απάρνηση/αποποίηση***: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
4. ***Πιστοποίηση***: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν :
    - τις ταυτότητές τους
    - την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

10.3 Η Κρυπτογράφηση δεν αποτελεί πρόσφατη επινόηση

10.3.1 Σπαρτιάτες στρατηγοί

Η τέχνη της κρυπτογράφησης χρησιμοποιήθηκε ιδιαίτερα για πολεμικούς σκοπούς. Οι Σπαρτιάτες στρατηγοί ακολουθούσαν την εξής μέθοδο: Τύλιγαν ταινία περγαμηνής ή υφάσματος ή δέρματος γύρω από ξύλινο κύλινδρο (σκυτάλη) και στη συνέχεια κατέγραφαν μηνύματα κατά μήκος της περιέλιξης. Όταν η ταινία ξετυλίγονταν, τα γράμματα βρίσκονταν σε αταξία, η οποία δεν επέτρεπε την ανάγνωση του μηνύματος. Ο παραλήπτης έπρεπε να γνωρίζει τη διάμετρο της σκυτάλης, ώστε να τυλίξει την ταινία σε κύλινδρο (σκυτάλη) ίδιας διαμέτρου προκειμένου να αποκαλύψει το μήνυμα.

Εικόνα 10-5: Σπαρτιατική Σκυτάλη Κρυπτογράφησης

Συνοπτικά, στη μέθοδο κρυπτογράφησης των Σπαρτιατών διακρίνονται:

- **Αλγόριθμος κρυπτογράφησης**: Η χρήση της ταινίας (παπύρου) και της σκυτάλης.
- **Διαδικασία κρυπτογράφησης**: Το ξετύλιγμα του ταινίας (παπύρου).
- **Κλειδί κρυπτογράφησης**: Η ακριβής διάμετρο που πρέπει να έχει η σκυτάλη για να λειτουργήσει η αποκρυπτογράφηση.
- **Διαδικασία αποκρυπτογράφησης**: το τύλιγμα της γραμμένης ταινίας (παπύρου) στη σωστής διάμετρος σκυτάλη.

10.3.2 Enigma Κρυπτομηχανή

Λόγω της μεγάλης ανάγκης που υπήρχε για μετάδοση πληροφοριών ζωτικής σημασίας μεταξύ των στρατευμάτων κατά τη διάρκεια των δύο παγκοσμίων πολέμων, αναπτύχθηκαν μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάστηκαν κρυπτομηχανές και αποτελούσαν πολύπλοκα κρυπτοσυστήματα. Η κρυπτανάλυση τους απαιτούσε μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα έγινε εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.

Μία τέτοια κατασκευή είναι η κρυπτομηχανή Enigma (πήρε το όνομά της από την ελληνική λέξη «Αίνιγμα») που χρησιμοποιήθηκε στη Ναζιστική Γερμανία κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου για κρυπτογράφηση δεδομένων.

Ο Marian Rejewski, στην Πολωνία, προσπάθησε και τελικά παραβίασε το 1932 την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma χρησιμοποιώντας θεωρητικά μαθηματικά. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός προέβη σε

ορισμένες σημαντικές αλλαγές που οι Πολωνοί δεν μπόρεσαν να παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν.

Ο Alan Turing, βρετανός μαθηματικός και επιστήμονας των υπολογιστών κατάφερε να **ανακαλύψει το κλειδί κρυπτογράφησης του Enigma,** γεγονός καθοριστικής σημασίας για την έκβαση του πολέμου.

Εικόνα 10-6: Enigma Machine

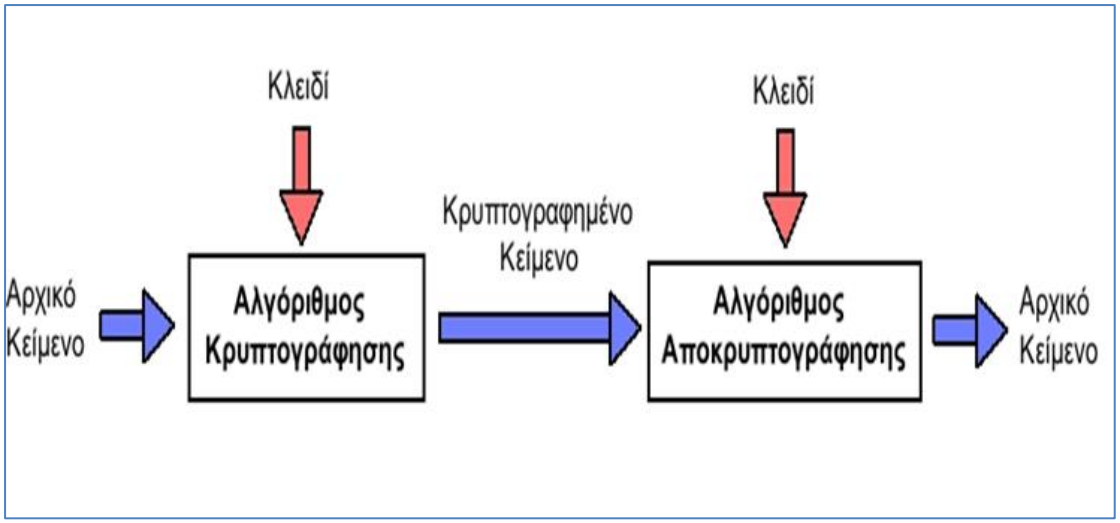
10.4 Είδη Κρυπτογράφησης

10.4.1 Συμμετρική Κρυπτογράφηση (Symmetric Cryptography)

Τα κυριότερα χαρακτηριστικά της Συμμετρικής Κρυπτογράφησης είναι τα εξής:

- Κατά τη διαδικασία της κρυπτογράφησης/αποκρυπτογράφησης χρησιμοποιείται **ένα κοινό κλειδί**.
- Η ασφάλεια βασίζεται στη **μυστικότητα του κλειδιού**.
- **Η ανταλλαγή του κλειδιού απαιτείται να γίνει μέσα από ένα ασφαλές κανάλι επικοινωνίας** ή με **φυσική παρουσία** των προσώπων.

Σχηματικά η διαδικασία της συμμετρικής κρυπτογράφησης παριστάνεται στο ακόλουθο σχήμα, όπου απεικονίζεται ότι υπάρχει ένα μόνο "κλειδί", το οποίο χρησιμοποιείται τόσο κατά τη διαδικασία της κρυπτογράφησης όσο και κατά τη διαδικασία της αποκρυπτογράφησης και επομένως θα πρέπει να βρίσκεται στην κατοχή τόσο του αποστολέα του μηνύματος όσο και του παραλήπτη. Ως εκ τούτου, για την ασφάλεια της επικοινωνίας απαιτείται ο αποστολέας και ο παραλήπτης να έχουν ανταλλάξει το κλειδί μέσω ενός ασφαλούς καναλιού επικοινωνίας ή με φυσική παρουσία.



Εικόνα 10-7: Συμμετρική Κρυπτογράφηση

Συνοπτικά, λοιπόν, η κρυπτογράφηση και αποκρυπτογράφηση γίνεται με τη βοήθεια:

- ενός **αλγόριθμου** κρυπτογράφησης, ο οποίος είναι δημόσιος/**γνωστός** και
- ενός **κλειδιού** κρυπτογράφησης το οποίο πρέπει να παραμείνει **μυστικό.**

Η **εμπιστευτικότητα** του κρυπτογραφημένου **μηνύματος** που μεταδίδεται βασίζεται κυρίως στη **μυστικότητα του κλειδιού** κρυπτογράφησης. Όσο **μεγαλύτερο είναι το κλειδί** τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς.

10.4.1.1 Αλγόριθμος Συμμετρικής Κρυπτογράφησης Advanced Encryption Standard (AES)

Ο αλγόριθμος συμμετρικής κρυπτογράφησης Advanced Encryption Standard (AES) δίνει τη δυνατότητα κρυπτογράφησης με κλειδιά διαφορετικού μήκους 128, 192 ή 256 bits. Με την αύξηση των bits του κλειδιού, οι πιθανοί συνδυασμοί ανεβαίνουν εκθετικά και ο αλγόριθμος γίνεται ισχυρότερος με την έννοια ότι μειώνονται οι πιθανότητες κάποιος να «μαντέψει το κλειδί». Για να γίνει αυτό κατανοητότερο αναφέρονται τα ακόλουθα:

- Ένα κλειδί 128-bit μπορεί να έχει πάνω από 300.000.000.000.000.000.000.000.000.000.000.000 πιθανούς συνδυασμούς.
- Ο μεγαλύτερος υπερυπολογιστής αυτή τη στιγμή στον κόσμο θα χρειαζόταν περίπου 250 δισεκατομμύρια χρόνια για να ελέγξει όλους τους συνδυασμούς του AES-128 και κατ' επέκταση να «μαντέψει το κλειδί».

10.4.1.2 Επιτυχής Χρήση Συμμετρικής Κρυπτογράφησης

Συμπερασματικά, για την επιτυχή χρήση της Συμμετρικής Κρυπτογράφησης απαιτούνται:

- Ένα ισχυρό κλειδί.
- Ένα ασφαλές κανάλι επικοινωνίας για την ανταλλαγή του κλειδιού.
- Ένας ισχυρός «αλγόριθμος συμμετρικής κρυπτογράφησης», όπως ο AES 256.
- Η συχνή αλλαγή του κοινού μυστικού κλειδιού, ώστε να μειωθεί η πιθανότητα αυτό να διαρρεύσει.

10.4.1.3 Εργαλείο Συμπίεσης και Συμμετρικής Κρυπτογράφησης 7-zip

Χρήση Συμμετρικής Κρυπτογράφησης γίνεται από το εργαλείο 7-zip (7zip), το οποίο διατίθεται δωρεάν (freeware). Πρόκειται για ένα εργαλείο συμπίεσης και συμμετρικής κρυπτογράφησης, το οποίο είναι διαθέσιμο για εγκατάσταση τόσο στον ιστότοπο https://www.7-zip.org/download.html όσο και στον εσωτερικό (intranet) ιστότοπο της Γενικής Γραμματείας Πληροφοριακών https://intranet.ggps.gsis.

Το εργαλείο 7zip μπορεί να το χρησιμοποιηθεί για τη συμπίεση και κρυπτογράφηση τόσο μεμονωμένων αρχείων όσο και φακέλων. Στην τελευταία περίπτωση θα δημιουργηθεί ένα συμπιεσμένο και κρυπτογραφημένο αρχείο, το οποίο θα περιέχει όλα τα αρχεία και τους υπό-φακέλους (μαζί με τα αρχεία που αυτοί περιέχουν) του επιλεγμένου φακέλου.

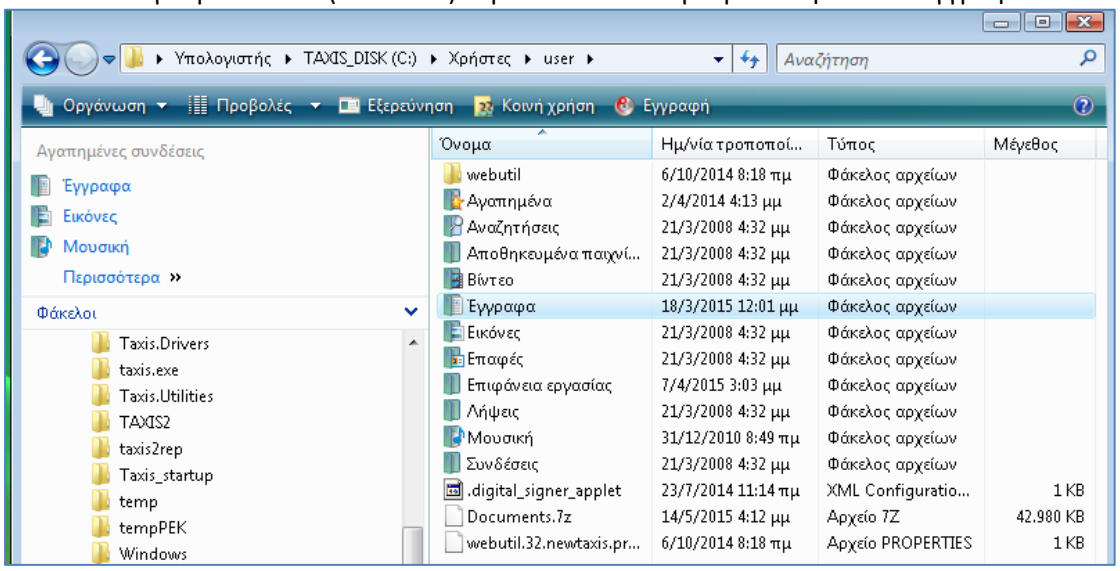
Το εργαλείο δύναται να χρησιμοποιήσει διαφορετικούς αλγορίθμους συμπίεσης και κρυπτογράφησης για να:

- συμπιέσει και αποσυμπιέσει
- κρυπτογραφήσει και αποκρυπτογραφήσει.

10.4.1.3.1 Συμπίεση - Κρυπτογράφηση

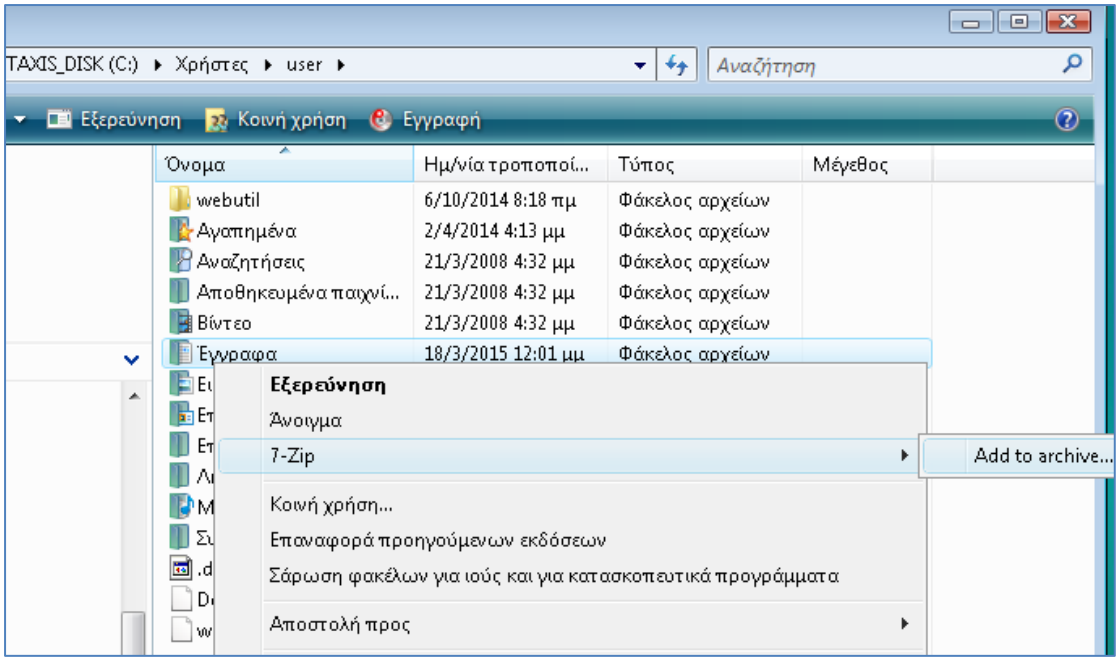
Στο παράδειγμα που ακολουθεί παρουσιάζεται η συμπίεση και κρυπτογράφηση του φακέλου «Έγγραφα» του Υπολογιστή:

- Ανοίγουμε τον File (Windows) Explorer και επιλέγουμε τον φάκελο «Έγγραφα».



