ΤΕΧΝΟΛΟΓΙΚΟ **Ε**ΚΠΑΙΔΕΥΤΙΚΟ **Ι**ΔΡΥΜΑ **Κ**ΡΗΤΗΣ

ΣΧΟΛΗ **Τ**ΕΧΝΟΛΟΓΙΚΩΝ **Ε**ΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ **Ε**ΦΑΡΜΟΣΜΕΝΗΣ **Π**ΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ **Π**ΟΛΥΜΕΣΩΝ

Πτυχιακή Εργασία

Καταγραφή Πολιτικών Ασφάλειας σύμφωνα με το πρότυπο ISO27002

Αλεξάκη Γ. Ευφροσύνη

Επόπτης Καθηγητής: ΔΡ. Μανιφάβας Χαράλαμπος

Ηράκλειο, Νοέμβριος 2008

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επόπτη καθηγητή της εργασίας μου κύριο Χαράλαμπο Μανιφάβα, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτή την εργασία, για την πολύτιμη βοήθεια και καθοδήγησή του καθ' όλη τη διάρκειά της και κυρίως για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα πολύ ενδιαφέρον αντικείμενο.

Περιγραφή Πτυχιακής Εργασίας

Ένας οργανισμός/υπηρεσία προκειμένου να έχει την δυνατότητα να επιτυγχάνει τους στόχους του θα πρέπει, μεταξύ άλλων, να διασφαλίσει όσο το δυνατό καλύτερα την απαιτούμενη ασφάλεια της υπολογιστικής υποδομής του καθώς και των ευαίσθητων δεδομένων (βάση νομικών υποχρεώσεων ή λόγω της φύσης του οργανισμού) που αποθηκεύονται η διακινούνται σε αυτή. Η εφαρμογή ενός σχεδίου ασφάλειας σήμερα, σύμφωνα με διεθνή πρότυπα και πρακτικές, αντιμετωπίζεται σαν μία σημαντική διαχειριστική λειτουργία και όχι απλά ως μία τεχνική λειτουργία.

Η παρούσα πτυχιακή ασχολείται με την ανάπτυξη, υλοποίηση και υποστήριξη στρατηγικών ασφάλειας σύμφωνα με το σύγχρονο πρότυπο ISO27002. Τα πλεονεκτήματα για τον οργανισμό συνοψίζονται στα εξής:

- Εκτίμηση της επικινδυνότητας της υπάρχουσας υποδομής και βελτιστοποίηση αυτής
- Καταγραφή των πολιτικών ασφάλειας που ορίζουν την ορθή χρήση της υποδομής
- Αποδεδειγμένη συμμόρφωση με το νομικό καθεστώς που διέπει τα πληροφοριακά συστήματα (π.χ. προστασία προσωπικών δεδομένων, ΑΔΑΕ, οδηγίες Ε.Ε.)

Το αποτέλεσμα της πτυχιακής είναι δυνατό να εφαρμοστεί στα πλαίσια του ΤΕΙ Κρήτης στο Ηράκλειο. Πρέπει να σημειωθεί ότι οι πολιτικές ασφάλειας αναφέρονται σε ένα σύνολο κανόνων και οδηγιών που οριοθετούν και οργανώνουν εσωτερικές διαδικασίες (εφόσον αυτές σχετίζονται με την ασφάλεια πληροφοριών). Ο στόχος αυτής της προσπάθειας είναι να εφαρμόσουμε ασφαλείς πρακτικές σεβόμενοι ταυτόχρονα την κουλτούρα που διέπει έναν εκπαιδευτικό/ερευνητικό οργανισμό. Για να επιτευχθεί το παραπάνω θα χρειαστεί συνεργασία από όλους η οποία θα κωδικοποιείται σαν διοικητική κατεύθυνση και δέσμευση όσο αφορά στους ρόλους και τις υποχρεώσεις των μελών του ιδρύματος.

Abstract

An organization/service in order to have the ability to achieve its objectives, should among all, reassure the required security of its calculating infrastructure as well as sensitive data (based on legal obligations or due to the nature of the organization) which is stored or transmitted in it. The implementation of a security plan today, according to international standards and practices, is faced as an important management process and not just as a technical one. The present project deals with the development, concretization and support of security strategies according to modern standard ISO27002. The advantages for the organization are summarised in the followings:

- Risk assessment of existing infrastructure and its improvement.
- Documentation of security policies which address the proper use of infrastructure.
- Valid compliance to the legislation which characterizes the information systems (eg. personal data privacy, ADAE, guidance of European Communion)

The result of this project is possible to be applied in the frames of TEI of Crete at Heraklion. It should be mentioned that security policies are referred to a total of rules and guidelines which delimit and organize internal processes (provided that they are related to information security). The objective of this effort is to apply secure practices in respect to the culture that characterizes an educational/researching organization. In order to achieve the above, it will be needed collaboration from all, which is coded as administrative direction and commitment as regards the roles and the responsibilities of members of the institution.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων ήταν - από γενέσεως πληροφορικής - πάντα κρίσιμο. Αναμφισβήτητα, σήμερα ο κίνδυνος είναι πιο συνειδητός, καθώς τα συστήματα εκτίθενται σε ευρύ φάσμα χρηστών και συνεπώς κινδύνων. Η πληροφορία, οποιαδήποτε κι αν είναι η μορφή της, εφόσον είναι σημαντική απαιτείται να διαφυλάσσεται κατάλληλα και να είναι σωστά προστατευμένη. Αυτός είναι ο απώτερος σκοπός της ασφάλειας πληροφοριών: να προστατεύει την πληροφορία από ένα ευρύ φάσμα απειλών παρέχοντας εξασφάλιση στην επιχειρηματική κοινωνία, ελαχιστοποιώντας τη ζημία των επιχειρήσεων και αυξάνοντας το κέρδος από επενδύσεις και επιχειρηματικές ευκαιρίες. Η ασφάλεια των συστημάτων και των δεδομένων τους ορίζεται σε τρεις διαστάσεις: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα.

Τα τελευταία χρόνια παρατηρείται ότι η αξία των περιουσιακών στοιχείων μιας εταιρείας προέρχεται κυρίως από άυλα στοιχεία. Αναπόφευκτα, η εξάρτηση πάνω στα πληροφοριακά συστήματα και υπηρεσίες σημαίνει ότι οι οργανισμοί είναι πιο ευάλωτοι στις απειλές ασφάλειας. Τα δεδομένα, οι πληροφορίες, οι υποστηρικτικές διαδικασίες, τα συστήματα και τα δίκτυα είναι σημαντικά επιχειρηματικά αγαθά, οπότε διαφυλάσσοντας τα μία εταιρεία μπορεί να αποφύγει ανυπολόγιστα προβλήματα τα οποία ενδέχεται να προκύψουν. Η αλματώδης ανάπτυξη και αύξηση των εταιρειών, έχει ως συνέπεια να γίνονται πιο "θελκτικός" στόχος άρα τα συστήματα πληροφοριών και τα δίκτυα τους να έχουν να αντιμετωπίσουν απειλές από ένα ευρύ φάσμα πηγών, περιλαμβάνοντας computer-assisted fraud, espionage, sabotage, βανδαλισμό, φωτιά ή πλημμύρα. Πηγές ζημιάς, όπως ιοί υπολογιστών και computer hacking έχουν γίνει ολοένα και πιο συχνοί, πιο φιλόδοξοι και εντυπωσιακά ειδικευμένοι. Αντιλαμβανόμαστε λοιπόν την σπουδαιότητα που πρέπει να έχει η ασφάλεια των πληροφοριών σε μία επιχείρηση.

Σε αυτό το σημείο εγείρεται το ερώτημα: τι διαδικασίες και τι μηχανισμούς πρέπει να ακολουθήσει μία επιχείρηση έτσι ώστε να εξασφαλίσει την ακεραιτότητα της και να προστατέψει τα δεδομένα της; Σε θεωρητικό επίπεδο κατανοούμε ότι θα πρέπει να εφαρμοστούν έλεγχοι και διαδικασίες η οποίες θα διασφαλίσουν την συνοχή των δεδομένων της επιχείρησης. Συμπεραίνουμε ότι η διασύνδεση των δημοσίων και ιδιωτικών δικτύων και ο διαμοιρασμός πηγών πληροφορίας αυξάνει την δυσκολία να επιτευχθεί έλεγχος της πρόσβασης καθώς και ότι αυτή η τάση για διανεμημένη πληροφόρηση έχει εξουθενώσει την αποτελεσματικότητα του κεντρικού, εξειδικευμένου ελέγχου.

Είναι απολύτως κατανοητό και αναμενόμενο πολλά πληροφοριακά συστήματα να μην έχουν σχεδιαστεί με τις σωστές προδιαγραφές ώστε να είναι ασφαλή. Η ασφάλεια που μπορεί να επιτευχθεί μέσα από τεχνικά μέσα είναι περιορισμένη, και θα πρέπει να υποστηρίζεται από κατάλληλη διαχείριση και διαδικασίες. Η διαχείριση της ασφάλειας πληροφοριών χρειάζεται συμμετοχή, όχι μόνο απ' τους εργαζομένους στην επιχείρηση, αλλά και όλους που συνεργάζονται με αυτήν, ενδεχομένως και με ειδικούς εμπειρογνώμονες έτσι ώστε να εξασφαλιστεί το καλύτερο δυνατό αποτέλεσμα. Αναγνωρίζοντας τι είδους έλεγχοι χρειάζονται, και ποιες είναι οι απαιτήσεις της επιχείρησης σε ασφάλεια προχωράμε με προσοχή στη λεπτομέρεια στον προσεχτικό σχεδιασμό της πολιτικής ασφάλειας. Είναι σαφές λοιπόν το ότι στις μέρες μας είναι απαραίτητο να ακολουθείται και να εφαρμόζεται μία πολιτική ασφάλειας εδραιώνοντας έτσι την ασφάλεια σε κάθε δυνατό επίπεδο και παρέχοντας την απαιτούμενη προστασία στην επιχείρηση.

ΚΕΦΑΛΑΙΟ 1
ΕΚΤΙΜΗΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

1.1 ΕΙΣΑΓΩΓΗ

Στις μέρες μας, οι οργανισμοί λειτουργούν σε έναν κόσμο υψηλής πολυπλοκότητας και διασύνδεσης και βασίζονται στα πληροφοριακά συστήματα προκειμένου να εκπληρώσουν τους στόχους τους και να διεκπεραιώσουν επιχειρηματικές διεργασίες. Όπως έχουμε προαναφέρει, οι επιθέσεις σε πληροφοριακά συστήματα σήμερα είναι οργανωμένες, πειθαρχημένες, και καλά ενισχυμένες. Συνεπώς, αντιλαμβανόμαστε ότι κρίσιμο στάδιο στην ανάπτυξη της πολιτικής ασφαλείας κατέχει η Εκτίμηση Επικινδυνότητας (Risk Assessment). Ο κίνδυνος που σχετίζεται με τον χειρισμό και τη χρήση των πληροφοριακών συστημάτων ένα συστατικό που πρέπει να ληφθεί σοβαρά υπόψη ώστε ένα σύστημα να μπορεί να χαρακτηριστεί ως ασφαλές και να είναι ικανό να προστατευτεί από ενδεχόμενους κινδύνους.

Ο έλεγχος και η εκτίμηση του κινδύνου δεν μπορεί να επιτευχθεί μόνο από τεχνικά μέσα, αλλά κρίνεται αναγκαία οι κριτική γνώμη των ανθρώπων που είναι υπεύθυνοι για τον στρατηγικό σχεδιασμό. Οι ομολογουμένως πολύπλοκες σχέσεις μεταξύ επιχειρηματικών λειτουργιών και η υποστήριξη τους από τα πληροφοριακά συστήματα απαιτούν μία ευρεία και αντικειμενική εικόνα για τον σωστό σχεδιασμό και πλήρη έλεγχο του κινδύνου.

Προκειμένου να υλοποιηθεί μία σωστή προσέγγιση της Εκτίμησης Επικινδυνότητας, θα πρέπει να τηρούνται κάποιες πάγιες διεργασίες έτσι ώστε να μπορούμε να εξασφαλίσουμε ότι ο έλεγχος και η αξιολόγηση του κινδύνου διεκπεραιώνονται με το σωστό τρόπο. Ένα αποτελεσματικό πρόγραμμα ασφάλειας πληροφοριών συνίσταται στα εξής ακόλουθα:

- Υλοποίηση περιοδικών εκτιμήσεων επικινδυνότητας, που περιλαμβάνουν την πιθανότητα ζημιάς που θα μπορούσε να συντελέσει την μη-εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, παραμετροποίηση ή καταστροφή της πληροφορίας και των πληροφοριακών συστημάτων που υποστηρίζουν τις λειτουργίες και τα αγαθά του οργανισμού.

- Να σχεδιαστούν πολιτικές και διαδικασίες που βασίζονται στις εκτιμήσεις κινδύνου, έτσι ώστε να επιτευχθεί η αποτελεσματική μείωση των κινδύνων της ασφάλειας πληροφοριών σε αποδεκτά όρια, και να εξασφαλισθεί η ασφάλεια πληροφοριών στον κύκλου ζωής κάθε επιχειρηματικού πληροφοριακού συστήματος.

- Εκπαίδευση προσωπικού και των αρμοδίων προκειμένου να είναι ικανοί να αναγνωρίσουν κινδύνους ασφάλειας πληροφοριών που σχετίζονται με τις δραστηριότητες τους, καθώς και να καθορίσουν τις υποχρεώσεις τους σε συνδυασμό με τις επιχειρηματικές πολιτικές και διαδικασίες που σχεδιάστηκαν.

- Εφαρμογή περιοδικού ελέγχου και αξιολόγηση της αποτελεσματικότητας των πολιτικών ασφάλειας, των διαδικασιών, των εφαρμογών, και των ελέγχων

ασφαλείας που θα εφαρμοστούν με συχνότητα που βασίζεται στο ενδεχόμενο εμφάνισης του εκάστοτε κινδύνου.

- Υλοποίηση μίας διαδικασίας σχεδιασμού, εφαρμογής, αξιολόγησης και αρχειοθέτησης διεργασιών προκειμένου να οριστεί οτιδήποτε ανεπαρκές στις πολιτικές ασφάλειας.

- Σχεδιασμός διαδικασίας για εντοπισμό, άμεση αναφορά και αντίδραση σε περιστατικά ασφαλείας.

- Σχέδια και διαδικασίες για την συνέχεια και την εξέλιξη των λειτουργιών των πληροφοριακών συστημάτων που υποστηρίζουν τις λειτουργίες και τα αγαθά του οργανισμού.

Η διαχείριση κινδύνου συνίσταται από τρεις διεργασίες, την εκτίμηση επικινδυνότητας, τον κατευνασμό κινδύνου και την εκτίμηση και αξιολόγηση. Παρακάτω θα παρουσιαστεί μία εμπεριστατωμένη ανάλυση της μεθοδολογίας της διαχείρισης κινδύνου. Ο οδηγός αυτός θα μας υποδείξει πως η διαχείριση κινδύνου εφαρμόζεται σε κάθε φάση των πληροφοριακών συστημάτων και πως η αυτή είναι στενά συνδεμένη με την διαδικασία του συστήματος εξουσιοδότησης.

1.2 ΕΝΣΩΜΑΤΩΣΗ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΟΥ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

.

Οι ουσιώδεις λόγοι για τους οποίους οι οργανισμοί εφαρμόζουν την διαδικασία διαχείρισης κινδύνου στα πληροφοριακά τους συστήματα πηγάζουν από την ανάγκη για την σωστή λήψη αποφάσεων. Προκειμένου να επιτευχθεί μία αποτελεσματική διαχείριση κινδύνου πρέπει να υπάρχει πλήρης ενσωμάτωση της στα πληροφοριακά συστήματα. Ένα πληροφοριακό σύστημα αποτελείται από πέντε φάσεις- αρχικοποίηση, ανάπτυξη ή απόκτηση, εφαρμογή, διαχείριση ή συντήρηση και απόρριψη. Σε μερικές περιπτώσεις, ένα πληροφοριακό σύστημα μπορεί να αξιοποιήσει άπειρες από αυτές τις φάσεις την ίδια περίοδο. Όμως, η μεθοδολογία της διαχείρισης κινδύνου είναι ίδια ανεξάρτητα από την φάση για την οποία υλοποιείται η εκτίμηση. Η διαχείριση κινδύνου είναι μία επαναληπτική διαδικασία που μπορεί να εφαρμοστεί κατά τη διάρκεια κάθε σημαντικής φάσης του πληροφοριακού συστήματος. Στον παρακάτω πίνακα παρουσιάζονται τα χαρακτηριστικά κάθε φάσης και με ποιες δραστηριότητες μπορεί να υποστηριχτεί η κάθε φάση.

Φάσεις Πληροφοριακού Συστήματος	**Χαρακτηριστικά Φάσης**	**Υποστήριξη από τις δραστηριότητες Διαχείρισης Κινδύνου**
Φάση 1 - Αρχικοποίηση	Εκφράζεται η ανάγκη για ένα πληροφοριακό σύστημα και καταγράφεται ο σκοπός του	Αναγνωρισμένοι κίνδυνοι είναι σύνηθες να χρησιμοποιούνται για την ανάπτυξη των απαιτήσεων του συστήματος, περιλαμβάνοντας τις απαιτήσεις ασφαλείας και το σκεπτικό της ασφάλειας και των λειτουργιών (στρατηγική)
Φάση 2- Ανάπτυξη ή Απόκτηση	Το πληροφοριακό σύστημα σχεδιάζεται, αγοράζεται, προγραμματίζεται, αναπτύσσεται ή εναλλακτικά κατασκευάζεται.	Οι κίνδυνοι που αναγνωρίζονται κατά τη διάρκεια αυτής της φάσης μπορούν να αξιοποιηθούν ώστε να υποστηρίζουν την ανάλυση ασφάλειας του πληροφοριακού συστήματος που μπορεί να οδηγήσει στην αρχιτεκτονική και τον σχεδιασμό κατά τη διάρκεια ανάπτυξης του συστήματος.
Φάση 3- Εφαρμογή	Τα χαρακτηριστικά ασφαλείας θα πρέπει να είναι διαμορφωμένα, ενεργοποιημένα και ελεγμένα.	Η διαδικασία διαχείρισης κινδύνου υποστηρίζει thv εκτίμηση της εφαρμογής του συστήματος ανάλογα των απαιτήσεων του και

		μέσω του μοντελοποιημένου λειτουργικού περιβάλλοντος. Οι αποφάσεις που αφορούν τα αναγνωρισμένα ρίσκα πρέπει να είναι πρωταρχικά στην λειτουργία του συστήματος.
Φάση 4- Λειτουργία ή Συντήρηση	Το σύστημα εφαρμόζει τις λειτουργίες του. Τυπικά ένα σύστημα τροποποιείται σε συνεχή βάση μέσω της προσθήκης hardware και software και από αλλαγές στις οργανωτικές διαδικασίες, πολιτικές και procedures.	Οι δραστηριότητες διαχείρισης κινδύνου εφαρμόζονται για την περιοδική αναθεώρηση του συστήματος ή όποτε γίνονται σημαντικές αλλαγές στο λειτουργικό, παραγωγικό περιβάλλον του πληροφοριακού συστήματος.
Φάση 5- Απόρριψη	Αυτή η φάση μπορεί να εμπεριέχει την διαγραφή πληροφοριών, hardware και software. Οι δραστηριότητες μπορούν να περιέχουν μετακίνηση, αρχειοθέτηση, απαλλαγή ή καταστροφή πληροφορίας.	Οι δραστηριότητες της Διαχείρισης Κινδύνου εφαρμόζονται στα στοιχεία του συστήματος που θα απορριφθούν ή αντικατασταθούν έτσι ώστε να εξασφαλίσουν ότι το hardware και Software είναι σωστά απορριφθέντα, ότι η υπολειμματικά δεδομένα είναι σωστά μεταχειριζόμενα και ότι μετατόπιση δεδομένων σε άλλο σύστημα διεκπεραιώνεται με ένα ασφαλή και συστηματικό τρόπο.

Όπως έχουμε προαναφέρει η Διαχείριση Κινδύνου είναι μία διοικητική ευθύνη. Αυτή η ενότητα περιγράφει τους κύριους ρόλους του προσωπικού που πρέπει να υποστηρίζει και να συμμετέχει στην διαδικασία διαχείρισης κινδύνου.

- Senior Management – Ο ρόλος του senior manager, πέρα από υπευθυνότητα που κατέχει για την εκπλήρωση της αποστολής, θα πρέπει να εξασφαλίσει και τις απαραίτητες πηγές για να αναπτυχθούν οι ικανότητες που απαιτούνται για να εκπληρώσουν την αποστολή. Επίσης θα πρέπει να εκτιμήσει και να ενσωματώσει τα αποτελέσματα της εκτίμησης επικινδυνότητας μέσα στην διαδικασία λήψης αποφάσεων.

- Chief Information Officer (CIO) είναι υπεύθυνος για τον σχεδιασμό του πληροφοριακού συστήματος της εταιρείας, τον προϋπολογισμό, και την επίδοση περιλαμβανομένου των στοιχείων της ασφάλειας πληροφοριών. Οι αποφάσεις που λαμβάνονται και σε αυτόν τον τομέα θα πρέπει να βασίζονται σε ένα αποτελεσματικό πρόγραμμα διαχείρισης κινδύνου.

- System and information Owners. Είναι υπεύθυνοι για να εξασφαλίσουν ότι υλοποιούνται οι σωστοί έλεγχοι για να διεκπεραιώσουν την ακεραιότητα, εμπιστευτικότητα και την διαθεσιμότητα των πληροφοριακών συστημάτων και των δεδομένων που περιέχουν. Τυπικά είναι υπεύθυνοι για τις αλλαγές σε ένα πληροφοριακό σύστημα, καθώς και πρέπει συνήθως να εγκρίνουν και να υπογράφουν τις αλλαγές στα πληροφοριακά τους συστήματα.

- Business and Functional Managers είναι υπεύθυνοι για τις επιχειρηματικές λειτουργίες και της διαδικασίας προμηθειών του πληροφοριακού συστήματος και πρέπει να λαμβάνουν ενεργό ρόλο στην διαδικασία διαχείρισης κινδύνου. Αυτοί οι managers είναι ιδιώτες με την εξουσιοδότηση και την ευθύνη να παίρνουν αποφάσεις ουσιώδεις για την εκπλήρωση των αποστολών. Η εμπλοκή τους στην διαδικασία διαχείρισης κινδύνου κάνει ικανή την επίτευξη σωστής ασφάλειας για τα πληροφοριακά συστήματα, τα οποία, αν τα διαχειριστούν σωστά, θα παρέχουν αποτελεσματικότητα των αποστολών με την ελάχιστη δαπάνη πηγών.

- ISSO - Οι managers της ασφάλειας πληροφοριακών συστημάτων είναι υπεύθυνοι για τα προγράμματα ασφαλείας των οργανισμών τους, περιλαμβάνοντας την διαχείριση κινδύνου. Ως εκ τούτου, κατέχουν ηγετικό ρόλο στο να εισάγουν μία κατάλληλη, δομημένη μεθοδολογία για να βοηθήσουν στην αναγνώριση, την εκτίμηση και την ελαχιστοποίηση των κινδύνων στα πληροφοριακά συστήματα. Επίσης λειτουργούν σαν κύριοι σύμβουλοι στην υποστήριξη της διοίκησης έτσι ώστε να διασφαλίσουν ότι αυτή η δραστηριότητα εκτελείται σε μία συνεχή βάση.

- Security Awareness Trainers – Το προσωπικό του οργανισμού είναι οι χρήστες του πληροφοριακού συστήματος. Η χρήση των πληροφοριακών συστημάτων και των δεδομένων, σύμφωνα με τις πολιτικές ενός οργανισμού, τις οδηγήτριες γραμμές τους και τους κανόνες συμπεριφοράς είναι κρίσιμη για τον κατευνασμό του κινδύνου και την προστασία των πηγών του πληροφοριακού συστήματος. Για να ελαχιστοποιηθεί ο κίνδυνος στα πληροφοριακά συστήματα είναι σημαντικό ότι οι χρήστες του συστήματος και των εφαρμογών να έχουν και την κατάλληλη εκπαίδευση. Έτσι λοιπόν, οι εκπαιδευτές των πληροφοριακών συστημάτων

πρέπει να κατανοήσουν την διαδικασία διαχείρισης κινδύνου έτσι ώστε να μπορούν να αναπτύξουν τα κατάλληλα εκπαιδευτικά υλικά και να ενσωματώσουν την εκτίμηση επικινδυνότητας μέσα στα προγράμματα εκπαίδευσης και να μορφώσουν τους χρήστες.

1.3 ΜΕΘΟΔΟΛΟΓΙΑ

Η εκτίμηση επικινδυνότητας είναι η πρώτη διεργασία στην μεθοδολογία της διαχείρισης κινδύνου. Οι οργανισμοί χρησιμοποιούν την εκτίμηση επικινδυνότητας για να καθορίσουν την έκταση των πιθανών απειλών και τον κίνδυνο που σχετίζεται με ένα πληροφοριακό σύστημα. Το αποτέλεσμα αυτής της διεργασίας βοηθά στο να αναγνωριστούν οι κατάλληλοι έλεγχοι για να μειώσουν ή να εξαλείψουν τον κίνδυνο κατά τη διάρκεια της διαδικασίας κατευνασμού του κινδύνου.

Για να καθορίσουμε την πιθανότητα ενός μελλοντικού αντίξοου γεγονότος, οι απειλές σε ένα πληροφοριακό σύστημα θα πρέπει να αναλύονται σε συσχετισμό με την πιθανότητα αδυναμιών και με τους ελέγχους που εκτελούνται στο πληροφοριακό σύστημα. Η επίπτωση αναφέρεται στο μέγεθος της ζημιάς που θα μπορούσε να προκληθεί από την εισβολή μιας απειλής σε μία ευπάθεια του συστήματος. Η μεθοδολογία της διαχείρισης κινδύνου εμπεριέχει εννέα πρωτεύοντα στάδια

Στάδιο 1	Χαρακτηρισμός του Συστήματος
Στάδιο 2	Αναγνώριση της Απειλής
Στάδιο 3	Αναγνώριση της Ευπάθειας
Στάδιο 4	Ανάλυση Ελέγχου
Στάδιο 5	Προσδιορισμός Πιθανότητας
Στάδιο 6	Ανάλυση Επιπτώσεων
Στάδιο 7	Προσδιορισμός Κινδύνου
Στάδιο 8	Συνιστώμενοι Ελέγχου
Στάδιο 9	Τεκμηρίωση Αποτελεσμάτων

ΣΤΑΔΙΟ 1: ΧΑΡΑΚΤΗΡΙΣΜΌΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Για την εκτίμηση επικινδυνότητας σε ένα πληροφοριακό σύστημα, το πρώτο βήμα είναι να καθορίσουμε την σκοπιά της προσπάθειας. Σε αυτό το βήμα, αναγνωρίζονται τα όρια ενός πληροφοριακού συστήματος, παράλληλα με τις πηγές και την πληροφορία που δομεί το σύστημα. Ο χαρακτηρισμός ενός πληροφοριακού συστήματος εδραιώνει τον σκοπό της εκτίμησης επικινδυνότητας, περιγράφει τα όρια της λειτουργικής εξουσιοδότησης, και παρέχει σημαντική πληροφόρηση στο καθορισμό του κινδύνου.

Η αναγνώριση του κινδύνου σε ένα πληροφοριακό σύστημα απαιτεί κατανόηση του διαδικαστικού περιβάλλοντος του συστήματος. Το πρόσωπο ή τα πρόσωπα που διενεργούν την εκτίμηση επικινδυνότητας πρέπει αρχικά να συλλέξουν συσχετιζόμενη με το σύστημα πληροφορία, όπως hardware, software, διασυνδέσεις του συστήματος, δεδομένα και πληροφορία, τα πρόσωπα που υποστηρίζουν και χρησιμοποιούν το πληροφοριακό σύστημα, την αποστολή του συστήματος και την ευαισθησία των δεδομένων του.

Επιπλέον, η πληροφορία που σχετίζεται με το λειτουργικό περιβάλλον του πληροφοριακού συστήματος και τα δεδομένα του περιλαμβάνει, αλλά δεν περιορίζεται, στα ακόλουθα: τις λειτουργικές απαιτήσεις ενός πληροφοριακού συστήματος, τους χρήστες του συστήματος, πολιτικές ασφαλείας, αρχιτεκτονική του συστήματος ασφαλείας, τωρινή τοπολογία δικτύου, διοικητικοί έλεγχοι, ροή της πληροφορίας που διεισδύει στο πληροφοριακό σύστημα, τεχνικοί και λειτουργικοί έλεγχοι και το φυσικό περιβάλλον ασφαλείας του πληροφοριακού συστήματος.

Οποιοσδήποτε, ή ένας συνδυασμός, από τις ακόλουθες τεχνικές μπορεί να χρησιμοποιηθεί για την συλλογή πληροφοριών σχετικές με το πληροφοριακό σύστημα και τα λειτουργικά του όρια.

- Ερωτηματολόγιο - Για να συλλέξουμε σχετική πληροφορία, μπορούμε να δημιουργήσουμε ένα ερωτηματολόγιο που σχετίζεται με την διαχείριση και τους λειτουργικούς ελέγχους που σχεδιάζονται ή χρησιμοποιούνται για το λειτουργικό σύστημα. Αυτό το ερωτηματολόγιο θα πρέπει να διανέμεται στο τεχνικό και μη τεχνικό προσωπικό που σχεδιάζει ή υποστηρίζει το πληροφοριακό σύστημα. Το ερωτηματολόγιο θα μπορούσε επίσης να χρησιμοποιηθεί κατά τη διάρκεια επισκέψεων ή συνεντεύξεων (Παράρτημα 4.1).
- Συνεντεύξεις - Συνεντεύξεις με το προσωπικό υποστήριξης και διοίκησης μπορούν να δώσουν αξιόλογες πληροφορίες σχετικά με το πληροφοριακό σύστημα. Οι on-site επισκέψεις επίσης επιτρέπουν την εκτίμηση ικανότητας του προσωπικού να παρατηρεί και να συλλέγει πληροφορία σχετικά με την φυσική, περιβαλλοντική και λειτουργική ασφάλεια του πληροφοριακού συστήματος. Για συστήματα που βρίσκονται ακόμη στην φάση σχεδιασμού, οι επισκέψεις θα συνέβαλαν στην άμεση συλλογή πληροφοριών και θα παρείχαν την δυνατότητα εκτίμησης του φυσικού περιβάλλοντος μέσα στο οποίο θα λειτουργήσει το πληροφοριακό σύστημα.
- Document Review - Έγγραφα ασφαλείας μπορούν να παρέχουν καλή πληροφόρηση σχετικά με τους ελέγχους ασφαλείας που χρησιμοποιούνται και σχεδιάζονται για το πληροφοριακό σύστημα. Η επίπτωση που έχει η αποστολή ενός οργανισμού παρέχει πληροφορία που σχετίζεται με το σύστημα, τα δεδομένα και την ευαισθησία τους.
- Χρήση αυτοματοποιημένου εργαλείου Scanning – Τεχνικές μέθοδοι μπορούν να χρησιμοποιηθούν για να συλλέξουν επαρκώς πληροφορίες του συστήματος.

ΣΤΑΔΙΟ 2: ΑΝΑΓΝΩΡΙΣΗ ΑΠΕΙΛΩΝ

Ο σκοπός αυτού του βήματος είναι να αναγνωρίσει τις πιθανές πηγές- απειλών και να συνδυάσει μία απειλή με μία λίστα πιθανών πηγών-απειλών που είναι δυνατόν να εφαρμοστούν στο πληροφοριακό σύστημα που αξιολογείται. Μία πηγή-απειλής ορίζεται ως κάθε περίσταση ή γεγονός με την πιθανότητα να προκαλέσει βλάβη σε ένα

πληροφοριακό σύστημα. Οι κοινές πηγές-απειλών μπορεί να είναι φυσικές, ανθρώπινες, ή περιβαλλοντικές. Στην εκτίμηση των πηγών-απειλών, είναι σημαντικό να θεωρήσουμε ότι όλες οι πιθανές πηγές-απειλών θα μπορούσαν να προκαλέσουν ζημιά σε ένα πληροφοριακό σύστημα και το διαδικαστικό του περιβάλλον.

Τα κίνητρα και οι πηγές μιας επίθεσης μας οδηγούν στο να θεωρήσουμε τους ίδιους τους ανθρώπους ως πιθανές πηγές απειλών. Πληροφορία σχετικά με τα κίνητρα των ανθρώπινων απειλών είναι χρήσιμη στους οργανισμούς που μελετούν τα ανθρώπινα περιβάλλοντα απειλών, έτσι ώστε να προσαρμόζουν κατάλληλα τις πολιτικές ασφαλείας. Επιπλέον, περιλήψεις του ιστορικού εισβολής στο σύστημα, αναφορές παραβίασης ασφαλείας, αναφορές περιστατικών και συνεντεύξεις με τους διαχειριστές του συστήματος, βοηθούν στο να αναγνωριστούν οι ανθρώπινες πηγές-απειλών που έχουν την δυνατότητα να βλάψουν ένα πληροφοριακό σύστημα και τα δεδομένα του.

Σε γενικές γραμμές, η πληροφορία πάνω στις φυσικές απειλές θα πρέπει να είναι άμεσα διαθέσιμη. Οι γνωστές απειλές έχουν αναγνωριστεί από πολλές κυβερνητικές και ιδιωτικού τομέα οργανώσεις. Επίσης, εργαλεία εντοπισμού αυθαίρετης εισχώρησης κυριαρχούν ολοένα και περισσότερο, και δίνεται η δυνατότητα στην κυβέρνηση και τις βιομηχανικές οργανώσεις να συλλέγουν δεδομένα στα γεγονότα ασφαλείας, παρέχοντας με αυτόν τον τρόπο την ικανότητα αναγνώρισης ρεαλιστικών απειλών.

ΣΤΑΔΙΟ 3: ΑΝΑΓΝΩΡΙΣΗ ΤΗΣ ΕΥΠΑΘΕΙΑΣ

Η ανάλυση μιας απειλής στο πληροφοριακό σύστημα πρέπει να περιλαμβάνει την ανάλυση των ευπαθειών που σχετίζονται με το περιβάλλον του συστήματος. Ο στόχος αυτού του βήματος είναι να αναπτύξει μία λίστα από ευπάθειες του συστήματος (λάθη ή αδυναμίες) που θα μπορούσαν να γίνουν αντικείμενο εκμετάλλευσης από ενδεχόμενες πηγές-απειλών.

Οι συνιστώμενες μέθοδοι για την αναγνώριση των ευπαθειών του συστήματος είναι ο έλεγχος επίδοσης του συστήματος και η ανάπτυξη μίας λίστας απαιτήσεων ασφαλείας. Θα πρέπει να σημειωθεί ότι τα είδη των ευπαθειών που θα υπάρξουν, και η μεθοδολογία που θα χρειαστεί για να καθορίσει αν οι ευπάθειες είναι παρούσες, συνήθως ποικίλει και εξαρτάται από την φύση του πληροφοριακού συστήματος και την φάση που βρίσκεται. Αν το πληροφοριακό σύστημα δεν έχει σχεδιαστεί ακόμη, η αναζήτηση αδυναμιών θα πρέπει να επικεντρωθεί στις πολιτικές ασφαλείας του οργανισμού, στις σχεδιασμένες διαδικασίες ασφαλείας, και τις απαιτήσεις του συστήματος. Αν το σύστημα είναι ήδη υπό εφαρμογή, η αναγνώριση των ευπαθειών θα πρέπει να επεκταθεί ώστε να περιέχει περισσότερη εξειδικευμένη πληροφορία, όπως σχεδιασμένα χαρακτηριστικά ασφάλειας μέσα στα έγγραφα του σχεδιασμού ασφαλείας και τα αποτελέσματα του ελέγχου και αξιολόγησης του συστήματος. Αν το πληροφοριακό σύστημα είναι λειτουργικό, η διαδικασία αναγνώρισης των αδυναμιών θα πρέπει να εμπεριέχει την ανάλυση των χαρακτηριστικών του συστήματος και τους ελέγχους ασφαλείας, τεχνικούς και διαδικαστικούς, που χρησιμοποιούνται για να προστατέψουν το σύστημα.