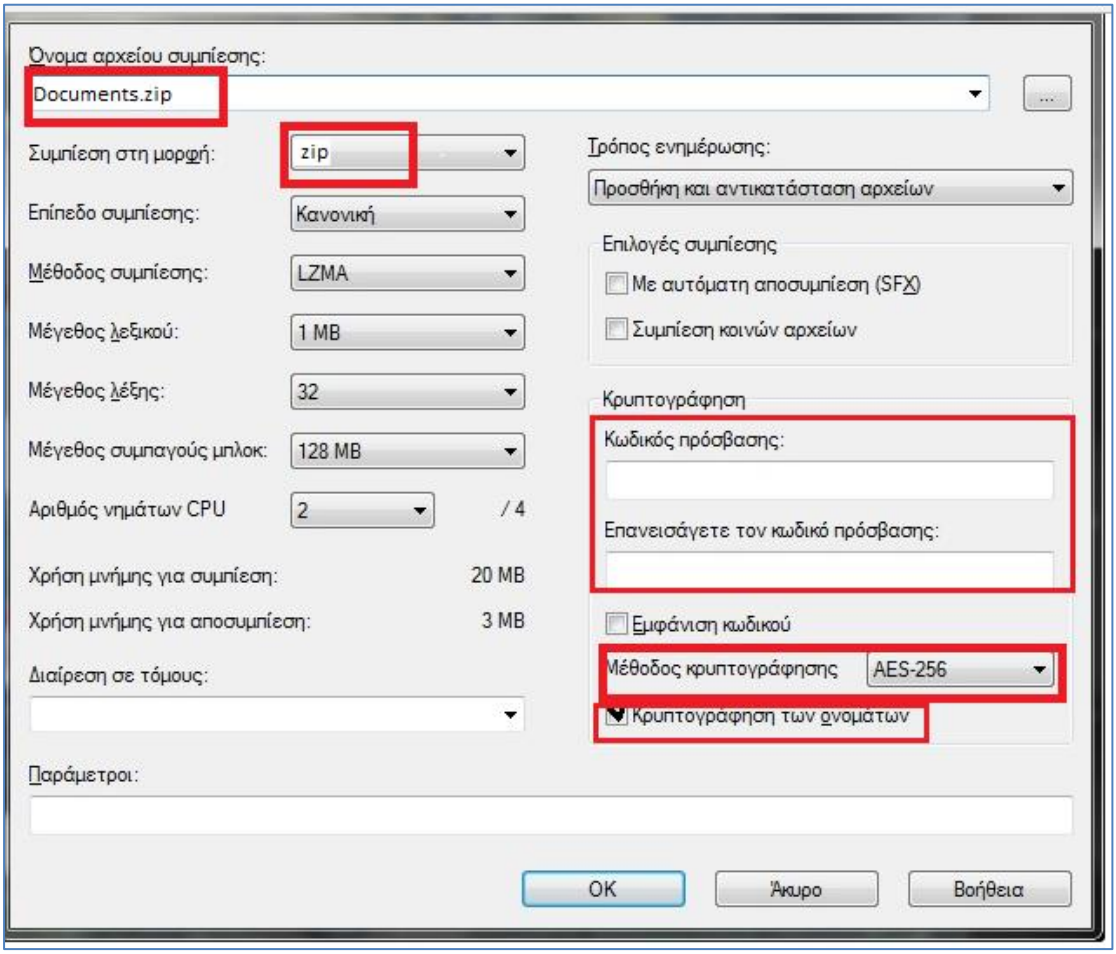
Εικόνα 10-8: Επιλογή φακέλου για Συμπίεση και Κρυπτογράφηση

- Πατάμε δεξί κλικ με το ποντίκι και επιλέγουμε 7-zip.
- Στη συνέχεια επιλέγουμε «Προσθήκη σε αρχείο συμπίεσης.../Add to archive …».



Εικόνα 10-9: Επιλογή 7zip - Προσθήκη σε αρχείο συμπίεσης…/Add to archive…

- Στο παράθυρο που εμφανίζεται θα πρέπει:
  - Να δηλώσουμε ένα όνομα για το προς αποθήκευση αρχείο.
    - Το όνομα του συμπιεσμένου και κρυπτογραφημένου αρχείου καλό είναι να παραμένει το ίδιο με το όνομα του αρχικού φακέλου / αρχείου. Αυτό θα μας βοηθήσει να θυμόμαστε το φάκελο/αρχείο που έχουμε συμπιέσει και κρυπτογραφήσει.
    - Εάν θέλουμε να αποθηκεύσουμε το συμπιεσμένο αρχείο μας σε διαφορετικό φάκελο από τον επιλεγμένο, τότε θα πρέπει να πατήσουμε στο κουμπί «…» και να επιλέξουμε τον φάκελο που θέλουμε να αποθηκευτεί το αρχείο.
  - Να επιλέξουμε «zip»στη «Συμπίεση στη μορφή /Archive format»
    - Η κατάληξη «zip» στο προς αποθήκευση αρχείο ενημερώνεται αυτόματα.
  - Να επιλέξουμε ένα «Συνθηματικό/Enter password», κωδικό δηλαδή, ο οποίος θα αποτελέσει το κλειδί της συμμετρικής κρυπτογράφηση και μετέπειτα αποκρυπτογράφησης του αρχείου μας.
    - Επιλέγουμε «Εμφάνιση Κωδικού» για να είμαστε σίγουροι για τον κωδικό που εισάγουμε.
    - Επιλέγουμε ισχυρό κωδικό (βλ. Κεφάλαιο Έβδομο).
    - Αν το αρχείο που συμπιέζουμε και κρυπτογραφούμε προορίζεται για κάποιο φορέα, με τον οποίο έχουμε συχνή επικοινωνία, τότε μπορούμε να χρησιμοποιούμε τον ίδιο κωδικό ώστε να μη χρειάζεται να τον επικοινωνούμε κάθε φορά.
  - Να επιλέξουμε ως «Μέθοδος Κρυπτογράφησης/Encryption Method» τον αλγόριθμο AES-256 (η ασφαλέστερη από τις παρεχόμενες μεθόδους).
  - Να επιλέξουμε την «Κρυπτογράφηση των ονομάτων/Encrypt file names»).



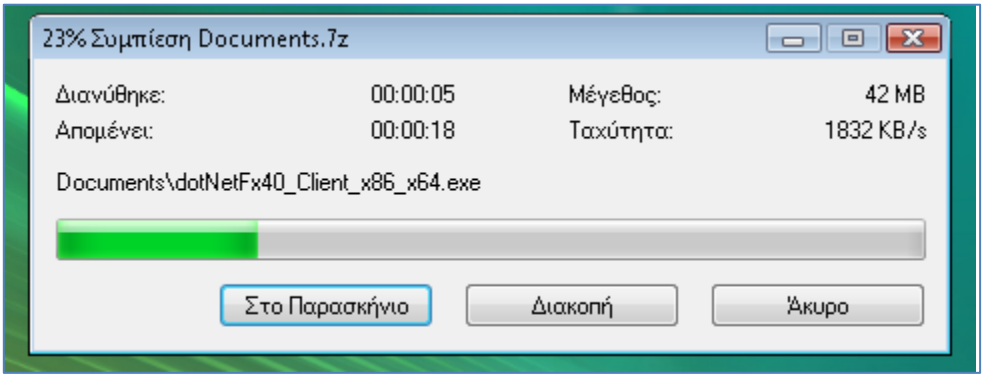
Εικόνα 10-10: Ρυθμίσεις Συμπίεσης και Κρυπτογράφησης

- Εάν θέλουμε να «σπάσουμε» σε κομμάτια το συμπιεσμένο αρχείο επιλέγουμε «Διαίρεση σε τόμους/Split to volumes, bytes» και μετά κάποιο από τα προτεινόμενα μεγέθη. Με τον τρόπο αυτό μπορούμε να αποθηκεύσουμε τα «κομμάτια» του αρχείου μας σε κάποιο/α cd ή dvd που θα επιλέξουμε. Η δυνατότητα αυτή διευκολύνει σε περίπτωση που το μέγεθος του αρχείου είναι πολύ μεγάλο και δεν μπορεί να αποθηκευτεί σε ένα μόνο φορητό αποθηκευτικό μέσο λόγω της περιορισμένης χωρητικότητας που αυτό έχει.

Εικόνα 10-11: Προτεινόμενα μεγέθη για διαίρεση συμπιεσμένου αρχείου

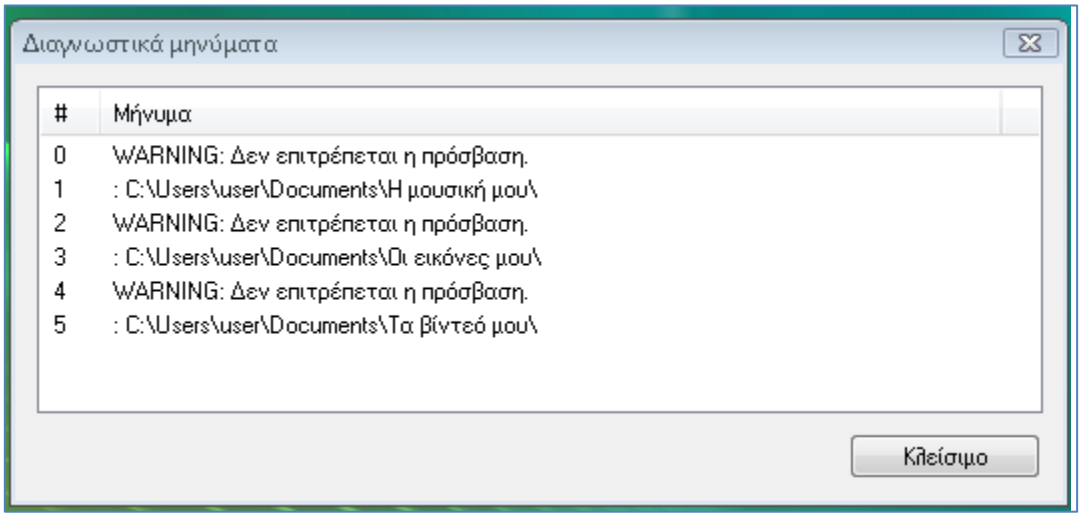
Ανάλογα με το μέγεθος του αρχείου και το μέγεθος κάθε «κομματιού» που μπορούμε να αποθηκεύσουμε, θα δημιουργηθεί αντίστοιχος αριθμός αρχείων (κομματιών) στον φάκελο. Για παράδειγμα, αν το συνολικό μέγεθος του αρχείου μας είναι 1,4 GB και επιλέξουμε να το συμπιέσουμε σε cd με χωρητικότητα 700 MB, τότε στον φάκελο αποθήκευσης θα εμφανιστούν 2 (δύο) αρχεία. Καθένα από αυτά θα έχει μέγεθος 700 MB. Στη συνέχεια θα εγγράψουμε το καθένα από τα δύο αρχεία σε ξεχωριστά cd.

- Για την ολοκλήρωση της διαδικασίας πατάμε «**ΟΚ**» και η συμπίεση και κρυπτογράφηση των αρχείων ξεκινά.



Εικόνα 10-12: Πρόοδος διαδικασίας συμπίεσης και κρυπτογράφησης

- Στο διαγνωστικό μήνυμα, το οποίο ενδέχεται να εμφανιστεί κατά την ολοκλήρωση της διαδικασίας, πατάμε «Κλείσιμο».



Εικόνα 10-13: Διαγνωστικό μήνυμα κατά τη διαδικασία συμπίεσης και κρυπτογράφησης

Με την επιτυχή ολοκλήρωση της διαδικασίας θα βρούμε το αρχείο μας συμπιεσμένο και κρυπτογραφημένο μέσα στον φάκελο που επιλέξαμε για αποθήκευση.

Προσοχή:

- Ανάλογα με το μέγεθος του προς συμπίεση αρχείου/φακέλου η διαδικασία μπορεί να διαρκέσει από λίγα δευτερόλεπτα έως αρκετά λεπτά.
- Εάν κάποιο αρχείο που θέλουμε να συμπιέσουμε και να κρυπτογραφήσουμε, χρησιμοποιείται κατά τη διάρκεια της συμπίεσης, τότε το εργαλείο 7zip θα εμφανίσει σφάλμα. Καλό θα ήταν πριν ξεκινήσει η διαδικασία, να είναι κλειστά όλα τα προς συμπίεση και κρυπτογράφηση αρχεία.

10.4.1.3.2 Αποστολή Κρυπτογραφημένου Αρχείου

Εάν το κρυπτογραφημένο αρχείο προορίζεται για αποστολή, τότε αποστέλλεται:

- ως συνημμένο μέσω ηλεκτρονικού ταχυδρομείου ή
- σε φορητό μέσω αποθήκευσης με συμβατικό τρόπο αποστολής.

Ο κωδικός ασφαλείας επικοινωνείται στον παραλήπτη μέσω διαφορετικού καναλιού επικοινωνίας σε σχέση με το αρχείο.