Οι τεχνικές και οι μη-τεχνικές αδυναμίες που σχετίζονται με το διαδικαστικό περιβάλλον ενός πληροφοριακού συστήματος, μπορούν να αναγνωριστούν μέσω τεχνικών συλλογής πληροφοριών. Μία περίληψη άλλων βιομηχανικών πηγών θα είναι χρήσιμη στην προετοιμασία των συνεντεύξεων και στην ανάπτυξη αποτελεσματικών ερωτηματολογίων στο να αναγνωριστούν οι ευπάθειες του συστήματος. Το Διαδίκτυο είναι μία άλλη πηγή πληροφόρησης για γνωστές αδυναμίες των συστημάτων που

δίνονται από τους πωλητές, μαζί με τις επιδιορθώσεις, τα πακέτα service, patches, και άλλα επανορθωτικά μέτρα που μπορούν να εφαρμοστούν. Οι αρχειοθετημένες πηγές αδυναμιών που πρέπει να συμπεριληφθούν στην λεπτομερή ανάλυση ευπαθειών περιλαμβάνουν, αλλά δεν περιορίζονται, στα ακόλουθα: Σε προηγούμενες εκτιμήσεις επικινδυνότητας που έχουν διενεργηθεί για το πληροφοριακό σύστημα, σε αναφορές ασφαλείας, αναφορές ανωμαλίας, αναφορές ελέγχου και αξιολόγησης του συστήματος, λίστες αδυναμιών, εταιρείες συμβούλων για θέματα ασφάλειας, συμβουλές πωλητών.

Προκειμένου να αξιολογηθούν οι ευπάθειες του συστήματος θα πρέπει να διενεργηθεί έλεγχος βασιζόμενος στην οξυδέρκεια του πληροφοριακού συστήματος και την επάρκεια των πηγών. Οι μέθοδοι μέσω των οποίων μπορεί να πραγματοποιηθεί ο έλεγχος περιλαμβάνουν: το αυτοματοποιημένο εργαλείο scanning ευπάθειας, έλεγχος ασφάλειας και αξιολόγησης, και penetration testing.

Κατά τη διάρκεια αυτού του βήματος, η εκτίμηση επικινδυνότητας θα καθορίσει αν οι απαιτήσεις ασφαλείας που έχουν οριστεί για το πληροφοριακό σύστημα και συλλέγονται κατά τη διάρκεια χαρακτηρισμού του συστήματος, πληρούν τους υπάρχοντες ή τους σχεδιασμένους ελέγχους ασφαλείας. Τυπικά, οι απαιτήσεις ασφάλειας του συστήματος μπορούν να παρουσιαστούν υπό μορφή πίνακα, με κάθε απαίτηση να συνοδεύεται από μια αιτιολόγηση του πως ο σχεδιασμός ενός συστήματος ή η εφαρμογή του, ικανοποιεί ή όχι την συγκεκριμένη απαίτηση ασφαλείας.

Η λίστα των ελέγχων ασφαλείας περιέχει τα βασικά στάνταρντ ασφαλείας που μπορούν να χρησιμοποιηθούν για να αξιολογούν συστηματικά και να αναγνωρίζουν τις ευπάθειες των επιχειρησιακών αγαθών, τις μη αυτοματοποιημένες διαδικασίες, τις λειτουργίες και τις μεταφορές πληροφοριών που σχετίζονται με ένα πληροφοριακό σύστημα στις ακόλουθες περιοχές ασφαλείας: Διοικητικές, Λειτουργικές και Τεχνικές.

ΣΤΑΔΙΟ 4: ΑΝΑΛΥΣΗ ΕΛΕΓΧΟΥ

Ο σκοπός αυτού του σταδίου είναι να αναλύσει τους ελέγχους που έχουν εφαρμοστεί, ή σχεδιάζονται για εφαρμογή, από τον οργανισμό για να ελαττώσουν ή να εξαλείψουν την πιθανότητα μία απειλή να επιτεθεί σε μία ευπάθεια του συστήματος.

Οι έλεγχοι ασφαλείας περιλαμβάνουν τη χρήση τεχνικών και μη τεχνικών μεθόδων. Οι τεχνικοί έλεγχοι είναι φύλακες ασφαλείας που ενσωματώνονται στο hardware, software ή firmware. Οι μη τεχνικοί έλεγχοι είναι διοικητικοί και λειτουργικοί έλεγχοι, όπως οι πολιτικές ασφαλείας, οι λειτουργικές διαδικασίες, το προσωπικό, η φυσική και η περιβαλλοντική ασφάλεια.

Εκτενέστερα, οι κατηγορίες ελέγχου για τις τεχνικές και μη- τεχνικές μεθόδους μπορούν περαιτέρω να ταξινομηθούν ως προληπτικές ή ως διερευνητικές.

Η ανάπτυξη των απαιτήσεων ασφαλείας ή η χρήση των ήδη διαθέσιμων απαιτήσεων θα δώσει μεγάλη βοήθεια στην ανάλυση ελέγχων με έναν επαρκή και συστηματικό τρόπο. Η λίστα των απαιτήσεων ασφαλείας μπορεί να χρησιμοποιηθεί ώστε να επικυρώσει την την συμβατικότητα. Έτσι, είναι σημαντικό να αναβαθμίζονται αυτές οι λίστες ώστε να ανταποκρίνονται στις αλλαγές στο περιβάλλον ελέγχου του οργανισμού.

ΣΤΑΔΙΟ 5: ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΠΙΘΑΝΟΤΗΤΑΣ

Για να δημιουργηθεί μία συνολική αξιολόγηση που υποδεικνύει την πιθανότητα μία δυνατή ευπάθεια να γίνει αντικείμενο επίθεσης από το συσχετιζόμενο περιβάλλον απειλών, πρέπει να ληφθούν υπόψη οι ακόλουθοι παράγοντες:

- Το κίνητρο των απειλών και η ικανότητα τους
- Η φύση της ευπάθειας
- Η ύπαρξη και η αποτελεσματικότητα των παρόντων ελέγχων

Επίπεδο Πιθανότητας	**Προσδιορισμός Πιθανότητας**
Υψηλή	Η πηγή απειλών έχει υψηλά κίνητρα και είναι επαρκώς ικανή, και οι έλεγχοι για να προστατέψουν της ευπάθειας είναι μη αποτελεσματικοί
Μεσαία	Η πηγή απειλών έχει κίνητρα και είναι ικανή, αλλά οι έλεγχοι είναι σε θέση να μπορούν να εμποδίσουν την εκμετάλλευση της ευπάθειας
Χαμηλή	Η πηγή απειλών δεν έχει κίνητρα ή ικανότητα, και οι έλεγχοι είναι σε θέση να προστατέψουν, ή τουλάχιστον να impede σημαντικά την εκμετάλλευση της ευπάθειας

ΣΤΑΔΙΟ 6: ΑΝΑΛΥΣΗ ΕΠΙΠΤΩΣΕΩΝ

Το επόμενο κύριο βήμα στον υπολογισμό του επιπέδου του κινδύνου είναι να καθορίσουμε τις επιπτώσεις που προκύπτουν από την επιτυχημένη εκμετάλλευση μίας αδυναμίας του συστήματος. Πριν ξεκινήσουμε την ανάλυση επιπτώσεων, είναι απαραίτητο να αποκτήσουμε πληροφορία η οποία σχετίζεται με την αποστολή του συστήματος, την οξυδέρκεια και την ευαισθησία του συστήματος και των δεδομένων.

Αν δεν υπάρχουν καταγεγραμμένα αρχεία ή εάν δεν έχουν εφαρμοστεί τέτοιου είδους εκτιμήσεις για τα πληροφοριακά αγαθά του οργανισμού, η ευαισθησία και τα δεδομένα του συστήματος μπορούν να καθοριστούν βασιζόμενα στο επίπεδο προστασίας που απαιτείται για να συντηρήσει την διαθεσιμότητα του συστήματος και των δεδομένων, την πληρότητα και την εμπιστευτικότητα. Χωρίς να μας απασχολεί η μέθοδος η οποία χρησιμοποιείται για να καθορίσει πόσο ευαίσθητο είναι ένα πληροφοριακό σύστημα και τα δεδομένα του, οι ιδιοκτήτες του συστήματος και των πληροφοριών είναι υπεύθυνοι για τον καθορισμό του επιπέδου των επιπτώσεων για τα δικά τους συστήματα. Συνεπώς, στην ανάλυση των επιπτώσεων, η κατάλληλη προσέγγιση είναι η συνέντευξη με τους ιδιοκτήτες του συστήματος και των δεδομένων.

Έτσι λοιπόν, η επίπτωση ενός γεγονότος ασφαλείας μπορεί να περιγραφεί με τους όρους της απώλειας ή της υποβάθμισης, ή συνδυασμό των οποιονδήποτε, από τους ακόλουθους τρεις σκοπούς ασφαλείας: ακεραιότητα, διαθεσιμότητα, και εμπιστευτικότητα. Η ακόλουθη λίστα παρέχει μία σύντομη περιγραφή καθενός από τους τρεις στόχους ασφαλείας και τις συνέπειες που προκύπτουν αν δεν εφαρμόζονται

- Απώλεια της ακεραιότητας- Η ακεραιότητα του συστήματος και των δεδομένων αναφέρεται στην απαίτηση ότι η πληροφορία πρέπει να προστατεύεται από ακανόνιστη παραμετροποίηση. Η ακεραιότητα χάνεται εάν γίνονται μη εξουσιοδοτημένες αλλαγές στα δεδομένα ή στο πληροφοριακό σύστημα είτε από επιτηδευμένα ή από τυχαία περιστατικά. Εάν η απώλεια της πληρότητας του συστήματος ή των δεδομένων δεν διορθωθεί, η συνεχής χρήση του μολυσμένου συστήματος ή των διεφθαρμένων δεδομένων θα μπορούσε να καταλήξει σε ανακρίβεια, απάτη, ή λανθασμένες αποφάσεις. Επίσης, η παραβίαση της πληρότητας μπορεί να είναι το πρώτο βήμα για την επιτυχημένη επίθεση ενάντια στην διαθεσιμότητα και την πληρότητα του συστήματος. Για όλους αυτούς τους λόγους, η απώλεια της πληρότητας ελαττώνει την ασφάλεια ενός πληροφοριακού συστήματος.
- Απώλεια της διαθεσιμότητας – Εάν ένα πληροφοριακό σύστημα δεν είναι διαθέσιμο στους τερματικούς του χρήστες, τότε η αποστολή ενός οργανισμού μπορεί να επηρεαστεί. Η απώλεια της λειτουργικότητας ενός συστήματος και η λειτουργική του αποτελεσματικότητα, για παράδειγμα, μπορεί να καταλήξει σε απώλεια του παραγωγικού χρόνου, επηρεάζοντας με αυτόν τον τρόπο την απόδοση των τερματικών χρηστών ή τις ενέργειες τους που υποστηρίζουν την αποστολή του οργανισμού.
- Απώλεια της Εμπιστευτικότητας – Η εμπιστευτικότητα του συστήματος και των δεδομένων αναφέρεται στην προστασία την πληροφορίας από μη εξουσιοδοτημένες γνωστοποιήσεις. Ο αντίκτυπος της μη εξουσιοδοτημένης γνωστοποίησης της εμπιστευτικής πληροφορίας κυμαίνεται από την διακινδύνευση της εθνικής ασφάλειας έως την αποκάλυψη ιδιωτικών δεδομένων. Μη εξουσιοδοτημένη, μη αναμενόμενη, ή μη επιτηδευμένη γνωστοποίηση θα μπορούσε να καταλήξει σε απώλεια της κοινής εμπιστοσύνης, ντρόπιασμα, ή νομική κίνηση ενάντια στον οργανισμό.

ΣΤΑΔΙΟ 7: ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΚΙΝΔΥΝΟΥ

Ο σκοπός αυτού του βήματος είναι να εκτιμήσει το επίπεδο του κινδύνου στο πληροφοριακό σύστημα. Ο καθορισμός του κινδύνου για μία συγκεκριμένη απειλή/ ευπάθεια μπορεί να εκφραστεί ως λειτουργία της πιθανότητας μία απειλή να εισβάλλει σε μία συγκεκριμένη ευπάθεια, του μεγέθους των επιπτώσεων που θα προκαλούσε η απειλή, και της επάρκειας των ελέγχων ασφαλείας για την ελάττωση ή την εξάλειψη του κινδύνου.

Η κλίμακα του κινδύνου, με τις αξιολογήσεις της σε Υψηλή, Μεσαία και Χαμηλή, αναπαριστά τον βαθμό του επιπέδου του κινδύνου στον οποίο ένα πληροφοριακό σύστημα, μία εγκατάσταση ή διαδικασία μπορεί να εκτεθεί αν υπάρχει μία ευπάθεια. Η κλίμακα του κινδύνου επίσης αναπαριστά δράσεις οι οποίες πρέπει να εκτελεστούν για κάθε επίπεδο κινδύνου.

Επίπεδο Κινδύνου	Περιγραφή κινδύνου και απαραίτητες δράσεις
Υψηλό	Αν μία παρατήρηση ή ένα εύρημα εκτιμάται ως υψηλού κινδύνου, τότε υπάρχει ισχυρή ανάγκη για διορθωτικά μέσα. Ένα υπάρχον σύστημα μπορεί να συνεχίσει να λειτουργεί, όμως ένα διορθωτικό σχέδιο δράσης πρέπει να μπει σε εφαρμογή όσο το δυνατόν συντομότερο.
Μεσαίο	Αν μία παρατήρηση βαθμολογείται ως μεσαίου κινδύνου, τότε χρειάζονται διορθωτικές δράσεις και πρέπει να αναπτυχθεί ένα σχέδιο για να ενσωματώσει αυτές τις δράσεις μέσα σε ένα λογικό πλαίσιο χρόνου.
Χαμηλό	Αν μία παρατήρηση περιγράφεται ως χαμηλού κινδύνου, τότε βάσει του συστήματος πρέπει να καθοριστεί αν απαιτούνται διορθωτικές δράσεις ή πρέπει να γίνει αποδοχή του κινδύνου.

ΣΤΑΔΙΟ 8: ΣΥΝΙΣΤΩΜΕΝΟΙ ΕΛΕΓΧΟΥ

Κατά τη διάρκεια αυτού του βήματος της διαδικασίας, παρέχονται οι έλεγχοι οι οποίοι θα μπορούσαν να περιορίσουν ή να ελαττώσουν τους αναγνωρισμένους κινδύνους. Ο σκοπός των συνιστώμενων ελέγχων είναι να μειώσει το επίπεδο κινδύνου του πληροφοριακού συστήματος και των δεδομένων του σε ένα επιτρεπτό επίπεδο. Οι ακόλουθοι παράγοντες θα μπορούσαν να ληφθούν υπόψη στους συνιστώμενους ελέγχους και τις εναλλακτικές λύσεις στο να μειώσουν ή να εξαλείψουν τους αναγνωρισμένους κινδύνους.

- Αποτελεσματικότητα των συνιστώμενων επιλογών
- Νομοθεσία και κανονισμοί
- Οργανωτική πολιτική
- Λειτουργικές επιπτώσεις
- Ασφάλεια και αξιοπιστία

Οι συνιστώμενοι έλεγχοι είναι το αποτέλεσμα της διαδικασίας της εκτίμησης επικινδυνότητας και συνεισφέρουν στην διαδικασία του κατευνασμού του κινδύνου, κατά τη διάρκεια της οποίας οι συνιστώμενες διαδικασίες και οι έλεγχοι τεχνικής ασφαλείας εκτιμούνται, , ιεραρχούνται και εφαρμόζονται.

Θα πρέπει να σημειωθεί ότι όλοι οι πιθανοί συνιστώμενοι έλεγχοι μπορούν να εφαρμοστούν για να ελαττώσουν την απώλεια. Για να καθορίσουμε ποιοι είναι κατάλληλοι και απαραίτητοι για έναν συγκεκριμένο οργανισμό, θα μπορούσαμε να διενεργήσουμε μία ανάλυση βασιζόμενη στο κόστος και τα οφέλη, για τους προτεινόμενους συνιστώμενους ελέγχους, για να επιδείξουμε ότι το κόστος της εφαρμογής των ελέγχων μπορεί να δικαιολογηθεί από την μείωση του επιπέδου του κινδύνου. Επιπρόσθετα, ο λειτουργικός αντίκτυπος και η εισαγωγή της συνιστώμενης επιλογής θα πρέπει να αξιολογείται προσεχτικά κατά την διάρκεια της διαδικασίας του κατευνασμού του κινδύνου.

ΣΤΑΔΙΟ 9: ΤΕΚΜΗΡΙΩΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Όταν η εκτίμηση επικινδυνότητας έχει ολοκληρωθεί, τα αποτελέσματα θα πρέπει να καταγραφούν σε μία επίσημη αναφορά.

Η αναφορά της εκτίμησης επικινδυνότητας είναι μία διοικητική αναφορά που βοηθά την διοίκηση, τους ιδιοκτήτες των αποστολών να λαμβάνουν αποφάσεις στην πολιτική, την διαδικαστική, τον προϋπολογισμό και τις λειτουργικές και διοικητικές αλλαγές του συστήματος. Η αναφορά της εκτίμησης επικινδυνότητας θα πρέπει να παρουσιάζεται ως μία συστηματική και αναλυτική προσέγγιση στην εκτίμηση κινδύνου έτσι ώστε η διοίκηση να κατανοεί τους κινδύνους και να διαθέσει τις πηγές ώστε να μειώσει και να διορθώσει τις πιθανές απώλειες.

1.4. ΚΑΤΕΥΝΑΣΜΟΣ ΚΙΝΔΥΝΟΥ

Όπως είναι κατανοητό, η εξάλειψη όλων των κινδύνων είναι συνήθως μη – πρακτική ή σχεδόν ακατόρθωτη, γι' αυτό έγκειται στην ευθύνη της διοίκησης και των λειτουργικών και επιχειρηματικών διοικητών να χρησιμοποιήσουν την προσέγγιση με το λιγότερο δυνατό κόστος και να εφαρμόσουν τους κατάλληλους ελέγχους για να μειώσουν τον κίνδυνο των αποστολών σε ένα αποδεκτό επίπεδο, με τις λιγότερες δυνατές επιπτώσεις στις πηγές ενός οργανισμού.

Ο κατευνασμός κινδύνου είναι η δεύτερη διαδικασία της διαχείρισης κινδύνου, που εμπεριέχει, ιεράρχηση, αξιολόγηση και εφαρμογή των κατάλληλων ελέγχων μείωσης κινδύνου που συνιστούνται από την διαδικασία εκτίμησης κινδύνου. Είναι μία συστηματική μεθοδολογία που χρησιμοποιείται από τη διοίκηση προκειμένου να ελαττώσει τον κίνδυνο των αποστολών. Ο κατευνασμός κινδύνου είναι δυνατό να επιτευχθεί μέσω οποιοδήποτε από τις ακόλουθες επιλογές.

- Risk Assumption- Για να αποδεχθούμε ένα δυνατό ρίσκο και να συνεχίσουμε να χειριζόμαστε το πληροφοριακό σύστημα ή να εφαρμόζουμε τους ελέγχους για να χαμηλώσουμε τον κίνδυνο σε ένα αποδεκτό επίπεδο
- Risk Avoidance – Για να αποφύγουμε τον κίνδυνο, εξαλείφοντας την πηγή του κινδύνου ή τις συνέπειες της.
- Risk Limitation – Για να ελαττώσουμε τον κίνδυνο, εφαρμόζοντας ελέγχους που ελαχιστοποιούν τις αρνητικές επιπτώσεις μιας απειλής.
- Risk Planning – Για να διαχειριστούμε τον κίνδυνο αναπτύσσοντας έναν κατευνασμό κινδύνου ο οποίος δίνει προτεραιότητες, εφαρμόζει, και συντηρεί τους ελέγχους.
- Research and Acknowledgment - Για να χαμηλώσουμε τον κίνδυνο απώλειας γνωστοποιώντας την ευπάθεια ή το λάθος και αναζητώντας ελέγχους για να διορθώσουμε την ευπάθεια.

Οι σκοποί και οι αποστολές ενός οργανισμού θα πρέπει να ληφθούν υπόψη στην συλλογή οποιοδήποτε από αυτών των επιλογών κατευνασμού κινδύνου. Μπορεί να μην είναι πρακτικό να περιοριστούν όλα τα αναγνωρισμένα ρίσκα, άρα η προτεραιότητα θα πρέπει να δοθεί στις απειλές οι οποίες προτίθενται να προκαλέσουν ζημιά σε σημαντικές αποστολές του οργανισμού. Επειδή το περιβάλλον και οι σκοποί κάθε οργανισμού είναι μοναδικοί, η επιλογή που χρησιμοποιείται για να μειώσει τον κίνδυνο και οι μέθοδοι που χρησιμοποιούνται για να εφαρμοστούν οι έλεγχοι, ποικίλουν. Η καλύτερη προσέγγιση είναι να χρησιμοποιήσουμε τις κατάλληλες μεθοδολογίες, μαζί με τον κατάλληλο κατευνασμό κινδύνου και μη τεχνικά, διαχειριστικά μέτρα.

Πρέπει λοιπόν να ακολουθηθεί μία συγκεκριμένη στρατηγική προκειμένου να είναι εφικτό να αναγνωρίσουμε υπό ποιες συνθήκες πρέπει να εφαρμοστούν οι απαραίτητοι έλεγχοι. Η στρατηγική υλοποιείται με την εφαρμογή των ακόλουθων κανόνων, οι οποίοι παρέχουν καθοδήγηση πάνω σε δράσεις για τον περιορισμό κινδύνου από επιτηδευμένες ανθρώπινες απειλές

Όταν υπάρχει ευπάθεια – εφαρμόζουμε τεχνικές εξασφάλισης για να μειώσουμε την πιθανότητα εισβολής σε μία ευπάθεια

Όταν μία ευπάθεια μπορεί γίνει αντικείμενο επίθεσης – εφαρμόζουμε προστασίες, αρχιτεκτονικά σχέδια, και διαχειριστικούς ελέγχους για να ελαχιστοποιήσουμε τον κίνδυνο ή να παρεμποδίσουμε αυτό το περιστατικό

Όταν το κόστος του εισβολέα είναι λιγότερο από το δυνατό κέρδος – εφαρμόζουμε προστασία για να μειώσουμε το κίνητρο του επιτιθέμενου, αυξάνοντας το κόστος του.

Όταν υπάρχει πολύ μεγάλη απώλεια- εφαρμόζουμε σχεδιαστικές αρχές, αρχιτεκτονικά σχέδια, και τεχνική και μη τεχνική προστασία για να περιορίσουμε το μέγεθος της επίθεσης, μειώνοντας έτσι την απώλεια.

Στην ακόλουθη μεθοδολογία κατευνασμού κινδύνου περιγράφεται αναλυτικά η προσέγγιση για την εφαρμογή ελέγχου

Βήματα	**Περιγραφή**	**Αποτέλεσμα**
Βήμα 1- Ιεράρχηση των δραστηριοτήτων	Βασίζεται στα επίπεδα κινδύνου που παρουσιάζονται στην αναφορά εκτίμησης επικινδυνότητας. Η πρώτη προτεραιότητα θα πρέπει να δοθεί στα αντικείμενα με μη επιτρεπτά επίπεδα επικινδυνότητας. Αυτές οι αδυναμίες του συστήματος θα απαιτήσουν την άμεση διορθωτική δράση για να προστατέψουν τα συμφέροντα του οργανισμού.	Δράσεις που κυμαίνονται από Υψηλές έως Χαμηλές
Βήμα 2 – Αξιολόγηση των προτεινόμενων επιλογών ελέγχου	Αυτοί οι έλεγχοι συνιστώνται στην διαδικασία εκτίμησης επικινδυνότητας και μπορεί να μην είναι οι πιο κατάλληλες και εφαρμόσιμες επιλογές για έναν συγκεκριμένο οργανισμό και το πληροφοριακό του σύστημα. Κατά τη διάρκεια αυτού του βήματος, αναλύονται η καταλληλότητα και η αποτελεσματικότητα των	Λίστα των εφικτών ελέγχων

	συνιστώμενων επιλογών ελέγχων. Ο σκοπός είναι να συλλέξουμε τις πιο κατάλληλες επιλογές ελέγχου για την ελαχιστοποίηση του κινδύνου.	
Βήμα 3 – Διεξαγωγή ανάλυσης κέρδους – κόστους	Για να βοηθηθεί η διοίκηση στην λήψη αποφάσεων και να αναγνωρίσει τους ελέγχους cost-effective, διενεργείται μία ανάλυση κέρδους-κόστους.	Η ανάλυση κέρδους – κόστους περιγράφει το κόστος και τα οφέλη από την εφαρμογή ή την μη εφαρμογή των ελέγχων
Βήμα 4- Επιλογή Ελέγχου	Βάσει των αποτελεσμάτων της ανάλυσης κόστους –κέρδους, η διοίκηση καθορίζει τον πιο cost-effective έλεγχο για την μείωση του κινδύνου στην αποστολή του οργανισμού. Οι έλεγχοι που επιλέγονται θα πρέπει να συνδυάζουν τεχνικά, λειτουργικά, και διαχειριστικά στοιχεία ελέγχου για να διασφαλίσουν επαρκή ασφάλεια για το πληροφοριακό σύστημα και τον οργανισμό.	Οι επιλεγμένοι έλεγχοι
Βήμα 5 – Ανάθεση Ευθυνών	Αναγνωρίζονται τα κατάλληλα πρόσωπα τα οποία έχουν την κατάλληλη ειδίκευση και ικανότητες για να εφαρμόσουν τους επιλεγμένους ελέγχους, και η ευθύνη ανατίθεται.	Λίστα των υπεύθυνων προσώπων
Βήμα 6- Ανάπτυξη ενός ασφαλούς σχεδίου εφαρμογής	Κατά τη διάρκεια αυτού του βήματος, αναπτύσσεται ένα ασφαλές σχέδιο εφαρμογής. Το σχέδιο θα πρέπει, στο ελάχιστο, να περιέχει την ακόλουθη πληροφορία. • Κίνδυνοι και συσχετιζόμενα επίπεδα κινδύνου • Συνιστώμενοι έλεγχοι • Ιεραρχημένες δράσεις • Επιλεγμένα σχέδια ελέγχου • Απαιτούμενες πηγές για την εφαρμογή των επιλεγμένων σχεδίων ελέγχου • Λίστες των υπευθύνων ομάδων και προσωπικού • Ημερομηνία έναρξης της εφαρμογής • Μέρα ολοκλήρωσης της εφαρμογής • Απαιτήσεις συντήρησης	Σχέδιο εφαρμογής ασφαλείας

	Το σχέδιο εφαρμογής ασφαλείας δίνει προτεραιότητα στις δράσεις εφαρμογής και προγραμματίζει την έναρξη και την ημερομηνία ολοκλήρωσης. Αυτό το σχέδιο θα βοηθήσει την διαδικασία περιορισμού κινδύνου.	
Βήμα 7 – Εφαρμογή των Επιλεγμένων Ελέγχων	Βασιζόμενοι σε ξεχωριστές καταστάσεις, οι εφαρμοσμένοι έλεγχοι μπορεί να χαμηλώσουν το επίπεδο κινδύνου αλλά δεν εξαλείφουν τον κίνδυνο.	Υπολειπόμενος Κίνδυνος

1.4.1 Κατηγορίες Ελέγχου

Στην εφαρμογή των συνιστώμενων ελέγχων για τον περιορισμό του κινδύνου, ένας οργανισμός θα πρέπει να λάβει υπόψη τεχνικούς, διοικητικούς και λειτουργικούς ελέγχους ασφαλείας, ή έναν συνδυασμό τέτοιων ελέγχων, για να μεγιστοποιήσει την αποτελεσματικότητα των ελέγχων των πληροφοριακών συστημάτων και του οργανισμού. Οι έλεγχοι ασφαλείας, όταν χρησιμοποιούνται κατάλληλα, μπορούν να παρεμποδίσουν, να ελαττώσουν, ή να αποθαρρύνουν πηγές-απειλών από το να δημιουργήσουν ζημιά στην αποστολή ενός οργανισμού.

Η διαδικασία σύστασης των ελέγχων εμπεριέχει την επιλογή ανάμεσα σε ένα συνδυασμό τεχνικών, διοικητικών και λειτουργικών ελέγχων για την βελτίωση της ασφάλειας του οργανισμού. The trade offs τα οποία θα πρέπει να λάβει υπόψη ο οργανισμός are σκιαγραφούνται βλέποντας τις αποφάσεις που έχουν ληφθεί στη χρήση των πολύπλοκων κωδικών των χρηστών για να ελαχιστοποιήσουν την ανεύρεση των κωδικών. Σε αυτή την περίπτωση, ένας τεχνικός έλεγχος που απαιτεί επιπρόσθετη ασφάλεια του λογισμικού θα ήταν πιο πολύπλοκος και δαπανηρός από μία διαδικασία ελέγχου, αλλά οι τεχνικοί έλεγχοι είναι πιο πιθανόν να είναι πιο αποτελεσματικοί γιατί η υλοποίηση γίνεται αυτοματοποιημένα από το σύστημα. Από την άλλη πλευρά, ένας διαδικαστικός έλεγχος θα μπορούσε να εφαρμοστεί απλά μέσω υπομνήματος σε όλους τους ενδιαφερόμενους και μίας βελτίωσης των οδηγιών ασφαλείας για τον οργανισμό, αλλά το να διασφαλιστεί ότι οι χρήστες θα ακολουθούν συνεχώς το υπόμνημα και τις οδηγίες είναι δύσκολο και θα απαιτήσει εκπαίδευση αναγνώρισης της ασφάλειας και αποδοχή των χρηστών.

Οι τεχνικοί έλεγχοι ασφαλείας για τον περιορισμό του κινδύνου μπορούν να διαμορφωθούν για να παρέχουν προστασία ενάντια γνωστών απειλών. Αυτοί οι έλεγχοι μπορεί να κυμαίνονται από απλά έως σύνθετα μέτρα και συνήθως εμπεριέχουν αρχιτεκτονικές συστήματος, μηχανικές πειθαρχίες, και πακέτα ασφαλείας με έναν συνδυασμό hardware, software and firmware. Όλα αυτά τα μέτρα θα πρέπει να δουλέψουν μαζί για να ασφαλίσουν τα ευαίσθητα δεδομένα, την πληροφορία και τις λειτουργίες του πληροφοριακού συστήματος. Οι τεχνικοί έλεγχοι μπορούν να ομαδοποιηθούν στις παρακάτω κύριες κατηγορίες, σύμφωνα με τον πρωταρχικό σκοπό.

- Υποστήριξη – Υποστηρίζοντας τους ελέγχους είναι γενετικοί και υπογραμμίζουν τις περισσότερες από τις ικανότητες του συστήματος. Αυτοί οι έλεγχοι πρέπει να είναι σε θέση να ενσωματώσουν και άλλους ελέγχους.
- Προστασία – Οι προστατευτικοί έλεγχοι επικεντρώνονται στο να αποτρέψουν τα προβλήματα ασφαλείας.
- Εντοπισμός και Ανάρρωση – Αυτοί οι έλεγχοι επικεντρώνονται στο να εντοπίσουν και να ανακάμψουν από ένα ρήγμα ασφαλείας.

1.4.1.1 Υποστήριξη Τεχνικών Ελέγχων

Η υποστήριξη ελέγχων, από την φύση τους, είναι αλληλένδετοι με πολλούς άλλους ελέγχους. Οι υποστηρικτικοί έλεγχοι είναι οι ακόλουθοι.

- Ταυτοποίηση – Αυτός ο έλεγχος παρέχει την ικανότητα να αναγνωρίζει μοναδικά τους χρήστες, διαδικασίες και πηγές πληροφοριών. Για να εφαρμοστούν και άλλοι έλεγχοι ασφάλειας, είναι σημαντικό ότι τα αντικείμενα και τα υποκείμενα να είναι αναγνωρίσιμα.
- Διαχείριση κρυπτογραφικών κλειδιών - Πρέπει να διαχειρίζονται με ασφάλεια όταν εφαρμόζονται κρυπτογραφικές διαδικασίες. Η διαχείριση του κρυπτογραφικού κλειδιού περιλαμβάνει, των δημιουργία του κλειδιού, τη διανομή του, αποθήκευση και συντήρηση.
- Διαχείριση Ασφαλείας – Τα χαρακτηριστικά ασφαλείας ενός πληροφοριακού συστήματος πρέπει να διαμορφώνονται έτσι ώστε να καλύπτουν τις ανάγκες μιας συγκεκριμένης εγκατάστασης και να υπολογίζουν τις αλλαγές στο λειτουργικό περιβάλλον. Η ασφάλεια του συστήματος μπορεί να δομηθεί μέσα στην ασφάλεια του λειτουργικού συστήματος ή της εφαρμογής.
- Προστασία συστήματος – Υπογραμμίζοντας τις ικανότητες της ασφάλειας των λειτουργιών είναι η βάση για την αυτοπεποίθηση στην τεχνική εφαρμογή. Αυτό αναπαριστά την ποιότητα της εφαρμογής από την οπτική των διαδικασιών σχεδιασμού που χρησιμοποιούνται αλλά και με τον τρόπο με τον οποίο πραγματοποιείται η εφαρμογή.

1.4.1.2 Τεχνικοί έλεγχοι συντήρησης

Αυτοί οι έλεγχοι μπορούν να ανακόψουν προσπάθειες να παραβιαστούν οι πολιτικές ασφαλείας, περιλαμβάνοντας τις εξής παρακάτω

- Πιστοποίηση – Η πιστοποίηση ελέγχου παρέχει τα μέσα για την επαλήθευσης ταυτότητας, για να εξασφαλίσει ότι μία ταυτότητα είναι επικυρωμένη. Οι μηχανισμοί πιστοποίησης περιλαμβάνουν κωδικούς, προσωπικούς αριθμούς ταυτοποίησης, ή PINs, και ανερχόμενη τεχνολογία πιστοποίησης η οποία παρέχει ισχυρή πιστοποίηση.
- Εξουσιοδότηση – Οι έλεγχοι εξουσιοδότησης ενεργοποιούν την ειδίκευση και την μεταγενέστερη διαχείριση των επιτρεπόμενων ενεργειών για το σύστημα.
- Εφαρμογή Ελέγχου πρόσβασης – Η ακεραιότητα και η εμπιστευτικότητα εφαρμόζεται από τους ελέγχους πρόσβασης. Όταν ένας χρήστης κάνει αίτηση για πρόσβαση έχει εξουσιοδοτηθεί να έχει πρόσβαση σε συγκεκριμένες διαδικασίες, άρα είναι απαραίτητο να εφαρμόζεται η καθορισμένη πολιτική ασφαλείας. Αυτοί οι έλεγχοι, βασιζόμενοι στην πολιτική, εφαρμόζονται μέσω των μηχανισμών ελέγχου πρόσβασης και διανέμονται μέσα από το σύστημα. Η

αποτελεσματικότητα και η δυναμική των ελέγχων πρόσβασης βασίζεται στην σωστή των αποφάσεων για τους ελέγχους πρόσβασης.

- Μη άρνηση – Η αξιοπιστία του συστήματος βασίζεται στην ικανότητα του να διασφαλίσει ότι οι αποστολείς δεν μπορούν να αρνηθούν την αποστολή της πληροφορίας και ότι οι υποδοχείς δεν μπορούν να αρνηθούν να την λάβουν. Έχει τοποθετηθεί στην κατηγορία πρόληψης επειδή οι μηχανισμοί που εφαρμόζονται προλαμβάνουν την επιτυχημένη άρνηση μίας δράσης. Σαν αποτέλεσμα, αυτός ο έλεγχος τυπικά εφαρμόζεται στο σημείο της μετάδοσης ή της αποδοχής.
- Προστατευμένες Επικοινωνίες – Σε ένα κατανεμημένο σύστημα, η ικανότητα να επιτυγχάνει σκοπούς ασφάλειας εξαρτάται σε μεγάλο βαθμό από επικοινωνίες άξιες εμπιστοσύνης. Οι έλεγχοι προστατευμένων επικοινωνιών διασφαλίσουν την ακεραιότητα, την διαθεσιμότητα, και την εμπιστευτικότητα της ευαίσθητης πληροφορίας όσο βρίσκεται υπό μετάδοση. Οι προστατευμένες επικοινωνίες χρησιμοποιούν μεθόδους κρυπτογράφησης δεδομένων, και ανάπτυξης των κρυπτογραφικών τεχνολογιών για να ελαχιστοποιήσουν τις απειλές δικτύου όπως επανάληψη, υποκλοπή, απώλεια πακέτων, wiretapping, or eavesdropping.
- Transaction Privacy – Τα κυβερνητικά αλλά και τα συστήματα δημοσίου φορέα απαιτείται να συντηρούν την ασφάλεια των ιδιωτών. Οι έλεγχοι Transaction Privacy παρέχουν προστασία ενάντια στην απώλεια της ασφάλειας με σεβασμό στις διεξαγωγές που υλοποιούνται από τους ιδιώτες.

1.4.1.3 Τεχνικοί έλεγχοι εντοπισμού και επανόρθωσης

Οι έλεγχοι εντοπισμού προειδοποιούν για παραβιάσεις ή προσπάθειες παραβιάσεων της πολιτικής ασφαλείας και περιλαμβάνουν τέτοιους ελέγχους όπως audit trails, intrusion detection methods, and checksums. Οι έλεγχοι επανόρθωσης μπορούν να χρησιμοποιηθούν για να επαναφέρουν χαμένες πληροφοριακές πηγές. Χρειάζονται σαν συμπλήρωμα στα υποστηρικτικά και συντηρητικά τεχνικά μέτρα, γιατί κανένα από τα μέτρα σε αυτές τις περιοχές δεν είναι τέλειο.

1.4.1.4 Έλεγχοι Διαχείρισης Ασφαλείας

Οι Έλεγχοι Διαχείρισης Ασφαλείας, σε συνδυασμό με τους τεχνικούς και τους λειτουργικούς ελέγχους, εφαρμόζονται για να διαχειριστούν και να ελαττώσουν τον κίνδυνο απώλειας και για να προστατέψουν την αποστολή ενός οργανισμού. Οι έλεγχοι διαχείρισης επικεντρώνονται στην πολιτική προστασίας της πληροφορίας, τις οδηγήτριες γραμμές, και στα standards, τα οποία διεκπεραιώνονται μέσω λειτουργικών διαδικασιών για να εκπληρώσουν τους στόχους του οργανισμού. Οι Έλεγχοι Διαχείρισης Ασφαλείας κατηγοριοποιούνται στους προληπτικούς, εντοπιστικούς, και επανορθωτικούς

1.4.1.5 Λειτουργικοί Έλεγχοι Ασφαλείας

Τα στάνταρντ ασφαλείας ενός οργανισμού θα πρέπει να εδραιώνουν μία ομάδα ελέγχων και καθοδηγητικών γραμμών ώστε να διασφαλίσουν ότι οι διαδικασίες ασφαλείας είναι κατάλληλα ενισχυμένες and εφαρμοσμένες σε εναρμόνιση με τους σκοπούς και την αποστολή του οργανισμού. Η διαχείριση παίζει ζωτικό ρόλο στην εφαρμογή της πολιτικής και στην διασφάλιση την εδραίωσης των κατάλληλων λειτουργικών ελέγχων.

Οι λειτουργικοί έλεγχοι, που εφαρμόζονται σε αρμονία με τις απαιτήσεις και τις καλές βιομηχανικές πρακτικές, χρησιμοποιούνται για να διορθώσουν λειτουργικές ανεπάρκειες

που θα μπορούσαν να εκμεταλλευτούν πιθανές πηγές-απειλών. Για να διασφαλίσουμε την συνοχή και την ομοιομορφία στις λειτουργίες ασφαλείας, οι βήμα προς βήμα διαδικασίες και οι μέθοδοι για την εφαρμογή των λειτουργικών ελέγχων θα πρέπει να είναι καθαρά καθορισμένοι, καταγεγραμμένοι, και συντηρημένοι.

1.4.1.6 Προληπτικοί Λειτουργικοί Έλεγχοι

Οι προληπτικοί λειτουργικοί έλεγχοι ασφαλείας είναι οι ακόλουθοι:

- Έλεγχος πρόσβασης δεδομένων
- Περιορισμός της εξερχόμενης διανομής πληροφοριών
- Έλεγχος ιών λογισμικού
- Φύλαξη της πληροφοριακής εγκατάστασης
- Ασφάλεια καλωδιώσεων
- Παροχή ικανότητας back up
- Εδραίωση off-site διαδικασιών αποθήκευσης και ασφάλειας
- Προστασία των laptops, των προσωπικών υπολογιστών και των σταθμών εργασίας
- Προστασία των πληροφοριακών αγαθών από ζημιά που μπορεί να προκληθεί από ζημιά
- Παροχή πηγής ενέργειας έκτακτης ανάγκης
- Έλεγχος υγρασίας και της θερμοκρασίας την πληροφορικής εγκατάστασης

1.4.1.7 Λειτουργικοί έλεγχοι εντοπισμού

Οι λειτουργικοί έλεγχοι εντοπισμού εμπεριέχουν τα ακόλουθα

- Παρέχουν φυσική ασφάλεια
- Εξασφαλίζουν την περιβαλλοντική ασφάλεια

1.4.2 Ανάλυση κέρδους - κόστους

Οι οργανισμοί, προκειμένου να κατανεμηθούν οι πηγές και να εφαρμοστούν cost-effective έλεγχοι, αφότου αναγνωρίσουν όλους τους πιθανούς ελέγχους και αξιολογήσουν την εφαρμογή και την αποτελεσματικότητα, θα πρέπει να διεξάγουν μία ανάλυση κόστους – οφέλους για κάθε προτεινόμενο έλεγχο για να καθορίσει ποιοι έλεγχοι απαιτούνται και είναι κατάλληλοι για την κάθε περίσταση.

Η ανάλυση κόστους – κέρδους μπορεί να είναι ποσοτική ή ποιοτική. Ο σκοπός της είναι να επιδείξει ότι το κόστος των εφαρμοσμένων ελέγχων μπορεί να δικαιολογηθεί από την μείωση στο επίπεδο του κινδύνου.

Μία ανάλυση κέρδους – κόστους για τους προτεινόμενους νέους ελέγχους ή τους ήδη ανεπτυγμένους ελέγχους συνίσταται τα ακόλουθα

- Καθορίζει τον αντίκτυπο της εφαρμογής νέων ελέγχων

- Καθορίζει τον αντίκτυπο της μη εφαρμογής νέων ελέγχων
- Υπολογίζει το κόστος της εφαρμογής
- Εκτιμώντας το κόστος και το κέρδος από την εφαρμογή απέναντι στο σύστημα και τα δεδομένα για να καθορίσουν την σπουδαιότητα εφαρμογής αυτών των νέων ελέγχων στον οργανισμό, δίνοντας το κόστος τους και τον σχετικό αντίκτυπο.

Ο οργανισμός θα χρειαστεί να εκτιμήσει τα οφέλη των ελέγχων με σκοπό να συντηρήσει μία αποδεχτή δομή αποστολής για τον οργανισμό. Συσχετίζοντας το αποτέλεσμα του να μην εφαρμόζουμε τον έλεγχο στην αποστολή, οι οργανισμοί μπορούν να καθορίσουν εάν είναι απαραίτητο να προχωρήσουν στην εφαρμογή του.

1.5 ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΕΚΤΙΜΗΣΗ

Στους περισσότερους οργανισμούς, το δίκτυο θα εξαπλώνεται και θα αναβαθμίζεται συνεχώς, τα συστατικά του θα αλλάζουν και οι εφαρμογές του λογισμικού του θα αντικαθίστανται ή θα αναβαθμίζονται με νεώτερες εκδόσεις. Επιπλέον, θα πραγματοποιηθούν αλλαγές στο προσωπικό και είναι πιθανό να αλλάξουν και οι πολιτικές ασφαλείας, σε βάθος χρόνου. Αυτές οι αλλαγές σημαίνουν ότι θα έρθουν στην επιφάνεια νέοι κίνδυνοι και οι κίνδυνοι που είχαν στο παρελθόν αντιμετωπιστεί, μπορεί ξανά να επανεμφανιστούν. Έτσι λοιπόν, η διαδικασία εκτίμησης επικινδυνότητας είναι συνεχής και εξελισσόμενη.

Η διαδικασία εκτίμησης επικινδυνότητας συνήθως επαναλαμβάνεται τουλάχιστον κάθε 3 χρόνια. Όμως η εκτίμηση επικινδυνότητας θα έπρεπε να διενεργείται και ενσωματώνεται στα πληροφοριακά συστήματα, όχι επειδή απαιτείται από το νόμο ή τη νομοθεσία, αλλά επειδή είναι μία καλή εξάσκηση και υποστηρίζει τους επιχειρηματικούς στόχους της επιχείρησης. Θα έπρεπε να υπάρχει ένα συγκεκριμένο πρόγραμμα για την εκτίμηση και τον περιορισμό των κινδύνων, αλλά η περιοδικώς εφαρμοσμένη διαδικασία θα πρέπει επίσης να έχει την εμβέλεια να επιτρέπει αλλαγές όπου χρειάζεται, όπως σημαντικές αλλαγές στο πληροφοριακό σύστημα και στο διαδικαστικό περιβάλλον εξαιτίας αλλαγών που προκύπτουν από πολιτικές και νέες τεχνολογίες.

Σε γενικές γραμμές, ένα επιτυχημένο πρόγραμμα διαχείρισης κινδύνου βασίζεται στην στους παρακάτω παράγοντες:

- Την δέσμευση του senior management
- Την πλήρη υποστήριξη και συμμετοχή της πληροφοριακής ομάδας
- Την ικανότητα της ομάδας διαχείρισης κινδύνου, η οποία θα πρέπει να έχει ειδικευτεί για να εφαρμόσει την μεθοδολογία διαχείρισης κινδύνου σε ένα συγκεκριμένο σύστημα, να αναγνωρίσει τους κινδύνους της αποστολής, και να παρέχει cost-effective ασφάλειες που καλύπτουν τις ανάγκες του οργανισμού
- Την επίγνωση και την συνεργασία των μελών της κοινωνίας των χρηστών, οι οποίοι θα πρέπει να ακολουθούν τις διαδικασίες και να συμμορφώνονται με τους εφαρμοσμένους ελέγχους ώστε να ασφαλίσουν την αποστολή του οργανισμού
- Μία συνεχή αξιολόγηση και εκτίμηση των κινδύνων που σχετίζονται με το πληροφοριακό σύστημα

ΚΕΦΑΛΑΙΟ 2
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

2.1 ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

Η πολιτική ασφάλειας αναπτύσσεται και καθορίζεται βασιζόμενη σε προκαθορισμένους κανόνες και μεθοδολογίες σε συνάρτηση με την εκάστοτε περίπτωση που έχουμε να αντιμετωπίσουμε. Εφαρμόζοντας το πρότυπο ISO-27002 στον σχεδιασμό της πολιτικής επιτυγχάνουμε την εξασφάλιση της απαιτούμενης ασφάλειας. Το πρότυπο αυτό μπορεί να εφαρμοστεί σε όλες τις επιχειρήσεις ανεξαρτήτως μεγέθους και εντάσσονται στο πλαίσιο ανάπτυξης και διοίκησης ενός αποτελεσματικού συστήματος ασφάλειας πληροφοριών.

Οι βασικές αρχές που χαρακτηρίζουν το πρότυπο ISO-27002 είναι ότι θεωρεί τις πληροφορίες ως σημαντικό περιουσιακό στοιχείο, καλύπτοντας όλες τις δυνατές μορφές τους. Με τη πλήρη συμμόρφωση της πολιτικής στις απαιτήσεις του προτύπου, στοχεύουμε στην εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας, και της διαθεσιμότητας.

Προκειμένου να αναπτύξουμε μία πολιτική η οποία θα είναι πλήρης και ολοκληρωμένη, θα πρέπει να ακολουθήσουμε κάποια προκαθορισμένα στάδια τα οποία εμπεριέχονται στο πρότυπο που εφαρμόζουμε. Το αρχικό στάδιο απαιτεί το διάλογο και τη συζήτηση με την επιχείρηση, και πιο συγκεκριμένα, με την διοίκηση της προκειμένου να καθοριστεί ο γενικός στόχος της πολιτικής ασφάλειας. Κρίσιμο ζήτημα είναι να υπάρξει η δέσμευση της διοίκησης για διάθεση των απαιτούμενων πόρων, υποστήριξη, αλλά και αλλαγή ή προσαρμογή της νοοτροπίας και φιλοσοφίας εργασίας ώστε να συμβάλλει δυναμικά στην τήρηση των νέων προδιαγραφών. Επίσης είναι αναγκαίο να προσδιοριστεί η έκταση εφαρμογής της πολιτικής, καθώς είναι απαραίτητο να καθοριστούν τα τμήματα ή οι δραστηριότητες στις οποίες θα γίνει η εφαρμογή, καθώς και να εξεταστούν οι διασυνδέσεις/ αλληλεπιδράσεις με άλλα συστήματα. Μέσω αυτών των διεργασιών η εταιρεία ουσιαστικά στοχεύει στην προστασία των κεφαλαίων της, την προστασία της παραγωγικής διαδικασίας, τη διαφύλαξη των εταιρικών και μη πληροφοριών και τέλος τη προστασία των πελατών και των συνεργατών με τον καλύτερο δυνατό τρόπο.

Το επόμενο βήμα μας περιλαμβάνει τον καθορισμό των πολιτικών που θα ακολουθηθούν, δηλαδή αν θα υπάρχει μία γενικευμένη πολιτική ή θα σχεδιαστούν υπο-πολιτικές οι οποίες θα είναι εξειδικευμένες σε ένα τομέα, και όλες μαζί με την ιεραρχία που θα οριστεί θα περιλαμβάνονται στην βασική πολιτική. Είναι αυτονόητο λοιπόν ότι για να προχωρήσουμε στον σχεδιασμό της πολιτικής θα πρέπει αρχικά να προσδιορίσουμε τα περιουσιακά στοιχεία της εταιρείας (assets), την αξία ή τη χρησιμότητα τους, την οικονομική τους αξία και τα οφέλη τους. Τα στοιχεία που εντάσσονται στα πλαίσια του σχεδιασμού της πολιτικής μπορεί να είναι πληροφορίες, hardware, software, δίκτυα, τηλεπικοινωνίες, συστήματα επεξεργασίας και αποθήκευσης, επιχειρησιακές διαδικασίες, brand names, πνευματική περιουσία, εικόνα, φήμη και προσωπικό.

Για κάθε ένα από τα παραπάνω στοιχεία στα οποία η εταιρεία θα αποφασίσει να εφαρμόσει την πολιτική ασφάλειας, θα πρέπει να υλοποιηθεί διεξοδικός έλεγχος για να καθοριστούν τα σημεία στα οποία εντοπίζονται οι αδυναμίες και χρήζουν βελτίωσης ή απαιτούν προσαρμογή στα νέα δεδομένα. Θα πρέπει να γίνει προσδιορισμός των

κινδύνων που ενέχουν, και έπειτα να αξιολογηθούν, να υπολογισθεί η πιθανότητα εμφάνισης τους και οι επιπτώσεις τους. Η πολιτική ασφάλειας που θα σχεδιαστεί θα περιλαμβάνει όλα αυτά τα στοιχεία, σε αυτοτελής ‘‘υπο-πολιτικές’’ έτσι ώστε να είναι εφικτή η εξειδίκευση σε κάθε θέμα αλλά και παράλληλα να είναι πιο ευέλικτες ως προς μελλοντικές αλλαγές και προσθήκες.

2.2 ΟΡΓΑΝΩΤΙΚΗ ΑΣΦΑΛΕΙΑ

Η οργανωτική ασφάλεια έχει ως σκοπό να διαχειριστεί την ασφάλεια πληροφοριών μέσα στον οργανισμό. Προαπαιτείται να εδραιωθεί ένα διοικητικό δίκτυο ώστε πρώτα να αρχικοποιήσει και στη συνέχεια να ελέγχει την εφαρμογή των πολιτικών ασφαλείας μέσα στον οργανισμό. Η διοίκηση θα πρέπει να εγκρίνει την πολιτική ασφαλείας και να αναθέσει τους ρόλους ασφαλείας στο προσωπικό. Η ασφάλεια των πληροφοριών ενός οργανισμού είναι ένα θέμα που αφορά όλους τους υπαλλήλους του, οπότε είναι σαφές ότι όλοι οι υπάλληλοι θα πρέπει να είναι ενήμεροι για την πολιτική ασφάλειας που ακολουθείται και θα πρέπει να την εφαρμόζουν με προσοχή.
Όπως προαναφέραμε, η διοίκηση θα πρέπει να υποστηρίζει ενεργά την ασφάλεια μέσα στον οργανισμό μέσω της παροχής σωστής καθοδήγησης, της δέσμευσης, της εξειδικευμένης ανάθεσης αρμοδιοτήτων, και της αναγνώριση των ευθυνών που απαιτεί η ασφάλεια πληροφοριών.
Η διοίκηση θα πρέπει:

- να διασφαλίσει ότι αναγνωρίζονται οι στόχοι της ασφαλείας πληροφοριών, να καλύπτει τις απαιτήσεις του οργανισμού, και να τις εντάσσει σε διάφορες διαδικασίες
- να αναμορφώσει, να ανασκοπήσει, και να αποδεχτεί την πολιτική ασφάλειας πληροφοριών
- να ανασκοπήσει την αποτελεσματικότητα της εφαρμογής της πολιτικής ασφαλείας
- να παρέχει καθαρή καθοδήγηση και ορατή διοικητική υποστήριξη για πρωτοβουλίες ασφαλείας
- να αποδεχτεί την ανάθεση ειδικευμένων ρόλων και υπευθυνοτήτων για την ασφάλεια πληροφοριών μέσα στον οργανισμό
- να αρχικοποιήσει τα σχέδια και τα προγράμματα που συντηρούν την επίγνωση της ασφάλειας πληροφοριών
- να διασφαλίσει ότι η εφαρμογή των ελέγχων ασφαλείας πληροφοριών είναι συντονισμένη μέσα στον οργανισμό

2.3 ΠΟΛΙΤΙΚΗ ΑΠΟΔΕΚΤΗΣ ΧΡΗΣΗΣ

Σκοπός

Ο σκοπός της Πολιτικής Αποδεκτής Χρήσης (acceptable or appropriate use policy) είναι να περιγράψει τον αποδεκτό τρόπο χρήσης του εξοπλισμού (υπολογιστικών και τηλεπικοινωνιακών συστημάτων) ενός οργανισμού.

Αυτοί οι κανόνες υπάρχουν για να προστατεύσουν τον εργαζόμενο αλλά και τον οργανισμό. Ανάρμοστη χρήση θέτουν σε κίνδυνο τον οργανισμό είτε μέσω της δημιουργίας αδυναμιών στην υποδομή οι οποίες θα ήταν δυνατό να γίνουν αντικείμενο επιθέσεων είτε μέσω ενεργειών οι οποίες παραβιάζουν τις νομικές υποχρεώσεις και εκθέτουν τον οργανισμό.

Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται σε κάθε χρήστη του δικτύου δεδομένων του οργανισμού (φοιτητές, ερευνητές, μόνιμο προσωπικό, συμβασιούχοι, εξωτερικοί συνεργάτες, σύμβουλοι, προσωπικό που σχετίζονται με τρίτους). Όσον αφορά τον εξοπλισμό, η πολιτική εφαρμόζεται σε όλο τον εξοπλισμό που κατέχει ή έχει ενοικιάσει ο οργανισμός.

Ο οργανισμός στα πλαίσια της καλής λειτουργίας του δικτύου δεδομένων υποχρεούται να δίνει πρόσβαση στο δίκτυο στους χρήστες κατόπιν αποδοχής της πολιτικής αποδεκτής χρήσης και να λαμβάνει μέτρα στο μέτρο του δυνατού για την ασφάλεια των συστημάτων που διαχειρίζεται και μέτρα για την διασφάλιση του απόρρητου των τηλεπικοινωνιών μέσα στα όρια του δικτύου του. Επίσης, υποχρεούται να τηρεί τις αρχές προστασίας δεδομένων προσωπικού χαρακτήρα σύμφωνα με την ισχύουσα νομοθεσία και τις διαδικασίες που προβλέπονται από την πολιτική ασφάλειας του δικτύου.

Πολιτική

- **Γενική Χρήση Και Ιδιοκτησία**

Οι χρήστες δικαιούνται πρόσβαση στην υποδομή και στις ηλεκτρονικές υπηρεσίες του οργανισμού για σκοπούς που συνάδουν με τον ακαδημαϊκό – ερευνητικό χαρακτήρα του ιδρύματος πάντα τηρουμένης της κείμενης νομοθεσίας και των κανονισμών λειτουργίας του οργανισμού.
Ο οργανισμός επιθυμεί να παρέχει ένα ικανοποιητικό επίπεδο όσο αφορά την εμπιστευτικότητα των επικοινωνιών και την προστασία των προσωπικών δεδομένων. Οι χρήστες θα πρέπει να είναι ενήμεροι ότι δεδομένα που δημιουργούνται στα συστήματα του οργανισμού παραμένουν και στην ιδιοκτησία του.
Εξαιτίας της ανάγκης για ασφαλή διαχείριση του δικτύου του η διεύθυνση δεν μπορεί να εγγυηθεί την εμπιστευτικότητα των πληροφοριών που αποθηκεύονται στην υποδομή του οργανισμού. Για την ασφάλεια και την συντήρηση του δικτύου προσωπικό του οργανισμού(συγκεκριμένα από την ομάδα IT) μπορεί να παρακολουθεί τους σταθμούς εργασίας, τον λοιπό εξοπλισμό και την κίνηση του δικτύου ανά πάσα στιγμή. Γενικότερα, η υπεύθυνη ομάδα έχει το δικαίωμα να ελέγχει τα συστήματα και το δίκτυο περιοδικά προκειμένου να διασφαλίζεται η συμμόρφωση με το παρών κείμενο.

- **Αποδεκτή Χρήση**

Οι κωδικοί πρόσβασης (passwords, private keys, κλπ) είναι αυστηρά προσωπικοί και θα πρέπει να φυλάσσονται με ασφαλή τρόπο. Οι λογαριασμοί χρηστών δεν θα πρέπει να μοιράζονται. Οι εξουσιοδοτημένοι χρήστες είναι υπεύθυνοι για την ασφάλεια των κωδικών τους και των λογαριασμών τους. Οι κωδικοί που αφορούν συστήματα θα πρέπει να αλλάζουν κάθε Χ μήνες και κωδικοί των χρηστών κάθε Υ μήνες.
Οι χρήστες δεσμεύονται να αποκτούν πρόσβαση αποκλειστικά σε δεδομένα που αναφέρονται στους ίδιους ή είναι δημοσίως ανακοινώσιμα και να κάνουν λελογισμένη χρήση των υπολογιστικών και δικτυακών πόρων του δικτύου.
Όλοι οι υπολογιστές θα πρέπει να κλειδώνουν αυτόματα μετά από 10 λεπτά μη χρήσης.
Όλοι οι υπολογιστές που συνδέονται στο δίκτυο του οργανισμού, είτε ανήκουν στο οργανισμού είτε όχι, θα πρέπει να ελέγχονται τακτικά για ιούς σύμφωνα με τη Πολιτική Ασφάλειας Για Το Anti-Virus καθώς και να υπάρχει συμμόρφωση με τους κανόνες που περιγράφονται σε αυτήν την πολιτική.
Συστήνεται κάθε πληροφορία που οι χρήστες κρίνουν ευαίσθητη ή ευάλωτη να είναι κρυπτογραφημένη σύμφωνα με την Πολιτική Ασφάλειας Για Την Κωδικοποίηση. Για οδηγίες σχετικά με την εμπιστευτικότητα των πληροφοριών συμβουλευτείτε τη Πολιτική Ασφάλειας Για Την Ευαισθησία Των Πληροφοριών.
Θα πρέπει να δοθεί ιδιαίτερη προσοχή στην προστασία των πληροφοριών που περιέχονται σε φορητούς υπολογιστές οι οποίοι είναι περισσότερο ευάλωτοι. Για οδηγίες σχετικά με την εμπιστευτικότητα των πληροφοριών σε φορητούς υπολογιστές συμβουλευτείτε τη Πολιτική Ασφάλειας Για Την Προστασία Δεδομένων σε φορητούς Υπολογιστές / 'Άλλες Συσκευές..
Οι χρήστες θα πρέπει να ενημερώνουν αμέσως τους υπεύθυνους του εκάστοτε συστήματος αν υποπέσει στην αντίληψη τους οποιοδήποτε κενό ασφάλειας.

- **Μη Αποδεκτή Χρήση**

Στο παρών τμήμα περιγράφονται λειτουργίες οι οποίες είναι γενικά απαγορευμένες. Οι εργαζόμενοι μπορεί να απαλλαχθούν από τους περιορισμούς αυτούς προκειμένου να ικανοποιήσουν τους σκοπούς μίας εργασίας που τους έχει ανατεθεί στα πλαίσια των καθηκόντων τους. Σε καμία περίπτωση και για κανέναν λόγο ένας εργαζόμενος δεν έχει την άδεια να προβεί σε παράνομες πράξεις.

Οι εργαζόμενοι είναι υπεύθυνοι για να κρίνουν ποιά χρήση θεωρείται λογική. Αν υπάρχει κάποια αβεβαιότητα σε σχέση με τον τρόπο χρήσης τότε οι εργαζόμενοι θα πρέπει να συμβουλευτούν τον προϊστάμενο τους. Γενικότερα, θα πρέπει να τηρούν τους γραπτούς και άγραφους κανόνες της καλής δικτυακής συμπεριφοράς (π.χ. Netiquette RFC 1855).

Η παρακάτω λίστα δεν είναι εξαντλητική αλλά παρέχει ένα πλαίσιο ενεργειών που θεωρούνται μη αποδεκτές.

Δραστηριότητες Συστήματος

- Παραβίαση των πνευματικών δικαιωμάτων κάθε ιδιώτη ή εταιρίας τα οποία προστατεύονται από copyright, εμπορικό απόρρητο, πατέντες, νόμους και κανονισμούς.

- Μη εξουσιοδοτημένη αντιγραφή προστατευόμενου από copyright υλικού όπως φωτογραφίες, βιβλία, προγράμματα-κώδικες, λογισμικό, τεχνικές πληροφορίες. Σε περίπτωση που είναι αναγκαία η εξαγωγή θα πρέπει να συμβουλευτούμε τον κατάλληλο διαχειριστή πρώτα.

- Αποκάλυψη των κωδικών πρόσβασης σε τρίτους ή χρήση του προσωπικού λογαριασμού από άλλους.

- Παράκαμψη της ταυτοποίησης του χρήστη ή οποιασδήποτε διαδικασίας ασφάλειας για κάθε υπολογιστή ή λογαριασμό.

- Εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο και τους υπολογιστές του ΙΠ (πχ ιοί ή άλλα βλαβερά προγράμματα – malware)

- Ενέργειες όπως το port-scanning, network monitoring απαγορεύονται αυστηρά, εκτός και αν περιλαμβάνονται στα καθήκοντα του εργαζόμενου και έχει προηγουμένως ειδοποιηθεί η ομάδα IT η άδεια της οποίας απαιτείται.

- Οποιαδήποτε κακόβουλη ενέργεια προς υπολογιστές άλλους από αυτούς του χρήστη, όπως άρνησης παροχής υπηρεσιών (DoS attacks), terminating user sessions.

- Διαφήμιση απατηλών προσφορών μέσω του Internet, χρησιμοποιώντας την υποδομή του ΙΠ.

- ‘Ασκηση εμπορικών δραστηριοτήτων μέσω του δικτύου δεδομένων του ΙΠ όπως η πώληση αγαθών ή υπηρεσιών, η υπεκμίσθωση χωρητικότητας

Δραστηριότητες Επικοινωνίας Και Αλληλογραφίας

- Απαγορεύεται η αποστολή οποιονδήποτε e-mails εκτός των προσωπικών και αυτών που είναι απαραίτητα για την διεκπεραίωση των καθηκόντων του εργαζόμενου.

- Οποιαδήποτε ενόχληση μέσω του περιεχόμενου, του μεγέθους ή της συχνότητας των e-mails απαγορεύεται αυστηρά (πχ αποστολή μαζικού ηλεκτρονικού ταχυδρομείου – Spam)

- Η αποστολή fake-mails δεν επιτρέπεται.

- Απαγορεύεται η προώθηση οποιουδήποτε e-mail του τύπου "chain letter".

Επιβολή

Ο οργανισμός παρέχει πρόσβαση σε συστήματα και υπηρεσίες μόνο στους χρήστες που αποδέχονται την πολιτική ασφάλειας και την πολιτική αποδεκτής χρήσης του δικτύου δεδομένων.

Εργαζόμενοι που παραβιάζουν αυτήν την πολιτική, υπόκεινται σε πειθαρχικό έλεγχο ο οποίος είναι δυνατό να έχει σαν αποτέλεσμα μέχρι και τον τερματισμό της σύμβασης εργασίας.

Σε περίπτωση διαπίστωσης παραβίασης κάποιας από τις υποχρεώσεις χρηστών, ο οργανισμός έχει δικαίωμα όταν κρίνεται απαραίτητο, ακόμη και χωρίς προειδοποίηση λόγω διαχειριστικών αναγκών:

να αναστείλει τη σύνδεση του χρήστη στο δίκτυο δεδομένων ή τη πρόσβαση του σε συγκεκριμένες υπηρεσίες.

να προβεί σε ενέργειες για την άρση του απορρήτου των επικοινωνιών σύμφωνα με τις ισχύουσες νομοθετικές διατάξεις.

2.4 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΗΝ ΕΥΑΙΣΘΗΣΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Σκοπός

Η πολιτική για την ευαισθησία των πληροφοριών σκοπεύει στο να βοηθήσει και να καθοδηγήσει σωστά τους εργαζόμενους ώστε να κρίνουν ποίες πληροφορίες μπορούν να αποκαλυφθούν σε άλλους εκτός των υπαλλήλων ενός οργανισμού καθώς επίσης και την σχετική ευαισθησία των πληροφοριών που δεν θα έπρεπε να αποκαλυφθούν σε τρίτους χωρίς ειδική άδεια. Η καθοδήγηση αυτή είναι δυνατό να επιτευχθεί μέσω της ταξινόμησης των πληροφοριών η οποία διασφαλίσει ότι η πληροφορία λαμβάνει ένα κατάλληλο επίπεδο προστασίας. Η πληροφορία θα πρέπει να ταξινομείται προκειμένου να υποδεικνύει την ανάγκη, τις προτεραιότητες, και τον αναμενόμενο βαθμό προστασίας κατά την χρησιμοποίηση της. Η πληροφορία έχει ποικίλους βαθμούς ευαισθησίας και κρισιμότητας, άρα ενδεχομένως κάποια αντικείμενα μπορεί να απαιτούν ένα επιπρόσθετο επίπεδο προστασίας ή ειδική μεταχείριση. Ένα σχέδιο ταξινόμησης της πληροφορίας θα πρέπει να χρησιμοποιηθεί προκειμένου να καθορίσει το κατάλληλο επίπεδο προστασίας και την ανάγκη για ειδικά μέτρα διαχείρισης.

Παράλληλα, η πολιτική αυτή παρέχει διοικητική κατεύθυνση και υποστήριξη για την ασφάλεια των πληροφοριών σε συσχετισμό με τις επιχειρηματικές απαιτήσεις και τους σχετικούς νόμους και κανονισμούς. Η διοίκηση θα πρέπει να καθορίσει μία καθαρή κατεύθυνση πολιτικής σε συνδυασμό με τους επιχειρηματικούς στόχους και να παρέχει υποστήριξη, και αφοσίωση στην ασφάλεια πληροφοριών.

Ένα έγγραφο πολιτικής ασφάλειας πληροφοριών θα πρέπει να είναι αποδεκτό από την διοίκηση, να εκδοθεί και να είναι διαθέσιμο σε όλους τους εργαζομένους και τους εξωτερικούς συνεργάτες. Οι πληροφορίες για τις οποίες αναφερόμαστε στο παρών κείμενο περιλαμβάνουν, χωρίς να περιορίζονται μόνο σε αυτές, πληροφορίες που είναι αποθηκευμένες σε οποιοδήποτε μέσω αποθήκευσης, όπως ηλεκτρονικές πληροφορίες, πληροφορίες σε χαρτί, και πληροφορίες που μπορούμε να πάρουμε ακουστικά ή οπτικά.

Πεδίο Εφαρμογής

Οι πληροφορίες ενός οργανισμού διακρίνονται σε δυο κατηγορίες:

- Δημόσιες πληροφορίες

Δημόσιες πληροφορίες ενός οργανισμού θεωρούνται όσες έχουν οριστεί έτσι από τον αρμόδιο με το δικαίωμα να κατηγοριοποιεί τις πληροφορίες και μπορούν ελεύθερα να δοθούν σε οποιονδήποτε χωρίς να διακινδυνεύεται η θέση, η ακεραιότητα και τα συμφέροντα του οργανισμού.

- Εμπιστευτικές πληροφορίες

Εμπιστευτικές πληροφορίες ενός οργανισμού θεωρούνται όλες οι άλλες πληροφορίες. Είναι σημαντικό να γίνει σαφές ότι μερικές πληροφορίες είναι πιο σημαντικές και θα πρέπει να προστατευθούν με περισσότερη προσοχή από τις υπόλοιπες. Τέτοιες μπορεί να

είναι εμπορικά μυστικά, προγράμματα υπό ανάπτυξη, πιθανοί μελλοντικοί στόχοι και άλλες πληροφορίες που σχετίζονται με την επιτυχή πορεία της εταιρίας. Πληροφορίες όπως τηλεφωνικοί κατάλογοι του οργανισμού ή προσωπικά στοιχεία εργαζομένων και πελατών της είναι εξίσου σημαντικές αλλά δεν χρήζουν τόσο αυστηρής προστασίας.

Ένα υποσύνολο των εμπιστευτικών πληροφοριών είναι οι εμπιστευτικές πληροφορίες τρίτων. Τέτοιες πληροφορίες είναι αυτές που ανήκουν σε τρίτους και τις οποίες έχουν εμπιστευτεί στον οργανισμό μέσω μια συμφωνίας ή ενός συμβολαίου. Αυτές οι πληροφορίες μπορεί να προκύψουν από μια από κοινού ανάπτυξη ενός προγράμματος, από παραγγελίες πελατών κ.α. Τέτοιου είδους πληροφορίες θεωρούνται ως εξαιρετικά ευαίσθητες.

Είναι στην κρίση του προσωπικού ενός οργανισμού να ορίσει την ευαισθησία των πληροφοριών, πάντα με γνώμονα την κοινή λογική και την πολιτική ασφαλείας που ακολουθεί ο οργανισμός. Ωστόσο σε περιπτώσεις αμφιβολίας κρίνεται απαραίτητη η παρέμβαση κάποιου αρμόδιου, ανώτερου διοικητικού στελέχους προκειμένου να διασφαλιστεί η σωστή διαχείριση των πληροφοριών.

Πολιτική

Η πληροφορία θα πρέπει να ταξινομείται ανάλογα με την αξία της, τις νομικές απαιτήσεις, και την κρισιμότητα της στον οργανισμό. Οι ταξινομήσεις που σχετίζονται με τους ελέγχους προστασίας της πληροφορίας θα πρέπει να λαμβάνουν υπόψη τις επιχειρηματικές ανάγκες για διαμοιρασμό ή περιορισμό των πληροφοριών και τους επιχειρηματικούς αντίκτυπους που σχετίζονται με τέτοιου είδους ανάγκες.