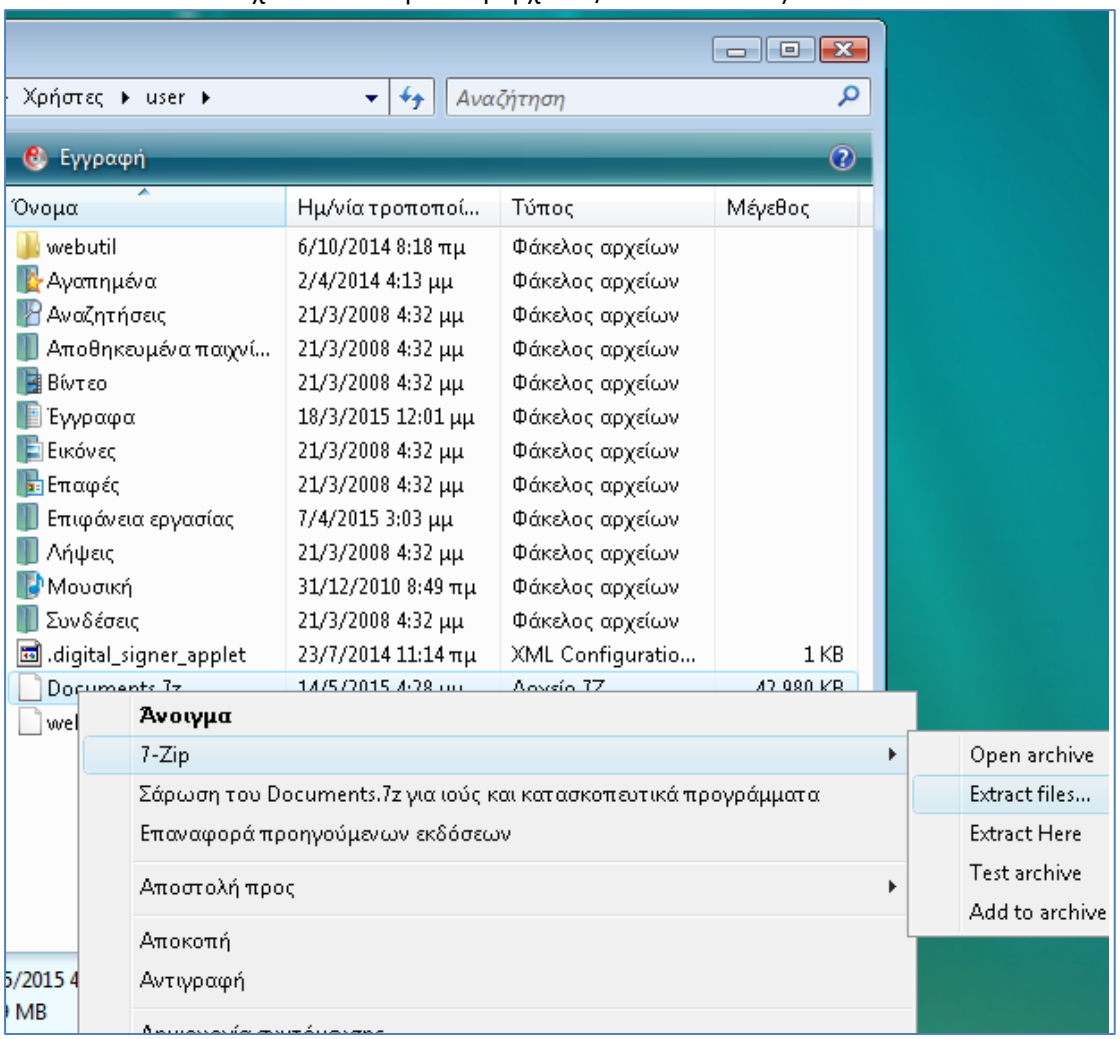
Η αποστολή του κρυπτογραφημένου αρχείου συνοδεύεται από τις ακόλουθες οδηγίες:

«…Λόγω εφαρμογής της πολιτικής ασφαλείας του Υπουργείου Οικονομικών, σας επισυνάπτουμε κρυπτογραφημένο αρχείο, το οποίο περιέχει τα αρχεία που σας αποστέλλουμε. Για τον κωδικό αποκρυπτογράφησης του αρχείου σας παρακαλούμε είτε να επικοινωνήσετε μαζί μας στο τηλέφωνο XXXXXXXXXX είτε να μας αποστείλετε ένα τηλέφωνο επικοινωνίας ώστε να επικοινωνήσουμε εμείς μαζί σας…»

10.4.1.3.3 Αποσυμπίεση - Αποκρυπτογράφηση

Για τη διαδικασία αποσυμπίεσης και αποκρυπτογράφησης:

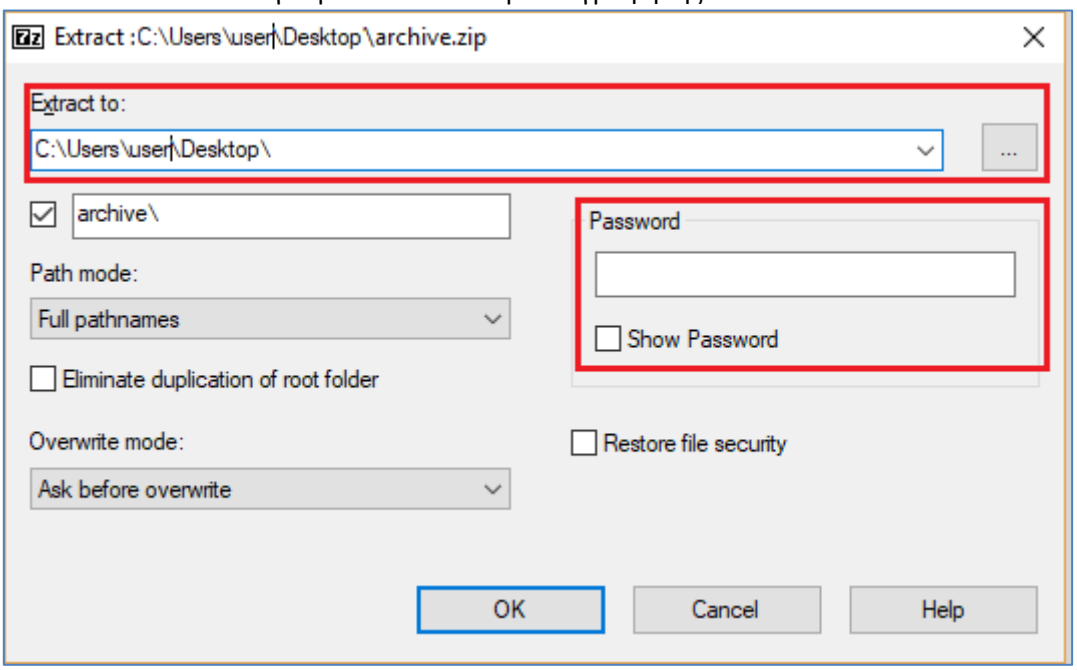
- Ανοίγουμε τον File (Windows) Explorer και επιλέγουμε το σημείο (μέσο αποθήκευσης και φάκελος) που έχει αποθηκευτεί το συμπιεσμένο και κρυπτογραφημένο αρχείο.
- Επιλέγουμε το εν λόγω αρχείο, πατάμε δεξί κλικ με το ποντίκι και επιλέγουμε 7-zip.
- Στη συνέχεια επιλέγουμε «Αποσυμπίεση αρχείων/Extract files»…
    - Σε περίπτωση που κατά τη συμπίεση είχαμε επιλέξει «Διαίρεση σε τόμους/Split to volumes, bytes» και επομένως το συμπιεσμένο αρχείο αποτελείται από διάφορα «κομμάτια» τότε φροντίζουμε να επιλέξουμε να ξεκινήσει η αποσυμπίεση στο πρώτο «κομμάτι» (δηλαδή επιλέγουμε το πρώτο «κομμάτι», πατάμε δεξί κλικ με το ποντίκι , επιλέγουμε 7-zip και στη συνέχεια «Αποσυμπίεση αρχείων/Extract files»…).



Εικόνα 10-14: Επιλογή 7zip – Αποσυμπίεση αρχείων/Extract files…

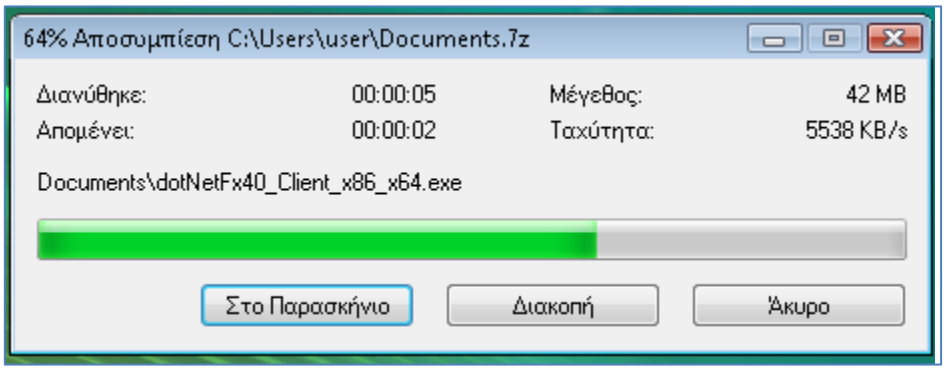
- Στη συνέχεια θα μας ζητηθεί:

- Να προσδιορίσουμε τον φάκελο που θέλουμε να αποσυμπιεστούν τα συμπιεσμένα αρχεία (π.χ. επιλέγουμε την Επιφάνεια Εργασίας).
- Να εισάγουμε τον κωδικό κρυπτογράφησης.



Εικόνα 10-15: Ρυθμίσεις Αποσυμπίεσης και Αποκρυπτογράφησης

➢ Στη συνέχεια πατάμε **OK** και η διαδικασία αποσυμπίεσης και αποκρυπτογράφησης ξεκινά.



Εικόνα 10-16: Πρόοδος διαδικασίας αποσυμπίεσης και αποκρυπτογράφησης

Με την επιτυχή ολοκλήρωση της διαδικασίας εμφανίζεται ο φάκελος και τα αρχεία που αποσυμπιέσαμε και αποκρυπτογραφήσαμε στην Επιφάνεια Εργασίας καθώς αυτήν ορίσαμε ως χώρο αποστολής των εξαγόμενων αρχείων.

Εικόνα 10-17: Ολοκλήρωση Αποσυμπίεσης και Αποκρυπτογράφησης

10.4.2 Μη Συμμετρική (Asymmetric Cryptography) Κρυπτογράφηση ή Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Cryptography)

Η Μη Συμμετρική (Asymmetric) Κρυπτογράφηση ή διαφορετικά Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Cryptography) καλύπτει την αδυναμία μεταφοράς/ανταλλαγής κλειδιών που παρουσιάζει η Συμμετρική Κρυπτογράφηση.

Το κυριότερο χαρακτηριστικό της είναι ότι υπάρχει ένα **ζεύγος κλειδιών,** ένα **ιδιωτικό** και ένα **δημόσιο**:

- Το δημόσιο είναι διαθέσιμο (γνωστό) σε όλους ενώ το ιδιωτικό είναι μυστικό (αυστηρά προσωπικό).
- Η σχέση των κλειδιών έγκειται στο **ότι κρυπτογραφεί το ένα μπορεί να το αποκρυπτογραφήσει μόνο το άλλο** (μοιάζει δηλαδή με το ταίριασμα κλειδιού και λουκέτου).

10.4.2.1 Διαδικασία Μη Συμμετρικής Κρυπτογράφησης και Αποκρυπτογράφησης

Ας υποθέσουμε ότι ο αποστολέας (Bob) θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον παραλήπτη (Alice). Επομένως, στο συγκεκριμένο παράδειγμα:

- Αποστολέας είναι ο Bob
- Παραλήπτης είναι η Alice
- Μήνυμα του Bob προς την Alice: «Hello Alice!»

Καταρχήν, ο παραλήπτης (Alice) θα πρέπει να έχει στην κατοχή του/της ένα ζεύγος κλειδιών (ιδιωτικό κλειδί - δημόσιο κλειδί). Όπως προαναφέρθηκε το ιδιωτικό κλειδί είναι αυστηρά προσωπικό (μυστικό) ενώ το δημόσιο μπορεί να διατεθεί.

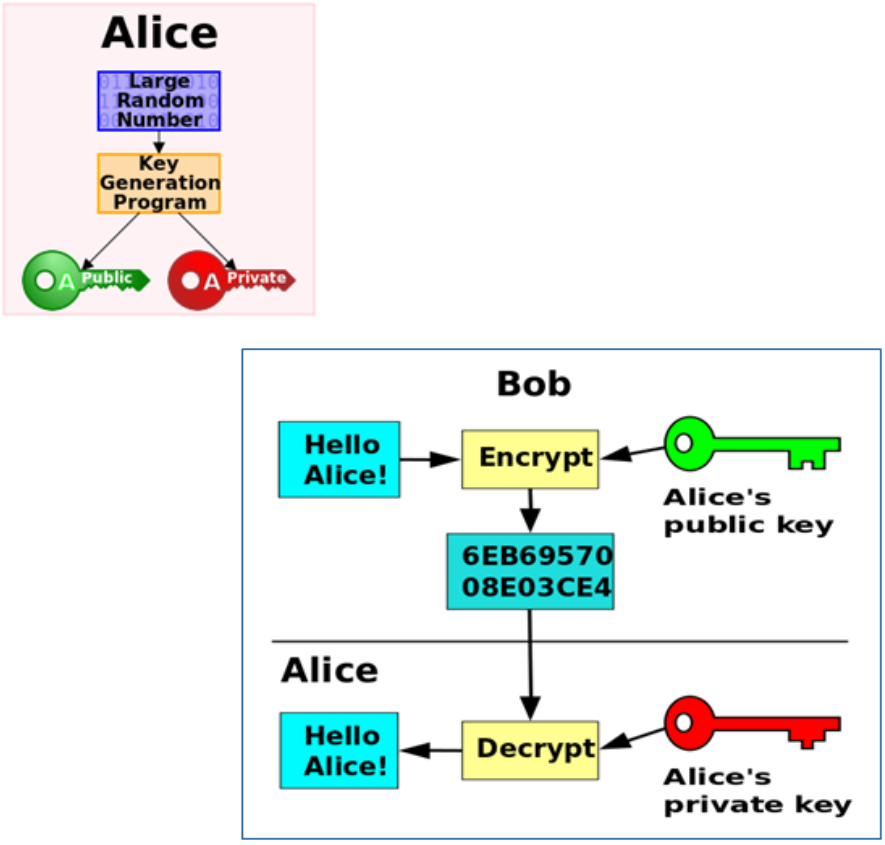
Στη συνέχεια, ο παραλήπτης (Alice) θα πρέπει να φροντίσει ώστε ο αποστολέας (Bob) να λάβει το δημόσιο κλειδί του/της (το δημόσιο κλειδί του παραλήπτη, δηλαδή το κλειδί της

Alice). Καθώς πρόκειται για δημόσιο κλειδί μπορεί να διατεθεί χωρίς να απαιτείται ένα ασφαλές κανάλι επικοινωνίας για τη μεταφορά/κοινοποίησή του.