Παρακάτω, ακολουθούν αναλυτικές οδηγίες ταξινόμησης για την ευαισθησία των πληροφοριών, παρέχοντας λεπτομέρειες για τον τρόπο χειρισμού των πληροφοριών διαφορετικής ευαισθησίας. Αυτές οι οδηγίες μπορούν να χρησιμοποιηθούν ως πρότυπο και να εφαρμοστούν για κάθε ειδική περίπτωση ανάλογα με τις συγκεκριμένες καταστάσεις και την φύση των προς κατηγοριοποίηση πληροφοριών. Ωστόσο, οι οδηγίες ταξινόμησης θα πρέπει να περιλαμβάνουν συμβάσεις για αρχική ταξινόμηση και ταξινόμηση στο βάθος χρόνου – σε συσχετισμό με κάποια προκαθορισμένη πολιτική ελέγχου πρόσβασης. Για να διασφαλιστεί ότι οι πληροφορίες είναι κατάλληλα ταξινομημένες, θα πρέπει να υλοποιείται περιοδικά μία ανασκόπηση του επιπέδου προστασίας των πληροφοριών, και σε περίπτωση που απαιτείται κάποια ενημέρωση ή αλλαγή, η πληροφορία να ταξινομείται σε κάποιο άλλο επίπεδο.

Το επίπεδο της προστασίας μπορεί να εκτιμηθεί από την ανάλυση της εμπιστευτικότητας, της ακεραιότητας, και της διαθεσιμότητας και οποιονδήποτε άλλων απαιτήσεων που λαμβάνονται υπόψη για την πληροφορία. Η πληροφορία συχνά παύει να είναι ευαίσθητη ή κρίσιμη μετά από μία συγκεκριμένη περίοδο χρόνου, για παράδειγμα όταν μία πληροφορία γίνεται δημόσια. Αυτές οι πτυχές θα πρέπει να λαμβάνονται υπόψη, καθώς η λάθος ταξινόμηση μπορεί να οδηγήσει στην εφαρμογή μη απαραίτητων ελέγχων, καταλήγοντας σε επιπρόσθετα έξοδα. Σε γενικές γραμμές, η ταξινόμηση που δίνεται στην πληροφορία είναι ένας σύντομος τρόπος στο να καθοριστεί πως αυτή η πληροφορία χειρίζεται και προστατεύεται.

Κρίνεται απαραίτητο να αναπτυχθεί μία κατάλληλη ομάδα διαδικασιών για τον χαρακτηρισμό και την διαχείριση πληροφοριών και να εφαρμοστεί σε συσχετισμό με το πλάνο ταξινόμησης που έχει υιοθετηθεί από τον οργανισμό. Η ονομασία των πληροφοριών θα πρέπει να αντανακλά την ταξινόμηση σύμφωνα με τους κανόνες που έχουν εδραιωθεί.

- **Ελάχιστη Ευαισθησία**

Σε αυτήν την κατηγόρια ανήκουν γενικές πληροφορίες του οργανισμού, μερικές πληροφορίες που αφορούν το προσωπικό της και μερικές τεχνικές πληροφορίες. Ο κάτοχος των πληροφοριών αυτών μπορεί να γράψει σε εμφανές σημείο την φράση «Εμπιστευτικές Πληροφορίες» καθώς επίσης και άλλου είδους επισημάνσεις ως προς την εμπιστευτικότητα των πληροφοριών.

Πρόσβαση	Προσωπικό του οργανισμού και όσων τα καθήκοντα απαιτούν πρόσβαση στις πληροφορίες αυτές.
Διανομή μέσα στην εταιρία	Αλληλογραφία εντός της εταιρίας και με αποδεκτές μεθόδους ηλεκτρονικής ανταλλαγής πληροφοριών
Διανομή έξω από την εταιρία	Μέσω ταχυδρομείου ή ιδιωτικών couriers και με αποδεκτές μεθόδους ηλεκτρονικής ανταλλαγής πληροφοριών
Ηλεκτρονική διανομή	Ο παραλήπτης θα πρέπει να έχει πρόσβαση σε πληροφορίες αυτής της κατηγορίας
Καταστροφή / Διαγραφή	Πληροφορίες σε χάρτινο μέσο θα πρέπει να πετάγονται σε κάδους εντός της εταιρίας. Πληροφορίες σε ηλεκτρονική μορφή θα πρέπει να σβήνονται εντελώς ή να καταστρέφεται το αποθηκευτικό μέσο στο οποίο βρίσκονται.
Ποινή αποκάλυψης	Μέχρι και σε τερματισμό της σύμβασης εργασίας και πλήρης έκθεση στις ανάλογες νομικές συνέπειες.

- **Κανονική Ευαισθησία**

Σε αυτήν την κατηγορία ανήκουν οικονομικές, εταιρικές, τεχνικές καθώς και οι περισσότερες πληροφορίες για το προσωπικό. Μπορούν να χρησιμοποιηθούν οι εξής εκφράσεις πάνω στις πληροφορίες:

«Εμπιστευτικές πληροφορίες τρίτων»
«Εμπιστευτικές πληροφορίες του οργανισμού»
«Ιδιοκτησία του οργανισμού»
«Για χρήση εντός του οργανισμού»

Πρόσβαση	Μόνο άτομα με ειδική έγγραφη άδεια που τους επιτρέπει την πρόσβαση σε τέτοιου είδους πληροφορίες
Διανομή μέσα στην εταιρία	Αλληλογραφία εντός της εταιρίας και με αποδεκτές μεθόδους ηλεκτρονικής ανταλλαγής πληροφοριών.
Διανομή έξω από την εταιρία	Μέσω ταχυδρομείου ή ιδιωτικών couriers.
Ηλεκτρονική διανομή	Ο παραλήπτης θα πρέπει να έχει πρόσβαση σε πληροφορίες αυτής της κατηγορίας και να είναι εντός του οργανισμού. Ακόμα η πληροφορίες θα πρέπει να είναι κωδικοποιημένες.
Καταστροφή /	Πληροφορίες σε χάρτινο μέσο θα πρέπει να πετάγονται σε κάδους

Διαγραφή	εντός της εταιρίας. Πληροφορίες σε ηλεκτρονική μορφή θα πρέπει να σβήνονται εντελώς ή να καταστρέφεται το αποθηκευτικό μέσο στο οποίο βρίσκονται.
Ποινή αποκάλυψης	Μέχρι και σε τερματισμό της σύμβασης εργασίας και πλήρης έκθεση στις ανάλογες νομικές συνέπειες

- **Εξαιρετικά Ευαίσθητες Πληροφορίες**

Σε αυτές ανήκουν εμπορικά μυστικά, τακτικές marketing, πληροφορίες για το προσωπικό, οικονομικά, πηγαίοι κώδικες και τεχνικές πληροφορίες Μπορούν να χρησιμοποιηθούν οι εξής εκφράσεις πάνω στις πληροφορίες¨
«Εμπιστευτικές πληροφορίες τρίτων»
«ΕΞΑΙΡΕΤΙΚΑ Εμπιστευτικές πληροφορίες του οργανισμού»
«Ιδιοκτησία του οργανισμού»
«Για χρήση εντός του οργανισμού»

Πρόσβαση	Μόνο άτομα με ειδική έγγραφη άδεια που τους επιτρέπει την πρόσβαση σε τέτοιου είδους πληροφορίες
Διανομή μέσα στην εταιρία	Παράδοση αυτοπροσώπως και ενυπόγραφα ή με αποδεκτές μεθόδους ηλεκτρονικής ανταλλαγής πληροφοριών.
Διανομή έξω από την εταιρία	Συστημένο μέσω ταχυδρομείου ή ιδιωτικών couriers.
Ηλεκτρονική διανομή	Ο παραλήπτης θα πρέπει να έχει πρόσβαση σε πληροφορίες αυτής της κατηγορίας και να είναι εντός της του οργανισμού. Ακόμα η πληροφορίες θα πρέπει απαραίτητος να είναι κωδικοποιημένες.
Καταστροφή / Διαγραφή	Πληροφορίες σε χάρτινο μέσο θα πρέπει να πετάγονται σε κάδους εντός της εταιρίας. Πληροφορίες θα σε ηλεκτρονική μορφή θα πρέπει να σβήνονται εντελώς ή να καταστρέφετε το αποθηκευτικό μέσο στο οποίο βρίσκονται.
Ποινή αποκάλυψης	Μέχρι και σε τερματισμό της σύμβασης εργασίας και πλήρης έκθεση στις ανάλογες νομικές συνέπειες

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

2.5 ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΟΥ

- **Πριν την πρόσληψη**

Σκοπός

Να διασφαλίσει ότι οι εργαζόμενοι και οι συμβασιούχοι θα κατανοήσουν τις ευθύνες τους, και είναι θα κατάλληλοι για τους ρόλους για τους οποίους προορίζονται. Παράλληλα βέβαια θα πρέπει να ελεγχθεί η ακεραιότητα τους ως άτομα ώστε να αποκλειστεί η περίπτωση ληστείας, απάτης ή κακής χρήσης των εγκαταστάσεων.

Όλοι οι υποψήφιοι για εργασία θα πρέπει να εξετάζονται επαρκώς, ειδικά για ευαίσθητες δουλειές. Οι εργαζόμενοι και οι συμβασιούχοι οι οποίοι θα εργάζονται στις εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να υπογράψουν σαν συμφωνία τους ρόλους ασφαλείας και τις αρμοδιότητες τους.

Ρόλοι και ευθύνες

Οι ρόλοι ασφαλείας και οι ευθύνες των εργαζομένων θα πρέπει να καθορίζονται σε συσχετισμό με την πολιτική ασφαλείας που ακολουθεί ο οργανισμός. Θα πρέπει να περιλαμβάνουν τα εξής:

- Να εφαρμόζονται και να δρουν σε αρμονία με τις πολιτικές ασφαλείας του οργανισμού.
- Να προστατεύουν τα αγαθά από μη – εξουσιοδοτημένη πρόσβαση, δημοσιοποίηση, τροποποίηση, καταστροφή ή παρέμβαση.
- Να εκτελούν ειδικές διαδικασίες ή δραστηριότητες ασφαλείας
- Να διασφαλίσουν την ευθύνη που έχει ανατεθεί στους ιδιώτες για τις δράσεις που εκτελούνται.
- Να αναφέρουν τα περιστατικά ασφαλείας ή τα πιθανά περιστατικά ή άλλους κινδύνους ασφαλείας για τον οργανισμό.

Οι ρόλοι ασφαλείας και οι αρμοδιότητες θα πρέπει να καθορίζονται και να διευκρινίζονται καθαρά στους υποψήφιους εργασίας κατά την διάρκεια της διαδικασίας της πρόσληψης.

Έλεγχος

Είναι απαραίτητο να διεξάγονται έλεγχοι στο παρελθόν των υποψηφίων για την πρόσληψη, σε συσχετισμό με τους σχετικούς νόμους και τους κανονισμούς του οργανισμού. Οι έλεγχοι επιβεβαίωσης θα πρέπει να λαμβάνουν υπόψη όλη την σχετική εργασιακή νομοθεσία, την προστασία των προσωπικών δεδομένων και θα πρέπει, όπου επιτρέπεται, να περιλαμβάνει τα ακόλουθα

- Διαθεσιμότητα συστάσεων από προηγούμενους εργοδότες του υποψηφίου.
- Ένας έλεγχος (για ολοκλήρωση και ακρίβεια) του βιογραφικού σημειώματος του υποψηφίου.
- Επιβεβαίωση των ισχυριζόμενων ακαδημαϊκών ή επαγγελματικών προσόντων.

- Ανεξάρτητος έλεγχος ταυτότητας (διαβατήριο ή παρόμοιο έγγραφο)
- Περισσότερο λεπτομερείς έλεγχοι, όπως έλεγχοι πιστωτικών καρτών ή έλεγχοι ποινικού μητρώου.

Μία επιπλέον διαδικασία ελέγχου θα πρέπει να πραγματοποιείται για τους συμβασιούχους. Όταν παρέχονται συμβασιούχοι μέσω ενός πρακτορείου, τότε το συμβόλαιο με το πρακτορείο θα πρέπει να καθορίζει καθαρά τις ευθύνες του πρακτορείου για ελέγχους και τις διαδικασίες ειδοποιήσεων που χρειάζεται να ακολουθήσουν εάν ο έλεγχος δεν έχει ολοκληρωθεί ή τα αποτελέσματα δίνουν έναν λόγο για αμφιβολία

Η πληροφορία για όλους τους υποψηφίους που προορίζονται για τις θέσεις του οργανισμού, θα πρέπει να συλλέγεται και να διαχειρίζεται σε συσχετισμό με την κατάλληλη νομοθεσία.

Όροι και συνθήκες εργασίας

Σαν ένα μέρος της συμβολαιογραφικής τους υποχρέωσης, οι εργαζόμενοι θα πρέπει να συμφωνήσουν και να υπογράψουν τους όρους και τις συνθήκες του εργασιακού τους συμβολαίου, στο οποίο θα πρέπει να αναφέρουν τις αρμοδιότητες τους αλλά και αυτές που θα πρέπει να τηρήσει ο οργανισμός για την ασφάλεια των πληροφοριών.

Οι όροι και οι συνθήκες εργασίας θα πρέπει να αντανακλούν την πολιτική ασφαλείας του οργανισμού και πρόσθετα να διευκρινίζουν και να δηλώνουν ότι όλοι οι εργαζόμενοι ή συμβασιούχοι που τους έχει δοθεί πρόσβαση σε ευαίσθητη πληροφορία θα πρέπει να υπογράψουν συμφωνία άκρας εμπιστοσύνης ή μη-δημοσιοποίησης πριν δοθεί πρόσβαση στις εγκαταστάσεις επεξεργασίας πληροφοριών.

- Οι αρμοδιότητες και τα δικαιώματα των εργαζομένων και των συμβασιούχων
- Οι αρμοδιότητες για την ταξινόμηση της πληροφορίας και τη διαχείριση των επιχειρησιακών αγαθών που σχετίζονται με πληροφοριακά συστήματα.
- Οι αρμοδιότητες του εργαζομένου ή του συμβασιούχου για την διαχείριση πληροφορίας που λαμβάνεται από άλλες εταιρίες ή εξωτερικούς παράγοντες.
- Οι αρμοδιότητες του οργανισμού για την διαχείριση των προσωπικών πληροφοριών, περιλαμβάνοντας πληροφορία που δημιουργείται κατά την διάρκεια εργασίας στον οργανισμό
- Οι αρμοδιότητες που επεκτείνονται πέρα από το συμβόλαιο του εργαζομένου με τον οργανισμό και έξω από τις κανονικές ώρες εργασίας
- Ποιες δράσεις πρέπει να ληφθούν υπόψη αν ο εργαζόμενος ή ο συμβασιούχος παραβλέψει τις απαιτήσεις ασφαλείας του οργανισμού.

Ο οργανισμός πρέπει να διασφαλίσει ότι οι εργαζόμενοι και οι συμβασιούχοι θα συμφωνήσουν με τους όρους και τις συνθήκες που αφορούν την ασφάλεια πληροφοριών και την έκταση της πρόσβασης που θα έχουν στα αγαθά του οργανισμού που σχετίζονται με τα πληροφοριακά συστήματα και τις υπηρεσίες. Όπου είναι κατάλληλο, οι αρμοδιότητες που περιέχονται μέσα στους όρους και τις συνθήκες εργασίας θα πρέπει να συνεχιστούν για μια καθορισμένη περίοδο μετά το τέλος της εργασίας

- **Κατά τη διάρκεια της εργασίας**

Σκοπός

Για να διασφαλιστεί ότι οι εργαζόμενοι ή οι συμβασιούχοι είναι ενήμεροι των απειλών της ασφάλειας πληροφοριών, των αρμοδιοτήτων τους και είναι εξοπλισμένοι κατάλληλα ώστε να υποστηρίξουν την πολιτική ασφαλείας του οργανισμού κατά τη διάρκεια της εργασίας τους, προκειμένου να μειωθεί ο κίνδυνος του ανθρώπινου λάθους.

Οι αρμοδιότητες της διοίκησης θα πρέπει να καθοριστούν ώστε να διασφαλίσουν ότι η ασφάλεια εφαρμόζεται μέσω του της εργασίας του κάθε ιδιώτη στον οργανισμό. Ένα επαρκές επίπεδο αναγνώρισης, μόρφωσης και εκπαίδευσης στις διαδικασίες ασφαλείας και η σωστή χρήση των εγκαταστάσεων επεξεργασίας πληροφοριών θα πρέπει να παρέχεται σε όλους τους εργαζομένους προκειμένου να ελαχιστοποιήσει τους πιθανούς κινδύνους ασφαλείας.

Οι αρμοδιότητες της διοίκησης

Η διοίκηση θα έπρεπε να απαιτεί οι εργαζόμενοι να εφαρμόζουν την ασφάλεια σε συσχετισμό με τις εδραιωμένες πολιτικές και τις διαδικασίες του οργανισμού. Οι εργαζόμενοι θα πρέπει να διασφαλιστεί ότι:

- Είναι κατάλληλα καταρτισμένοι στους ρόλους τους για την ασφάλεια πληροφοριών και τις αρμοδιότητες τους πριν εξουσιοδοτηθούν με πρόσβαση στις ευαίσθητες πληροφορίες ή στα πληροφοριακά συστήματα
- Τους παρέχονται οδηγίες για να καθορίσουν τις προσδοκίες ασφαλείας του ρόλου τους μέσα στον οργανισμό.
- Του δίνεται κίνητρο για να πραγματοποιήσουν τις πολιτικές ασφαλείας του οργανισμού.
- Επιτυγχάνουν ένα επίπεδο αναγνώρισης της ασφάλειας που είναι σχετική με τους ρόλους τους και τις αρμοδιότητες τους μέσα στον οργανισμό
- Συμμορφώνονται τους όρους και τις συνθήκες εργασίας, τις οποίες περιλαμβάνει η πολιτική ασφαλείας του οργανισμού και τις κατάλληλες μεθόδους εργασίας.
- Συνεχίζουν να έχουν τις κατάλληλες ικανότητες και προσόντα.

Αναγνώριση, μόρφωση και εκπαίδευση για την ασφάλεια πληροφοριών

Όλοι οι εργαζόμενοι του οργανισμού θα πρέπει να λαμβάνουν κατάλληλη εκπαίδευση αναγνώρισης και τακτικές αναβαθμίσεις στις πολιτικές και τις διαδικασίες του οργανισμού που είναι σχετικές με την εργασία τους.

Η εκπαίδευση θα πρέπει να ξεκινήσει με μία επίσημη εισαγωγική διαδικασία ώστε να γνωστοποιήσει τις πολιτικές ασφαλείας και τις προσδοκίες του οργανισμού, πριν την πρόσβαση στις πληροφορίες ή στις υπηρεσίες. Μετέπειτα, η συνεχής εκπαίδευση θα πρέπει να περιλαμβάνει τις απαιτήσεις ασφαλείας, νομικές αρμοδιότητες και επιχειρηματικούς ελέγχους, καθώς επίσης εκπαίδευση στην καλή χρήση των εγκαταστάσεων επεξεργασίας πληροφοριών. Είναι αυτονόητο ότι η αναγνώριση της ασφάλειας, η μόρφωση, και οι δραστηριότητες εκπαίδευσης θα πρέπει να είναι σχετικές στο ρόλο του προσωπικού, τις αρμοδιότητες του και τα προσόντα του.

Πειθαρχική διαδικασία

Θα πρέπει να υπάρχει μία επίσημη πειθαρχική διαδικασία για τους εργαζομένους οι οποίοι έχουν διαπράξει μία παραβίαση των κανόνων ασφαλείας. Θα πρέπει να εξασφαλίζει την σωστή και δίκαιη μεταχείριση των εργαζομένων που είναι ύποπτοι για την πραγματοποίηση της παραβίασης.

Η επίσημη πειθαρχική διαδικασία θα πρέπει να παρέχει μία κλιμακούμενη ανταπόκριση που λαμβάνει υπόψη παράγοντες όπως η φύση και η βαρύτητα της παράβασης και τον αντίκτυπο της στην επιχείρηση, εάν είναι η πρώτη παράβαση, εάν ο εργαζόμενος είχε εκπαιδευτεί κατάλληλα, την σχετική νομοθεσία, τα επιχειρηματικά συμβόλαια και τους άλλους απαιτούμενους παράγοντες. Σε σοβαρές περιπτώσεις κακής διαχείρισης, η διαδικασία θα πρέπει να επιτρέπει την άμεση αφαίρεση των καθηκόντων, των δικαιωμάτων πρόσβασης και των προνομίων.

Επίσης, η πειθαρχική διαδικασία μπορεί επίσης να χρησιμοποιείται ως ένα αποθαρρυντικό ώστε να εμποδίσει τους εργαζόμενους να παραβιάζουν τις πολιτικές ασφαλείας του οργανισμού και τις διαδικασίες του.

- **Τερματισμός ή αλλαγή εργασίας**

Σκοπός

Να διασφαλίσει ότι οι εργαζόμενοι και οι συμβασιούχοι αποχωρούν από τον οργανισμό ή αλλάζουν εργασία με έναν σωστό τρόπο. Οι αρμοδιότητες θα πρέπει να είναι σε θέση να εξασφαλίζουν ότι η αποχώρηση του εργαζομένου ή του συμβασιούχου από τον οργανισμό διαχειρίζεται σωστά, και ότι ολοκληρώνεται η επιστροφή όλου του εξοπλισμού και η αφαίρεση όλων των δικαιωμάτων πρόσβασης.

Αρμοδιότητες τερματισμού

Οι αρμοδιότητες για την εφαρμογή τερματισμού ή αλλαγής εργασίας θα πρέπει να είναι πλήρως καθορισμένες. Ο τερματισμός των καθηκόντων θα πρέπει να περιλαμβάνει τις απαιτήσεις ασφαλείας, τις νομικές αρμοδιότητες και ότι οι όροι και οι συνθήκες εργασίας συνεχίζουν για μία καθορισμένη περίοδο μετά το τέλος της εργασίας ενός εργαζομένου. Το ότι οι αρμοδιότητες και τα καθήκοντα παραμένουν σε ισχύ μετά τον τερματισμό της εργασίας θα πρέπει να περιέχεται εξ αρχής στα συμβόλαια των εργαζομένων.

Το τμήμα του ανθρώπινου δυναμικού είναι κυρίως υπεύθυνο για την γενική διαδικασία τερματισμού εργασίας και δουλεύει μαζί με την επιβλέποντα μανατζερ του ατόμου που αποχωρεί για να καταφέρει την τήρηση των απαιτήσεων ασφαλείας των σχετικών διαδικασιών. Στην περίπτωση ενός συμβασιούχου, η διαδικασία τερματισμού μπορεί να την αναλάβει το πρακτορείο που είναι υπεύθυνο για τον συμβασιούχο. Επίσης, μπορεί να είναι απαραίτητο να ενημερωθούν οι εργαζόμενοι, οι πελάτες, ή οι συμβασιούχοι για τις αλλαγές στο προσωπικό και τους λειτουργικούς κανονισμούς.

Επιστροφή των αγαθών

Όλοι οι εργαζόμενοι θα πρέπει να επιστρέψουν όλα τα αγαθά του οργανισμού που έχουν στην κατοχή τους από την στιγμή που τερματίζεται η εργασία τους, το συμβόλαιο ή η συμφωνία τους.

Η διαδικασία τερματισμού θα πρέπει να σχηματίζεται έτσι ώστε να περικλείει την επιστροφή του λογισμικού, εγγράφων, και του εξοπλισμού. Άλλα επιχειρηματικά αγαθά όπως κινητές υπολογιστικές συσκευές, πιστωτικές κάρτες, κάρτες πρόσβασης, λογισμικό, εγχειρίδια και αποθηκευμένη πληροφορία σε ηλεκτρονικά μέσα θα πρέπει επίσης να επιστραφούν.

Σε περιπτώσεις όπου ένας εργαζόμενος αγοράζει τον εξοπλισμό του οργανισμού ή χρησιμοποιεί τον δικό του προσωπικό εξοπλισμό, οι διαδικασίες θα πρέπει να ακολουθηθούν ώστε να διασφαλίσουν ότι όλη η σχετική πληροφορία μεταφέρεται στον οργανισμό και διαγράφεται ασφαλώς από τον εξοπλισμό του εργαζομένου.

Σε περιπτώσεις όπου ένας εργαζόμενος έχει την γνώση που είναι σημαντική στις συνεχείς διαδικασίες ασφαλείας, αυτή η πληροφορία θα πρέπει να αρχειοθετείται και να μεταφέρεται στον οργανισμό.

Αφαίρεση των δικαιωμάτων πρόσβασης

Τα δικαιώματα πρόσβασης των εργαζομένων ή των συμβασιούχων στην πληροφορία και στις εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να αφαιρείται μετά των τερματισμό της εργασίας τους, του συμβολαίου ή της συμφωνίας.

Κατά τον τερματισμό εργασίας, θα πρέπει να λαμβάνεται σοβαρά υπόψη η αφαίρεση των δικαιωμάτων πρόσβασης ενός ιδιώτη στα αγαθά που σχετίζονται με τα πληροφοριακά συστήματα και τις υπηρεσίες του οργανισμού. Στην περίπτωση που ο εργαζόμενος αλλάζει εργασία μέσα στον οργανισμό, οι αλλαγές θα πρέπει να αντικατοπτριστούν στην αφαίρεση όλων των δικαιωμάτων πρόσβασης που δεν έγιναν αποδεκτά για την νέα εργασία. Τα δικαιώματα πρόσβασης που θα πρέπει να αφαιρεθούν ή να προσαρμοστούν περιλαμβάνουν φυσική και λογική πρόσβαση, κλειδιά, κάρτες αναγνώρισης, εγκαταστάσεις επεξεργασίας πληροφοριών, και αφαίρεση από κάθε έγγραφο που τον αναγνωρίζει ως ενεργό μέλος τους οργανισμού. Εάν ο αποχωρών εργαζόμενος γνωρίζει κωδικούς για λογαριασμούς που παραμένουν ενεργοί, αυτοί θα πρέπει να αλλαχτούν μετά τον τερματισμό ή την αλλαγή εργασίας, του συμβολαίου ή της συμφωνίας.

Τα δικαιώματα πρόσβασης για τα πληροφοριακά αγαθά και τις εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να μειωθούν ή να αφαιρεθούν πριν τερματιστεί η εργασία, βάσει της εκτίμησης των παραγόντων κινδύνου όπως

- Εάν ο τερματισμός ή η αλλαγή γίνεται με πρωτοβουλία του εργαζομένου, και τον λόγο του τερματισμού.
- Τις τωρινές αρμοδιότητες του εργαζομένου.
- Την αξία των αγαθών στα οποία υπάρχει πρόσβαση.

Σε περιπτώσεις που ο τερματισμός γίνεται με πρωτοβουλία της διοίκησης οι εργαζόμενοι ή οι συμβασιούχοι να διαφθείρουν πληροφορία ή να κάνουν σαμποτάζ στις εγκαταστάσεις επεξεργασίας πληροφοριών.

2.6 ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

- **Ασφαλείς περιοχές**

Σκοπός

Να προλάβει την μη εξουσιοδοτημένη φυσική πρόσβαση, ζημιά και παρέμβαση στις πληροφορίες του οργανισμού.

Κρίσιμες ή ευαίσθητες εγκαταστάσεις επεξεργασίας πληροφορίας θα πρέπει να οικοδομούνται σε ασφαλείς περιοχές, να προστατεύονται από την καθορισμένη περίμετρο ασφαλείας, με κατάλληλα σύνορα ασφαλείας και ελέγχους εισόδου. Θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, ζημιά και παρέμβαση.

Φυσικοί έλεγχοι εισόδου

Οι ασφαλείς περιοχές θα πρέπει να προστατεύονται από κατάλληλους ελέγχους εισόδου ώστε να διασφαλίσουν ότι επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό. Για να είναι εφικτό αυτό θα πρέπει να λαμβάνονται υπόψη οι ακόλουθες οδηγίες:

- Η ημερομηνία και ώρα της εισόδου και αναχώρησης των επισκεπτών θα πρέπει να καταγράφεται, και όλοι οι επισκέπτες θα πρέπει να επιτηρούνται εκτός κι αν η πρόσβαση τους έχει γίνει αποδεχτεί προηγουμένως. Θα πρέπει να τους έχει δοθεί άδεια πρόσβασης για ειδικούς, εξουσιοδοτημένους σκοπούς και θα πρέπει να τους δοθούν οδηγίες για τις απαιτήσεις ασφαλείας της περιοχής και σε περιπτώσεις έκτατης ανάγκης.
- Η πρόσβαση σε περιοχές όπου η ευαίσθητη πληροφορία επεξεργάζεται ή αποθηκεύεται θα πρέπει να ελέγχεται και να είναι περιορισμένη σε εξουσιοδοτημένα άτομα μόνο και να υπάρχουν έλεγχοι εξουσιοδότησης.
- Όλοι οι εργαζόμενοι, οι συμβασιούχοι και όλοι οι επισκέπτες θα πρέπει να απαιτείται να φορούν κάποιου είδους ορατής αναγνώρισης και θα πρέπει αμέσως να ειδοποιούν το προσωπικό ασφαλείας εάν εντοπίσουν μη συνοδευμένους επισκέπτες και οποιονδήποτε που δεν φοράει την ορατή αναγνώριση.
- Τα δικαιώματα πρόσβασης σε ασφαλείς περιοχές θα πρέπει να ανασκοπούνται τακτικά και να αναβαθμίζονται, ή να αναιρούνται αν κριθεί απαραίτητο.

Εργασία σε ασφαλείς περιοχές

Θα πρέπει να σχεδιαστεί και να εφαρμοστεί φυσική προστασία και οδηγίες για την εργασία σε ασφαλείς περιοχές.

Θα πρέπει να ληφθούν υπόψη οι ακόλουθες οδηγίες:

- Το προσωπικό θα πρέπει να είναι ενήμερο για την ύπαρξη δραστηριοτήτων σε μία ασφαλή περιοχή.
- Μη επιτηρούμενη πρόσβαση σε ασφαλείς περιοχές θα πρέπει να αποφεύγεται για λόγους ασφαλείας αλλά και για την πρόληψη επιβλαβών δραστηριοτήτων.
- Οι κενές περιοχές ασφαλείας θα πρέπει να κλειδώνονται και να ελέγχονται περιοδικά.
- Φωτογραφικός, video, audio, ή άλλος εξοπλισμός καταγραφής, όπως κάμερες σε κινητές συσκευές, δεν θα πρέπει να επιτρέπεται, εκτός κι αν έχει εξουσιοδοτηθεί.

Οι κανονισμοί για την εργασία σε ασφαλείς περιοχές περιλαμβάνει ελέγχους για τους εργαζόμενους και τους συμβασιούχους που δουλεύουν στις περιοχές αυτές.

- **Εξοπλισμός ασφαλείας**

Σκοπός

Να προλάβει την απώλεια, τη ζημιά, τη ληστεία των αγαθών και την παρέμβαση στις δραστηριότητες του οργανισμού.

Ο εξοπλισμός θα πρέπει να προστατεύεται από φυσικές και περιβαλλοντολογικές απειλές. Η προστασία του εξοπλισμού είναι απαραίτητη για την μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης και για να παρέχει προστασία ενάντια στην απώλεια ή τη ζημιά. Μπορεί να απαιτηθούν ειδικοί έλεγχοι για να παρέχουν προστασία ενάντια σε φυσικές απειλές και για να ασφαλίσουν τις υποστηρικτικές εγκαταστάσεις, την παροχή ηλεκτρικού ρεύματος ή τη δομή καλωδίωσης.

Προστασία του εξοπλισμού

Ο εξοπλισμός θα πρέπει να προστατεύεται για να μειώσει τους κινδύνους από περιβαλλοντολογικές απειλές ή κινδύνους για μη εξουσιοδοτημένη πρόσβαση.

Οι ακόλουθες οδηγίες θα πρέπει να ληφθούν υπόψη προκειμένου να παρέχουν προστασία στον εξοπλισμό.

- Ο εξοπλισμός θα πρέπει να προστατεύεται ώστε να ελαχιστοποιηθεί η μη απαραίτητη πρόσβαση σε περιοχές εργασίας
- Οι εγκαταστάσεις επεξεργασίας πληροφοριών που διαχειρίζονται ευαίσθητα δεδομένα θα πρέπει να τοποθετούνται με τέτοιον τρόπο ώστε να μειωθεί ο κίνδυνος η πληροφορία να είναι ορατή από μη εξουσιοδοτημένα άτομα κατά την διάρκεια της χρήσης της, και οι αποθηκευτικές εγκαταστάσεις θα πρέπει να ασφαλίζονται για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση.
- Αντικείμενα τα οποία απαιτούν ειδική προστασία θα πρέπει να απομονώνονται ώστε να μειώσουν το γενικό επίπεδο προστασίας που απαιτείται.
- Οι έλεγχοι θα πρέπει να υιοθετούνται ώστε να ελαχιστοποιήσουν τον κίνδυνο των πιθανών φυσικών απειλών.
- Θα πρέπει να εδραιωθούν οδηγίες για φαγητό, ποτό και κάπνισμα κοντά στις εγκαταστάσεις επεξεργασίας πληροφορίας.

- Οι περιβαλλοντολογικές συνθήκες, όπως η θερμοκρασία και η υγρασία, θα πρέπει να παρακολουθούνται για συνθήκες οι οποίες θα μπορούσαν να επηρεάσουν την λειτουργία των εγκαταστάσεων επεξεργασίας πληροφοριών.
- Η χρήση ειδικών μεθόδων προστασίας, όπως μεμβράνες πληκτρολογίου, θα πρέπει ληφθούν υπόψη για τον εξοπλισμό σε βιομηχανικά περιβάλλοντα.
- Ο εξοπλισμός που επεξεργάζεται ευαίσθητη πληροφορία θα πρέπει να προστατεύεται ώστε να ελαχιστοποιήσει τον κίνδυνο διαρροής πληροφοριών.

Συντήρηση εξοπλισμού

Ο εξοπλισμός θα πρέπει να συντηρείται σωστά ώστε να διασφαλίσει την συνεχή του διαθεσιμότητα και ακεραιότητα.

- Ο εξοπλισμός θα πρέπει να συντηρείται βάσει των οδηγιών που συνιστώνται από τον προμηθευτή.
- Μόνο το εξουσιοδοτημένο προσωπικό συντήρησης θα πρέπει να πραγματοποιεί τις επιδιορθώσεις και το σέρβις του εξοπλισμού.
- Θα πρέπει να καταγράφονται τα λάθη, και όλη η προληπτική και διορθωτική συντήρηση.
- Κατάλληλοι έλεγχοι θα πρέπει να εφαρμόζονται όταν ο εξοπλισμός προγραμματίζεται για συντήρηση, λαμβάνοντας υπόψη εάν η συντήρηση πραγματοποιείται από το προσωπικό της επιχείρησης ή από εξωτερικό προσωπικό.
- Όλες οι απαιτήσεις που επιβάλλονται από τις πολιτικές ασφαλείας θα πρέπει να τηρούνται.

Ασφαλής διάθεση ή επαναχρησιμοποίηση του εξοπλισμού

Όλα τα αντικείμενα που περιέχουν αποθηκευτικά μέσα θα πρέπει να ελέγχονται ώστε να διασφαλιστεί ότι οποιοδήποτε ευαίσθητο δεδομένο και λογισμικό έχει αφαιρεθεί ή έχει ασφαλώς παραγραφτεί πριν να γίνουν διαθέσιμα.

Οι συσκευές που περιέχουν ευαίσθητη πληροφορία θα πρέπει να καταστρέφονται φυσικά ή η πληροφορία θα πρέπει να καταστρέφεται, να διαγράφεται ή ξαναγράφεται χρησιμοποιώντας τεχνικές που κάνουν την αυθεντική πληροφορία μη ανιχνεύσιμη από το να χρησιμοποιείται η καθιερωμένη λειτουργία του delete ή του format.

Οι χαλασμένες συσκευές που περιέχουν ευαίσθητα δεδομένα μπορεί να απαιτήσουν μία εκτίμηση επικινδυνότητας ώστε να καθοριστεί εάν τα αντικείμενα αυτά θα πρέπει να καταστραφούν φυσικά από το να σταλούν για επισκευή.