Στην συνέχεια, ο αποστολέας (Bob) κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη (το δημόσιο κλειδί της Alice) και αποστέλλει το κρυπτογραφημένο μήνυμα στον παραλήπτη (Alice).

Ο παραλήπτης (Alice) αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί (ιδιωτικό της Alice).

Κανείς άλλος δεν μπορεί να αποκρυπτογραφήσει το συγκεκριμένο κρυπτογραφημένο μήνυμα παρά μόνο η Alice, η οποία έχει στην αποκλειστική κατοχή της το ιδιωτικό της κλειδί.



Εικόνα 10-18: Διαδικασία Μη Συμμετρικής Κρυπτογράφησης και Αποκρυπτογράφησης

10.4.3 Διαφορές Συμμετρικής και Μη Συμμετρικής Κρυπτογράφησης

Συνοπτικά οι διαφορές των δύο μεθόδων είναι οι εξής:

Συμμετρική Κρυπτογράφηση:

- Μοναδική δικλείδα ασφαλείας είναι το **κοινό** μυστικό κλειδί (κωδικός), το οποίο:
  - Πρέπει να είναι ισχυρό.
  - Πρέπει να κοινοποιηθεί με ασφάλεια.
- Πρόκειται για απλή, εύχρηστη, γρήγορη μέθοδο.

- Η μοναδική δυσκολία της έγκειται στην **ανταλλαγή** του μυστικού κλειδιού (κωδικού).

Μη Συμμετρική Κρυπτογράφηση:

- Παρέχει διπλή δικλείδα ασφαλείας:
  - Κάτι που κατέχω: το ιδιωτικό κλειδί.
  - Κάτι που γνωρίζω: τον μυστικό κωδικό του ιδιωτικού κλειδιού.
- Πρόκειται για πολύπλοκη μέθοδος με την έννοια ότι απαιτεί σημαντική υπολογιστική δύναμη.
- Μπορεί να αποβεί **καταστροφική** αν χαθεί το ιδιωτικό κλειδί!!!

10.4.4 Pretty Good Privacy (PGP)

Πρόκειται για υβριδική μέθοδο κρυπτογράφησης, η οποία συνδυάζει **συμμετρική και μη συμμετρική κρυπτογράφηση.** Επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων , διασφαλίζοντας το απόρρητο και πιστοποιώντας την ταυτότητα σε συνδυασμό με την ταχύτητα και ευκολία λειτουργίας.

Πιο συγκεκριμένα, κατοχυρώνει ότι:

- μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα θα μπορέσει να το διαβάσει (**διασφάλιση του απορρήτου**)
- μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο (**πιστοποίηση της ταυτότητας**)
- η διασφάλιση του απόρρητου και η πιστοποίηση της ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία (**ευκολία**). Δεν είναι δηλαδή αναγκαία ασφαλή κανάλια επικοινωνίας για την ανταλλαγή των κλειδιών, διότι η μέθοδος PGP βασίζεται σε μια δυναμική νέα τεχνολογία (κρυπτογράφηση "δημοσίων κλειδιών").

10.4.4.1 Διαδικασία PGP

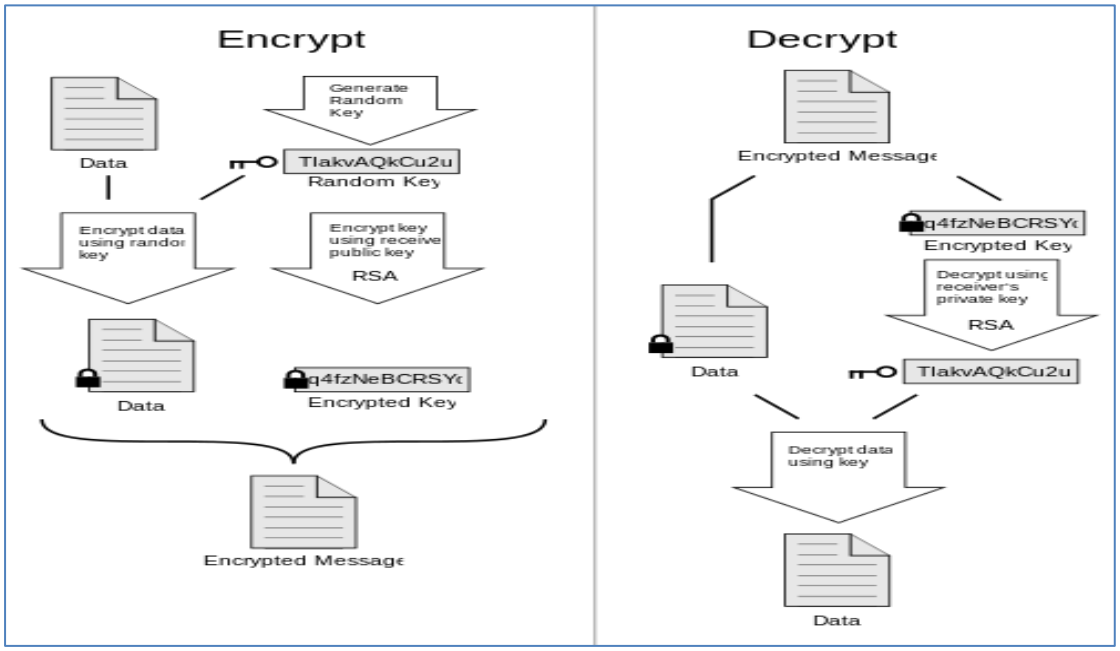
Όπως προαναφέρθηκε, η PGP μέθοδος είναι μια υβριδική λύση που συνδυάζει Συμμετρική και Μη Συμμετρική Κρυπτογράφηση. Η Συμμετρική Κρυπτογράφηση χρησιμοποιείται για την κρυπτογράφηση του κυρίως κειμένου και η Μη Συμμετρική Κρυπτογράφηση για την κρυπτογράφηση του κλειδιού κρυπτογράφησης του κυρίως κειμένου, το οποίο θα πρέπει να κοινοποιηθεί από τον αποστολέα του μηνύματος στον παραλήπτη.

Αναλυτικότερα τα βήματα της διαδικασίας είναι τα εξής:

- **Συμμετρική** Κρυπτογράφηση
  - Ένα προσωρινό τυχαίο κλειδί (**session key**) δημιουργείται μόνο για μια συγκεκριμένη φορά.
  - Το αρχικό κείμενο κρυπτογραφείται με το κλειδί αυτό (session key).
  - Το κρυπτογραφημένο κείμενο αποστέλλεται στον παραλήπτη, ο οποίος χρειάζεται και το session key για να μπορέσει να το αποκρυπτογραφήσει.
- **Μη Συμμετρική** Κρυπτογράφηση
  - Το session key κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.
  - Το κρυπτογραφημένο session key αποστέλλεται στον παραλήπτη (είναι ο μόνος που θα μπορέσει το αποκρυπτογραφήσει με το ιδιωτικό του κλειδί).

- Έχοντας το session key ο παραλήπτης θα αποκρυπτογραφήσει το αρχικά κρυπτογραφημένο κείμενο.

Στο ακόλουθο σχήμα παριστάνεται σχηματικά η διαδικασία με την οποία η μέθοδος PGP επιτυγχάνει την κρυπτογράφηση και την αποκρυπτογράφηση.



Εικόνα 10-19: Κρυπτογράφηση και Αποκρυπτογράφηση με τη μέθοδο PGP

10.4.4.2 OpenPGP, PGP και GPG (GNU Privacy Guard)

Ακολούθως γίνεται μια προσπάθεια αποσαφήνισης των όρων OpenPGP, PGP και GPG, οι οποίοι χρησιμοποιούνται ευρέως δημιουργώντας συχνά σύγχυση:

- **OpenPGP:** Πρόκειται για Πρότυπο, το οποίο έχει εγκριθεί από το Internet Engineering Task Force (IETF) και περιγράφει τεχνολογίες κρυπτογράφησης.
- **PGP:** Πρόκειται για ιδιόκτητη λύση κρυπτογράφησης βασισμένη στο πρότυπο OpenPGP. Τα δικαιώματα για το λογισμικό της ανήκουν στη Symantec.
- **GnuPG (GNU Privacy Guard):** Πρόκειται για ελεύθερο λογισμικό κρυπτογράφησης (βλ. ενότητα 10.4.4.3 Εργαλείο Gpg4win - Kleopatra) βασισμένο στο πρότυπο OpenPGP. Μπορεί να χρησιμοποιηθεί, να τροποποιηθεί και να διανεμηθεί ελεύθερα υπό τους όρους της GNU General Public License.

10.4.4.3 Εργαλείο Gpg4win - Kleopatra

Το εργαλείο Gpg4win (**Kleopatra**) είναι freeware (δωρεάν λογισμικό) και είναι διαθέσιμο στην ιστοσελίδα https://www.gpg4win.org/. Πρόκειται για λογισμικό κρυπτογράφησης βασισμένο στο OpenPGP πρότυπο, το οποίο:

- επιτρέπει τη δημιουργία ζεύγους κλειδιών
- παρέχει τη δυνατότητα προσθήκης ψηφιακής υπογραφής σε αρχεία και μηνύματα
- παρέχει τη δυνατότητα κρυπτογράφησης και αποκρυπτογράφησης αρχείων / μηνυμάτων συνδυάζοντας Συμμετρική και Μη Συμμετρική Κρυπτογράφηση.

10.5 Εφαρμογές Κρυπτογράφησης

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη τη μεταφορά της πληροφορίας σε:

- ✓ Τραπεζικά δίκτυα - ATM (Ασφάλεια συναλλαγών)
- ✓ Κινητή τηλεφωνία, σταθερή τηλεφωνία (cryptophones)
- ✓ Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
- ✓ Διπλωματικά δίκτυα (Τηλεγραφήματα)
- ✓ Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
- ✓ Ηλεκτρονική ψηφοφορία
- ✓ Ηλεκτρονική δημοπρασία
- ✓ Ηλεκτρονικό γραμματοκιβώτιο
- ✓ Εταιρικές πληροφορίες
- ✓ Συστήματα συναγερμών, συστήματα βιομετρικής αναγνώρισης, κτλ.

10.6 Ενδεδειγμένες Χρήσεις Κρυπτογράφησης στο Υπουργείο Οικονομικών

10.6.1 Ανταλλαγή πληροφοριών (αρχείων) με άλλες υπηρεσίες

Στις υπηρεσίες του Υπουργείου Οικονομικών εμφανίζεται συχνά η ανάγκη ανταλλαγής πληροφοριών (αρχείων) με άλλες υπηρεσίες του Υπουργείου, του δημοσίου ή τρίτους φορείς. Οι οδηγίες που πρέπει να ακολουθούνται για την ασφαλή αποστολή/μεταφορά των πληροφοριών είναι οι εξής:

- ➢ Το αρχείο που εμπεριέχει τις πληροφορίες θα πρέπει να συμπιεστεί και να κρυπτογραφεί με Συμμετρική Κρυπτογράφηση (χρήση του εργαλείου 7zip – βλ. 10.4.1.3 Εργαλείο Συμπίεσης και Συμμετρικής Κρυπτογράφησης 7-zip).
- ➢ Σε περίπτωση που το μέγεθος του συμπιεσμένου και κρυπτογραφημένου αρχείου είναι **μικρό** (δεν ξεπερνά τα 10MB) τότε η αποστολή του μπορεί να γίνει:
  - **Μέσω ηλεκτρονικού ταχυδρομείου** (ηλεκτρονική αλληλογραφία).
- ➢ Σε περίπτωση που το μέγεθος του συμπιεσμένου και κρυπτογραφημένου αρχείου είναι **μεγάλο** (ξεπερνά τα 10MB) τότε η αποστολή του μπορεί να γίνει:
  - Με συμβατικό τρόπο και **χρήση φορητού αποθηκευτικού μέσου** (κυρίως οπτικού).
- ➢ Το κλειδί της Συμμετρικής Κρυπτογράφησης (κωδικός) θα πρέπει να επικοινωνηθεί στον παραλήπτη του συμπιεσμένου και κρυπτογραφημένου αρχείου μέσω ασφαλούς καναλιού επικοινωνίας, διαφορετικού από το κανάλι που χρησιμοποιήθηκε για την αποστολή του αρχείου.

10.6.2 Τακτική ασφαλής ανταλλαγή αρχείων με τρίτους φορείς

Στις υπηρεσίες του Υπουργείου Οικονομικών εμφανίζεται η ανάγκη **τακτικής** ασφαλούς αποδοχής πληροφοριών (αρχείων) από τρίτους φορείς (π.χ. Χρηματοπιστωτικά Ιδρύματα). Οι οδηγίες που πρέπει να ακολουθούνται είναι οι εξής:

- ➢ Χρήση Open PGP / GnuPG (βλ. ενότητα 10.4.4.3 Εργαλείο Gpg4win - Kleopatra) για τη δημιουργία ζεύγους κλειδιών.
- ➢ Ανταλλαγή δημοσίων κλειδιών μέσω θεσπισμένης διαδικασίας.
- ➢ Χρήση Open PGP / GnuPG (βλ. ενότητα 10.4.4.3 Εργαλείο Gpg4win - Kleopatra) για την ψηφιακή υπογραφή και κρυπτογράφηση των αρχείων.

- Χρήση του SFTP Server (secure FTP) της Γενικής Γραμματείας Πληροφοριακών Συστημάτων - Δ/νση Διαχείρισης Υπολογιστικών Υποδομών/Τμήμα Α' για την μεταφορά (upload) του κρυπτογραφημένου αρχείου.
    - Αν ο όγκος της πληροφορίας είναι πολύ μεγάλος (το μέγεθος του αρχείου ξεπερνά τα 100MB) προτείνεται η χρήση φορητού αποθηκευτικού μέσου (USB stick, USB HDD, CD Rom, DVD Rom) για την αποθήκευση του κρυπτογραφημένου αρχείου και η αποστολή του αποθηκευτικού μέσου με συμβατικό τρόπο.

10.6.3 Ασφαλής εφεδρική αποθήκευση ευαίσθητης πληροφορίας σε φορητό μέσο αποθήκευσης

Είναι απαραίτητη η διατήρηση αντιγράφων ασφαλείας των σημαντικών μας αρχείων σε ένα τουλάχιστον επιπλέον αποθηκευτικό μέσο ώστε να διασφαλίσουμε τα πολύτιμα δεδομένα μας σε περίπτωση κλοπής, φθοράς ή απώλειας γενικότερα του κύριου αποθηκευτικού μέσου. Για την **ασφαλή** εφεδρική αποθήκευση ευαίσθητων πληροφοριών σε φορητά μέσα αποθήκευσης (USB stick, USB HDD, CD Rom, DVD Rom, Κινητό τηλέφωνο) θα πρέπει να γίνεται χρήση κρυπτογράφησης (αποθήκευση των πληροφοριών στο εφεδρικό μέσο αποθήκευσης με τη μορφή κρυπτογραφημένου αρχείου).

10.7 Ψηφιακή Υπογραφή

10.7.1 Ηλεκτρονική Διακίνηση Εγγράφων και Ψηφιακή Υπογραφή

Η ψηφιακή υπογραφή χρειάζεται για την ασφαλή ηλεκτρονική διακίνηση εγγράφων και μηνυμάτων καθώς εξασφαλίζει την εγκυρότητα τους, δηλαδή προστατεύει την αυθεντικότητα και την ακεραιότητά τους.

Μερικά από τα οφέλη που επιφέρει η ηλεκτρονική διακίνηση εγγράφων είναι τα ακόλουθα:

- Εξοικονόμηση πόρων και επίτευξη οικονομιών κλίμακας.
    - Μέγιστη δημοσιονομική εξοικονόμηση της τάξεως των 421 εκατ. ευρώ ανά έτος σύμφωνα με τη σχετική μελέτη του Ιδρύματος Οικονομικών και Βιομηχανικών Ερευνών (ΙΟΒΕ) – 2014-2015.
- Ταχύτερη διεκπεραίωση καθημερινών διαδικασιών.
- Εκσυγχρονισμός της Δημόσιας Διοίκησης.
- Αύξηση της αποδοτικότητας των Δημόσιων Υπηρεσιών με χρήση σύγχρονων μεθόδων, πρακτικών και εργαλείων.
- Μείωση των γραφειοκρατικών δομών.
    - Καλύτερη εξυπηρέτηση πολιτών και επιχειρήσεων.
- Διαφάνεια στη δημόσια διοίκηση.
- Δημόσια διοίκηση πιο φιλική προς το περιβάλλον.
- Συμμόρφωση της χώρας με Κοινοτικές Οδηγίες και Κανονισμούς / Αντιμετώπιση διεθνών υποχρεώσεων.
    - Η πλειοψηφία των κρατών μελών της ΕΕ έχει υιοθετήσει εδώ και χρόνια την ηλεκτρονική διακίνηση εγγράφων.
    - Ο **Κανονισμός 910/2014** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ – γνωστός και με τη συντομογραφία eIDAs Regulation (βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014R0910&from=EN).

10.7.2 Ορισμός Ψηφιακής Υπογραφής

Σύμφωνα με το Άρθρο 2 του Π.Δ. 150/2001 (ΦΕΚ 125/Α΄/2001) ως «**προηγμένη ηλεκτρονική υπογραφή**» ή «**ψηφιακή υπογραφή**» νοείται η ηλεκτρονική υπογραφή, που πληρεί τους εξής όρους:

α) συνδέεται μονοσήμαντα με τον υπογράφοντα,

β) είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος,

γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και

δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

Επομένως, μια έγκυρη ψηφιακή υπογραφή **δίνει στον παραλήπτη τη διαβεβαίωση** ότι το έγγραφο/μήνυμα στο οποίο έχει ενσωματωθεί:

- ✓ ανήκει στον συντάκτη που το υπέγραψε ψηφιακά και
- ✓ δεν παραποιήθηκε κατά την ψηφιακή διαδρομή του.

Επιπλέον, ο υπογράφων δεν μπορεί να αρνηθεί τη συμβολή του στην εν λόγω συναλλαγή (δηλαδή δεν μπορεί να αποποιηθεί ευθύνη).

Σύμφωνα με το Άρθρο 3 του Π.Δ. 150/2001 (ΦΕΚ 125/Α΄/2001):

> «η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρης υπογραφής, τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο».

Επομένως, η ψηφιακή υπογραφή έχει την **ίδια νομική ισχύ** με την ιδιόχειρη και παρέχει μεγαλύτερη ασφάλεια, αφού:

- Είναι αδύνατον να πλαστογραφηθεί.
- Είναι διαφορετική για κάθε έγγραφο.
- Προστατεύει από αποποίηση και μονομερείς τροποποιήσεις
  - Μετά την προσθήκη ψηφιακής υπογραφής το αυθεντικό περιεχόμενο του εγγράφου δεν τροποποιείται.

10.7.3 Ψηφιακό Πιστοποιητικό

Το ψηφιακό πιστοποιητικό:

- Είναι μια Ηλεκτρονική Ταυτότητα που αποδεικνύει την ταυτότητα μιας οντότητας στον ηλεκτρονικό κόσμο,αποτελεί, δηλαδή, ένα είδος Ηλεκτρονικού Διαβατηρίου.
- Εκδίδεται από έναν Πάροχο Υπηρεσιών Πιστοποίησης που εγγυάται για τα στοιχεία του κατόχου του, ακριβώς όπως η αρμόδια κρατική αρχή εγγυάται για την έκδοση του διαβατηρίου.

Το ψηφιακό πιστοποιητικό αποτελείται από:

- Το **ιδιωτικό** κλειδί (ψηφιακά δεδομένα υπό την αποκλειστική κατοχή του κατόχου)
- Το **δημόσιο** κλειδί (ψηφιακά δεδομένα που δημοσιεύονται και χρησιμοποιούνται για επαλήθευση της κατοχής του πιστοποιητικού).

Υπάρχουν διάφοροι τύποι ψηφιακών πιστοποιητικών, για παράδειγμα

- Πιστοποιητικά Υπογραφής Αρχείων και Μηνυμάτων,

- Πιστοποιητικά Κρυπτογράφησης,
- Πιστοποιητικά Υπογραφής Κώδικα,
- SSL πιστοποιητικά.

Στην πραγματικότητα οτιδήποτε χρειάζεται να αποδείξει την ταυτότητα του στον ηλεκτρονικό κόσμο (φυσικό πρόσωπο, νομικό πρόσωπο, εφαρμογή, server, κτλ.) χρησιμοποιεί ένα ψηφιακό πιστοποιητικό.

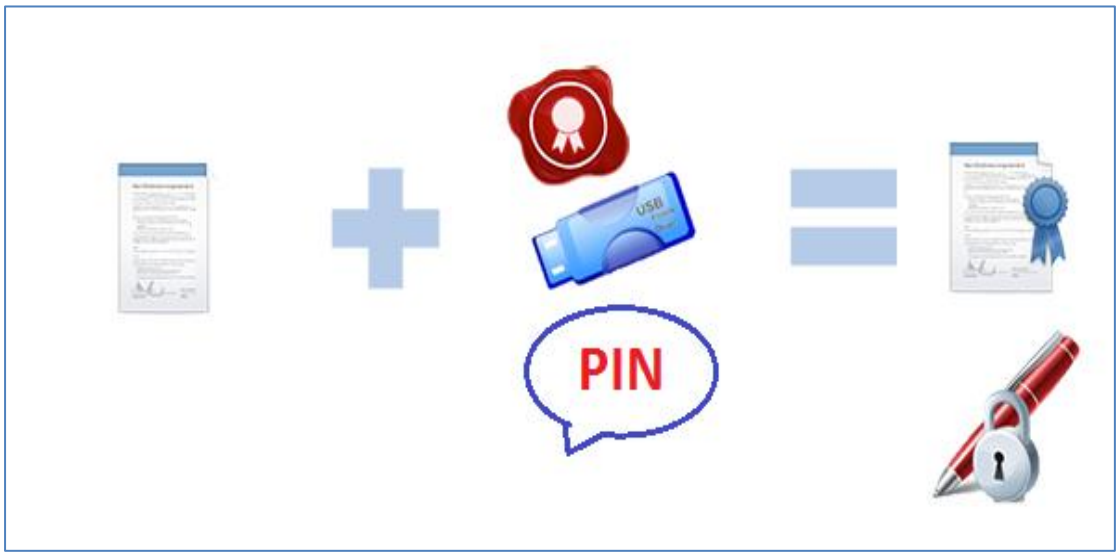
Επιπλέον, τα ψηφιακά πιστοποιητικά, ανάλογα με το αποθηκευτικό μέσο στο οποίο αποθηκεύονται, διακρίνονται σε ψηφιακά πιστοποιητικά **Σκληρής Αποθήκευσης** και ψηφιακά πιστοποιητικά **Χαλαρής Αποθήκευσης.** Πιο συγκεκριμένα:

- **Τα Ψηφιακά Πιστοποιητικά Σκληρής Αποθήκευσης**
  - Αποθηκεύονται σε Ασφαλής Διάταξη Δημιουργίας Υπογραφής (π.χ. έξυπνη κάρτα, usb token).
  - Η Ψηφιακή Υπογραφή που δημιουργείται με αυτά έχει ισχύ ισοδύναμη της ιδιόχειρης.
- **Τα Ψηφιακά Πιστοποιητικά Χαλαρής Αποθήκευσης**
  - Αποθηκεύονται στον υπολογιστή του τελικού χρήστη.
  - Η Ψηφιακή Υπογραφή που δημιουργείται με αυτά δεν έχει ισχύ ισοδύναμη της ιδιόχειρης.

10.7.4 Δημιουργία Ψηφιακής Υπογραφής

Η ψηφιακή υπογραφή δημιουργείται:

- με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και
- τα προς υπογραφή δεδομένα



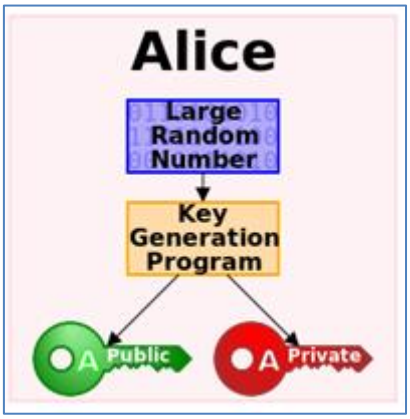
Εικόνα 10-20: Δημιουργία Ψηφιακής Υπογραφής

Ας υποθέσουμε ότι η Alice θέλει να στείλει ένα ψηφιακά υπογεγραμμένο μήνυμα στον Bob. Επομένως, στο συγκεκριμένο παράδειγμα:

- Αποστολέας είναι η Alice
- Παραλήπτης είναι ο Bob

- Μήνυμα της Alice προς τον Bob: «Hi Bob!»

Καταρχήν, ο υπογράφων (αποστολέας) θα πρέπει να έχει στην κατοχή του ένα ψηφιακό πιστοποιητικό, δηλαδή ένα ζεύγος κλειδιών (ιδιωτικό κλειδί - δημόσιο κλειδί).



Εικόνα 10-21: Ψηφιακό Πιστοποιητικό Alice

Στην συνέχεια, ο αποστολέας (Alice) υπογράφει το μήνυμα με το ιδιωτικό του/της κλειδί (το ιδιωτικό κλειδί της Alice) και αποστέλλει το ψηφιακά υπογεγραμμένο μήνυμα στον παραλήπτη (Bob).

Ο παραλήπτης (Bob) ελέγχει την αυθεντικότητα και ακεραιότητα του υπογεγραμμένου μηνύματος χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (το δημόσιο κλειδί της Alice).

10.8 Ψηφιακή Υπογραφή - Κρυπτογράφηση

Τόσο για την ψηφιακή υπογραφή όσο και για την κρυπτογράφηση χρησιμοποιούνται ψηφιακά πιστοποιητικά (ζεύγη δημόσιων και ιδιωτικών κλειδιών). Ωστόσο, στην:

Ψηφιακή Υπογραφή

- ***Υπογράφω:***
  - Με το ιδιωτικό μου κλειδί υπογραφής
- ***Η εγκυρότητα της υπογραφής μου ελέγχεται:***
  - Με το δημόσιο κλειδί μου (το δημόσιο κλειδί του υπογράφοντος)

Κρυπτογράφηση

- ***Κρυπτογραφώ:***
  - Με το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη
- *Ο παραλήπτης* ***αποκρυπτογραφεί****:*
  - Με το δικό του ιδιωτικό κλειδί κρυπτογράφησής (ιδιωτικό κλειδί του παραλήπτη)

Ο συνδυασμός Ψηφιακής Υπογραφής και Κρυπτογράφησης θα πρέπει να ακολουθεί την εξής σειρά:

- Πρώτα «υπογράφω με το ιδιωτικό μου κλειδί υπογραφής» και μετά «κρυπτογραφώ με το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη».

Αντίστοιχα ο παραλήπτης του ψηφιακά υπογεγραμμένου και κρυπτογραφημένου εγγράφου/μηνύματος:

- Πρώτα «αποκρυπτογραφεί με το ιδιωτικό κλειδί κρυπτογράφησής του» και μετά «ελέγχει την εγκυρότητα της υπογραφής με το δημόσιο κλειδί του υπογράφοντος».

10.9 Υπάρχουν Ασφαλή Συστήματα;

Λαμβάνοντας υπόψη όλα τα παραπάνω, εύλογα κάποιος οδηγείται στο **συμπέρασμα** ότι η Κρυπτογράφηση είναι η "κλειδαριά" που κρατάει την ψηφιακή μας ζωή ασφαλή και ότι οι σύγχρονοι αλγόριθμοι για την κρυπτογράφηση δεδομένων είναι «αδύνατον να σπάσουν». Αν αυτά ισχύουν τότε γιατί δεν είναι όλα τα συστήματα απαραβίαστα; Γιατί ακόμα και δίκτυα όπως του Πενταγώνου, της Apple, του Twitter, και των New York Times πέφτουν θύματα hackers;

Η απάντηση βρίσκεται στο ότι η πιο **επικίνδυνη επίθεση που μπορεί να παραβιάσει ακόμα και το πιο ασφαλές σύστημα** στον κόσμο χτυπάει στον πιο **αδύναμο κρίκο**: **τον άνθρωπο!**

10.10 Παραπομπές

4. https://en.wikipedia.org
5. https://el.wikipedia.org

11 Ασφάλεια Συστημάτων και Πληροφοριών

11.1 Γενικά

Οι υπηρεσίες του Υπουργείου Οικονομικών διαχειρίζονται συχνά διαβαθμισμένες υπηρεσιακές πληροφορίες. Η Πολιτική Ορθής Χρήσης Συστημάτων και Πληροφοριών ορίζει τους κανόνες και τους τρόπους με τους οποίους θα γίνεται η διαχείριση αυτή ώστε να διατηρείται η **εμπιστευτικότητα** της πληροφορίας.