Αφαίρεση περιουσίας

Ο εξοπλισμός, η πληροφορία ή το λογισμικό θα πρέπει να μην φεύγει από τον οργανισμό χωρίς να έχει δοθεί εξουσιοδότηση.

- Οι εργαζόμενοι και οι συμβασιούχοι οι οποίοι έχουν την εξουσιοδότηση να επιτρέπουν την απομάκρυνση των αγαθών εκτός οργανισμού θα πρέπει να καθορίζονται καθαρά.
- Τα όρια χρόνου για την αφαίρεση του εξοπλισμού θα πρέπει να είναι καθορισμένα.
- Όπου είναι απαραίτητο και κατάλληλο, ο εξοπλισμός θα πρέπει να καταγράφεται όταν απομακρύνεται από τον οργανισμό και να καταγράφεται ξανά όταν επιστρέφει.

Σημεία ελέγχου, που αναλαμβάνονται για να εντοπίσουν την μη εξουσιοδοτημένη αφαίρεση περιουσίας, μπορούν επίσης να εφαρμοστούν για να εντοπίσουν μη εξουσιοδοτημένες συσκευές καταγραφής, όπλα κτλ. και να προλάβουν την είσοδο τους στον οργανισμό. Τέτοια σημεία ελέγχου θα πρέπει να εκτελούνται σε συσχετισμό με τη σχετική νομοθεσία και τους κανονισμούς. Οι ιδιώτες θα πρέπει να είναι ενήμεροι για το που πραγματοποιούνται τα σημεία ελέγχου, και οι έλεγχοι θα πρέπει να εφαρμόζονται με εξουσιοδότηση για τις νομικές απαιτήσεις.

2.7 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΧΡΗΣΗΣ E-MAIL

Σκοπός

Να αποτρέψει την αμαύρωση της δημόσιας εικόνας του οργανισμού. Όταν ένα ηλεκτρονικό μήνυμα εξέρχεται από τον οργανισμό τότε το κοινό θα θεωρήσει το μήνυμα ως μία δήλωση επίσημης πολιτικής από αυτόν.

Πεδίο Εφαρμογής

Αυτή η πολιτική καλύπτει την κατάλληλη χρήση οποιουδήποτε ηλεκτρονικού μηνύματος από την ηλεκτρονική διεύθυνση του οργανισμού και έχει εφαρμογή σε όλους τους εργαζόμενους, τους πωλητές ή τους πράκτορες εκ μέρους του οργανισμού.

Πολιτική

- **Απαγορευμένη χρήση**

Το όνομα του οργανισμού δεν θα πρέπει να χρησιμοποιείται για τη χρήση, τη δημιουργία ή τη διανομή οποιονδήποτε διάτρητων ή προσβλητικών μηνυμάτων, συμπεριλαμβανομένων και προσβλητικών μηνυμάτων σχετικά με τη φυλή, το φύλο, τις ανικανότητες, την ηλικία, τους σεξουαλικούς προσανατολισμούς, την πορνογραφία, τα θρησκευτικά πιστεύω, τις πολιτικές απόψεις ή την εθνική προέλευση. Οι εργαζόμενοι οι οποίοι θα λάβουν μηνύματα με τέτοιο περιεχόμενο από οποιοδήποτε υπάλληλο του οργανισμού θα πρέπει άμεσα να αναφέρουν το συμβάν στον υπεύθυνο.

- **Προσωπική χρήση**

Χρησιμοποιώντας μία λογική ποσότητα για προσωπικά ηλεκτρονικά μηνύματα μέσω του οργανισμού είναι αποδεκτό, αλλά email τα οποία δεν σχετίζονται με την δουλειά θα πρέπει να αποθηκεύονται σε διαφορετικό φάκελο από τα email της δουλειάς. Η αποστολή αλυσιδωτών μηνυμάτων ή email με ανέκδοτα με τη χρήση του ονόματος του οργανισμού είναι κάτι το απαγορευμένο. Ιοί ή άλλες επιβλαβείς προειδοποιήσεις και ομαδικά emails με τη χρήση του ηλεκτρονικού συστήματος του οργανισμού θα πρέπει να γίνουν αποδεκτά από τους υπεύθυνους πριν την αποστολή τους. Αυτοί οι περιορισμοί επίσης βρίσκουν εφαρμογή στην προώθηση των email που λαμβάνονται από έναν εργαζόμενο του οργανισμού.

- **Παρακολούθηση**

Οι υπάλληλοι του οργανισμού δεν θα πρέπει να έχουν προσδοκίες για privacy οτιδήποτε αποθηκεύουν, στέλνουν ή λαμβάνουν από το σύστημα ηλεκτρονικών μηνυμάτων της εταιρείας. Είναι πιθανό να γίνεται παρακολούθηση των μηνυμάτων χωρίς προηγούμενη προειδοποίηση, χωρίς βέβαια η παρακολούθηση να είναι υποχρεωτικό να εφαρμοστεί από τον οργανισμό.

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

2.8 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΑ ANTI-VIRUS

Σκοπός

Αυτή η πολιτική ορίζει τις απαιτήσεις που πρέπει να πληρούν όλοι οι υπολογιστές που συνδέονται στο δίκτυο του οργανισμού ώστε να διασφαλισθεί ο αποτελεσματικός εντοπισμός και πρόληψη από ιούς έτσι ώστε να προστατεύονται οι πόροι, τα κεφάλαια , οι πληροφορίες και οι παραγωγικές διαδικασίες της εταιρίας.

Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται σε όλους τους υπολογιστές του οργανισμού. Αυτό περιλαμβάνει υπολογιστές στο εργαστήριο του οργανισμού και στο εσωτερικό δίκτυο του, φορητούς υπολογιστές και όλους τους servers.

Πολιτική

Όλα τα μηχανήματα του οργανισμού στα οποία εφαρμόζεται η πολιτική πρέπει να τρέχουν ένα anti-virus πρόγραμμα το οποίο να είναι εγκεκριμένο από τον οργανισμό και να είναι ρυθμισμένο να εξετάζει το σύστημα για ιούς σε τακτά χρονικά διαστήματα. Ακόμα το ίδιο το πρόγραμμα το anti-virus αλλά και τα πρότυπα των ιών (βιβλιοθήκη ιών) θα πρέπει να ενημερώνονται για προσθήκες και βελτιώσεις

Τα μηχανήματα που έχουν προσβληθεί από ιούς θα πρέπει να αποσυνδέονται από το δίκτυο της εταιρίας μέχρι να βεβαιωθούμε ότι δεν είναι πια μολυσμένα, μέσω του anti-virus.

Οι διαχειριστές των εργαστηρίων είναι υπεύθυνοι για την δημιουργία διαδικασιών που θα εγγυώνται τον τακτικό έλεγχο των μηχανημάτων για ιούς και που θα πιστοποιούν ότι τα μηχανήματα δεν είναι μολυσμένα.

Οποιεσδήποτε δραστηριότητες έχουν σκοπό να διασπείρουν ή να δημιουργήσουν κακόβουλο λογισμικό μέσα στο δίκτυο και τους υπολογιστές του οργανισμού απαγορεύονται σύμφωνα με την Πολιτική Ασφάλειας Αποδεκτής Χρήσης.

Κανόνες Για Τα Anti-Virus

- Πάντα να τρέχετε το προτεινόμενο από την εταιρία anti-virus πρόγραμμα. Να το κρατάτε ενημερωμένο με τις τελευταίες διορθώσεις και ενημερώσεις.
- Ποτέ μη ανοίγετε αρχεία, macros ή scripts που έρχονται συνημμένα σε e-mails από άγνωστος, ύποπτο ή μη έμπιστο προς εσάς αποστολέα. Τέτοια e-mails πρέπει να σβήνονται αμέσως και να διαγράφονται και από τον trash directory.
- Οποιαδήποτε spam, chain ή junk mails θα πρέπει να σβήνονται και να μην προωθούνται..
- Ποτέ μην κατεβάζετε αρχεία από άγνωστες, ύποπτες ή μη έμπιστες πηγές.
- Μην επιτρέπετε το άμεσο μοίρασμα σκληρών δίσκων με read/write privileges αν δεν είναι απαραίτητο για την διεκπεραίωση κάποιας συγκεκριμένης εργασίας.
- Πάντα να ελέγχετε για ιούς τα removable storage devices πριν τα χρησιμοποιήσετε.
- Αν για κάποια εργασία το anti-virus πρέπει να απενεργοποιηθεί τότε πριν το απενεργοποιήσετε θα πρέπει να ελέγξετε τον υπολογιστή για ιούς και μόλις σιγουρευτείτε ότι είναι καθαρός μπορείτε να το απενεργοποιήσετε. Εκτελέστε την

εργασία σας με προσοχή ώστε να μην εκτελέσετε ύποπτο λογισμικό και όταν τελειώσετε ενεργοποιήστε το anti-virus και ελέγξτε

Επειδή πολύ συχνά βγαίνουν καινούρια anti-virus προγράμματα και καινούργιοι τύποι ιών περιοδικά πρέπει να ελέγχονται τα προτεινόμενα προγράμματα αλλά και οι κανόνες που περιγράφονται στο κείμενο αυτό για τυχόν αλλαγές και προσθήκες.

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

2.9 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΑ PASSWORDS

Σκοπός

Ο σκοπός αυτής της πολιτικής είναι να εδραιώσει ένα πρότυπο για την δημιουργία ισχυρών passwords, την προστασία αυτών των passwords και την συχνότητα αλλαγής τους.

Πεδίο Εφαρμογής

Αυτή η πολιτική βρίσκει εφαρμογή σε όλο το προσωπικό που είναι υπεύθυνο για κάποιον λογαριασμό σε οποιοδήποτε σύστημα το οποίο υπάρχει σε κάποια εγκατάσταση του οργανισμού, και έχει πρόσβαση στο δίκτυο, ή αποθηκεύει μη δημόσια πληροφορία του οργανισμού.

Πολιτική

Γενικά

- Όλα τα passwords των συστημάτων θα πρέπει να αλλάζουν σε τακτική βάση.
- Όλα τα passwords των χρηστών θα πρέπει να αλλάζουν τουλάχιστον κάθε έξη μήνες.
- Οι λογαριασμοί των χρηστών που έχουν εξουσιοδοτηθεί με προνόμια στα συστήματα μέσω ομαδικών συνδρομών ή προγραμμάτων πρέπει να χρησιμοποιούν ένα μοναδικό password για τον συγκεκριμένο λογαριασμό.
- Τα passwords δεν πρέπει να εισέρχονται μέσα σε ηλεκτρονικά μηνύματα ή άλλα μέσα ηλεκτρονικής επικοινωνίας.
- Όλα τα passwords που χρησιμοποιούνται είτε από τους χρήστες είτε από το σύστημα θα πρέπει να συμμορφώνονται στις οδηγίες που περιγράφονται παρακάτω.

Οδηγίες

Α. Οδηγίες για την κατασκευή passwords

Τα passwords χρησιμοποιούνται για ποικίλους σκοπούς στον οργανισμό. Κάποιες από τις πιο κοινές χρήσεις περιλαμβάνουν: τους λογαριασμούς χρηστών, τους λογαριασμούς του διαδικτύου, λογαριασμούς ηλεκτρονικού ταχυδρομείου, προστασία του screen saver, voicemail password, και τοπικές router logins. Εφόσον πολύ λίγα συστήματα υποστηρίζουν τα δυναμικά passwords τα οποία χρησιμοποιούνται μόνο μία φορά, καθένας θα πρέπει να είναι ενήμερος για το πώς να επιλέξει ισχυρά passwords.

Τα φτωχά, αδύναμα passwords έχουν τα ακόλουθα χαρακτηριστικά:

- Το password περιέχει λιγότερους από δεκαπέντε χαρακτήρες.
- Το password είναι μία λέξη που υπάρχει σε λεξικό.
- Το password είναι μία λέξη κοινής χρήσης όπως:
    - Όνομα οικογένειας, κατοικίδιων ζώων, φίλων, συναδέλφων, χαρακτήρων φαντασίας κτλ.
    - Όρους και ονόματα υπολογιστών, εντολών, sites, εταιριών, λογισμικού

- Το όνομα του οργανισμού
- Γενέθλια και άλλη προσωπική πληροφορία, όπως διευθύνσεις ή τηλεφωνικοί αριθμοί.
- Λέξεις ή αριθμοί όπως aaabbb, qwerty, zyxwvuts, 123321 κτλ.
- Λέξεις στις οποίες προηγείται ή ακολουθεί ένας ακέραιος (πχ. Secret1, 1secret)

Τα ισχυρά passwords έχουν τα ακόλουθα χαρακτηριστικά:

- Περιέχουν κεφαλαίους και μικρούς χαρακτήρες
- Περιέχουν αριθμούς, γράμματα και σύμβολα
- Έχουν μήκος τουλάχιστον δεκαπέντε αλφαριθμητικών χαρακτήρων
- Δεν υφίστανται ως λέξεις σε οποιαδήποτε γλώσσα
- Δεν βασίζονται σε προσωπικές πληροφορίες, ονόματα κτλ.
- Τα passwords δεν θα πρέπει ποτέ να γράφονται ή να αποθηκεύονται on-line

Β. Πρότυπα προστασίας passwords

Να μην χρησιμοποιείτε το ίδιο password για λογαριασμούς του οργανισμού όπως για πρόσβαση εκτός του οργανισμού. Όπου είναι δυνατό, μην χρησιμοποιείτε το ίδιο password για διαφορετικές ανάγκες πρόσβασης του οργανισμού. Μην μοιράζεστε τα passwords του οργανισμού με κανέναν, συμπεριλαμβανομένου και των βοηθών διαχείρισης ή γραμματέων. Όλα τα passwords θα πρέπει να διαχειρίζονται ως ευαίσθητη, εμπιστευτική πληροφορία που ανήκει στον οργανισμό.

Παρακάτω ακολουθεί μία λίστα από πράγματα που πρέπει να αποφευχθούν:

- Μην αποκαλύπτετε το password μέσω τηλεφώνου σε κανέναν
- Μην αποκαλύπτετε το password σε ένα ηλεκτρονικό μήνυμα
- Μην αποκαλύπτετε το password στο αφεντικό
- Μην μιλάτε για το password μπροστά σε άλλους
- Μην υποδεικνύετε την μορφή του password
- Μην αποκαλύπτετε το password σε ερωτηματολόγια ή σε φόρμες ασφαλείας
- Μην μοιράζεστε το password με μέλη της οικογένειας σας
- Μην αποκαλύπτετε το password σε συναδέλφους κατά την διάρκεια διακοπών

Εάν κάποιος απαιτεί το password, να του υποδείξετε το συγκεκριμένο έγγραφο ή να του πείτε να καλέσει το Τμήμα Ασφάλειας Πληροφοριών του οργανισμού.
Μην χρησιμοποιείτε την επιλογή "Remember Password" των εφαρμογών.

Ένα ένας λογαριασμός ή ένα password υποπτεύεστε ότι έχει παραβιαστεί ή αποκαλυφθεί, θα πρέπει να αναφέρετε αυτό το περιστατικό στην InfoSec και να αλλάξετε όλα τα passwords.

C. Passphrases

Οι Passphrases χρησιμοποιούνται γενικά για την πιστοποίηση του δημόσιου/ιδιωτικού κλειδιού. Ένα σύστημα δημόσιου/ιδιωτικού κλειδιού καθορίζει την μαθηματική σχέση μεταξύ των δημόσιο κλειδί που είναι γνωστό σε όλους, και το ιδιωτικό κλειδί, το οποίο είναι γνωστό μόνο σε έναν χρήστη. Χωρίς την Passphrases για να ξεκλειδώσει το ιδιωτικό κλειδί, ο χρήστης δεν μπορεί να αποκτήσει πρόσβαση.

Οι Passphrases δεν χρησιμοποιούνται με τον ίδιο τρόπο όπως τα passwords. Μία Passphrase είναι μία εκτενέστερη έκδοση ενός password, και κατ' επέκταση είναι πιο ασφαλής. Μία Passphrase τυπικά αποτελείται από πολλαπλές λέξεις. Εξαιτίας αυτού, μία Passphrase είναι πιο ασφαλής ενάντια στις "dictionary attacks".

Μία καλή Passphrase είναι σχετικά μακριά και περιέχει ένα συνδυασμό κεφαλαίων και μικρών γραμμάτων και αριθμητικών και συμβολικών χαρακτήρων. Ένα παράδειγμα μίας καλής Passphrase είναι το εξής:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

Όλοι οι παραπάνω κανόνες που εφαρμόζονται στα passwords εφαρμόζονται και για τις passphrazes.

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

2.10 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟΥΣ SERVERS

Σκοπός

Ο σκοπός αυτής της πολιτικής ασφάλειας είναι να θέσει τα πρότυπα βάσει των οποίων οι servers που χρησιμοποιούνται στο εσωτερικό δίκτυο του οργανισμού θα πρέπει να είναι ρυθμισμένοι. Η αποτελεσματική υλοποίηση αυτής της πολιτικής θα ελαχιστοποιήσει την ανεπιθύμητη πρόσβαση σε πληροφορίες και τεχνολογίες του οργανισμού.

Πεδίο Εφαρμογής

Αυτή η πολιτική εφαρμόζεται σε εξοπλισμό που κατέχει ή χρησιμοποιεί ο οργανισμός και βρίσκεται στο εσωτερικό δίκτυο της εταιρίας. Δεν εφαρμόζεται σε servers που βρίσκονται στο DMZ

Πολιτική

Ιδιοκτησία Και Ευθύνες

Όλους τους εσωτερικούς servers που χρησιμοποιεί ο οργανισμός πρέπει να τους χειρίζεται μια, ικανή ομάδα η οποία θα είναι υπεύθυνη για τη διαχείριση τους. Κάθε ομάδα θα πρέπει να δημιουργήσει οδηγίες ρυθμίσεων, τις οποίες θα πρέπει να συντηρεί και να αναβαθμίζει. Αυτές οι οδηγίες θα πρέπει να βασίζονται στις επιχειρησιακές ανάγκες της εταιρίας και να εγκριθούν από την εταιρία που έχει σχεδιάσει τις πολιτικές ασφαλείας. Η ομάδα αυτή θα πρέπει να ελέγξει την ελαστικότητα των ρυθμίσεων και να υλοποιήσει και μια αναφορά εξαιρέσεων βασισμένη στην εξοπλισμό. Ακόμα θα πρέπει να δημιουργήσει διαδικασίες για την αλλαγή των οδηγιών οι οποίες θα περιέχουν μελέτη και έγκριση από την εταιρεία που έχει σχεδιάσει τις πολιτικές ασφαλείας.

- Τα ελάχιστα στοιχεία τα οποία πρέπει να διατηρούνται είναι:
- Η τοποθεσία του server.
    - Ο τύπος του υλικού και η έκδοση του λειτουργικού συστήματος.
    - Οι κύριες λειτουργίες που εξυπηρετεί και οι εφαρμογές που τρέχει.
    - Στοιχεία επαφής με τον υπεύθυνο για τον server.
- Οι παραπάνω πληροφορίες θα πρέπει να ενημερώνονται σε κάθε αλλαγή τους.
- Οι αλλαγές των ρυθμίσεων των servers θα πρέπει να γίνονται με βάση τις ανάλογες διαδικασίες που έχουν οριστεί.

Γενικές Οδηγίες Ρυθμίσεων

- Οι ρυθμίσεις του λειτουργικού συστήματος θα πρέπει να είναι σύμφωνες με τις εγκεκριμένες από την εταιρία που έχει σχεδιάσει τις πολιτικές ασφαλείας οδηγίες.
- Υπηρεσίες και εφαρμογές που δεν χρησιμοποιούνται θα πρέπει να αφαιρούνται.
- Η πρόσβαση στις υπηρεσίες θα πρέπει να καταγράφονται και να ελέγχονται από τεχνολογίες όπως TCP Wrappers, αν είναι δυνατόν.

- Όλα τα πρόσφατα security patches θα πρέπει να εφαρμόζονται στο σύστημα μόλις είναι διαθέσιμα. Εξαιρούνται όσα security patches θα έρχονταν σε σύγκρουση με τις επιχειρησιακές ανάγκες της εταιρίας.
- Σχέσεις εμπιστοσύνης ανάμεσα στα συστήματα αποτελούν κίνδυνο για την ασφάλεια και θα πρέπει να αποφεύγονται.
- Πρέπει πάντα να ακολουθούνται οι αρχές ασφάλειας για έρθει σε πέρας μια λειτουργία.
- Μην χρησιμοποιείτε τον root λογαριασμό για κάποια λειτουργία που θα μπορούσατε να κάνετε και με λογαριασμό χρήστη.
- Όπου είναι δυνατόν θα πρέπει να χρησιμοποιούνται ασφαλή κανάλια επικοινωνίας.
- Οι servers (ως συσκευές) θα πρέπει να τοποθετούνται σε ασφαλές περιβάλλον όπου η πρόσβαση ελέγχεται.

Παρακολούθηση (Monitoring)

Όλα τα γεγονότα που σχετίζονται με την ασφάλεια ευαίσθητων συστημάτων πρέπει να καταγράφονται και να ελέγχονται σύμφωνα με τα παρακάτω.

- Όλα τα security logs θα πρέπει να παραμένουν διαθέσιμα στο δίκτυο για τουλάχιστον μια βδομάδα.
- Ημερήσια (προσθετικά) backups σε ταινίες θα πρέπει να παίρνονται για τουλάχιστον ένα μήνα.
- Τα backups του κάθε μήνα θα πρέπει να διατηρούνται για δυο χρόνια.
- Γεγονότα που σχετίζονται με την ασφάλεια των συστημάτων θα πρέπει να αναφέρονται στους υπεύθυνους κι έπειτα να εξετάζονται. Στην συνέχεια θα πρέπει να οριστούν διορθωτικά μέτρα. Μερικά χαρακτηριστικά γεγονότα που σχετίζονται με την ασφάλεια είναι:
    - Port Scanning
    - Στοιχεία μη εγκεκριμένης πρόσβασης σε προνομιούχους λογαριασμούς.
    - Ασυνήθιστα περιστατικά που δεν προέρχονται από κάποια συγκεκριμένη εφαρμογή του συστήματος.

Έλεγχος

Σε τακτά χρονικά διαστήματα θα πρέπει να διενεργούνται έλεγχοι στα μηχανήματα του οργανισμού. Τα αποτελέσματα θα πρέπει να μελετώνται και στη συνέχεια να παρέχονται λύσεις. Κάθε δυνατή προσπάθεια πρέπει να καταβάλλεται ώστε κατά την διάρκεια των ελέγχων να μην εμποδίζεται η ομαλή λειτουργία την εταιρίας.

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

2.11 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ VPN

Σκοπός

Ο σκοπός αυτής της πολιτικής είναι να ορίσει τις οδηγίες για σύνδεση στο δίκτυο του οργανισμού μέσω του Virtual Private Network(VPN).

Πεδίο Εφαρμογής

Αυτή η πολιτική ασφάλειας απευθύνεται σε όλους τους υπαλλήλους, συνεργάτες, πράκτορες, και συμβασιούχους οι οποίοι μέσω οποιουδήποτε υπολογιστή έχουν πρόσβαση στο δίκτυο της εταιρίας για να εκτελέσουν κάποια εργασία για τον οργανισμό. Αυτή η πολιτική βρίσκει εφαρμογή στο VPN το οποίο διευθύνεται μέσω ενός IPSec Concentrator.

Πολιτική

- Είναι ευθύνη των υπαλλήλων με τα δικαιώματα χρήσης του VPN να εξασφαλίσουν ότι οι μη εξουσιοδοτημένοι χρήστες δεν έχουν πρόσβαση στο δίκτυο του οργανισμού.
- Η χρήση του VPN πρέπει να ελέγχεται με τη χρήση διαφορετικού κωδικού πρόσβασης κάθε φορά ή με το σύστημα δημοσίου/ιδιωτικού κλειδιού με μία ισχυρή passphrase.
- Όταν υπάρχει ενεργή σύνδεση στο δίκτυο του οργανισμού, VPNs θα εξαναγκάσει όλη την κίνηση προς και από τον υπολογιστή μέσω της σύνδεσης VPN. Έτσι όλη η υπόλοιπη κίνηση θα σταματήσει.
- Δεν επιτρέπεται διπλής ροής κίνηση, μόνο μία σύνδεση δικτύου θεμιτή.
- Οι πύλες της VPN θα πρέπει να διαχειρίζονται από τις ομάδες διαχείρισης δικτύου του οργανισμού.
- Όλοι οι υπολογιστές οι οποίοι συνδέονται στο εσωτερικό δίκτυο του οργανισμού μέσω VPN ή άλλου είδους τεχνολογία υα πρέπει να χρησιμοποιούν ενημερωμένο anti-virus λογισμικό.
- Οι χρήστες του VPN θα αποσυνδέονται αυτόματα από το δίκτυο του οργανισμού μετά από τριάντα λεπτά μη ενεργούς δράσης. Ο χρήστης θα πρέπει να ξανασυνδεθεί στο δίκτυο.
- Ο VPN concentrator είναι περιορισμένος σε έναν απόλυτο χρόνο σύνδεσης των 24 ωρών.
- Οι χρήστες των υπολογιστών οι οποίοι χρησιμοποιούν εξοπλισμό που δεν ανήκει στον οργανισμό, θα πρέπει να κάνουν τις κατάλληλες ρυθμίσεις ώστε να συμμορφωθούν τα μηχανήματα με το VPN δίκτυο του οργανισμού και την Πολιτική Ασφαλείας του δικτύου.
- Με τη χρήση της VPN τεχνολογίας με προσωπικό εξοπλισμό, οι χρήστες θα πρέπει να κατανοήσουν ότι τα μηχανήματα τους είναι η προέκταση του δικτύου του οργανισμού, και υπόκεινται στους ίδιους κανόνες και κανονισμούς που εφαρμόζονται στον εξοπλισμό του οργανισμού.

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

2.12 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΗΝ ΑΣΥΡΜΑΤΗ ΕΠΙΚΟΙΝΩΝΙΑ

Σκοπός

Αυτή η πολιτική καθορίζει τις συνθήκες τις οποίες πρέπει να πληρεί ο ασύρματος εξοπλισμός ώστε να συνδεθεί στο δίκτυο του οργανισμού. Μόνο συστήματα που τηρούν τις απαιτήσεις που ορίζονται μέσα στην πολιτική και έχουν εγκριθεί θα μπορούν να χρησιμοποιηθούν σε δίκτυα του οργανισμού.

Πεδίο Εφαρμογής

Αυτή η πολιτική ασφάλειας καλύπτει όλες τις συσκευές ασύρματης επικοινωνίας οι οποίες συνδέονται σε δίκτυα της εταιρίας. Αυτό περιλαμβάνει κάθε είδους συσκευή οποία μπορεί να μεταδώσει πληροφορίες σε πακέτα. Ασύρματες συσκευές ή δίκτυα που δεν συνδέονται με το δίκτυο του οργανισμού δεν εμπίπτουν σε αυτήν την πολιτική ασφάλειας.

Πολιτική

Access Points Και Κάρτες

Όλα τα Access Points και οι ασύρματες κάρτες δικτύου θα πρέπει να έχουν εγκριθεί από τους υπευθύνους. Ακόμα τα Access Points θα πρέπει να τοποθετούνται σε σημεία που είναι δύσκολη η φυσική πρόσβαση σε αυτά. Αυτές οι συσκευές θα υπόκεινται σε περιοδικούς ελέγχους, penetration tests και audits.

Αποδεκτή Τεχνολογία

Όλες οι συσκευές ασύρματης πρόσβασης θα πρέπει να είναι εγκεκριμένες για εταιρική χρήση.

VPN Authentication Και Κρυπτογράφηση

Όλοι οι υπολογιστές με ασύρματο δίκτυο θα πρέπει να χρησιμοποιούν την τεχνολογία VPN. Κάθε υπολογιστής ο οποίος δεν πληρεί τις απαιτήσεις κρυπτογράφησης και ασφάλειας θα πρέπει να του απαγορεύεται η πρόσβαση. Τέτοιες απαιτήσεις ασφάλειας είναι:

- Το κλειδί κρυπτογράφησης της επικοινωνίας θα πρέπει να είναι τουλάχιστον 128bits.
- Όλες οι συσκευές θα πρέπει να υποστηρίζουν MAC Address οι οποίες θα μπορούν να καταγραφούν.
- Θα πρέπει να υποστηρίζεται η πιστοποίηση μέσω προγραμμάτων τύπου: TACACS+ και RADIUS.

Θέτοντας Το SSID

Το SSID θα πρέπει να επιλεγεί έτσι ώστε να μην περιέχει πληροφορίες που θα μπορούσαν να οδηγήσουν στη ταυτότητα της εταιρίας.

Ρύθμισης ασφαλείας

Όλες οι συσκευές που χρησιμοποιούνται σε ένα ασύρματο δίκτυο θα πρέπει να είναι ρυθμισμένες σύμφωνα με τα παρακάτω πρότυπα.

- Η πρόσβαση στο ασύρματο δίκτυο θα πρέπει να περιορίζεται από MAC filtering. Ο διαχειριστής του δικτύου είναι υπεύθυνος για την συντήρηση της λίστας με τις διευθύνσεις MAC. Αυτό σημαίνει ότι εκείνος πρέπει να προσθέτει αφού ακολουθήσει τις απαραίτητες διαδικασίες μια διεύθυνση στην λίστα.
- Τα ασύρματα δίκτυα θα πρέπει να έχουν ενεργοποιημένη την κωδικοποίηση σύμφωνα με ένα από τα πρότυπα WPA, WEP2 και WEPplus. Το απλό WEP δεν είναι αρκετό γιατί είναι τρωτό σε διάφορες επιθέσεις.
- Τα κλειδιά της κρυπτογράφησης θα πρέπει να αλλάζουν είτε δυναμικά είτε χειροκίνητα κάθε έξι μήνες.
- Τα Access Points θα πρέπει να τοποθετούνται αν είναι εφικτό σε τέτοια σημεία ώστε η εμβέλεια του σήματος τους να εξαντλείται εντός του κτηρίου της εταιρίας.
- Τα νέα Access Points θα πρέπει να εγκαθίστανται και να ρυθμίζονται όταν το δίκτυο δεν είναι σε λειτουργία.
- Τα κανάλια στα οποία εκπέμπει κάθε Access Point θα πρέπει να μελετώνται έτσι ώστε να μην υπάρχουν παρεμβολές. Κατά την διάρκεια αυτής της μελέτης θα πρέπει να μελετηθούν οι θέσεις και η εμβέλεια των συσκευών αυτών.
- Αν είναι δυνατόν θα πρέπει η πρόσβαση στις ρυθμίσεις της συσκευής να γίνεται μέσω TACACS+ και να καταγράφονται οι κινήσεις κάθε χρήστη. Αν αυτό δεν είναι δυνατόν μόνο ο διαχειριστής του δικτύου μπορεί να έχει πρόσβαση στις συσκευές αυτές.

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

2.13 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ SERVER MALWARE

Σκοπός

Ο σκοπός αυτής της πολιτικής είναι να ορίσει που συστήματα server απαιτούνται ώστε να έχουμε εφαρμογές anti-virus ή anti-spyware.

Πεδίο Εφαρμογής

Αυτή η πολιτική βρίσκει εφαρμογή σε όλους τους servers για τον οποίων την διαχείριση είναι υπεύθυνος ο οργανισμός. Αυτό κατηγορηματικά περιλαμβάνει οποιοδήποτε σύστημα για το οποίο ο οργανισμός έχει συμβολαιογραφική υποχρέωση για την διαχείριση του.

Πολιτική

Το προσωπικό του οργανισμού θα πρέπει να εφαρμόσει αυτή την πολιτική προκειμένου να αποφασίσει σε ποιους servers θα εγκατασταθούν εφαρμογές anti-virus και/ή anti-spyware και να φροντίσει για την κατάλληλη διαχείριση αυτών των εφαρμογών.

Anti-virus

Όλοι οι servers πρέπει να έχουν εγκατεστημένη μία εφαρμογή anti-virus η οποία παρέχει συνεχή προστασία σε αρχεία και προγράμματα του συστήματος εάν συναντήσουν μία ή και περισσότερες από τις ακόλουθες καταστάσεις

- Να έχουν πρόσβαση μη-εξουσιοδοτημένοι χρήστες
- Το σύστημα να είναι ένα file server
- NBT/Microsoft Share πρόσβαση είναι ανοιχτή στον server από συστήματα που χρησιμοποιούνται από μη εξουσιοδοτημένους χρήστες
- HTTP/FTP access είναι ανοιχτή από το Διαδίκτυοt
- Υπάρχουν επικίνδυνα πρωτόκολλα/εφαρμογές στο σύστημα μέσω του Διαδικτύου

Mail server anti-virus

Εάν το σύστημα είναι ένα mail server θα πρέπει να έχει είτε εξωτερική είτε εσωτερική anti-virus scanning εφαρμογή οι οποία ελέγχει όλα τα ηλεκτρονικά μηνύματα που διακινούνται μέσω του server. Οι τοπικές anti-virus scanning εφαρμογές μπορεί να απενεργοποιηθούν κατά την διάρκεια back-ups εάν όμως συνεχίζεται η λειτουργία μίας εξωτερικής anti-virus εφαρμογής κατά τη διάρκεια που υλοποιείται το back-up.

Anti-spyware

Όλοι οι servers πρέπει να έχουν εγκατεστημένη μία εφαρμογή anti-virus η οποία παρέχει συνεχή προστασία στο σύστημα στην περίπτωση που παρουσιαστεί μία από τις ακόλουθες περιπτώσεις

Οποιοδήποτε σύστημα όπου μη-τεχνικοί ή μη εξουσιοδοτημένοι χρήστες έχουν συνδεθεί μέσω απομακρυσμένης σύνδεσης και για οποιαδήποτε outbound πρόσβαση που επιτρέπεται στο διαδίκτυο.

Οποιοδήποτε σύστημα όπου μη-τεχνικοί ή μη εξουσιοδοτημένοι χρήστες έχουν την ικανότητα να εγκαταστήσουν λογισμικό με δικοί τους πρωτοβουλία

Αξιοσημείωτες εξαιρέσεις

Μία εξαίρεση στα παραπάνω πρότυπα είναι στην περίπτωση που εφαρμόζονται οι ακόλουθες συνθήκες στο σύστημα

Το σύστημα είναι ένας SQL server

Το σύστημα χρησιμοποιείται αποκλειστικά ως mail server

Το λειτουργικό σύστημα δεν βασίζεται στα Windows

Επιβολή

Αν βρεθεί υπάλληλος που έχει παραβιάσει αυτήν την πολιτική, υπόκειται σε πειθαρχική πράξη μέχρι και σε τερματισμό της σύμβασης εργασίας.

ΚΕΦΑΛΑΙΟ 3
ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.1 ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

Σύμφωνα με τις κατευθυντήριες γραμμές ασφάλειας του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) και της Ευρωπαϊκής Ένωσης, η ασφάλεια των τηλεπικοινωνιακών δικτύων και πληροφοριών αποτελεί ευθύνη όλων των ενδιαφερόμενων μερών. Με άλλα λόγια, τα μέτρα που λαμβάνει η Πολιτεία και οι εταιρείες παροχής υπηρεσιών επικοινωνιών για την ασφάλεια των επικοινωνιών είναι απαραίτητο να συμπληρώνονται από την εφαρμογή κανόνων ασφαλείας από τους ίδιους τους χρήστες και συνδρομητές ηλεκτρονικών επικοινωνιών για τη δική τους πρωτίστως προστασία. Η πλήρης επίγνωση των κινδύνων και των διαθέσιμων μέσων ασφαλείας σε προσωπικό επίπεδο αποτελεί την πρώτη γραμμή άμυνας για την ασφάλεια συστημάτων, πληροφοριών και δικτύων. Κρίσιμο ρόλο στην προστασία του απορρήτου των επικοινωνιών διαδραματίζουν :

- Η Πολιτεία

Η Πολιτεία θεσπίζει το κατάλληλο θεσμικό πλαίσιο, το οποίο προσαρμόζει στις εκάστοτε τεχνολογικές εξελίξεις, για την προάσπιση του απορρήτου των επικοινωνιών. Στα πλαίσια του παραπάνω θεσμικού πλαισίου δημιουργήθηκε η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), κατ' εντολή
του άρθρου 19 παρ. 2 του Συντάγματος.