Το διαδίκτυο και το ηλεκτρονικό ταχυδρομείο αποτελούν χώρους ύπαρξης σημαντικών απειλών όπως:

- Η διακίνηση κακόβουλου λογισμικού.
- Το πεδίο δράσης των hackers.

Αυτό έχει ως αποτέλεσμα να δημιουργούνται μεγάλοι κίνδυνοι για τα πληροφοριακά συστήματα και τις διαβαθμισμένες πληροφορίες και να απειλείται η έξωθεν εικόνα του Υπουργείου. Τα Πληροφοριακά Συστήματα, οι διαβαθμισμένες πληροφορίες και η φήμη του οργανισμού αποτελούν τα αγαθά του και θα πρέπει να προστατεύονται.

Γενικά σε ότι αφορά την ανταλλαγή υπηρεσιακής πληροφορίας, διαβαθμισμένης ή μη, ισχύουν τα κάτωθι τα οποία αποτελούν τους θεμελιώδεις κανόνες του Πλαισίου Ασφαλείας του Υπουργείου:

- Η αποστολή / διακίνηση **Διαβαθμισμένων Πληροφοριών** με τη χρήση υπηρεσιών ηλεκτρονικής αλληλογραφίας (email) ή φορητών αποθηκευτικών μέσων πρέπει να είναι **κρυπτογραφημένη,** έτσι ώστε να διασφαλιστεί ότι κανένας μη εξουσιοδοτημένος χρήστης δεν έχει πρόσβαση στα αρχεία αυτά.
- Δεν επιτρέπεται διακίνηση **υπηρεσιακής πληροφορίας** με μεθόδους που ενδέχεται να οδηγήσουν σε απώλεια εμπιστευτικότητας σε μη έχοντες εξουσιοδότηση ή σε μη γνήσιους παραλήπτες.

Αναλυτικότερα, σε ότι αφορά την ασφάλεια συστημάτων και πληροφοριών ισχύουν τα κάτωθι, τα οποία συνοψίζονται σε τρεις άξονες:

- Ασφαλής Χρήση Διαδικτύου.
- Ασφαλής Χρήση Ηλεκτρονικού Ταχυδρομείου.
- Ασφαλή χρήση Φορητών Αποθηκευτικών Μέσων.

11.2 Ασφαλής Χρήση Διαδικτύου

Η χρήση του διαδικτύου από το περιβάλλον εργασίας του χρήστη αποτελεί μεγάλη απειλή. Ενδέχεται ο χρήστης, εν αγνοία του, να κάνει ενέργειες οι οποίες θα εκθέσουν σε κίνδυνο υπηρεσιακά δεδομένα, τα οποία είτε βρίσκονται στον προσωπικό υπολογιστή του χρήστη είτε βρίσκονται σε κοινόχρηστους φακέλους της υπηρεσίας.

Η χρήση του διαδικτύου μπορεί να γίνεται έμμεσα με το άνοιγμα επισυναπτόμενων αρχείων ηλεκτρονικής αλληλογραφίας, χωρίς ο χρήστης να συνειδητοποιεί ή να υποψιάζεται την επικινδυνότητα της ενέργειας του. Εν γένει, η χρήση του διαδικτύου θα πρέπει να γίνεται μόνο για υπηρεσιακούς λόγους και με βάσει τους ακόλουθους κανόνες:

- Δεν επιτρέπεται το άνοιγμα ύποπτων συνδέσμων ή επισυναπτόμενων αρχείων ηλεκτρονικής αλληλογραφίας χωρίς να έχει ελεγχθεί η γνησιότητα του αποστολέα. Τα αρχεία αυτά ενδέχεται να περιέχουν σύνδεση σε κακόβουλες ιστοσελίδες και να δημιουργήσουν πρόβλημα στο περιβάλλον εργασίας του χρήστη.

- Δεν επιτρέπεται χρήση του διαδικτύου και του υπηρεσιακού ηλεκτρονικού ταχυδρομείου με τρόπο που αντιβαίνει τον υπηρεσιακό σκοπό και προσβάλλει το κύρος του Οργανισμού.
- Ιδιαίτερη προσοχή πρέπει να δίδεται όσον αφορά στη χρήση ιστοτόπων κοινωνικής δικτύωσης, όπου σε καμία περίπτωση δεν θα πρέπει να αναφέρονται υπηρεσιακές, εμπιστευτικές ή μη, πληροφορίες.

11.3 Ασφαλής Χρήση Ηλεκτρονικού Ταχυδρομείου

Η χρήση του Ηλεκτρονικού Ταχυδρομείου, είτε είναι υπηρεσιακό είτε είναι προσωπικό, περιορίζεται από τους παρακάτω, κατά περίπτωση, κανόνες:

- Απαγορεύεται η χρήση προσωπικού ηλεκτρονικού ταχυδρομείου (gmail, yahoo, κλπ.) καθώς και προσωπικών υπηρεσιών νέφους (google drive, ms cloud, κλπ.) για την αποστολή και αποθήκευση υπηρεσιακών πληροφοριών. Μπορεί να επιτραπεί μόνο:
  - μετά από έγγραφη άδεια του αρμόδιου Υπεύθυνου Χρηστών
  - βάσει δικαιολογημένης υπηρεσιακής ανάγκης και
  - με χρήση κατάλληλων μεθόδων κρυπτογράφησης.

  Στα πλαίσια του ίδιου κανόνα, απαγορεύεται ρητά η αυτόματη προώθηση ηλεκτρονικού ταχυδρομείου σε μη υπηρεσιακούς λογαριασμούς, τόσο σε επίπεδο προσωπικού υπολογιστή όσο και σε επίπεδο Εξυπηρετητή Ηλεκτρονικού Ταχυδρομείου (Mail Server) του Οργανισμού. Εφόσον υπάρχει υπηρεσιακή ανάγκη, θα υποβάλλεται τεκμηριωμένο αίτημα, το οποίο για να υλοποιηθεί, θα πρέπει να εγκριθεί γραπτώς από τον αρμόδιο Υπεύθυνο Χρηστών.
- Διακίνηση υπηρεσιακής πληροφορίας σε παραλήπτη εκτός του Οργανισμού θα πρέπει να γίνεται μόνο με χρήση κατάλληλων μεθόδων κρυπτογράφησης.
- Κατά την αποστολή υπηρεσιακού email σε παραλήπτες εκτός του Οργανισμού θα πρέπει να ελέγχεται με προσοχή η λίστα των παραληπτών πριν την εκτέλεση της εντολής «Αποστολή».

Ανεξάρτητα από τη διακίνηση της υπηρεσιακής πληροφορίας η χρήση ηλεκτρονικού ταχυδρομείου και διαδικτύου από το **εργασιακό περιβάλλον** ενέχει κινδύνους. Για το λόγο αυτό ο χρήστης θα πρέπει να προσέχει τα κάτωθι κατά τη χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου από τον υπηρεσιακό του υπολογιστή:

- Απαγορεύεται η διακίνηση μηνυμάτων με παράνομο ή άσεμνο περιεχόμενο και με κακόβουλο/ιομορφικό λογισμικό, συμπεριλαμβανομένων ανεπιθύμητων ηλεκτρονικών μηνυμάτων (unsolicited mails ή junk mails) ή μηνυμάτων διαφημιστικού ή προωθητικού περιεχομένου (spams).
- Πρέπει να αποφεύγεται η αποστολή ιδιωτικών (μη υπηρεσιακών) δεδομένων/αρχείων μέσω του υπηρεσιακού ηλεκτρονικού ταχυδρομείου.
- Κάθε χρήστης πρέπει να είναι προσεκτικός ως προς τη διατύπωση, το περιεχόμενο και τη μορφοποίηση του κειμένου και κυρίως τους αποδέκτες των ηλεκτρονικών μηνυμάτων που αποστέλλει.

11.4 Ασφαλής Χρήση Φορητών Αποθηκευτικών Μέσων

Τα Φορητά Αποθηκευτικά Μέσα είναι συσκευές χρήσιμες για την αποθήκευση δεδομένων και πληροφοριών που χρησιμοποιούνται ευρέως εξαιτίας της κατασκευής, του μεγέθους και του βάρους τους. Παραδείγματα τέτοιων μέσων αποτελούν τα ακόλουθα:

- USB sticks (π.χ. για μεταφορά αρχείων)
- Εξωτερικοί σκληροί δίσκοι (π.χ. για backup αρχείων)
- Φορητοί υπολογιστές
- Tablets
- Έξυπνα κινητά
- Κάμερες
- κτλ.

Τα κυριότερα **πλεονεκτήματα** των φορητών αποθηκευτικών μέσων είναι:

- Οι υψηλές ταχύτητες εγγραφής / ανάγνωσης
- Η μεγάλη αποθηκευτική χωρητικότητα
- Η αυτονομία ρεύματος
- Η εύκολη μεταφορά (μικρό μέγεθος, χαμηλό βάρος)
- Ενδεχομένως το χαμηλό κόστος (π.χ. usb)
- Η μεγάλη διάδοση (κάποιος μπορεί να έχει στην κατοχή του πολλαπλά τέτοια μέσα)

Το κυριότερο **μειονέκτημα** των φορητών αποθηκευτικών μέσων είναι ο υψηλός κίνδυνος απώλειας (ακούσια απώλεια ή κλοπή). Μάλιστα, ο κίνδυνος αυτός γίνεται εξαιρετικά σημαντικός λόγω του ότι τα φορητά αποθηκευτικά μέσα είναι πλέον ευρέως διαδεδομένα εξαιτίας των προαναφερόμενων πλεονεκτημάτων τους με αυτό, πρακτικά, να σημαίνει ότι ένας τεράστιος όγκος δεδομένων βρίσκεται πλέον εκτεθειμένος.

11.4.1 Πολιτική Ορθής Χρήσης Πληροφοριακών Συστημάτων και Τρόποι Προστασίας των Φορητών Αποθηκευτικών Μέσων

11.4.1.1 Απαγόρευση χρήσης προσωπικού εξοπλισμού

Δεν επιτρέπεται να χρησιμοποιούνται προσωπικές συσκευές για την αποθήκευση υπηρεσιακών πληροφοριών χωρίς άδεια από τον άμεσο Υπεύθυνο Χρηστών. Προσωπικές συσκευές δύναται να χρησιμοποιούνται μόνο βάσει υπηρεσιακής ανάγκης με την τήρηση των κανόνων εμπιστευτικότητας της παραγράφου 4.3 της Πολιτικής Ορθής Χρήσης Πληροφοριακών Συστημάτων.

Οποιαδήποτε υπηρεσιακή πληροφορία θα πρέπει να διαγράφεται από προσωπικό εξοπλισμό σε περίπτωση αποχώρησης υπαλλήλου ή αλλαγής αρμοδιοτήτων καθώς και σε περίπτωση μη ύπαρξης πλέον της υπηρεσιακής ανάγκης.

11.4.1.2 Προστασία Υπηρεσιακής Πληροφορίας

Ιδιαίτερη προσοχή θα πρέπει να δίδεται στο χειρισμό των αποθηκευτικών μέσων που χρησιμοποιούνται για υπηρεσιακή ανάγκη ώστε να αποφευχθεί ο **κίνδυνος κλοπής ή απώλειας**. Για το λόγο αυτό, τα εν λόγω αποθηκευτικά μέσα θα πρέπει:

- είτε να παραμένουν κλειδωμένα σε ντουλάπια εντός γραφείων
- είτε να κρυπτογραφούνται με μεθόδους που προτείνονται από το Αυτοτελές Τμήμα Ασφάλειας (π.χ. συμπίεση και κρυπτογράφηση αρχείου, προστασία αρχείου με κωδικό – βλ. Κεφάλαιο 10) έτσι ώστε σε περίπτωση απώλειας ή κλοπής του φορητού αποθηκευτικού μέσου τα δεδομένα να μην είναι κατανοητά.

Ακόμα και στις περιπτώσεις που έχει δοθεί άδεια χρήσης φορητών αποθηκευτικών μέσων για υπηρεσιακούς σκοπούς αυτά **θα πρέπει να χρησιμοποιούνται με ιδιαίτερη προσοχή και να προστατεύονται επισταμένως!**

11.4.2 Κίνδυνοι από χρήση φορητών μέσων αποθήκευσης

Η σύνδεση φορητών μέσων σε υπηρεσιακό δίκτυο εγκυμονεί σοβαρούς κινδύνους, όπως:

- Διαρροή δεδομένων - ενδεχομένως ΜΑΖΙΚΗ!
- Μετάδοση ιομορφικών λογισμικών.
- Εκτέλεση / εγκατάσταση **κατασκοπευτικού** λογισμικού.
- Εκτέλεση / εγκατάσταση λογισμικού **υποκλοπής**.
- Εκτέλεση / εγκατάσταση λογισμικού που μπορεί **να μεταβάλλει ή να καταστρέψει δεδομένα**.

Επισημαίνεται ότι παγκοσμίως έχουν παρατηρηθεί πολύ σοβαρά περιστατικά σε οργανισμούς με πολύ σοβαρές συνέπειες για αυτούς.

11.4.3 Πρακτικές Οδηγίες Ασφάλειας Φορητών Μέσων

1. **Τήρηση πρακτικής λίστας με τα φορητά μέσα που κατέχουμε** και με αναφορά του λόγου χρήσης τους. Η συνεχής πτώση των τιμών στα USB sticks και τους εξωτερικούς σκληρούς δίσκους σε συνδυασμό με την εξέλιξη της τεχνολογίας που επιτρέπει μεγάλες αποθηκευτικές δυνατότητες έχουν σαν αποτέλεσμα να παρατηρείται μια ευρύτατη διάδοση αυτών των φορητών μονάδων αποθήκευσης τα τελευταία χρόνια με επακόλουθο συχνά ένας χρήστης να έχει στην κατοχή του πολλαπλά τέτοια μέσα, των οποίων την απώλεια ενδεχομένως να μην παρατηρήσει άμεσα.