- Οι εταιρείες παροχής υπηρεσιών επικοινωνιών

(ηλεκτρονικών επικοινωνιών, παροχής δικτύου & ταχυδρομικών υπηρεσιών) Οι εταιρείες αυτές οφείλουν να προστατεύουν το απόρρητο των επικοινωνιών για τις υπηρεσίες που παρέχουν και να ενημερώνουν τους χρήστες /συνδρομητές τους για πιθανούς κινδύνους και τα ενδεικνυόμενα μέτρα αυτοπροστασίας.

- Οι χρήστες και οι συνδρομητές ηλεκτρονικών επικοινωνιών

Οι χρήστες και οι συνδρομητές ηλεκτρονικών επικοινωνιών πρέπει να λαμβάνουν τα απαραίτητα μέτρα αυτοπροστασίας.

Τι θεωρείται απόρρητο στις επικοινωνίες;

Μερικά βασικά στοιχεία που καλύπτει η νομοθεσία περί απορρήτου των επικοινωνιών είναι:

Για τις ηλεκτρονικές επικοινωνίες

• Το περιεχόμενο της επικοινωνίας (φωνή, εικόνα, δεδομένα)
• Η ταυτότητα του καλούντος και του καλουμένου
• Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου
• Τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός)

Για τις ταχυδρομικές υπηρεσίες

• Το περιεχόμενο της αλληλογραφίας
• Ο αποστολέας
• Ο παραλήπτης

Ποιες είναι οι περιοχές ευθύνης παρόχων και χρηστών/συνδρομητών ηλεκτρονικών επικοινωνιών ;

Οι πάροχοι ηλεκτρονικών επικοινωνιών είναι υπεύθυνοι για τη διασφάλιση του απορρήτου των επικοινωνιών στο δημόσιο τηλεπικοινωνιακό δίκτυο (δίκτυα κορμού και πρόσβασης). Οι συνδρομητές και οι χρήστες οφείλουν να μεριμνούν για το απόρρητο της επικοινωνίας στα ιδιωτικά δίκτυα τα οποία περιλαμβάνουν τις καλωδιώσεις στα κτίρια, τα εσωτερικά δίκτυα (LAN) και τις τερματικές συσκευές (σταθερά ενσύρματα και ασύρματα τηλέφωνα, κινητά τηλέφωνα, fax, προσωπικοί υπολογιστές). Ακολουθούν μέτρα αυτοπροστασίας για τις πλέον διαδεδομένες μορφές επικοινωνίας.

Αυτοπροστασία χρηστών/ συνδρομητών για τις σταθερές και κινητές επικοινωνίες

1. Σταθερές Επικοινωνίες

- Για να προστατεύσετε το απόρρητο της επικοινωνίας σας μέσω σταθερών τερματικών συσκευών (σταθερών τηλεφώνων) μπορείτε να λάβετε βασικά μέτρα ασφάλειας όπως:
- Να μην είναι δυνατή η πρόσβαση στη τηλεφωνική σας συσκευή ή στο χώρο που βρίσκεται η συσκευή, από ανθρώπους που δε γνωρίζετε.
- Αν χρησιμοποιείτε ασύρματη συσκευή (DECT), θα πρέπει να ελέγχετε αρχικά εάν είναι πιστοποιημένη αναφορικά με τις χρησιμοποιούμενες συχνότητες για το σκοπό αυτό. Επιπλέον, δε θα πρέπει να γίνεται χρήση της συσκευής σε πολύ απομακρυσμένα σημεία από το σταθμό βάσης διότι είναι πιθανό να υπάρχουν παρεμβολές από παρόμοιες ασύρματες συσκευές γειτονικών οικιών και να γίνεται συνακρόαση του περιεχομένου των συνομιλιών σας.
- Το κουτί διανομής (box) στις κατοικίες και ο πίνακας διανομής (εσκαλίτ), στις πολυκατοικίες στα οποία τερματίζει το δημόσιο τηλεπικοινωνιακό δίκτυο, θα πρέπει να είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα. Επίσης, θα πρέπει να ελέγχετε τα εν λόγω σημεία σε τακτά χρονικά διαστήματα για πιθανή παραβίασή τους.

- Να ελέγχετε τα τμήματα της εσωτερικής καλωδίωσης από τον πίνακα διανομής μέχρι την τηλεφωνική συσκευή, τα οποία δεν είναι επαρκώς προστατευμένα, για πιθανή παραβίασή τους.
- Πολλές συσκευές fax κρατούν στη μνήμη τους το κείμενο που έχετε στείλει. Αν δεν φροντίσετε να το σβήσετε από τη μνήμη, ενδεχομένως, κάποιος τρίτος να το τυπώσει και να το διαβάσει.

2. Κινητές Επικοινωνίες

Για να προστατεύσετε την επικοινωνία μέσω του κινητού σας τηλεφώνου μπορείτε να λάβετε κάποια βασικά και απλά προληπτικά μέτρα ασφαλείας, όπως:

- Να μην ανακοινώνετε τον αριθμό PIN σε τρίτους. Αλλάξτε τον αρχικό αριθμό PIN και χρησιμοποιήστε κάποιον καινούργιο με όσο το δυνατόν πιο δύσκολο συνδυασμό.
- Επειδή το κινητό τηλέφωνο περιέχει πολλές πληροφορίες και προσωπικά σας στοιχεία, μην το αφήνετε εκτεθειμένο και προστατεύστε το από το ενδεχόμενο κλοπής.
- Όταν χρησιμοποιείτε την τεχνολογία Bluetooth να έχετε ενεργοποιημένη τη δυνατότητα σύνδεσης με κωδικό ασφαλείας. Το Bluetooth πρέπει να παραμένει απενεργοποιημένο ή σε κατάσταση μη εντοπισμού από άλλες συσκευές (invisible mode), όταν δε χρησιμοποιείται.
- Να μην εγκαθιστάτε εφαρμογές και να μην αποθηκεύετε άγνωστα αρχεία που δέχεστε μέσω Bluetooth.
- Να μην εγκαθιστάτε εφαρμογές και να μην αποθηκεύετε άγνωστα επισυναπτόμενα αρχεία που λαμβάνετε μέσω μηνυμάτων MMS.
- Να μην αποθηκεύετε αρχεία ή εφαρμογές στο κινητό σας τηλέφωνο από άγνωστες ιστοσελίδες WAP ή Internet.
- Να μην ανοίγετε ή αποθηκεύετε αρχεία, που λαμβάνετε στο κινητό σας μέσω e-mail από αποστολείς που δε γνωρίζετε.
- Να ελέγχετε συστηματικά τους λογαριασμούς σας για τυχόν χρεώσεις σε μηνύματα SMS/MMS που δεν έχετε στείλει ή χρεώσεις για δεδομένα (GPRS/3GWAP, GPRS/3GInternet) που δεν έχετε «κατεβάσει».

Αυτοπροστασία χρηστών στο διαδίκτυο

Πρακτικές συμβουλές για την προστασία της επικοινωνίας σας μέσω διαδικτύου περιλαμβάνουν:

- Να χρησιμοποιείτε λογισμικό ανίχνευσης και αντιμετώπισης ιών και spyware (antivirus & anti-spyware software) και να το ενημερώνετε τακτικά
- Να διατηρείτε ενημερωμένο το λειτουργικό σύστημα του υπολογιστή και ειδικότερα τα προγράμματα περιήγησης στο διαδίκτυο.
- Να εγκαταστήσετε και να χρησιμοποιείτε τείχος προστασίας (firewall).
- Να επιβεβαιώνετε ότι χρησιμοποιείτε μια ασφαλή σύνδεση όταν στέλνετε ευαίσθητες προσωπικές πληροφορίες μέσω του web. Αυτό φαίνεται από το

εικονίδιο του κλειδωμένου λουκέτου, ενώ η διεύθυνση που συνδέεστε πρέπει να αρχίζει με https://

- Να επιβεβαιώνετε ότι οι ρυθμίσεις ασφάλειας του προγράμματος πλοήγησης στον Παγκόσμιο Ιστό (Web) είναι επαρκώς υψηλές.
- Να χρησιμοποιείτε κωδικούς ασφαλείας για την προστασία της πρόσβασης στον υπολογιστή σας και της προσπέλασης δεδομένων τα οποία έχετε αποθηκεύσει στον υπολογιστή σας ή σε διαδικτυακούς λογαριασμούς.
- Οι κωδικοί ασφαλείας πρέπει να ανανεώνονται συχνά και να είναι ισχυροί, δηλαδή να είναι δύσκολο κάποιος να τους μαντέψει ή να τους «σπάσει».
- Μην αποκαλύπτετε ή μοιράζεστε τους κωδικούς ασφαλείας σας με κανέναν!
- Μην ανοίγετε συνημμένα αρχεία που έχετε λάβει μέσω ηλεκτρονικού ταχυδρομείου από αποστολείς που δε γνωρίζετε. Να είστε όμως ιδιαίτερα επιφυλακτικοί και με συνημμένα αρχεία τα οποία λαμβάνετε από γνωστούς σας αποστολείς.
- Μη χρησιμοποιείτε τη βασική σας διεύθυνση ηλεκτρονικού ταχυδρομείου για ηλεκτρονικές
- αγορές, συμμετοχή σε δωμάτια συζητήσεων(chat rooms), διαγωνισμούς, συμπλήρωση ερωτηματολογίων, και άλλα. Για τέτοιες u960 περιπτώσεις μπορεί να χρησιμοποιείτε κάποια ιδιωτική διεύθυνση που μπορεί να καταργηθεί χωρίς άλλο κόστος.
- Να είστε ιδιαίτερα επιφυλακτικοί κατά τη χρήση προγραμμάτων άμεσων μηνυμάτων (instant messengers). Να μην αποκαλύπτετε ποτέ ευαίσθητα προσωπικά δεδομένα σε άγνωστους και να μην ανοίγετε αρχεία που λαμβάνετε από άτομα που δε γνωρίζετε.
- Να είστε ιδιαίτερα επιφυλακτικοί όταν λαμβάνετε μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν στοιχεία και πρέπει να αποφεύγετε να απαντάτε σε αυτά, εκτός εάν είστε απόλυτα σίγουροι ότι προέρχονται από έμπιστα πρόσωπα. Ειδικότερα, σχετικά με την περίπτωση ασύρματης πρόσβασης στο Διαδίκτυο, προτείνονται τα εξής μέτρα:

- Να ενεργοποιείτε τους μηχανισμούς κρυπτογράφησης στον Ασύρματο Δρομολογητή που διαθέτετε και να το διαμορφώνετε κατάλληλα με βάση τις ισχυρότερες ρυθμίσεις.
- Να απενεργοποιείτε το μηχανισμό «identifier broadcasting».
- Να αλλάξετε τον προσδιοριστή SSID από την τιμή που έχει θέσει ο κατασκευαστής.
- Να αλλάξετε τον κωδικό ασφαλείας του Ασύρματου Δρομολογητή από την τιμή που έχει θέσει ο κατασκευαστής.
- Να ρυθμίσετε το ασύρματο δίκτυο έτσι ώστε να δέχεται συνδέσεις μόνο από συγκεκριμένους υπολογιστές.
- Να απενεργοποιείτε εντελώς το ασύρματο δίκτυο όταν δεν το χρησιμοποιείτε. Μη θεωρείτε δεδομένο ότι τα δημόσια ασύρματα σημεία πρόσβασης έχουν ασφαλείς ρυθμίσεις. Να αποφεύγετε την ανταλλαγή ευαίσθητης προσωπικής πληροφορίας σε αυτές τις περιπτώσεις.

Τι είναι η Α.Δ.Α.Ε. και ποιος ο σκοπός της;

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών είναι μια από τις συνταγματικά καθιερωμένες Ανεξάρτητες Αρχές με διοικητική αυτοτέλεια, η οποία συστάθηκε ως ειδικός εποπτεύοντας φορέας για να προστατεύσει το απόρρητο της επικοινωνίας. Η Α.Δ.Α.Ε. στο πλαίσιο των αρμοδιοτήτων της, οι οποίες περιγράφονται παρακάτω, έχει σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο. Επιπλέον, στις αρμοδιότητές της, περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου που προβλέπονται από το νόμο.

Ποιες είναι οι σημαντικότερες αρμοδιότητες της Α.Δ.Α.Ε.;

Η Α.Δ.Α.Ε. για την εκπλήρωση του σκοπού της σύμφωνα με το νόμο μπορεί:

- Να εκδίδει κανονισμούς, να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων προστασίας του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.
- Να διενεργεί αυτεπάγγελτα ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.
- Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.

Στα πλαίσια αυτά η Αρχή έχει εκδώσει κανονισμούς οι οποίοι προβλέπουν πολιτικές ασφάλειας που θα πρέπει να εφαρμόζουν οι εταιρείες παροχής επικοινωνιακών υπηρεσιών και παρακολουθεί με ελέγχους την εφαρμογή τους για την προστασία του απορρήτου των επικοινωνιών. Επιπλέον, οι χρήστες και οι συνδρομητές ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών μπορούν να υποβάλλουν καταγγελίες στην Αρχή, όταν αντιληφθούν ότι υπάρχει παραβίαση του απορρήτου των επικοινωνιών τους. Η Α.Δ.Α.Ε. διερευνά τις καταγγελίες αυτές προκειμένου να διαπιστώσει την πιθανή παραβίαση του απορρήτου και την ευθύνη την οποία φέρει ο εμπλεκόμενος πάροχος τηλεπικοινωνιακών ή ταχυδρομικών υπηρεσιών. Σε περίπτωση που κατά τον έλεγχο της καταγγελίας διαπιστωθεί παραβίαση του απορρήτου, η Α.Δ.Α.Ε. μπορεί να επιβάλει διοικητικά πρόστιμα, να κατασχέσει τα μέσα με τα οποία πραγματοποιείται η παραβίαση αυτή, ενώ παράλληλα καταστρέφει τις πληροφορίες, τα δεδομένα ή τα στοιχεία που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

Πηγές ενημέρωσης για το απόρρητο των επικοινωνιών

Ηλεκτρονικές διευθύνσεις για περισσότερες πληροφορίες σχετικά με το απόρρητο παρέχονται στη διεύθυνση : http://www.adae.gr

3.2 ΝΟΜΟΙ ΚΑΙ ΔΙΑΤΑΞΕΙΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ηλεκτρονική υπογραφή: Το νομικό πλαίσιο στην Ελλάδα

Η ηλεκτρονική υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσης του περιεχομένου των ηλεκτρονικών εγγράφων. Έχει δηλαδή μία επιβεβαιωτική λειτουργία, βοηθώντας τον παραλήπτη να βεβαιωθεί ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις.

Τι είναι η ηλεκτρονική υπογραφή;

Με τον όρο "ηλεκτρονική ή ψηφιακή υπογραφή" εννοούμε δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.

Ποιους όρους πρέπει να πληρεί η ηλεκτρονική υπογραφή;

Η ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή πρέπει να πληροί τους εξής όρους:
α) Να συνδέεται μονοσήμαντα με τον υπογράφοντα.
β) Να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος.
γ) Να δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο.
δ) Να συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

Η ηλεκτρονική υπογραφή έχει την ίδια ισχύ με την ιδιόχειρη υπογραφή;

Σύμφωνα με το άρθρο 3 του Προεδρικού Διατάγματος 150/2001, η ψηφιακή υπογραφή εξομοιώνεται με την ιδιόχειρη. Η 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.

Τι είναι η κρυπτογραφία και που βοηθά;

Με τον όρο Κρυπτογραφία εννοούμε τη μετατροπή αρχικού κειμένου σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο) με τη χρήση κάποιας μαθηματικής συνάρτησης από τον αποστολέα. Ο παραλήπτης του μηνύματος αποκρυπτογραφεί το κείμενο στην αρχική του μορφή έχοντας γνώση του τρόπου κρυπτογράφησης. Η κρυπτογραφία βοηθά στο να παραμείνει εμπιστευτικό το μήνυμα και να μη διαβάζεται από ανεπιθύμητους τρίτους. Η κρυπτογράφηση βασίζεται στη χρήση ενός "κλειδιού", δηλαδή ενός μαθηματικού κώδικα.

Πώς ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα;

Με την ηλεκτρονική υπογραφή ο παραλήπτης βεβαιώνεται ότι το μήνυμα που έλαβε είναι ακέραιο, αλλά είναι απαραίτητο να είναι σίγουρος και για την ταυτότητα του αποστολέα. Αυτή διασφαλίζεται μέσω των ιδιωτικών και δημόσιων κλειδιών, τα οποία επαληθεύουν την υπογραφή του αποστολέα.

Πώς εφοδιάζονται ο αποστολέας και ο παραλήπτης τα δημόσια και ιδιωτικά κλειδιά;

Ο αποστολέας και ο παραλήπτης εφοδιάζονται τα κλειδιά που χρειάζονται για την κρυπτογράφηση και επαλήθευση της ηλεκτρονικής υπογραφής από Παρόχους Υπηρεσιών Πιστοποίησης (ΠΥΠ). Οι ΠΥΠ είναι οργανισμοί που παρέχουν την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Εκδίδουν δηλαδή ένα πιστοποιητικό (ένα ηλεκτρονικό αρχείο) στο οποίο πιστοποιούν την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Πώς προστατεύεται η αξιοπιστία της δημιουργίας ηλεκτρονικής υπογραφής;

Η δημιουργία ηλεκτρονικής υπογραφής υλοποιείται μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, που εξασφαλίζουν ότι τα δεδομένα που χρησιμοποιούνται προς παραγωγή υπογραφών:
α) υπάρχουν μόνο μία φορά και ότι το απόρρητο είναι διασφαλισμένο.
β) δεν μπορούν να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας.
γ) μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρήσης από τρίτους.

Τι πρέπει να περιλαμβάνουν τα πιστοποιητικά των ΠΥΠ ώστε να είναι έγκυρα (αναγνωρισμένα πιστοποιητικά);

Τα αναγνωρισμένα πιστοποιητικά πρέπει σύμφωνα με το Παράρτημα Ι του Π.Δ. 150/2001 να περιλαμβάνουν:
α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό.
β) τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης καθώς και το κράτος στο οποίο είναι εγκατεστημένος.
γ) το όνομα του υπογράφοντος.
δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με το σκοπό για τον οποίο προορίζεται το πιστοποιητικό.
ε) δεδομένα επαλήθευσης υπογραφής, που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος.
στ) ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού.
ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού.
η) την προηγμένη ηλεκτρονική υπογραφή του παρόχου των υπηρεσιών πιστοποίησης που το εκδίδει.
θ) τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού.
ι) τυχόν όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να

χρησιμοποιηθεί.

Ποιες είναι οι υποχρεώσεις των ΠΥΠ;

Οι πάροχοι υπηρεσιών πιστοποίησης πρέπει:
α) να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης.
β) να διασφαλίζουν την παροχή ασφαλών και άμεσων υπηρεσιών καταλόγου και ανάκλησης.
γ) να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορούν να προσδιοριστούν επακριβώς.
δ) να προβαίνουν σε επαλήθευση της ταυτότητας του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό.
ε) να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών, και σε περίπτωση που ο πάροχος πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής, να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων.
στ) να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν σε ένα αναγνωρισμένο πιστοποιητικό για χρονικό διάστημα τριάντα (30) ετών, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες.
ζ) να μην αποθηκεύουν ή αντιγράφουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο ΠΥΠ παρείχε υπηρεσίες διαχείρισης κλειδιών.
η) προτού συνάψουν συμβατική σχέση με πρόσωπο που ζητά πιστοποιητικό από αυτούς, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρήσης του πιστοποιητικού.
θ) να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή.

Ποιος ελέγχει τους ΠΥΠ ώστε να διασφαλίζεται η συμμόρφωσή τους;

Οι εταιρίες που παρέχουν υπηρεσίες πιστοποίησης αλλά και βεβαιώσεις για την ασφάλεια της ηλεκτρονικής υπογραφής ελέγχονται από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ). Η Ε.Ε.Τ.Τ. έχει την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης, και σε περίπτωση που πάροχος υπηρεσιών πιστοποίησης ενεργεί ως διαπιστευμένος χωρίς να είναι, του επιβάλλει πρόστιμο από εξήντα χιλιάδες (60.000) έως τριακόσιες χιλιάδες (300.000) ευρώ.

Νομοθεσία

- Προεδρικό Διάταγμα 150/2001 Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
- Απόφαση ΕΕΤΤ 295/63/2003 Κανονισμός Ορισμού Φορέων για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων και Φορέων για τη Διαπίστωση Συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα Κριτήρια Εθελοντικής Διαπίστευσης.

- Απόφαση ΕΕΤΤ 295/64/2003 Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων.

Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφέςΤο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης, Έχοντας υπόψη: τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας, και ιδίως το άρθρο 47 παράγραφος 2 και τα άρθρα 55 και 95, την πρόταση της Επιτροπής(1), τη γνώμη της Οικονομικής και Κοινωνικής Επιτροπής(2), της γνώμη της Επιτροπής των Περιφερειών(3), Αποφασίζοντας σύμφωνα με τη διαδικασία του άρθρου 251 της συνθήκης(4), Εκτιμώντας τα ακόλουθα:

1. στις 16 Απριλίου 1997, η Επιτροπή υπέβαλε στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών ανακοίνωση σχετικά με ευρωπαϊκή πρωτοβουλία στο ηλεκτρονικό εμπόριο·

2. στις 8 Οκτωβρίου 1997 η Επιτροπή υπέβαλε στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών ανακοίνωση για την κατοχύρωση της ασφάλειας και εμπιστοσύνης στις ηλεκτρονικές επικοινωνίες - προς ένα ευρωπαϊκό πλαίσιο για ψηφιακές υπογραφές και κρυπτοθέτηση·

3. την 1η Δεκεμβρίου 1997, το Συμβούλιο κάλεσε την Επιτροπή να υποβάλει το ταχύτερο δυνατό πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις ψηφιακές υπογραφές·

4. για τις ηλεκτρονικές επικοινωνίες και το εμπόριο απαιτούνται "ηλεκτρονικές υπογραφές" και συναφείς υπηρεσίες που παρέχουν τη δυνατότητα απόδειξης της γνησιότητας των δεδομένων· η ύπαρξη αποκλινόντων κανόνων όσον αφορά τη νομική αναγνώριση των ψηφιακών υπογραφών και διαπίστευση "παροχών υπηρεσιών πιστοποίησης" στα κράτη μέλη ενδέχεται να αποτελέσει σημαντικό φραγμό για τη χρήση των ηλεκτρονικών επικοινωνιών και του ηλεκτρονικού εμπορίου· από την άλλη πλευρά, ένα σαφές κοινοτικό πλαίσιο σχετικά με τις προϋποθέσεις που θα εφαρμόζονται στις ηλεκτρονικές υπογραφές θα ενισχύσει την εμπιστοσύνη στις νέες τεχνολογίες και θα συμβάλει στη γενική αποδοχή τους· οι νομοθεσίες στα κράτη μέλη δεν θα πρέπει να εμποδίζουν την ελεύθερη κυκλοφορία αγαθών και υπηρεσιών στην εσωτερική αγορά·

5. θα πρέπει να προαχθεί η λειτουργικότητα των προϊόντων ηλεκτρονικής υπογραφής· σύμφωνα με το άρθρο 14 της συνθήκης, η εσωτερική αγορά περιλαμβάνει ένα χώρο χωρίς εσωτερικά σύνορα μέσα στον οποίο εξασφαλίζεται η ελεύθερη κυκλοφορία των εμπορευμάτων· πρέπει να ικανοποιηθούν βασικές απαιτήσεις που αναφέρονται σε προϊόντα ηλεκτρονικής υπογραφής για τη διασφάλιση της ελεύθερης κυκλοφορίας εντός της εσωτερικής αγοράς και για την οικοδόμηση εμπιστοσύνης στις ηλεκτρονικές υπογραφές, με την επιφύλαξη του κανονισμού (ΕΚ) αριθ. 3381/94 του Συμβουλίου, της 19ης Δεκεμβρίου 1994, περί κοινοτικού καθεστώτος ελέγχου της εξαγωγής αγαθών διπλής χρήσης(5) και της απόφασης 94/942/ΚΕΠΠΑ του Συμβουλίου, της 19ης Δεκεμβρίου 1994, σχετικά με την κοινή δράση που ενεκρίθη από το Συμβούλιο σχετικά με τον έλεγχο της εξαγωγής αγαθών διπλής χρήσης·

6. η παρούσα οδηγία δεν εναρμονίζει την παροχή υπηρεσιών όσον αφορά το απόρρητο

των πληροφοριών όταν καλύπτονται από εθνικές διατάξεις περί δημόσιας τάξης ή δημόσιας ασφάλειας·

7. η εσωτερική αγορά εξασφαλίζει την ελεύθερη κυκλοφορία των προσώπων, η οποία έχει ως συνέπεια ότι οι πολίτες και οι κάτοικοι της Ευρωπαϊκής Ένωσης, έρχονται όλο και συχνότερα αντιμέτωποι με αρχές κρατών μελών διαφορετικών εκείνου στο οποίο διαμένουν· η ηλεκτρονική επικοινωνία θα μπορούσε να αποδειχθεί εξαιρετικά χρήσιμη από αυτή την άποψη·

8. η ταχεία τεχνολογική ανάπτυξη και ο παγκόσμιος χαρακτήρας του Internet επιβάλλουν προσέγγιση που θα είναι ανοικτή σε διάφορες τεχνολογίες και υπηρεσίες ηλεκτρονικής αναγνώρισης της γνησιότητας δεδομένων·

9. οι ηλεκτρονικές υπογραφές θα χρησιμοποιούνται σε πολλές διαφορετικές συνθήκες και εφαρμογές, έχοντας ως αποτέλεσμα ευρύ φάσμα νέων υπηρεσιών και προϊόντων που θα συνδέονται με ή θα χρησιμοποιούν ηλεκτρονικές υπογραφές· ο ορισμός αυτών των προϊόντων και υπηρεσιών δεν θα πρέπει να περιοριστεί στην έκδοση και διαχείριση πιστοποιητικών αλλά θα πρέπει να συμπεριλαμβάνει όλες τις υπηρεσίες και τα προϊόντα που χρησιμοποιούν ή σχετίζονται με ηλεκτρονικές υπογραφές, όπως οι υπηρεσίες καταχώρησης, οι υπηρεσίες χρονοσήμανσης, οι υπηρεσίες καταλόγου, οι υπηρεσίες πληροφορικής ή οι υπηρεσίες μελετών σχετικά με τις ηλεκτρονικές υπογραφές·

10. η εσωτερική αγορά επιτρέπει στους παρόχους υπηρεσιών πιστοποίησης την ανάπτυξη των διασυνοριακών δραστηριοτήτων τους αποβλέποντας στην αύξηση της ανταγωνιστικότητάς τους, προσφέροντας έτσι στους καταναλωτές και τις επιχειρήσεις νέες ευκαιρίες ασφαλούς ανταλλαγής πληροφοριών και ηλεκτρονικών συναλλαγών, ανεξαρτήτως συνόρων· για την τόνωση της παροχής υπηρεσιών πιστοποίησης μέσω ανοικτών δικτύων σε κοινοτική κλίμακα, θα πρέπει οι πάροχοι υπηρεσιών πιστοποίησης να είναι ελεύθεροι να παρέχουν τις υπηρεσίες τους χωρίς προηγούμενη έγκριση· ως προηγούμενη έγκριση νοείται, όχι μόνο κάθε άδεια για την οποία απαιτείται απόφαση των εθνικών αρχών προτού επιτραπεί στον ενδιαφερόμενο να παρέχει υπηρεσίες πιστοποίησης, αλλά και κάθε άλλο μέτρο ισοδυνάμου αποτελέσματος·

11. οι μηχανισμοί εθελοντικής διαπίστευσης που αποσκοπούν σε βελτιωμένο επίπεδο παροχής υπηρεσιών ενδέχεται να προσφέρουν στους παρόχους υπηρεσιών πιστοποίησης το κατάλληλο πλαίσιο για την περαιτέρω ανάπτυξη των υπηρεσιών τους στα επίπεδα εμπιστοσύνης, ασφάλειας και ποιότητας που απαιτούνται από την εξελισσόμενη αγορά· αυτοί οι μηχανισμοί θα πρέπει να ενθαρρύνουν την ανάπτυξη βέλτιστης πρακτικής μεταξύ των παρόχων υπηρεσιών πιστοποίησης· οι πάροχοι υπηρεσιών πιστοποίησης θα πρέπει να είναι ελεύθεροι να επιλέγουν και να επωφελούνται από τους εν λόγω μηχανισμούς διαπίστευσης·

12. οι υπηρεσίες πιστοποίησης μπορούν να παρέχονται είτε από δημόσιο φορέα είτε από νομικό ή φυσικό πρόσωπο, εφόσον είναι εγκατεστημένο σύμφωνα με το εθνικό δίκαιο· τα κράτη μέλη δεν θα πρέπει να απαγορεύουν στους παρόχους υπηρεσιών πιστοποίησης να λειτουργούν εκτός των εν λόγω μηχανισμών εθελοντικής διαπίστευσης· θα πρέπει να διασφαλίζεται ότι οι μηχανισμοί εθελοντικής διαπίστευσης δεν περιορίζουν τον ανταγωνισμό στις υπηρεσίες πιστοποίησης·

13. τα κράτη μέλη μπορούν να αποφασίζουν με ποιό τρόπο θα εξασφαλίσουν τον έλεγχο

της τήρησης των διατάξεων της παρούσας οδηγίας· η παρούσα οδηγία δεν αποκλείει τη θέσπιση συστημάτων ελέγχου βασισμένων στον ιδιωτικό τομέα· η παρούσα οδηγία δεν υποχρεώνει τους παρόχους υπηρεσιών πιστοποίησης να υπόκεινται σε έλεγχο δυνάμει τυχόν μηχανισμών περί διαπίστευσης·

14. είναι σημαντικό να ευρεθεί μία ισορροπία μεταξύ των αναγκών των καταναλωτών και των επιχειρήσεων·

15. το παράρτημα ΙΙΙ καλύπτει απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής ούτως ώστε να εξασφαλιστεί η λειτουργικότητα των προηγμένων ηλεκτρονικών υπογραφών· δεν καλύπτει ολόκληρο το περιβάλλον του συστήματος στο οποίο λειτουργούν οι διατάξεις αυτές· η λειτουργία της εσωτερικής αγοράς υποχρεώνει την Επιτροπή και τα κράτη μέλη να αναλάβουν ταχέως μέτρα για το διορισμό των φορέων που θα αναλάβουν την αξιολόγηση της πιστότητας των ασφαλών διατάξεων υπογραφής με το παράρτημα ΙΙΙ· για να ικανοποιούνται οι ανάγκες της αγοράς η αξιολόγηση της πιστότητας πρέπει να διενεργείται έγκαιρα και αποτελεσματικά·

16. η παρούσα οδηγία συμβάλλει στη χρήση και νομική αναγνώριση των ηλεκτρονικών υπογραφών εντός της Κοινότητας· δεν απαιτείται κανονιστικό πλαίσιο για ηλεκτρονικές υπογραφές που χρησιμοποιούνται αποκλειστικά μέσα σε συστήματα που στηρίζονται σε εθελούσιες συμφωνίες ιδιωτικού δικαίου μεταξύ συγκεκριμένου αριθμού συμμετεχόντων· θα πρέπει να γίνει σεβαστή η ελευθερία των μερών να συμφωνούν μεταξύ τους τους όρους όρους και τις προϋποθέσεις βάσει των οποίων αποδέχονται ηλεκτρονικά υπογεγραμμένα δεδομένα, στο βαθμό που τούτο επιτρέπεται από την εθνική νομοθεσία, θα πρέπει να αναγνωρίζεται η νομική ισχύς των ηλεκτρονικών υπογραφών που χρησιμοποιούνται σε αυτά τα διαστήματα καθώς και η αποδοχή τους ως αποδεικτικών στοιχείων σε νομικές διαδικασίες·

17. η παρούσα οδηγία δεν αποσκοπεί σε εναρμόνιση εθνικών κανόνων που αφορούν το ενοχικό δίκαιο, ιδίως την κατάρτιση και εκτέλεση των συμβάσεων ή άλλες διατυπώσεις μη συμβατικού χαρακτήρα σχετικά με τις υπογραφές· επομένως, οι διατάξεις που αφορούν τις έννομες συνέπειες των ηλεκτρονικών υπογραφών θα πρέπει να ισχύουν με την επιφύλαξη των απαιτήσεων ως προς τον τύπο δυνάμει της εθνικής νομοθεσίας σχετικά με τη σύναψη συμβάσεων ή τους κανόνες που καθορίζουν τον τόπο σύναψης μιας σύμβασης·

18. η αποθήκευση και η αντιγραφή δεδομένων δημιουργίας υπογραφής θα μπορούσε να αποτελέσει απειλή για την νομική ισχύ των ηλεκτρονικών υπογραφών·

19. οι ηλεκτρονικές υπογραφές θα χρησιμοποιούνται στο δημόσιο τομέα στο πλαίσιο εθνικών και κοινοτικών διοικητικών υπηρεσιών και για την επικοινωνία μεταξύ αυτών των υπηρεσιών και των πολιτών και οικονομικών φορέων, π.χ. για τις δημόσιες συμβάσεις, τη φορολογία, την κοινωνική ασφάλιση, την υγεία και την απονομή δικαιοσύνης·

20. η ύπαρξη εναρμονισμένων κριτηρίων όσον αφορά τις έννομες συνέπειες των ηλεκτρονικών υπογραφών θα διαφυλάξει εάν συνεκτικό νομικό πλαίσιο σε ολόκληρη την έκταση της Κοινότητας· στις εθνικές νομοθεσίες προβλέπονται διαφορετικές απαιτήσεις για τη νομική ισχύ των ιδιόχειρων υπογραφών· τα πιστοποιητικά μπορούν να χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας προσώπου που υπογράφει

ηλεκτρονικά· οι προηγούμενες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό στοχεύουν υψηλότερο επίπεδο ασφάλειας· οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και έχουν δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής μπορούν να θεωρηθούν ως νομικά ισοδύναμες προς ιδιόχειρες υπογραφές μόνον εφόσον πληρούνται οι εν λόγω προϋποθέσεις για ιδιόχειρες υπογραφές·

21. ως συμβολή στη γενική αποδοχή των ηλεκτρονικών μεθόδων απόδειξης γνησιότητας πρέπει να διασφαλιστεί η δυνατότητα χρησιμοποίησης των ηλεκτρονικών υπογραφών ως αποδεικτικού στοιχείου σε νομικές διαδικασίες σε όλα τα κράτη μέλη· η νομική αναγνώριση των ηλεκτρονικών υπογραφών θα πρέπει να βασίζεται σε αντικειμενικά κριτήρια και να μη συνδέεται με την εξουσιοδότηση του εμπλεκόμενου παρόχου υπηρεσιών πιστοποίησης· ο καθορισμός των τομέων δικαίου στους οποίους επιτρέπεται η χρήση ηλεκτρονικών εγγράφων και ηλεκτρονικών υπογραφών διέπεται από το εθνικό δίκαιο· η παρούσα οδηγία δεν θίγει την αρμοδιότητα εθνικού δικαστηρίου να αποφασίζει ως προς τη συμμόρφωση με τις απαιτήσεις της οδηγίας και δεν επηρεάζει εθνικούς κανόνες που διέπουν την ελεύθερη εκτίμηση αποδείξεων υπό του δικαστηρίου·

22. οι πάροχοι υπηρεσιών πιστοποίησης που παρέχουν υπηρεσίες πιστοποίησης στο κοινό υπάγονται στους εθνικούς κανόνες περί ευθύνης·

23. για την ανάπτυξη του διεθνούς ηλεκτρονικού εμπορίου απαιτούνται διασυνοριακές ρυθμίσεις με συμμετοχή τρίτων χωρών· προκειμένου να διασφαλισθεί η λειτουργικότητα σε παγκόσμιο επίπεδο, θα μπορούσαν να αποβούν χρήσιμες συμφωνίες με τρίτες χώρες για πολυμερείς ρυθμίσεις όσον αφορά την αμοιβαία αναγνώριση υπηρεσιών πιστοποίησης·

24. για την τόνωση της εμπιστοσύνης των χρηστών στην ηλεκτρονική επικοινωνία και στο ηλεκτρονικό εμπόριο μέσω της διασφάλισης της εμπιστοσύνης των χρηστών, οι πάροχοι υπηρεσιών πιστοποίησης πρέπει να τηρούν τη νομοθεσία περί προστασίας των δεδομένων και της ιδιωτικής ζωής·

25. διατάξεις περί της χρήσης ψευδωνύμων στα πιστοποιητικά δεν θα πρέπει να εμποδίζουν τα κράτη μέλη να ζητούν εξακρίβωση της ταυτότητας των προσώπων σύμφωνα με το κοινοτικό ή το εθνικό δίκαιο·

26. τα αναγκαία μέτρα για την εφαρμογή της παρούσας οδηγίας πρέπει να θεσπισθούν σύμφωνα με την απόφαση 1999/468/ΕΚ του Συμβουλίου, της 28ης Ιουνίου 1999, για τον καθορισμό των όρων άσκησης των εκτελεστικών αρμοδιοτήτων που ανατίθενται στην Επιτροπή(7)·

27. η Επιτροπή θα επανεξετάσει την παρούσα οδηγία δύο έτη μετά την εφαρμογή της, μεταξύ άλλων για να εξασφαλίσει ότι η πρόοδος της τεχνολογίας ή οι αλλαγές των νομικών συνθηκών δεν έχουν δημιουργήσει εμπόδια για την επίτευξη των στόχων που θέτει η παρούσα οδηγία· θα πρέπει να εξετάσει τις συνέπειες των συνδεδεμένων τεχνικών τομέων και να υποβάλει σχετική έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο·

28. σύμφωνα με τι αρχές της επικουρικότητας και της αναλογικότητας που αναφέρονται στο άρθρο 5 της συνθήκης, ο στόχος της δημιουργίας εναρμονισμένου νομοθετικού

πλαισίου για την παροχή ηλεκτρονικών υπογραφών και συναφών υπηρεσιών δεν μπορεί να επιτευχθεί αποτελεσματικά από τα κράτη μέλη και, ως εκ τούτου, είναι δυνατόν, να επιτευχθεί καλύτερα από την Κοινότητα· η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη του εν λόγω στόχου,

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

Άρθρο 1
Πεδίο εφαρμογής
Στόχος της παρούσας οδηγίας είναι να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους. Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς.
Δεν καλύπτει πτυχές που αφορούν τη σύναψη και την ισχύ συμβάσεων ή άλλων νομικών υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή του κοινοτικού δικαίου και δεν θίγει κανόνες και περιορισμούς σχετικά με τη χρήση εγγράφων οι οποίοι περιέχονται στο εθνικό ή κοινοτικό δίκαιο.