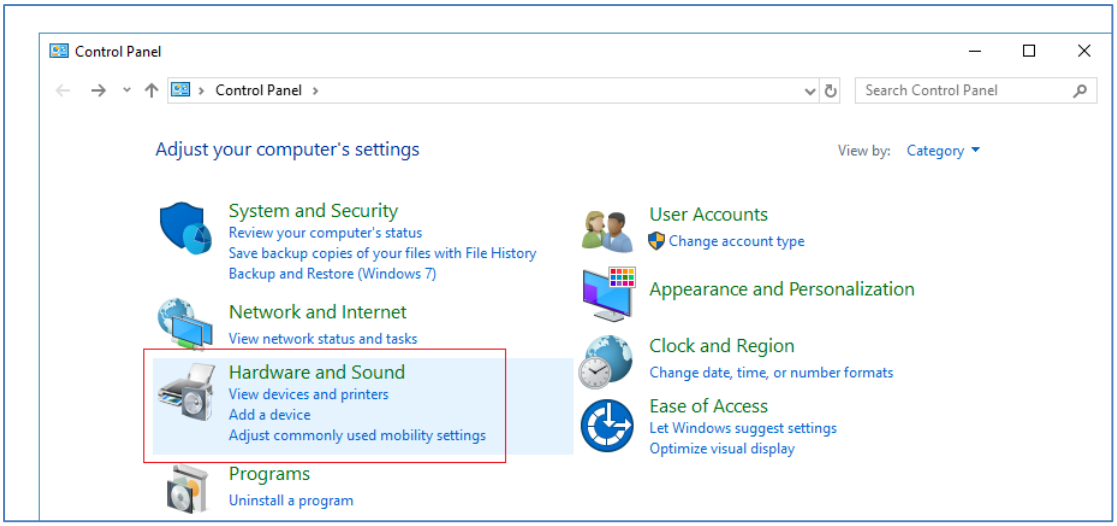
2. **Εκτέλεση ελέγχου ύπαρξης ιού κατά τη σύνδεση** των φορητών μέσων σε υπηρεσιακό σύστημα και πριν τη χρήση αυτών.

   Αμέσως μετά τη σύνδεση ενός φορητού αποθηκευτικού μέσου σε υπηρεσιακό σύστημα και πριν την πρόσβαση στα περιεχόμενα του φορητού αποθηκευτικού μέσου πηγαίνουμε στον File (Windows) Explorer, πατάμε δεξί κλικ στο εικονίδιο του αποθηκευτικού μέσου που μόλις συνδέσαμε και στη συνέχεια επιλέγουμε «Σάρωση για ιούς και κατασκοπευτικά προγράμματα…».

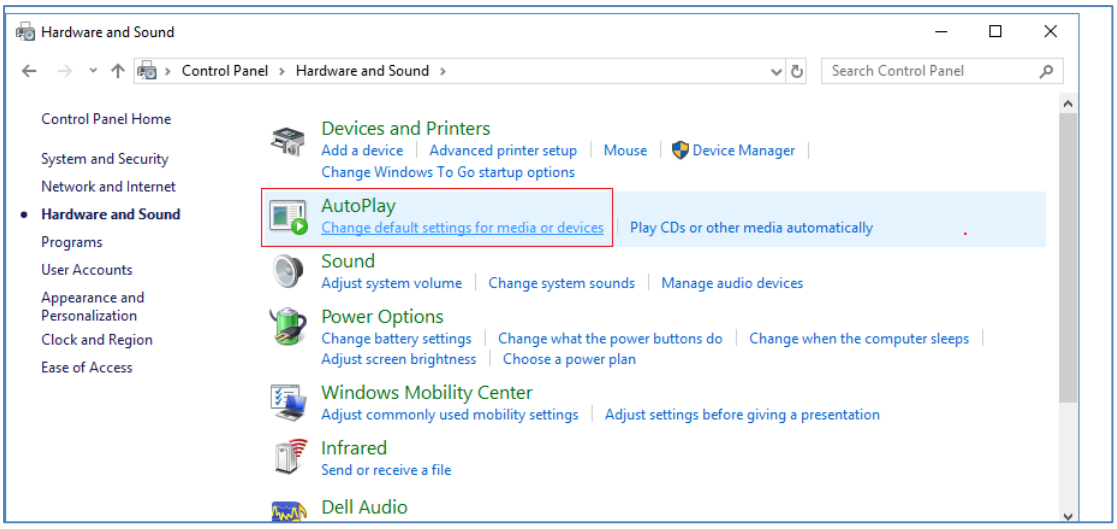
   Τα παραπάνω προϋποθέτουν ότι είναι ενημερωμένο το αντι-ικό λογισμικό(antivirus) του σταθμού εργασίας (PC) που συνδέθηκε το φορητό αποθηκευτικό μέσο.

3. **Απενεργοποίηση της αυτόματης εκτέλεσης λογισμικού** φορητών μέσων.

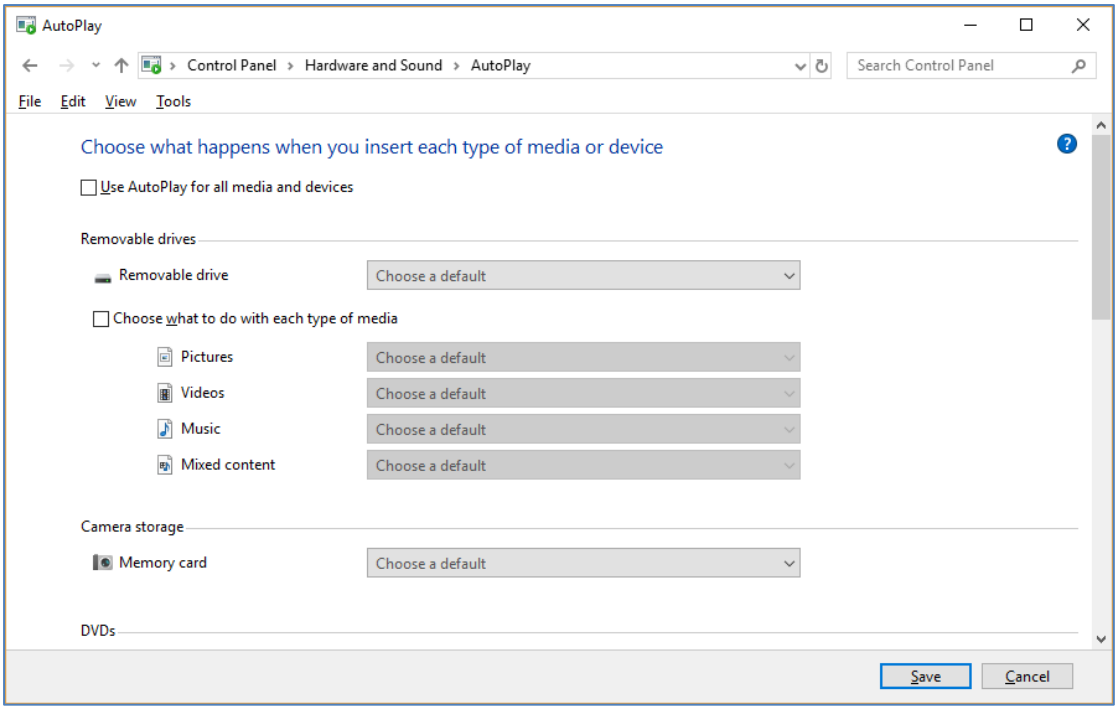
   Φροντίζουμε να απενεργοποιήσουμε την «Αυτόματη εκτέλεση λογισμικού φορητών μέσων» πηγαίνοντας στον Πίνακα Ελέγχου (Control Panel)– Υλικό και Ήχος (Hardware and Sound) – Αυτόματη Εκτέλεση (AutoPlay).



Εικόνα 11-22: Πίνακας Ελέγχου - Υλικό και Ήχος



Εικόνα 11-23: Πίνακας Ελέγχου - Υλικό και Ήχος - Αυτόματη Εκτέλεση



Εικόνα 11-24: Πίνακας Ελέγχου - Υλικό και Ήχος - Αυτόματη Εκτέλεση - Ρυθμίσεις

4. Τα προσωπικά μας USB sticks που δεν περιέχουν υπηρεσιακή πληροφορία προτείνεται να τα έχουμε προσαρμοσμένα στα κλειδιά μας.
5. **Αποφυγή χρήσης** για υπηρεσιακούς σκοπούς **φορητών μέσων που μας χάρισαν** σε κάποια εκδήλωση καθώς ενδέχεται να περιέχουν κάποιο ύποπτο λογισμικό.

11.4.4 Προστασία πληροφοριών σε φορητά μέσα με χρήση κρυπτογράφησης

Ο ευκολότερος τρόπος συμπίεσης και κρυπτογράφησης αρχείων είναι με χρήση του εργαλείου 7-zip (ή αλλιώς 7zip).

Το εν λόγω εργαλείο είναι freeware (δωρεάν λογισμικό). Εγκαθίσταται στους σταθμούς εργασίας (PCs) των υπαλλήλων του Υπουργείου Οικονομικών και της Ανεξάρτητης Αρχής Δημοσίων Εσόδων από τη Διεύθυνση Διαχείρισης Υπολογιστικών Υποδομών.

Κάθε φορά που θέλουμε να προστατεύσουμε κάποιο αρχείο ακολουθούμε τη διαδικασία Συμπίεσης και Κρυπτογράφηση με χρήση συνθηματικού.

Κατά τη διαδικασία της Αποσυμπίεσης, για να γίνει η Αποκρυπτογράφηση, απαιτείται η γνώση του συνθηματικού.

Για λεπτομέρειες χρήσης του εργαλείου 7zip και της συγκεκριμένης διαδικασίας βλ. Κεφάλαιο 10 (10.4.1.3 Εργαλείο Συμπίεσης και Συμμετρικής Κρυπτογράφησης 7-zip).

11.4.4.1 Παράδειγμα

Κατόπιν σχετικής έγκρισης από τον προϊστάμενό μου, έχω αποθηκευμένα σε φορητό μέσο (USB) τα υπηρεσιακά αρχεία μου κρυπτογραφημένα, με χρήση του εργαλείου 7zip, σε ένα ενιαίο αρχείο με ισχυρό κωδικό. Είμαι εκτός χώρου εργασίας και χρειάζεται να επεξεργαστώ ένα από τα αρχεία μου. Τα βήματα που ακολουθώ είναι τα ακόλουθα:

- Ανοίγω το ενιαίο κρυπτογραφημένο αρχείο και εξάγω το αρχείο που χρειάζομαι **ΕΝΤΟΣ** του φορητού μου μέσου και όχι στον υπολογιστή που έχω στη διάθεσή μου αφού πρόκειται για μη υπηρεσιακό υπολογιστή.
- Επεξεργάζομαι το αρχείο, το αποθηκεύω **ΕΝΤΟΣ** του φορητού μου μέσου και στη συνέχεια ενημερώνω μ' αυτό το ενιαίο κρυπτογραφημένο αρχείο στο φορητό μέσο αποθήκευσης προκειμένου να το μεταφέρω στο χώρο εργασίας μου όταν επιστρέψω.
- Τέλος, δεν ξεχνώ να σβήσω το προσωρινά αποθηκευμένο –μη προστατευμένο- αρχείο από το φορητό μου μέσο.

11.5 Παραπομπές

6. Πολιτική Ορθής Χρήσης Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών
7. https://en.wikipedia.org
8. https://el.wikipedia.org

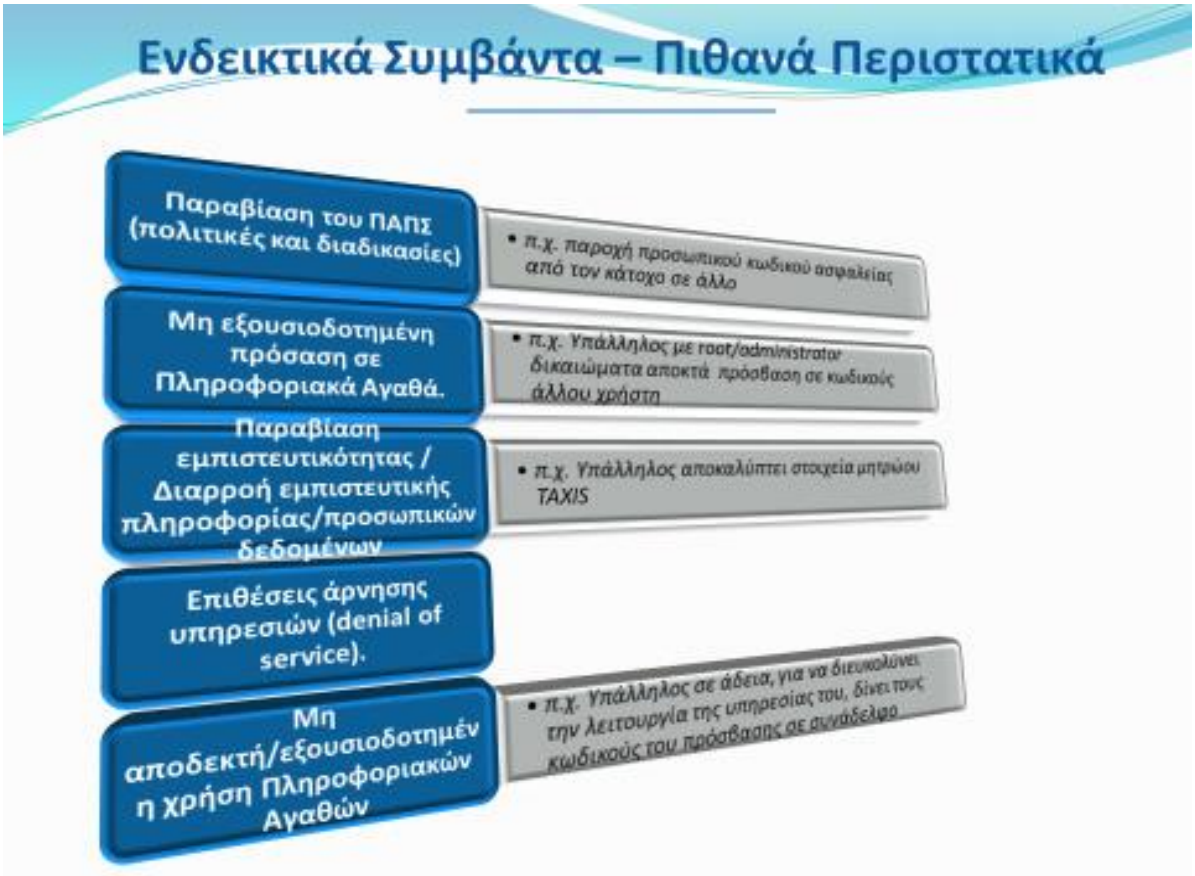
12 Συμβάντα – Περιστατικά Ασφαλείας

Ως **Συμβάν Ασφαλείας** νοείται οποιοδήποτε συμβάν που πιθανώς αφορά την ασφάλεια πληροφοριών και πληροφοριακών αγαθών ενώ ως **Περιστατικό ασφαλείας** ενός ΟΠΣ ορίζεται η επιβεβαιωμένη τέλεση γεγονότων ή βεβαιωμένη ύπαρξη καταστάσεων που επηρεάζουν την ασφάλεια ή συμμόρφωση ως προς το Πλαίσιο Ασφαλείας του ΟΠΣ.