Άρθρο 2
Ορισμοί
Για τους σκοπούς της παρούσας οδηγίας νοούνται ως:
1. "ηλεκτρονική υπογραφή": δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας,
2. "προηγμένη ηλεκτρονική υπογραφή": ηλεκτρονική υπογραφή που ανταποκρίνεται στις εξής απαιτήσεις:
α) συνδέεται μονοσήμαντα με τον υπογράφοντα·
β) είναι ικανή να ταυτοποιήσει τον υπογράφοντα·
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 εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.
3. "υπογράφων": φυσικό ή νομικό πρόσωπο που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε για λογαριασμό του είτε εξ ονόματος φυσικού ή νομικού προσώπου ή φορέα που αντιπροσωπεύει,
4. "δεδομένα δημιουργίας υπογραφής": μονοσήμαντα δεδομένα όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής,
5. "διάταξη δημιουργίας υπογραφής": διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής,
6. "ασφαλής διάταξη δημιουργίας υπογραφής": διάταξη δημιουργίας υπογραφής που πληροί τις απαιτήσεις του παραρτήματος ΙΙΙ,
7. "δεδομένα δημιουργίας υπογραφής": δεδομένα, όπως κώδικες ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής,
8. "δεδομένα επαλήθευσης υπογραφής": διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων επαλήθευσης υπογραφής,
9. "πιστοποιητικό": ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο που επιβεβαιώνει την ταυτότητά του,
10. "αναγνωρισμένο πιστοποιητικό": πιστοποιητικό που ανταποκρίνεται στις οριζόμενες

στο παράρτημα Ι απαιτήσεις και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης ο οποίος πληροί τις οριζόμενες στο παράρτημα ΙΙ απαιτήσεις,
11. "πάροχος υπηρεσιών πιστοποίησης": φορέας ή φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές,
12. "προϊόν ηλεκτρονικής υπογραφής": υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται για χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την παροχή υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών,
13. "εθελοντική διαπίστευση": κάθε άδεια, στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσειςς που διέπουν την παροχή υπηρεσιών πιστοποίησης και η οποία χορηγείται κατόπιν αιτήσεως του ενδιαφερόμενου παρόχου υπηρεσιών πιστοποίησης από το δημόσιο ή ιδιωτικό φορέα ο οποίος είναι υπεύθυνος για τον καθορισμό αυτών των δικαιωμάτων και υποχρεώσεων και για τον έλεγχο της τήρησής τους, όταν ο πάροχος των υπηρεσιών πιστοποίησης δεν δικαούται να ασκεί τα δικαιώματα που απορρέουν από την άδεια προτού λάβει την απόφαση του εν λόγω φορέα.

Άρθρο 3
Πρόσβαση στην αγορά
1. Τα κράτη μέλη δεν εξαρτούν την παροχή υπηρεσιών πιστοποίησης από εκ των προτέρων έγκριση.
2. Με την επιφύλαξη των διατάξεων της παραγράφου 1, τα κράτη μέλη δύνανται να διατηρούν μηχανισμούς εθελοντικής διαπίστευσης που αποσκοπούν στην επίτευξη βελτιωμένου επιπέδου παροχής υπηρεσιών πιστοποίησης. Όλες οι προϋποθέσεις που συνδέονται με τους εν λόγω μηχανισμούς πρέπει να είναι αντικειμενικές, διαφανείς, ανάλογες και να μην οδηγούν σε διακρίσεις. Τα κράτη μέλη δεν μπορούν να περιορίζουν τον αριθμό των διαπιστευμένων παρόχων υπηρεσιών πιστοποίησης για λόγους που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.
3. Κάθε κράτος μέλος εξασφαλίζει την καθιέρωση κατάλληλου συστήματος που καθιστά δυνατή την επιτήρηση των εγκατεστημένων στο έδαφός τους παρόχων υπηρεσιών πιστοποίησης οι οποίοι εκδίδουν για το κοινό αναγνωρισμένα πιστοποιητικά.
4. Η συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής προς τις απαιτήσεις του παραρτήματος ΙΙΙ διαπιστώνεται από τους αρμόδιους δημόσιους ή ιδιωτικούς φορείς που ορίζουν τα κράτη μέλη. Η Επιτροπή καθορίζει, σύμφωνα με τη διαδικασία του άρθρου 9, κριτήρια βάσει των οποίων τα κράτη μέλη ορίζουν τους φορείς.
Η υπό των εν λόγω φορέων διαπίστωση της συμμόρφωσης προς τις απαιτήσεις του παραρτήματος ΙΙΙ αναγνωρίζεται από όλα τα κράτη μέλη.
5. Η Επιτροπή δύναται, σύμφωνα με τη διαδικασία του άρθρου 9, να καθορίζει και να δημοσιεύει αριθμούς αναφοράς γενικώς αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων. Τα κράτη μέλη τεκμαίρουν συμμόρφωση με τις απαιτήσεις που καθορίζονται στο στοιχείο στ) του παραρτήματος ΙΙ και στο παράρτημα ΙΙΙ, όταν ένα προϊόν ηλεκτρονικής υπογραφής ανταποκρίνεται στα εν λόγω πρότυπα.
6. Τα κράτη μέλη και η Επιτροπή συνεργάζονται για να προωθήσουν την ανάπτυξη και χρησιμοποίηση των διατάξεων επαλήθευσης υπογραφής, με βάση τις συστάσεις για την ασφαλή επαλήθευση της υπογραφής που προβλέπονται στο παράρτημα ΙV και προς όφελος του καταναλωτή.
7. Τα κράτη μέλη δύνανται να εξαρτούν τη χρήση ηλεκτρονικών υπογραφών στο δημόσιο τομέα από ενδεχόμενες πρόσθετες απαιτήσεις. Οι εν λόγω απαιτήσεις είναι αντικειμενικές, διαφανείς, ανάλογες και δεν οδηγούν σε διακρίσεις, αναφέρονται δε μόνο στα ειδικά χαρακτηριστικά της συγκεκριμένης εφαρμογής. Οι απαιτήσεις αυτές δεν

πρέπει να αποτελούν εμπόδιο στις διασυνοριακές υπηρεσίες για τους πολίτες.

Άρθρο 4
Αρχές της εσωτερικής αγοράς
1. Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει κατ' εφαρμογή της παρούσας οδηγίας για παρόχους υπηρεσιών πιστοποίησης εγκατεστημένους στην επικράτειά του, καθώς και για τις υπηρεσίες που αυτοί παρέχουν. Τα κράτη μέλη δεν μπορούν να περιορίσουν την παροχή υπηρεσιών πιστοποίησης που προέρχονται από άλλο κράτος μέλος στους τομείς που καλύπτονται από την παρούσα οδηγία.
2. Τα κράτη μέλη διασφαλίζουν ότι τα προϊόντα ηλεκτρονικής υπογραφής που συμμορφώνονται με την παρούσα οδηγία επιτρέπεται να κυκλοφορούν ελεύθερα στην εσωτερική αγορά.

Άρθρο 5
Έννομες συνέπειες των ηλεκτρονικών υπογραφών
1. Τα κράτη μέλη διασφαλίζουν ότι οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό κυι οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής:
α) ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με τα δεδομένα σε ηλεκτρονική μορφή κατά τον ίδιο τρόπο που μια ιδιόχειρη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με τα δεδομένα που καταχωρούνται επί χάρτου, και
β) γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες.
2. Τα κράτη μέλη διασφαλίζουν ότι δεν απορρίπτεται η νομική ισχύς και το παραδεκτό μιας ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι: είναι υπό μορφή ηλεκτρονικών δεδομένων, ή δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό, ή δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εξεδόθη από διαπιστευμένο παροχέα υπηρεσιών πιστοποίησης, ή δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Άρθρο 6
Ευθύνη

1. Τα κράτη μέλη διασφαλίζουν τουλάχιστον ότι με την έκδοση πιστοποιητικού ως αναγνωρισμένου πιστοποιητικού στο κοινό ή με την εγγύηση τέτοιου πιστοποιητικού στο κοινό, πάροχος υπηρεσιών πιστοποίησης υπέχει ευθύνη για την προκληθείσα ζημία έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου που ευλόγως βασίζεται στο πιστοποιητικό:
α) όσον αφορά την ακρίβεια, κατά τη στιγμή έκδοσής του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη στο πιστοποιητικό όλων των στοιχείων τα οποία απαιτούνται για ένα αναγνωρισμένο πιστοποιητικό·
β) για τη διαβεβαίωση ότι, κατά το χρόνο έκδοσης του πιστοποιητικού, ο υπογράφων που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό ήταν κάτοχος των δεδομένων δημιουργίας υπογραφής που αντιστοιχούν στα δεδομένα επαλήθευσης υπογραφής που αναφέρονται ή ταυτοποιούνται στο πιστοποιητικό·
γ) για τη διαβεβαίωση ότι τα δεδομένα δημιουργίας υπογραφής και τα δεδομένα επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, στις περιπτώσεις που αμφότερα προέρχονται από τον πάροχο υπηρεσιών πιστοποίησης, εκτός εάν ο πάροχος υπηρεσιών πιστοποίησης αποδείξει ότι δεν ενήργησε αμελώς.
2. Τα κράτη μέλη διασφαλίζουν τουλάχιστον ότι ο πάροχοςς υπηρεσιών πιστοποίησης που εξέδωσε πιστοποιητικό ως ανεγνωρισμένο πιστοποιητικό στο κοινό υπέχει ευθύνη

για τη ζημία που προξενείται σε οιοδήποτε φορέα ή φυσικό πρόσωπο, που ευλόγως βασίζεται στο πιστοποιητικό, λόγω παράλειψής του να καταγράψει την ανάκληση του πιστοποιητικού, εκτός εάν ο πάροχος υπηρεσιών πιστοποίησης αποδείξει ότι δεν ενήργησε αμελώς.
3. Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πιστοποίησης δύναται να αναγράφει σε αναγνωρισμένο πιστοποιητικό περιορισμούς χρήσεως αυτού του πιστοποιητικού, με την προϋπόθεση ότι οι περιορισμοί αυτοί είναι αναγνωρίσιμοι για τους τρίτους. Ο πάροχος υπηρεσιών πιστοποίησης δεν υπέχει ευθύνη για βλάβες που προκύπτουν από χρήση ενός αναγνωρισμένου πιστοποιητικού που υπερβαίνει τους περιορισμούς που αναγράφηκαν σε αυτό.
4. Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πιστοποίησης δύναται να αναγράφει στο αναγνωρισμένο πιστοποιητικό όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί, με την προϋπόθεση ότι τα όρια αυτά είναι αναγνωρίσιμα για τους τρίτους.
Ο πάροχος υπηρεσιών πιστοποίησης δεν ευθύνεται για ζημίες που απορρέουν από την υπέρβαση αυτών των ορίων.
5. Οι διατάξεις των παραγράφων 1 έως 4 ισχύουν με την επιφύλαξη της οδηγίας 93/13/ΕΟΚ του Συμβουλίου, της 13ης Απριλίου 1993, σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές(8).

Άρθρο 7
Διεθνείς πτυχές
1. Τα κράτη μέλη διασφαλίζουν ότι τα πιστοποιητικά που εκδίδονται στο κοινό ως αναγνωρισμένα πιστοποιητικά από πάροχο υπηρεσιών πιστοποίησης, εγκατεστημένο σε τρίτη χώρα, θεωρούνται νομικώς ισοδύναμα με πιστοποιητικά που εκδίδονται από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Κοινότητα εάν:
α) ο πάροχος υπηρεσιών πιστοποίησης πληροί τις απαιτήσεις που καθορίζονται στην παρούσα οδηγία και έχει διαπιστευθεί δυνάμει εθελοντικού μηχανισμού πιστοποίησης, καθιερωμένου σε κράτος μέλος, ή
β) πάροχος υπηρεσιών πιστοποίησης, εγκατεστημένος στην Κοινότητα, ο οποίος πληροί τις απαιτήσεις που καθορίζονται στην παρούσα οδηγία, εγγυάται για το πιστοποιητικό, ή
γ) το πιστοποιητικό παρόχου υπηρεσιών πιστοποίησης αναγνωρίζεται δυνάμει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Κοινότητας και τρίτων χωρών ή διεθνών οργανισμών.

2. Η Επιτροπή, για να διευκολύνει τις διασυνοριακές υπηρεσίες πιστοποίησης με τρίτες χώρες και την αναγνώριση προηγμένων ηλεκτρονικών υπογραφών προερχόμενων από τρίτες χώρες, διατυπώνει προτάσεις για την επίτευξη αποτελεσματικής εφαρμογής προτύπων και διεθνών συμφωνιών που ισχύουν για υπηρεσίες πιστοποίησης. Ειδικότερα, όπου κρίνει απαραίτητο, υποβάλλει προτάσεις προς το Συμβούλιο για την έκδοση κατάλληλων εντολών διαπραγμάτευσης διμερών και πολυμερών συμφωνιών με τρίτες χώρες και διεθνείς οργανισμούς. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία.
3. Οσάκις η Επιτροπή πληροφορείται τυχόν δυσκολίες που συναντούν οι κοινοτικές επιχειρήσεις όσον αφορά την πρόσβαση σε αγορές τρίτων χωρών, δύναται να υποβάλει στο Συμβούλιο, εφόσον παρίσταται ανάγκη, προτάσεις για τη δέουσα εντολή διαπραγμάτευσης αναλόγων δικαιωμάτων των κοινοτικών επιχειρήσεων σε αυτές τις τρίτες χώρες. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία.
Τα μέτρα που λαμβάνονται δυνάμει της παρούσας παραγράφου δεν θίγουν τις υποχρεώσεις της Κοινότητας και των κρατών μελών δυνάμει σχετικών διεθνών συμφωνιών.

Άρθρο 8
Προστασία δεδομένων
1. Τα κράτη μέλη διασφαλίζουν ότι οι πάροχοι υπηρεσιών πιστοποίησης και οι εθνικοί φορείς, αρμόδιοι για πιστοποίηση ή εποπτεία, συμμορφώνονται προς τις απαιτήσεις που καθορίζονται στην οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών(9).
2. Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πιστοποίησης που εκδίδει πιστοποιητικά στο κοινό δύναται να συλλέγει δεδομένα προσωπικού χαρακτήρα μόνο απευθείας από το πρόσωπο το οποίο αφορούν, ή με τη ρητή συγκατάθεσή του, και μόνον στο βαθμό που είναι απαραίτητο για τους σκοπούς έκδοσης και διατήρησης του πιστοποιητικού. Δεν επιτρέπεται συλλογή ή επεξεργασία των δεδομένων για οποιουσδήποτε άλλους σκοπούς χωρίς τη ρητή συναίνεση του εν λόγω προσώπου.
3. Με την επιφύλαξη των εννόμων συνεπειών των ψευδωνύμων δυνάμει της εθνικής νομοθεσίας, τα κράτη μέλη δεν εμποδίζουν τους παρόχους υπηρεσιών πιστοποίησης να αναφέρουν στο πιστοποιητικό ψευδώνυμο αντί του ονόματος του υπογράφοντος.

Άρθρο 9
Επιτροπή
1. Η Επιτροπή επικουρείται από την "επιτροπή ηλεκτρονικής υπογραφής", καλούμενη εφεξής "επιτροπή".
2. Όταν γίνεται αναφορά στην παρούσα παράγραφο, εφαρμόζονται τα άρθρα 4 και 7 της απόφασης 1999/468/ΕΚ, με την επιφύλαξη των διατάξεων του άρθρου 8 της εν λόγω απόφασης.
Η περίοδος που προβλέπεται στο άρθρο 4 παράγραφος 3 της απόφασης 1999/468/ΕΚ είναι τρεις μήνες.
3. Η επιτροπή θεσπίζει τον εσωτερικό κανονισμό της.

Άρθρο 10
Καθήκοντα της επιτροπής
Η επιτροπή διευκρινίζει, σύμφωνα με τη διαδικασία του άρθρου 9 παράγραφος 2, τις απαιτήσεις που ορίζονται στα παραρτήματα της παρούσας οδηγίας, τα κριτήρια που αναφέρονται στο άρθρο 3 παράγραφος 4 και τα γενικώς αναγνωρισμένα πρότυπα για προϊόντα ηλεκτρονικής υπογραφής, που καθορίστηκαν και δημοσιεύθηκαν σύμφωνα με το άρθρο 3 παράγραφος 5.

Άρθρο 11
Κοινοποίηση
1. Τα κράτη μέλη κοινοποιούν στην Επιτροπή και στα λοιπά κράτη μέλη τα ακόλουθα:
α) πληροφορίες σχετικά με εθνικά συστήματα εθελοντικής διαπίστευσης, συμπεριλαμβανομένων όλων των πρόσθετων απαιτήσεων σύμφωνα με το άρθρο 3 παράγραφος 7·
β) ονομασίες και διευθύνσεις των εθνικών φορέων που είναι αρμόδιοι για διαπίστευση και επίβλεψη, καθώς και των φορέων που αναφέρονται στο άρθρο 3 παράγραφος 4·
γ) ονομασίες και διευθύνσεις όλων των διαπιστευμένων εθνικών παρόχων υπηρεσιών πιστοποίησης.
2. Τα κράτη μέλη κοινοποιούν τα ταχύτερο δυνατόν το σύνολο των πληροφοριών που υποβάλλονται βάσει της παραγράφου 1 καθώς και τις σχετικές αλλαγές τους.

Άρθρο 12
Επανεξέταση
1. Η Επιτροπή εξετάζει τη λειτουργία της παρούσας οδηγίας και υποβάλλει σχετική έκθεση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, το αργότερο έως τις 19 Ιουλίου 2003.
2. Στην εξέταση εκτιμάται, μεταξύ άλλων, εάν θα πρέπει να τροποποιηθεί το πεδίο εφαρμογής της παρούσας οδηγίας λαμβανομένων υπόψη των τεχνολογικών, εμπορικών και νομοθετικών εξελίξεων. Στην έκθεση περιλαμβάνεται ιδίως αξιολόγηση, βάσει της κτηθείσας εμπειρίας, πτυχών της εναρμόνισης. Η έκθεση συνοδεύεται, κατά περίπτωση, από νομοθετικές προτάσεις.

Άρθρο 13
Εφαρμογή
1. Τα κράτη μέλη θέτουν σε ισχύ τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν με την παρούσα οδηγία πριν από τις 19 Ιουλίου 2001. Ενημερώνουν αμέσως την Επιτροπή σχετικά.
Οι διατάξεις αυτές, όταν θεσπίζονται από τα κράτη μέλη, αναφέρονται στην παρούσα οδηγία ή συνοδεύονται από την αναφορά αυτή κατά την επίσημη δημοσίευσή τους. Οι λεπτομερείς διατάξεις της αναφοράς αυτής καθορίζονται από τα κράτη μέλη.
2. Τα κράτη μέλη ανακοινώνουν στην Επιτροπή το κείμενο των ουσιωδών διατάξεων του εσωτερικού δικαίου που θεσπίζουν στον τομέα που διέπεται από την παρούσα οδηγία.

Άρθρο 14
Έναρξη ισχύος
Η παρούσα οδηγία αρχίζει να ισχύει την ημέρα της δημοσίευσής της στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων.

Άρθρο 15
Αποδέκτες
Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Βρυξέλλες, 13 Δεκεμβρίου 1999.
Για το Ευρωπαϊκό Κοινοβούλιο
Η Πρόεδρος
N. FONTAINE

Για το Συμβούλιο
Ο Πρόεδρος
S. HASSI

ΠΑΡΑΡΤΗΜΑ I
Όροι ισχύοντες για αναγνωρισμένα πιστοποιητικά
Τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν:
α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό·
β) τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένο·
γ) το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο·
δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό·

ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος·

στ) ένδειξη της έναρξης και τέλος της περιόδου ισχύος του πιστοποιητικού·

ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού·

η) την προηγμένη ηλεκτρονική υπογραφή του παρόχου υπηρεσιών πιστοποίησης που το εκδίδει·

θ) ενδεχομένως, περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και

ι) ενδεχομένως, όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

ΠΑΡΑΡΤΗΜΑ ΙΙ

Όροι ισχύοντες για παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά

Οι πάροχοι υπηρεσιών πιστοποίησης πρέπει:

α) να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης·

β) να διασφαλίζουν την παροχή ασφαλών και άμεσων υπηρεσιών καταλόγου και ανάκλησης·

γ) να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορεί να προσδιοριστεί επακριβώς·

δ) να προβαίνουν, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε επαλήθευση, της ταυτότητας και ενδεχομένως, τυχόν ειδικών χαρακτηριστικών του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό·

ε) να απασχολούν προσωπικό που διαθέτει την εμπειρογνωμοσύνη, την εμπειρία και τα προσόντα που είναι απαραίτητα για τις παρεχόμενες υπηρεσίες, ιδίως ικανότητα σε διαχειριστικό επίπεδο, εμπειρογνωμοσύνη στην τεχνολογία ηλεκτρονικών υπογραφών και εξοικείωση με τις κατάλληλες διαδικασίες ασφαλείας· πρέπει επίσης να χρησιμοποιούν κατάλληλες διοικητικές και διαχειριστικές διαδικασίες οι οποίες να αντιστοιχούν προς αναγνωρισμένα πρότυπα·

στ) να χρησιμοποιούν αξιόπιστα συστήματα και προϊόντα τα οποία προστατεύονται έναντι τροποποίησης και διασφαλίζουν την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά·

ζ) να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών και, σε περίπτωση που ο πάροχος υπηρεσιών πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής, να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων·

η) να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις που καθορίζονται στην οδηγία, ιδίως για την ανάληψη της ευθύνης ζημιών, π.χ. με τη σύναψη κατάλληλης ασφάλισης·

θ) να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο για κατάλληλη χρονική περίοδο, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες. Η καταγραφή αυτή δύναται να πραγματοποιείται με ηλεκτρονικά μέσα·

ι) να μην αποθηκεύουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο πάροχος υπηρεσιών πιστοποίησης παρέσχε υπηρεσίες διαχείρισης κλειδιών·

ια) προτού συνάψουν συμβατική σχέση με πρόσωπο που ζητά πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική του υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις

χρησιμοποίησης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών. Οι πληροφορίες αυτές, οι οποίες δύνανται να διαβιβάζονται ηλεκτρονικώς, πρέπει να παρέχονται εγγράφως, σε εύκολα καταληπτή γλώσσα. Σχετικά αποσπάσματα των πληροφοριών αυτών καθίστανται επίσης προσιτά κατόπιν αιτήματος τρίτων οι οποίοι βασίζονται στο πιστοποιητικό αυτό·

ιβ) να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή, ούτως ώστε:

* μόνον αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις,

* να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών,

* να είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνον στις περιπτώσεις εκείνες για τις οποίες έχει δοθεί η συγκατάθεση του κατόχου, και

* οι τυχόν τεχνικές αλλαγές που θέτουν σε κίνδυνο τις εν λόγω αιτήσεις ασφαλείας να γίνονται εμφανώς αντιληπτές από τον χειριστή.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ

Απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής

1. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν τουλάχιστον, ότι:

α) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ' ουσίαν μόνο μια φορά και ότι το απόρρητο είναι διασφαλισμένο·

β) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας·

γ) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους.

2. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής δεν μεταβάλλουν τα προς υπογραφή δεδομένα ούτε εμποδίζουν την υποβολή των δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής.

ΠΑΡΑΡΤΗΜΑ IV

Συστάσεις για την ασφαλή επαλήθευση της υπογραφής

Κατά τη διαδικασία επαλήθευσης της υπογραφής θα πρέπει να διασφαλίζεται, με εύλογη βεβαιότητα, ότι:

α) τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα·

β) η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με τον ορθό τρόπο·

γ) ο επαληθεύων μπορεί, ενδεχομένως, να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται·

δ) η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία·

ε) το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο·

στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς, και

ζ) μπορούν να εντοπιστούν τροποποιήσεις απτόμενες της ασφάλειας.

Ηλεκτρονικό Έγκλημα: Το νομικό πλαίσιο στην Ελλάδα

Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων.

Οι μορφές του Ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η συνεννόηση μεταξύ των κρατών και η εκπόνηση μιας αναλυτικής και αποτελεσματική στρατηγικής. Ο σκοπός αυτός επετέθη με το Συνέδριο για το Ηλεκτρονικό έγκλημα (Convention on Cybercrime), του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφει στην Βουδαπέστη στις 23.11.2001.
Στη συνθήκη της Βουδαπέστη, που υπέγραψε μεταξύ πολλών άλλων χωρών και η Ελλάδα υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

1. Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.
2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.
3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.
4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνεργεία, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση. Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος.

Στην Ευρωπαϊκή Ένωση ισχύουν:
1. Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.
2. Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.
3. Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.
4. Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν

ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.
5. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.
6. Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.
7. Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.

Στην Ελλάδα ισχύει ο νόμος 2928 του 2001 για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων.

Οι διάφορες μορφές του ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται ξεχωριστά και από άλλα ειδικότερα νομοθετήματα στην Ελλάδα και στην Ευρωπαϊκή Ένωση. Ειδικότερα αναλύονται οι εξής μορφές:

Κυβερνοσφετερισμός – Προστασία των Domain names

Κυβερνοσφετερισμός (cybersquatting) είναι το ηλεκτρονικό αδίκημα κατά το οποίο κάποιος χρήστης του Διαδικτύου για εμπορικούς σκοπούς κατοχυρώνει και χρησιμοποιεί ηλεκτρονική διεύθυνση (domain name) που περιέχει είτε την επωνυμία γνωστών επιχειρήσεων είτε σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νόμιμων δικαιούχων αλλά και αποκλεισμός τους από τη χρήση του Διαδικτύου με την επωνυμία τους.
Η προστασία των domain name παρέχεται ανάλογα με το περιεχόμενο του δεύτερου μέρους τους. Αν τη διαδικτυακή διεύθυνση αποτελεί ένα όνομα, τότε παρέχεται η προστασία των άρθρων 57 και 58 ΑΚ. Αν πρόκειται για εμπορική επωνυμία, δηλαδή ένα όνομα με το οποίο ο έμπορος διεξάγει τις συναλλαγές του ή για διακριτικό τίτλο τότε μαζί με την προστασία του άρθρου 58 ΑΚ παρέχεται και η προστασία του άρθρου 13 του νόμου 146/1914. Το άρθρο 13 του νόμου 1146/1914 εφαρμόζεται και όταν ένα domain name αποτελεί εικονικό κατάστημα που είναι γνωστό και επικρατεί στις ηλεκτρονικές συναλλαγές. Αν η ηλεκτρονική διεύθυνση ταυτίζεται με το σήμα και υπάρχει κίνδυνος σύγχυσης στις συναλλαγές παρέχεται η προστασία των άρθρων 4, 18 και 26 του νόμου 2239/1994 περί σημάτων.

Παράνομη διείσδυση σε δεδομένα (hacking, cracking)- Προστασία του απορρήτου στο Διαδίκτυο

Hacking αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή συστήματα υπολογιστών η οποία καταρχήν δε γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Η/Υ.
Cracking είναι η αλλαγή των κωδίκων πρόσβασης και η άρση της προστασίας των προγραμμάτων, η οποία καθιστά δυνατή την παράνομη αντιγραφή τους.
Η χωρίς δικαίωμα διείσδυση –πρόσβαση σε συστήματα επεξεργασίας δεδομένων έστω και όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το άρθρο 370Γ του Ποινικού

κώδικα. Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Αυτά είναι:
1.Η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών, μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων
2. Πρόταση Κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών.
3. Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό COM/2002/0173 - CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεση μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών

Ιοι- Προστασία των δεδομένων από ιούς

Μια ιδιαίτερα συχνή και επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο διαδίκτυο είναι η αλλοίωση ή διαγραφή των δεδομένων με ιούς. Οι ιοί των υπολογιστών είναι ειδικά προγράμματα που έχουν την ικανότητα να ανατυπώνονται από μόνα τους. Διακρίνονται σε δύο μορφές: στους ιούς των προγραμμάτων και στους ιούς των συστημάτων. Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος. Σε αυτές τις περιπτώσεις εφαρμόζονται τα άρθρα 577 και 578 του ΑΚ. Επίσης γεννά και αδικοπρακτική ευθύνη του δράστη κατά τα άρθρα 914, 919 ΑΚ. Ο υπαίτιος όμως υπέχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 ΠΚ. Στην Ευρωπαϊκή Ένωση υπάρχει η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά και λεπτομερής επεξήγηση της έννοιας του ιού, του τρόπου που λειτουργεί και των τρόπων αντιμετώπισης του. Το νομοθέτημα αυτό δεν έχει ακόμα ψηφιστεί ώστε να ισχύει.

Εγκλήματα κατά της ηθικής και της αξιοπρέπειας-Προστασία ανηλίκων-Προστασία από παράνομο και βλαβερό περιεχόμενο

Παράνομο και βλαβερό περιεχόμενο που θίγει την προσωπικότητα και την ηθική των ατόμων αποτελούν η δυσφήμηση μέσω του διαδικτύου και η διάδοση πορνογραφικού υλικού. Ο προσβληθείς στην προσωπικότητα του από κάποιο μήνυμα που διακινείται στο Διαδίκτυο προστατεύεται από τις διατάξεις 361, 362, 366 και 367 του Π.Κ. Δυσχερέστερο είναι το ζήτημα της διάδοσης πορνογραφικού υλικού στο διαδίκτυο ιδιαίτερα σε σχέση με τους ανηλίκους και την προστασία τους από την έκθεση σε αυτό.
Στην Ευρωπαϊκή Ένωση έχουν ληφθεί και ισχύουν αρκετά μέτρα για την αντιμετώπισης αυτού του είδους εγκληματικότητας.
1. Η Απόφαση του Συμβουλίου με αριθμό 2000/C 8/06 που περιέχει προτροπές του Συμβουλίου προς τα κράτη μέλη και την Επιτροπή ώστε να ληφθούν μέτρα για την προστασία των ανηλίκων στα οπτικοακουστικά μέσα και στο Ιντερνετ,

2. Η Σύσταση με αριθμό 98/560/ΕΚ όπου αναφέρονται οι συστάσεις του Συμβουλίου στα κράτη μέλη για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στις οπτικοακουστικές υπηρεσίες και τις υπηρεσίες πληροφόρησης ,
3. Η Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΥ όπου γίνεται λόγος για τα μέτρα που λαμβάνουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης ώστε οι χρήστες του διαδικτύου να βοηθήσουν στην ποινική δίωξη της παραγωγής, επεξεργασίας, διανομής και κατοχής πορνογραφικού υλικού με θέμα παιδιά,
4. Η Απόφαση του Συμβουλίου με αριθμό 2001/C 213/0301 όπου υπάρχουν οι προτροπές του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη για την προστασία των ανηλίκων σε όλα τα οπτικοακουστικά μέσα και για την προστασία των ανηλίκων στο ψηφιακό περιβάλλον και με την συμμετοχή των γονέων,
5. Η Απόφαση του Συμβουλίου με αριθμό 1999/C 362/06 όπου αναφέρεται ότι τα κράτη μεταξύ τους πρέπει να συνεργάζονται ώστε να διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη ποινικών αδικημάτων που αφορούν την παιδική πορνογραφία στο Ίντερνετ,
6. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 65/02 για την αξιολόγηση του περιεχομένου των βιντεοπαιχνιδιών και των ηλεκτρονικών παιχνιδιών
7. Η Απόφαση 276/1999/ΕΚ για την έγκριση, την διάρκεια, τη χρηματοδότηση και τους στόχους προγράμματος για την προώθηση της ασφαλέστερης χρήσης του Ίντερνετ,
8. Η Απόφαση 1151/2003/ΕΚ που τροποποιεί την απόφαση αριθ. 276/1999/ΕΚ και
9. Η Ανακοίνωση της Επιτροπής COM/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδίκυου (Ιντερνετ) μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα

Ένα ακόμα ζήτημα που τίθεται σχετικά με την χρήση του διαδικτύου από τους ανήλικους είναι η πραγματοποίηση συναλλαγών με ηλεκτρονικά μέσα. Είναι γνωστό ότι οποιαδήποτε συναλλαγή με ανήλικο είναι άκυρη και μπορεί να επισύρει ποινή για τον αντισυμβαλλόμενο εφόσον το περιεχόμενό της δεν απευθύνεται σε παιδία και εφήβους. Στην περίπτωση όμως των ηλεκτρονικών συναλλαγών δεν είναι πάντα δυνατή η εξακρίβωση των στοιχείων του καταναλωτή. Για την προστασία των προμηθευτών που δραστηριοποιούνται μέσω κάποιας ιστοσελίδας είναι απαραίτητη η αναγραφή στους όρους χρήσης του site ότι δεν επιτρέπονται οι συναλλαγές με ανηλίκους και ότι η ιστοσελίδα δεν φέρει καμία ευθύνη.

Προστασία δεδομένων προσωπικού χαρακτήρα

Η συγκέντρωση και επεξεργασία ηλεκτρονικών δεδομένων αντιμετωπίστηκε από πολύ νωρίς ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική και προσωπική σφαίρα. Τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση υπάρχει νομοθεσία που ρυθμίζει τα σχετικά με την επεξεργασίας δεδομένων όπως η Οδηγία 2002/58 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και η Οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού.
Αναλυτική αναφορά για αυτό το θέμα υπάρχει στο θέμα Προσωπικά Δεδομένα.