Πιθανά συμβάντα ασφαλείας θα μπορούσαν να χαρακτηριστούν :

- Πιθανή παραβίαση πλαισίου ασφάλειας
- Πιθανό κενό ασφάλειας (π.χ. σε εφαρμογή, σύστημα, ΒΔ)
- Κλοπή υλικού / λογισμικού
- Μη εξουσιοδοτημένη πρόσβαση
- Κλοπή ταυτότητας λογαριασμού

Αν κατόπιν της κατάλληλης διερεύνησης των ανωτέρω συμβάντων προκύψει ότι υφίσταται ύπαρξη καταστάσεων που επηρεάζουν την ασφάλεια τότε το συμβάν χαρακτηρίζεται ως περιστατικό όπως φαίνεται και στο επόμενο σχήμα :



Εικόνα 12-1: Ενδεικτικά συμβάντα – πιθανά περιστατικά

Αυτό σημαίνει ότι ένα συμβάν δεν αποτελεί κατ' ανάγκη και περιστατικό. Σε έναν οργανισμό ουσιαστικά συμβαίνουν καθημερινά πολλά συμβάντα και κάποια εξ αυτών χαρακτηρίζονται ως περιστατικά το οποίο σημαίνει ότι δεν μπορούμε να ισχυριστούμε ότι έχουμε απόλυτη ασφάλεια. Το ζητούμενο δεν είναι επομένως αν θα υπάρξει κάποια στιγμή

ένα ΠΕΡΙΣΤΑΤΙΚΟ Ασφαλείας αλλά ΠΟΤΕ θα υπάρξει και κυρίως ΠΩΣ θα το αντιμετωπίσουμε και θα περιορίσουμε την επανεμφάνιση του.

12.1 Πολιτική και Διαδικασία Διαχείρισης Περιστατικών Ασφαλείας

Στο Υπουργείο Οικονομικών έχει τεθεί σε ισχύ η Πολιτική Διαχείρισης Περιστατικών Ασφαλείας (Π.Δ.Π.Α.) και εφαρμόζεται από το Αυτοτελές Τμήμα Ασφάλειας η αντίστοιχη Διαδικασία.

Σκοπός της Π.Δ.Π.Α. είναι να διατυπωθούν μια σειρά συγκεκριμένων βημάτων για την αντιμετώπιση ενός περιστατικού έτσι ώστε να εξασφαλίζεται κατά το μέγιστο δυνατό :

1. η αποτελεσματική και αξιόπιστη αντιμετώπιση συμβάντων ασφαλείας και
2. η αξιοποίηση της εμπειρίας για βελτίωση του πλαισίου ασφαλείας.

Η πολιτική ουσιαστικά επιβάλλει την συνεχή εφαρμογή ενός κύκλου ενεργειών που αφορούν τρία βασικά στάδια τα οποία επαναλαμβάνονται συνεχώς ΕΝΤΟΠΙΣΜΟΣ – ΕΝΕΡΓΕΙΑ – ΒΕΛΤΙΩΣΗ.

Στόχος είναι η ετοιμότητα του οργανισμού στον έγκαιρο, έγκυρο, στοχευμένο και αποτελεσματικό εντοπισμό του περιστατικού ασφαλείας και η κατάλληλη διαχείριση του ώστε να επουλωθούν πρωτογενώς το συντομότερο δυνατό οι όποιες επιπτώσεις τυχόν έχουν δημιουργηθεί στο φορέα με το ελάχιστο δυνατό κόστος και δευτερογενώς να γίνουν οι κατάλληλες ενέργειες ώστε να αποφευχθεί η επανεμφάνιση του περιστατικού στο μέλλον.

Συνοπτικά τα βήματα της διαδικασίας διαχείρισης περιστατικού Ασφαλείας είναι τα ακόλουθα:

1. **Αναφορά Συμβάντος**

   Τα Συμβάντα αναφέρονται στο ΑΤΑ από διάφορες πηγές άμεσα ή έμμεσα. Το ΑΤΑ αποτελεί το μοναδικό σημείο για την αναφορά συμβάντων ασφαλείας. Για παράδειγμα μπορεί να οφείλονται στην παρατήρηση από έναν υπάλληλο μίας ασυνήθιστης συμπεριφοράς ενός συστήματος, ο οποίος οφείλει να ενημερώσει σχετικά τον προιστάμενο του και ο οποίος με τη σειρά του να ενημερώσει αρμοδίως το ΑΤΑ. Επίσης οι εγκεκριμένοι Διαχειριστές των Συστημάτων μπορούν να παρατηρήσουν συμβάντα είτε άμεσα είτε μέσω συστημάτων καταγραφής και να ενημερώσουν μέσω σχετικής διαδικασίας το ΑΤΑ. Τέλος αναφορά συμβάντος μπορεί να γίνει και μέσω συναλλασσόμενου πολίτη ή ακόμη μέσω των ΜΜΕ.

2. **Αρχική αναγνώριση και αξιολόγηση περιστατικού Ασφαλείας**

   Το ΑΤΑ, εφόσον λάβει γνώση για ένα συμβάν προχωράει σε μία πρώτη ανάλυση και αξιολόγηση των αναφερόμενων δεδομένων και κατόπιν αποφαίνεται εάν το συμβάν αποτελεί Περιστατικό Ασφαλείας. Εφόσον το συμβάν αποτελεί Περιστατικό, το αξιολογεί περαιτέρω ως προς την κρισιμότητα του βάσει υπαρχόντων ή πιθανών επιχειρησιακών επιπτώσεων και προχωράει στο επόμενο βήμα. Τα περιστατικά κατηγοριοποιούνται σε κλίμακα από «πολύ χαμηλή» έως «πολύ υψηλή» με την τελευταία να αφορά περιπτώσεις που είναι πολύ πιθανόν να έχουν διακυβευτεί ζωτικές πληροφορίες ή συστήματα και οι επιχειρησιακές επιπτώσεις είναι ή δύναται να είναι ιδιαίτερα μεγάλες έως καταστροφικές. Σε αντίθετη περίπτωση η αναφορά συμβάντος αρχειοθετείται ως μη περιστατικό.

3. **Σύσταση Ομάδας Διαχείρισης Περιστατικού Ασφαλείας – ΟΔΠΑ**

Για την αντιμετώπιση ενός Περιστατικού Ασφαλείας το ΑΤΑ έχει την δυνατότητα και αρμοδιότητα να ορίζει Ομάδα Διαχείρισης Περιστατικού Ασφαλείας – ΟΔΠΑ η οποία θα πρέπει να έχει την κατάλληλη σύνθεση και δικαιοδοσία για να μπορέσει να αντιμετωπίσει αποτελεσματικά το περιστατικό. Τα καθήκοντα και οι ευθύνες των συμμετεχόντων λαμβάνουν προτεραιότητα από τα λοιπά καθημερινά εργασιακά τους. Τα μέλη της ΟΔΠΑ καθορίζονται από το ΑΤΑ και μπορεί να είναι κατά περίπτωση ο υπεύθυνος Φυσικής Ασφάλειας κτηρίου, Εγκεκριμένοι Διαχειριστές, υπεύθυνος Διεύθυνσης προσωπικού, υπεύθυνος νομικής υποστήριξης, εξειδικευμένοι εξωτερικού συνεργάτες κλπ. Η ΟΔΠΑ συντονίζεται από το ΑΤΑ και οι εργασίες της θεωρούνται ΕΜΠΙΣΤΕΥΤΙΚΕΣ.

4. Λήψη Άμεσων μέτρων Αντιμετώπισης

Εφόσον κριθεί σκόπιμο και το περιστατικό δύναται να επηρεάσει την ασφάλεια των δεδομένων ή την επιχειρησιακή συνέχεια της Οργανικής Μονάδας το ΑΤΑ σε συνεργασία με την ΟΔΠΑ προβαίνουν σε ενέργειες λήψης άμεσων μέτρων αντιμετώπισης. Σε περίπτωση που αυτό δεν είναι εφικτό δύναται να εισηγηθεί στη Διοίκηση την ενεργοποίηση του Πλάνου Επιχειρησιακής Συνέχειας.

5. Συλλογή αποδεικτικών στοιχείων και ανάλυση

Για την καλύτερη αναγνώριση ενός περιστατικού το ΑΤΑ δύναται να ζητήσει την αύξηση του υφιστάμενου επιπέδου καταγραφής και παρακολούθησης σε ένα Πληροφοριακό Πόρο.

6. Εύρεση Αιτιών και επαναφορά κανονικής Λειτουργίας

Κάθε προσβεβλημένος Πληροφοριακός Πόρος πρέπει να ελέγχεται ενδελεχώς μετά από ένα Περιστατικό Ασφαλείας από εσωτερικό ή εξωτερικό ανεξάρτητο μέρος. Ο εν λόγω έλεγχος θα πρέπει να πραγματοποιείται βάσει της Πολιτικής Διαχείρισης Απειλών και Ευπαθειών του Υπουργείου.

Σε γενικές γραμμές θα πρέπει να διασφαλιστεί ότι ο συγκεκριμένος Πληροφοριακός Πόρος λειτουργεί κανονικά, δεν έχουν επηρεαστεί άλλες παράμετροι στο περιβάλλον του και δεν κινδυνεύουν άλλοι πληροφοριακοί πόροι της πληροφοριακής υποδομής μετά την επανένταξη του προσβεβλημένου στην παραγωγική λειτουργία. Σε περίπτωση εντοπισμού παραποίησης ή μη πληρότητας των πληροφοριών θα πρέπει να γίνεται επαναφορά τους από πρόσφορη διαθέσιμη πηγή.

7. Προτεινόμενες Ενέργειες για αποφυγή επανεμφάνισης του περιστατικού

Όλα τα αποδεικτικά στοιχεία που έχουν συλλεγεί πρέπει να μελετώνται και αναλύονται για να εξαχθούν συμπεράσματα για το Περιστατικό Ασφαλείας προκειμένου αυτά να καταγραφούν σε Αρχείο Περιστατικών Ασφαλείας υπό την ευθύνη του ΑΤΑ. Σκοπός του αρχείου είναι ο περιορισμός της συχνότητας, του κινδύνου και του κόστους από μελλοντικά περιστατικά ασφαλείας και η αποτίμηση / παρακολούθηση του κόστους των περιστατικών που περιλαμβάνουν διαρροή εμπιστευτικής πληροφορίας.

Επίσης για τον έλεγχο της ικανότητας απόκρισης της υπηρεσίας σε περιστατικά ασφάλειας, θα πρέπει να διεξάγονται έλεγχοι ετοιμότητας τουλάχιστον μία φορά τον χρόνο. Οι έλεγχοι θα είναι υπό μορφή ασκήσεως με υποθετικά σενάρια επί χάρτου η οποια θα παράγει και μία αναφορά με πιθανές βελτιωτικές προτάσεις σε υφιστάμενες διαδικασίες.

8. Ενέργειες μετά το περιστατικό

Μετά από κάθε Περιστατικό Ασφαλείας, το ΑΤΑ θα πρέπει να ενημερώνει τα πρόσωπα που ανέφεραν το συμβάν ότι έγιναν οι σχετικές ενέργειες και το συμβάν θεωρείται λήξαν.

Επιπλέον, συντάσσεται από το ΑΤΑ έγγραφη αναφορά περιστατικού ασφαλείας σε τυποποιημένο έγγραφο, με σκοπό την ενημέρωση της Διοίκησης ως προς την φύση του προβλήματος, τις λεπτομέρειες εξέλιξης του περιστατικού (οπωσδήποτε να καταγράφεται η αλληλουχία των γεγονότων με πιστή αποτύπωση του χρόνου), την σύνθεση της ΟΔΠΑ, τις συνέπειες που είχε στη λειτουργία της ΟΜ, τον τρόπο αντιμετώπισης και τυχόν διορθωτικά μέτρα που ελήφθησαν για την μη επανεμφάνιση παρόμοιων προβλημάτων.

Τα περιστατικά ασφαλείας πληροφοριών πρέπει να αναφέρονται στις αρχές, όποτε αυτό είναι αναγκαίο, έτσι ώστε να τηρούνται οι εκάστοτε κανόνες που επιβάλλονται από το υπάρχον κανονιστικό πλαίσιο, όπως αυτό ορίζεται από την Ελληνική, την Ευρωπαϊκή και κατά τόπους νομοθεσία και τις αποφάσεις των εποπτικών αρχών. Η αναφορά αυτή πραγματοποιείται κατόπιν έγκρισης από τη Διοίκηση.

12.2 Αξιολόγηση της Αποτελεσματικότητας Διαχείρισης Περιστατικών

Λίγες μέρες μετά από κάθε πολύ υψηλής κρισιμότητας Περιστατικού Ασφαλείας πρέπει το ΑΤΑ να προκαλεί συνάντηση - στην οποία θα συμμετέχουν τα μέλη της ΟΔΠΑ- που θα εξετάζει τι συνέβη, τα βήματα που ακολουθήθηκαν και την αποτελεσματικότητα των ενεργειών.

Σκοπός της συνάντησης είναι να αποτυπώσει την εμπειρία που αποκτήθηκε από το συγκεκριμένο περιστατικό και να αξιολογήσει την αποτελεσματικότητα της διαχείρισης περιστατικών συνολικά. Η αξιολόγηση αυτή, είναι πιθανό να οδηγήσει σε επικαιροποίηση της παρούσας πολιτικής καθώς και/ή άλλων σχετικών πολιτικών/διαδικασιών.

12.3 Νομικά Θέματα και Πειθαρχικές Διαδικασίες

Σε περίπτωση που θίγονται νομικά θέματα και πειθαρχικές διαδικασίες θα πρέπει να ενημερώνονται τα αρμόδια όργανα για τις ενέργειές τους.

Εφόσον ένα περιστατικό ασφάλειας έχει αποδεδειγμένα προκληθεί από υπάλληλο του Υπουργείου ή εξωτερικό συνεργάτη, αυτό θα εξετάζεται κατά περίπτωση και θα επιβάλλονται οι κατάλληλες πειθαρχικές ή / και ποινικές κυρώσεις από τα αρμόδια όργανα