Απάτη μέσω του Διαδικτύου

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης (ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του (ΠΚ 386Α). Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών .

Spamming

Το μεγαλύτερο πρόβλημα που αφορά στις διαδικτυακές διαφημίσεις είναι το λεγόμενο spamming, δηλαδή η αποστολή πολυάριθμων e-mails με διαφημιστικό περιεχόμενο σε χιλιάδες καταναλωτές-χρήστες του διαδικτύου . Η τακτική αυτή απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι « η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους» καθώς και από άλλα νομοθετήματα. Στην Ελλάδα υπάρχουν πολλά νομοθετήματα για την προστασία των καταναλωτών (βλέπε «Ηλεκτρονικό εμπόριο») αλλά αναφέρονται στα μηνύματα μέσω τηλεφώνου και φαξ κυρίως και μόνο αναλογικά στο ηλεκτρονικό ταχυδρομείο.

Προστασία της Πνευματικής Ιδιοκτησίας

Η εμφάνιση των βάσεων δεδομένων σε συνδυασμό με τη διάδοση του Διαδικτύου έχει κάνει την αντιγραφή και την ηλεκτρονική διάδοση των πνευματικών δημιουργημάτων αποτελεσματική και εξαιρετικά απλή. Με τον τρόπο αυτό όμως καταστρατηγούνται τα δικαιώματα της πνευματικής ιδιοκτησίας των δημιουργών πάνω στα δημιουργήματά τους. Λεπτομερειακή ανάλυση των τρόπων προστασίας της πνευματικής ιδιοκτησίας υπάρχει στο σχετικό θέμα.

Δικαιοδοσία στο Ιντερνετ

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες.

Α) Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.

Β) Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

Γ) Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

Δ) Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του.

Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και της λειτουργίας του Διαδικτύου αναπτύσσονται αναρίθμητες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς εμπλουτίζεται με νέες εκφάνσεις και καθίσταται σαφές ότι μεμονωμένες προσπάθειες εκ μέρους του νομοθέτη ή των ιδιωτών δεν αρκούν για να δώσουν λύσεις. Για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας απαιτείται συνεργασία μεταξύ όλων των κρατών όπως αναφέρεται σε πολλά νομοθετικά κείμενα.

Ηλεκτρονικό Εμπόριο: Το νομικό πλαίσιο στην Ελλάδα

Ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει Διαδικτυακή δέσμευση για αγορά η πώληση αγαθών ή υπηρεσιών Ηλεκτρονικό εμπόριο θεωρούνται επίσης και οι συναλλαγές μέσω τηλεφώνου και Φαξ. . Το ηλεκτρονικό εμπόριο αποτελεί έκφανση των λεγόμενων υπηρεσιών εξ αποστάσεως (ΠΔ 39.2001) .

Στο πρόσφατο παρελθόν οι συναλλαγές και οι αγορές των καταναλωτών και αντίστοιχα ο πωλήσεις των εμπόρων γίνονταν με καθαρά συμβατικά μέσα. Οι καταναλωτές προκειμένου να αγοράσουν αυτό που επιθυμούσαν ή να δεχτούν μία υπηρεσία έπρεπε να μεταβούν στην έδρα του προμηθευτή των αγαθών ή των υπηρεσιών. Στις μέρες μας ο τρόπος διεξαγωγής των συναλλαγών έχει αλλάξει ριζικά. Ενδεικτικό της καθυστερημένης ανάπτυξης του ηλεκτρονικού εμπορίου στην Ελλάδα είναι οι δύο υπουργικές αποφάσεις 3035/Β2-48.2001 και 7681/Β2-255.2001 που προωθούν τη διενέργεια δοκιμαστικής έρευνας για το ηλεκτρονικό εμπόριο. Οι αποφάσεις αυτές είναι του 2001, χρονιά που σε άλλες ευρωπαϊκές χώρες ανθούσε το ηλεκτρονικό εμπόριο. Αλλά και οι υπουργικές αποφάσεις 4708/2003, 36/2003 και 10220/Γ3-571/2004 που καταδεικνύουν το ίδιο πράγμα.

Ποιες οι έννοιες του προμηθευτή, του καταναλωτή και των μέσων επικοινωνίας εξ αποστάσεως;

Προμηθευτής (πωλητής) είναι κάθε φυσικό ή νομικό πρόσωπο που ενεργεί μέσα στα πλαίσια της επαγγελματικής του δραστηριότητας. Καταναλωτής (αγοραστής) είναι κάθε φυσικό πρόσωπο που ενεργεί για λόγους , οι οποίοι δεν εμπίπτουν στα πλαίσια της επαγγελματικής δραστηριότητας. Μέσο επικοινωνίας εξ αποστάσεως είναι κάθε μέσο που μπορεί να χρησιμοποιηθεί για τη σύναψη σύμβασης μεταξύ προμηθευτή και καταναλωτή χωρίς την αυτοπρόσωπη και ταυτόχρονη παρουσία τους.

Τι είναι η σύμβαση εξ αποστάσεως;

Η εξ αποστάσεως σύμβαση είναι αυτή που συνάπτεται μεταξύ ενός προμηθευτή και ενός καταναλωτή και για την κατάρτιση της οποίας ο προμηθευτής χρησιμοποιεί αποκλειστικά ένα ή περισσότερα μέσα επικοινωνίας εξ αποστάσεως, μέχρι και τη στιγμή σύναψης της σύμβασης.

.

Ποιες πληροφορίες πρέπει να έχει στη διάθεσή του ο καταναλωτής σε σχέση με τον προμηθευτή προτού δεσμευθεί από μια εξ αποστάσεως σύμβαση;

Ο καταναλωτής πρέπει να έχει απαραίτητα στη διάθεσή του στοιχεία που αφορούν τον προμηθευτή ή τον αντιπρόσωπο του προμηθευτή, όπως την ταυτότητα, την κύρια δραστηριότητά του, τη γεωγραφική διεύθυνση στην οποία είναι εγκατεστημένος, το

εμπορικό μητρώο στο οποίο είναι εγγεγραμμένος ο προμηθευτής, τον αριθμό καταχώρησής του αν είναι καταχωρημένος σε μητρώο καθώς και τα στοιχεία της αρμόδιας εποπτεύουσας αρχής αν η δραστηριότητα του προμηθευτή υπόκειται σε καθεστώς έγκρισης.

Ποιες πληροφορίες πρέπει να έχει στη διάθεσή του ο καταναλωτής σε σχέση με υπηρεσία/προϊόν προτού δεσμευθεί από μια εξ αποστάσεως σύμβαση;

Ο καταναλωτής πρέπει να έχει απαραίτητα στη διάθεσή του την περιγραφή των κυριοτέρων χαρακτηριστικών στοιχείων της υπηρεσίας/προϊόντος, το συνολικό τίμημα που πρέπει να πληρώσει συμπεριλαμβανομένων όλων των συναφών τελών, επιβαρύνσεων και δαπανών και όλων των φόρων, τις ρυθμίσεις σχετικά με την πληρωμή και την εκτέλεση της σύμβασης, το τυχόν ειδικό επιπλέον κόστος που συνεπάγεται για τον καταναλωτή η χρήση των μέσων επικοινωνίας εξ αποστάσεως και εάν αυτό το επιπλέον κόστος χρεώνεται. Επίσης πρέπει να έχει στη διάθεσή του την προθεσμία και τους όρους υπαναχώρησής του.

Τι είναι το δικαίωμα υπαναχώρησης;

Το δικαίωμα της υπαναχώρησης είναι το δικαίωμα που παρέχεται στον καταναλωτή να αποσυρθεί μέσα σε μικρό χρονικό διάστημα από την σύμβαση αφού έχει καταρτισθεί.

Πώς ασκείται το δικαίωμα υπαναχώρησης;

Σύμφωνα με το Ευρωπαϊκό δίκαιο (Οδηγία 97/7/ΕΚ άρθρο 6) ο καταναλωτής-χρήστης του Διαδικτύου διαθέτει προθεσμία τουλάχιστον επτά ημερολογιακών ημερών για να υπαναχωρήσει, χωρίς καμία ποινή και χωρίς να αναφέρει αιτιολογία από την εξ αποστάσεως σύμβαση . Η αντίστοιχη προθεσμία αναιτιολόγητης υπαναχώρησης στο Ελληνικό δίκαιο (άρθρο 4 παρ. 10 Νόμος 2251/1994) είναι δέκα εργάσιμες. Η προθεσμία εντός της οποίας μπορεί να ασκηθεί το δικαίωμα υπαναχώρησης αρχίζει να μετράται είτε από την ημέρα σύναψης της σύμβασης εξ αποστάσεως είτε από την ημέρα που ο καταναλωτής παρέλαβε τους συμβατικούς όρους και τις πληροφορίες.

Υπάρχουν εξαιρέσεις ως προς το δικαίωμα της υπαναχώρησης;

Το δικαίωμα υπαναχώρησης δεν εφαρμόζεται στις συμβάσεις των οποίων η εκτέλεση έχει ολοκληρωθεί πλήρως και από τα δύο μέρη με ρητή αίτηση του καταναλωτή προτού ασκήσει ο καταναλωτής το δικαίωμα υπαναχώρησης. Δεν ασκείται σε χρηματοοικονομικές υπηρεσίες η τιμή των οποίων εξαρτάται από διακυμάνσεις της κεφαλαιαγοράς επί των οποίων ο προμηθευτής δεν έχει καμία επίδραση και μπορεί να επέλθουν κατά τη διάρκεια της προθεσμίας υπαναχώρησης π.χ. υπηρεσίες που αφορούν πράξεις συναλλάγματος, τίτλους της χρηματαγοράς, διαπραγματεύσιμους τίτλους, μερίδια οργανισμών συλλογικών επενδύσεων και άλλα. Επίσης εξαιρούνται από την υπαναχώρηση ασφαλιστήρια συμβόλαια ταξιδιών και αποσκευών ή παρόμοια βραχυπρόθεσμα ασφαλιστήρια συμβόλαια με διάρκεια μικρότερη του ενός μηνός.

Τι είναι η ασφάλεια στις εξ αποστάσεως συμβάσεις του ηλεκτρονικού εμπορίου;

Ασφάλεια στις εξ αποστάσεως συμβάσεις αποτελεί η μη γνωστοποίηση ή διαρροή σε τρίτους των προσωπικών δεδομένων του καταναλωτή, όπως είναι τα προσωπικά στοιχεία του, ο αριθμός της πιστωτικής του κάρτας κλπ. τα οποία συλλέγονται από τον προμηθευτή κατά τη διάρκεια σύναψης της σύμβασης με ηλεκτρονικά μέσα.

Είναι υποχρεωτική η ασφάλεια στο ηλεκτρονικό εμπόριο;

Ο προμηθευτής οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Τα μέτρα αυτά είναι οι όροι των on line συμβάσεων, η ασφαλής σύνδεση με την τράπεζα και οι προστατευμένες περιοχές να έχουν κάλυψη ισχύος ψηφιακού πιστοποιητικού. Τα παραπάνω μέτρα πρέπει να κατοχυρώνουν επίπεδο ασφαλείας ανάλογο προς τον κίνδυνο παραβίασης του δικτύου. Σε περίπτωση ύπαρξης ιδιαίτερου κινδύνου παραβίασης της ασφάλειας του δικτύου στο οποίο γίνεται η συναλλαγή ο προμηθευτής οφείλει να ενημερώνει τους καταναλωτές για τον κίνδυνο αυτό .

Τι είναι η ηλεκτρονική πληρωμή;

Ηλεκτρονική πληρωμή αποτελούν οι εξής τρόποι εκκαθάρισης των διαδικτυακών συναλλαγών: 1. η ηλεκτρονική καταβολή μέσω της ηλεκτρονικής μεταφοράς κεφαλαίων (e- banking), 2. η χρήση πιστωτικών καρτών και 3. η ύπαρξη ηλεκτρονικού χρήματος. Η διαδικασία πληρωμής μέσω ηλεκτρονικού χρήματος στην Ελλάδα δεν έχει προχωρήσει ακόμα σε πρακτική εφαρμογή.

Πώς προστατεύεται ο καταναλωτής στις περιπτώσεις πληρωμής με κάρτα;

Προληπτικά ο καταναλωτής για να προστατευθεί από την δόλια χρήση της πιστωτικής του κάρτας πρέπει να ερευνήσει τα στοιχεία της εταιρίας με την οποία πρόκειται να συναλλαγεί, δηλαδή αν υφίσταται αυτή η εταιρία, αν μπορεί να επικοινωνήσει με αυτή και γενικότερα την αξιοπιστία της. Επίσης αν πληρούνται κάποιοι τεχνικοί όροι ασφαλείας των δεδομένων μέσα στις ιστοσελίδες όπου δίνονται τα στοιχεία για την κατάρτιση της συναλλαγής.
Αν πάρα ταύτα χρησιμοποιηθεί παράνομα η κάρτα του ο καταναλωτής πρέπει να προβεί σε έγγραφη διαμαρτυρία στην τράπεζα με την οποία να αρνείται την παράνομη συναλλαγή και να ζητήσει την επαναπίστωση του ποσού στην κάρτα του.

Νομοθεσία Ηλεκτρονικού Εμπορίου	
Ν.2251.1994	Προστασία Καταναλωτή
Ν.2854.2000	Δικαστική προστασία κατά το στάδιο που προηγείται της σύναψης συμβάσεων φορέων οι οποίοι λειτουργούν στους τομείς του ύδατος, της ενέργειας, των μεταφορών και των τηλεπικοινωνιών
Ν.3193.2003	Νόμος 3193.2003: Κανόνες τιμολόγησης, ρυθμίσεις Φ.Π.Α. ηλεκτρονικών υπηρεσιών και άλλες διατάξεις
Προεδρικά Διατάγματα	
Π.Δ. 39.2001	Για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της Κοινωνίας των Πληροφοριών
Π.Δ. 150.2001	Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
Π.Δ. 131.2003	Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο)
Υπουργικές Αποφάσεις	
Υ.Α. Ζ1-496/2000	Υπουργική απόφαση Ζ1-496/2000: Πωλήσεις από απόσταση - Συγκριτική διαφήμιση - Προσαρμογή του Νόμου 2251/1994 για την "Προστασία των καταναλωτών"
Υ.Α. 1023404/2001	Υπουργική απόφαση 1023404/1363/0016 του 2001 για την είσπραξη του Φόρου Προστιθέμενης Αξίας (Φ.Π.Α.) που υποβάλλεται ηλεκτρονικά, με χρέωση Τραπεζικών λογαριασμών των υποκειμένων
Υπουργικήαπόφαση 10220/Γ3-571/2004	Υπουργική απόφαση 10220/Γ3-571/2004 - Πιλοτική στατιστική έρευνα στο ηλεκτρονικό εμπόριο
Κοινοτικές Οδηγίες	
Οδηγία 87/102/ΕΟΚ	Για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη
Οδηγία 90/88/ΕΟΚ	Οδηγία 90/88/ΕΟΚ για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη
Οδηγία 93/13/ΕΟΚ	Οδηγία 93/13/ΕΟΚ του Συμβουλίου σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές
Οδηγία 97/7/ΕΚ	Οδηγία 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις

Οδηγία 2000/31/ΕΚ	Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου στην εσωτερική αγορά
Οδηγία 2000/35/ΕΚ	Οδηγία 2000/35/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την καταπολέμηση των καθυστερήσεων πληρωμών στις εμπορικές συναλλαγές
Οδηγία 2000/46/ΕΚ	Οδηγία 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος
Οδηγία 2002/38/ΕΚ	Οδηγία 2002/38/ΕΚ όσον αφορά το σύστημα φόρου προστιθεμένης αξίας που εφαρμόζεται στις ραδιοφωνικές και τηλεοπτικές υπηρεσίες και σε ορισμένες υπηρεσίες που παρέχονται ηλεκτρονικά
Οδηγία 2002/58/ΕΚ	Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)
Οδηγία 2002/65/ΕΚ	Οδηγία 2002/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές
Συμφωνία 2004/402	Συμφωνία 2004/402 μεταξύ της Ευρωπαϊκής Κοινότητας και της Δημοκρατίας της Κύπρου για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών υπηρεσιών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας της πληροφορίας.
Κοινοτικές Συστάσεις	
Σύσταση 92/295/ΕΟΚ	Σύσταση επιτροπής με αριθμό 92/295/ΕΟΚ σχετικά με τους κώδικες δεοντολογίας για την προστασία των καταναλωτών όσον αφορά συμβάσεις διαπραγματευόμενες από απόσταση
Σύσταση 97/489/ΕΚ	Σύσταση 97/489/ΕΚ σχετικά με τις συναλλαγές που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά στις σχέσεις μεταξύ του εκδότη και του κατόχου
Κοινοτικοί Κανονισμοί	
Κανονισμός 733/2002	Κανονισμός (ΕΚ) αριθ. 733/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την υλοποίηση του τομέα ανωτάτου επιπέδου
Κανονισμός 792/2002	Κανονισμός (ΕΚ) αριθ. 792/2002 του Συμβουλίου σχετικά με τη διοικητική συνεργασία στον τομέα των έμμεσων φόρων (ΦΠΑ) όσον αφορά πρόσθετα μέτρα για το ηλεκτρονικό εμπόριο

Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Η ανάπτυξη των νέων τεχνολογιών και οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών οδήγησαν στην αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Οι προσωπικές αυτές πληροφορίες που αναφέρονται σε κάθε είδους δραστηριότητα προσωπική είτε επαγγελματική του ατόμου ονομάζονται προσωπικά δεδομένα.

Οδηγία 97/66 για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα

Έχοντας υπόψη: τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας, και ιδίως το άρθρο 100 Α, την πρόταση της Επιτροπής (1), τη γνώμη της Οικονομικής και Κοινωνικής Επιτροπής (2), Αποφασίζοντας σύμφωνα με την διαδικασία του άρθρου 189 Β της συνθήκης (3), υπό το πρίσμα του κοινού σχεδίου το οποίο ενέκρινε η επιτροπή συνδιαλλαγής στις 6 Νοεμβρίου 199, Εκτιμώντας:

(1) ότι η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (4), επιβάλλει στα κράτη μέλη την υποχρέωση να διασφαλίζουν τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, και ιδίως το δικαίωμα σεβασμού της ιδιωτικής τους ζωής, προκειμένου να διασφαλίζεται η ελεύθερη ροή των δεδομένων προσωπικού χαρακτήρα στην Κοινότητα

(2) ότι το απόρρητο των επικοινωνιών κατοχυρώνεται σύμφωνα με τις διεθνείς διατάξεις σε ό,τι αφορά τα ανθρώπινα δικαιώματα (ιδίως την ευρωπαϊκή σύμβαση για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών) και με τα συντάγματα των κρατών μελών

(3) ότι ήδη εισάγονται στην Κοινότητα νέες προηγμένες ψηφιακές τεχνολογίες στα δημόσια τηλεπικοινωνιακά δίκτυα, οι οποίες δημιουργούν ειδικές απαιτήσεις όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής του χρήστη ότι η ανάπτυξη της κοινωνίας των πληροφοριών χαρακτηρίζεται από την καθιέρωση νέων τηλεπικοινωνιακών υπηρεσιών ότι η επιτυχής διασυνοριακή ανάπτυξη των υπηρεσιών αυτών, όπως το «βίντεο κατά βούληση» και η διαλογική τηλεόραση εξαρτώνται εν μέρει από την πεποίθηση των χρηστών ότι δεν τίθεται σε κίνδυνο η ιδιωτική τους ζωή

(4) ότι αυτό συμβαίνει ειδικότερα με την εγκατάσταση του ψηφιακού δικτύου ενοποιημένων υπηρεσιών (ISDN) και των ψηφιακών κινητών δικτύων

(5) ότι το Συμβούλιο, στο ψήφισμά του, της 30ής Ιουνίου 1988, σχετικά με την ανάπτυξη της κοινής αγοράς των υπηρεσιών και του εξοπλισμού στον τομέα των τηλεπικοινωνιών έως το 1992 (5), ζήτησε να ληφθούν μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα, προκειμένου να δημιουργηθεί κατάλληλο περιβάλλον για τη

μελλοντική ανάπτυξη των τηλεπικοινωνιών στην Κοινότητα ότι το Συμβούλιο τόνισε εκ νέου τη σημασία που ενέχει η προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στο ψήφισμά του, της 18ης Ιουλίου 1989, σχετικά με την ενίσχυση του συντονισμού για την εγκατάσταση στην Ευρωπαϊκή Κοινότητα του ψηφιακού δικτύου ενοποιημένων υπηρεσιών (ISDN) έως το 1992 (6)

(6) ότι το Ευρωπαϊκό Κοινοβούλιο έχει υπογραμμίσει τη σημασία που ενέχει η προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στα δίκτυα τηλεπικοινωνιών, όσον αφορά ιδίως την εγκατάσταση του ψηφιακού δικτύου ενοποιημένων υπηρεσιών (ISDN)

(7) ότι, στην περίπτωση των δημόσιων τηλεπικοινωνιακών δικτύων, πρέπει να θεσπισθούν ειδικές νομοθετικές, κανονιστικές και τεχνικές διατάξεις προκειμένου να προστατευθούν τα θεμελιώδη δικαιώματα και οι ελευθερίες των φυσικών προσώπων, καθώς και τα έννομα συμφέροντα των νομικών προσώπων, ιδίως έναντι των αυξανομένων κινδύνων που απορρέουν από την αυτόματη αποθήκευση και επεξεργασία δεδομένων που αφορούν συνδρομητές και χρήστες

(8) ότι οι νομοθετικές, κανονιστικές και τεχνικές διατάξεις που έχουν θεσπίσει τα κράτη μέλη όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα, της ιδιωτικής ζωής και των εννόμων συμφερόντων των νομικών προσώπων στον τομέα των τηλεπικοινωνιών, πρέπει να εναρμονιστούν ώστε να αποφεύγονται τα εμπόδια στην εσωτερική αγορά για τις τηλεπικοινωνίες σύμφωνα με το στόχο που εκτίθεται στο άρθρο Α της συνθήκης ότι η εναρμόνιση περιορίζεται στις απαραίτητες απαιτήσεις που αποβλέπουν στο να μην εμποδίζεται η προαγωγή και η ανάπτυξη νέων τηλεπικοινωνιακών υπηρεσιών και δικτύων μεταξύ των κρατών μελών

(9) ότι τα ενδιαφερόμενα κράτη μέλη, οι ενδιαφερόμενοι προμηθευτές και χρήστες, καθώς και οι αρμόδιοι κοινοτικοί οργανισμοί, θα πρέπει να συνεργάζονται για την εγκατάσταση και την ανάπτυξη των σχετικών τεχνολογικών μέσων, όπου αυτό είναι απαραίτητο, για την εφαρμογή των εγγυήσεων που προβλέπονται από τις διατάξεις της παρούσας οδηγίας

(10) ότι οι νέες υπηρεσίες περιλαμβάνουν τη διαλογική τηλεόραση και το «βίντεο κατά βούληση»

(11) ότι, στον τομέα των τηλεπικοινωνιών, ιδίως για όλα τα ζητήματα που αφορούν την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών που δεν καλύπτονται ρητά από τις διατάξεις της παρούσας οδηγίας, συμπεριλαμβανομένων των υποχρεώσεων του υπεύθυνου επεξεργασίας και των ατομικών δικαιωμάτων, εφαρμόζεται η οδηγία 95/46/ΕΚ ότι η οδηγία 95/46/ΕΚ εφαρμόζεται για τις μη διαθέσιμες στο κοινό τηλεπικοινωνιακές υπηρεσίες

(12) ότι η παρούσα οδηγία, όπως προβλέπεται και στο άρθρο 3 της οδηγίας 95/46/ΕΚ, δεν υπεισέρχεται σε θέματα προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών που συνδέονται με δραστηριότητες οι οποίες δεν διέπονται από το κοινοτικό δίκαιο ότι εναπόκειται στα κράτη μέλη να λάβουν τέτοια μέτρα, εφόσον κρίνουν ότι απαιτούνται για την προστασία της δημόσιας ασφάλειας, της εθνικής άμυνας, της ασφάλειας του κράτους (περιλαμβανομένης της οικονομικής ευημερίας του κράτους εφόσον οι δραστηριότητες συνδέονται με θέματα ασφάλειας του κράτους) και την εφαρμογή του

ποινικού δικαίου ότι η παρούσα οδηγία δεν πρέπει να θίγει τη δυνατότητα των κρατών μελών να προβαίνουν σε νόμιμη παρακολούθηση των τηλεπικοινωνιών, για οποιονδήποτε από αυτούς τους σκοπούς

(13) ότι οι συνδρομητές των διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών μπορεί να είναι φυσικά ή νομικά πρόσωπα ότι οι διατάξεις της παρούσας οδηγίας αποβλέπουν, συμπληρώνοντας την οδηγία 95/46/ΕΚ, στην προστασία των θεμελιωδών δικαιωμάτων των φυσικών προσώπων και ειδικότερα του δικαιώματος στην ιδιωτική ζωή, καθώς επίσης και των έννομων συμφερόντων των νομικών προσώπων ότι οι διατάξεις αυτές δεν συνεπάγονται επ' ουδενί υποχρέωση των κρατών μελών να επεκτείνουν την εφαρμογή της οδηγίας 95/46/ΕΚ στην προστασία των εννόμων συμφερόντων των νομικών προσώπων ότι η εν λόγω προστασία εξασφαλίζεται με την ισχύουσα κοινοτική και εθνική νομοθεσία

(14) ότι η εφαρμογή ορισμένων απαιτήσεων σχετικά με την ένδειξη της ταυτότητας και τον περιορισμό αναγνώρισης καλούσας και συνδεδεμένης γραμμής, και σχετικά με τις αυτόματα προωθούμενες κλήσεις στις γραμμές συνδρομητών που συνδέονται με αναλογικά κέντρα δεν πρέπει να είναι υποχρεωτικές σε ειδικές περιπτώσεις όπου μια τέτοια εφαρμογή θα ήταν τεχνικά αδύνατη ή θα απαιτούσε δυσανάλογα οικονομική επιβάρυνση ότι επειδή είναι σημαντικό για τα ενδιαφερόμενα μέρη να ενημερώνονται γι' αυτές τις περιπτώσεις, τα κράτη μέλη θα πρέπει να τις κοινοποιούν στην Επιτροπή

(15) ότι οι φορείς παροχής υπηρεσιών πρέπει να λαμβάνουν τα κατάλληλα μέτρα για να κατοχυρώνεται η ασφάλεια των υπηρεσιών τους, ενδεχομένως από κοινού με τον φορέα παροχής του δικτύου και να πληροφορούν τους συνδρομητές για τυχόν ιδιαίτερους κινδύνους παραβίασης της ασφάλειας του δικτύου ότι η ασφάλεια εκτιμάται σύμφωνα με τις διατάξεις του άρθρου 1 της οδηγίας 95/46/ΕΚ

(16) ότι πρέπει να ληφθούν μέτρα για την παρεμπόδιση της άνευ αδείας πρόσβασης στις επικοινωνίες, προκειμένου να προστατευθεί το απόρρητο των επικοινωνιών μέσω του δημοσίου τηλεπικοινωνιακού δικτύου και των διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών ότι η εθνική νομοθεσία σε ορισμένα κράτη μέλη απαγορεύει μόνον την ηθελημένη και άνευ αδείας πρόσβαση στις επικοινωνίες

(17) ότι τα δεδομένα που αφορούν συνδρομητές και υφίστανται επεξεργασία για την πραγματοποίηση
κλήσεων περιέχουν πληροφορίες για την ιδιωτική ζωή των φυσικών προσώπων και αφορούν το σεβασμό του απορρήτου της αλληλογραφίας τους ή τα έννομα συμφέροντα νομικών προσώπων ότι τα δεδομένα αυτά επιτρέπεται να αποθηκεύονται μόνο στο βαθμό που αυτό είναι απαραίτητο για την παροχή υπηρεσιών για τη χρέωση και την πληρωμή διασυνδέσεων, για περιορισμένο δε χρόνο ότι κάθε άλλη επεξεργασία την οποία επιθυμεί να διενεργήσει ο φορέας παροχής της διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας για την εμπορική προώθηση των ιδίων του τηλεπικοινωνιακών υπηρεσιών επιτρέπεται μόνον εφόσον συμφωνεί με αυτήν ο συνδρομητής, βάσει ακριβών και πλήρων πληροφοριών που παρέχει ο φορέας παροχής της διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας σχετικά με τα είδη περαιτέρω επεξεργασίας που σκοπεύει να διενεργήσει

(18) ότι η καθιέρωση αναλυτικών λογαριασμών βελτίωσε τις δυνατότητες του συνδρομητή να επαληθεύει την ορθότητα των τελών που του χρεώνει ο φορέας παροχής

της υπηρεσίας ότι ταυτόχρονα ενδέχεται να παραβλάπτει την ιδιωτική ζωή των χρηστών των διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών ότι, συνεπώς, για να διαφυλαχθεί η ιδιωτική ζωή του χρήστη, τα κράτη μέλη οφείλουν να ενθαρρύνουν την ανάπτυξη δυνατοτήτων επιλογής τηλεπικοινωνιακών υπηρεσιών, όπως οι εναλλακτικές δυνατότητες πληρωμής οι οποίες επιτρέπουν ανώνυμη ή αυστηρά εμπιστευτική πρόσβαση στις διαθέσιμες στο κοινό τηλεπικοινωνιακές υπηρεσίες, π.χ. τηλεκάρτες και διευκολύνσεις πληρωμής με πιστωτικές κάρτες ότι, ως εναλλακτική λύση, τα κράτη μέλη μπορούν να απαιτούν την διαγραφή ορισμένων ψηφίων από τους καλούμενους αριθμούς των αναλυτικών λογαριασμών

(19) ότι, όσον αφορά την αναγνώριση καλούσας γραμμής, είναι ανάγκη να προστατεύεται το δικαίωμα του καλούντος να μην επιτρέψει την ένδειξη της ταυτότητας της γραμμής από την οποία πραγματοποιείται η κλήση καθώς και το δικαίωμα του καλούμενου να αρνείται κλήσεις από γραμμές χωρίς προσδιορισμένη ταυτότητα ότι, σε ειδικές περιπτώσεις, δικαιολογείται να εμποδίζεται η απάλειψη της ένδειξης της ταυτότητας της καλούσας γραμμής ότι ορισμένοι συνδρομητές και ιδίως οι γραμμές των υπηρεσιών άμεσης επέμβασης ή άλλων αναλόγων οργανισμών ενδιαφέρονται να κατοχυρώνεται η ανωνυμία του καλούντος ότι, όσον αφορά την αναγνώριση καλούσας γραμμής, είναι ανάγκη να προστατεύεται το δικαίωμα και το έννομο συμφέρον του καλουμένου να μην επιτρέψει την ένδειξη της ταυτότητας της γραμμής με την οποία είναι εκάστοτε συνδεδεμένος ο καλών, ιδίως στην περίπτωση των προωθούμενων κλήσεων ότι οι φορείς παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών οφείλουν να ενημερώνουν τους συνδρομητές τους για την ύπαρξη υπηρεσιών αναγνώρισης καλούσας και συνδεδεμένης γραμμής στο δίκτυο, καθώς και για όλες τις υπηρεσίες που προσφέρονται επί τη βάσει της αναγνώρισης καλούσας και συνδεδεμένης γραμμής καθώς και για τις δυνατότητες που προσφέρονται για την προστασία της ιδιωτικής ζωής ότι αυτό θα επιτρέπει στους συνδρομητές να προβαίνουν εν γνώσει στην επιλογή των δυνατοτήτων απορρήτου που επιθυμούν να χρησιμοποιούν ότι οι επιλογές για την προστασία της ιδιωτικής ζωής που προσφέρονται για κάθε μία γραμμή δεν διατίθενται κατ' ανάγκη ως αυτόματη υπηρεσία δικτύου, αλλά μπορούν να αποκτηθούν με απλή αίτηση προς το φορέα παροχής των διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών

(20) ότι πρέπει να διασφαλίζονται οι συνδρομητές από την ενόχληση που μπορεί να προκαλεί η αυτόματη προώθηση κλήσεων από άλλους ότι, σε αυτές τις περιπτώσεις, πρέπει να είναι σε θέση ο συνδρομητής να ανακόπτει την προώθηση κλήσεων προς την τερματική του συσκευή με απλή αίτηση προς το φορέα παροχής των διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών

(21) ότι οι τηλεφωνικοί κατάλογοι διανέμονται ευρέως και διατίθενται στο κοινό ότι, για να προστατευθεί η ιδιωτική ζωή των φυσικών προσώπων και τα έννομα συμφέροντα των νομικών προσώπων, πρέπει ο συνδρομητής να είναι σε θέση να καθορίσει ο ίδιος τα δεδομένα προσωπικού χαρακτήρα που μπορούν να δημοσιευθούν στον κατάλογο ότι τα κράτη μέλη μπορούν να περιορίσουν αυτή τη δυνατότητα στους συνδρομητές που είναι φυσικά πρόσωπα

(22) ότι πρέπει να προστατεύονται οι συνδρομητές από την αυθαίρετη διείσδυση στην ιδιωτική τους ζωή μέσω τηλεφωνημάτων και φαξ που δεν έχουν ζητηθεί ότι τα κράτη μέλη μπορούν να περιορίσουν αυτή την προστασία στους συνδρομητές που είναι φυσικά

πρόσωπα

(23) ότι είναι ανάγκη να εξασφαλιστεί η εναρμονισμένη καθιέρωση τεχνικών χαρακτηριστικών του τηλεπικοινωνιακού εξοπλισμού με σκοπό την προστασία των δεδομένων, ώστε να συμβιβάζεται με τη λειτουργία της εσωτερικής αγοράς

(24) ότι ειδικότερα, όπως προβλέπεται και στο άρθρο 13 της οδηγίας 95/46/ΕΚ, τα κράτη μέλη μπορούν σε ορισμένες περιστάσεις να περιορίζουν την εμβέλεια των υποχρεώσεων και δικαιωμάτων των συνδρομητών, διασφαλίζοντας π.χ. ότι ένας φορέας παροχής διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας μπορεί να εμποδίζει την απάλειψη της ένδειξης της ταυτότητας της καλούσας γραμμής, σύμφωνα με την εθνική νομοθεσία και με σκοπό την πρόληψη ή τη διαπίστωση ποινικών παραβάσεων ή για την ασφάλεια του κράτους

(25) ότι, στην περίπτωση που δεν γίνονται σεβαστά τα δικαιώματα των χρηστών και των συνδρομητών, η εθνική νομοθεσία πρέπει να προβλέπει ένδικα μέσα ότι πρέπει να επιβάλλονται κυρώσεις σε κάθε πρόσωπο που δεν συμμορφώνεται με τα εθνικά μέτρα που θεσπίζονται δυνάμει της παρούσας οδηγίας, είτε είναι πρόσωπο ιδιωτικού είτε δημοσίου δικαίου

(26) ότι, στα πλαίσια της εφαρμογής της παρούσας οδηγίας, είναι σκόπιμο να αξιοποιηθεί η πείρα της ομάδας προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία απαρτίζεται από αντιπροσώπους των αρχών ελέγχου των κρατών μελών και έχει συσταθεί δυνάμει του άρθρου 29 της οδηγίας 95/46/ΕΚ

(27) ότι, δεδομένων των τεχνολογικών εξελίξεων στον τομέα των τηλεπικοινωνιών και της συνακόλουθης εξέλιξης των προσφερόμενων υπηρεσιών, είναι αναγκαίο να προσδιορισθούν από τεχνική άποψη οι κατηγορίες δεδομένων, που περιλαμβάνονται στο παράρτημα της παρούσας οδηγίας για την εφαρμογή του άρθρου 6 της παρούσας οδηγίας, με τη βοήθεια της επιτροπής της απαρτιζόμενης από αντιπροσώπους των κρατών μελών η οποία έχει συσταθεί δυνάμει του άρθρου 31 της οδηγίας 95/46/ΕΚ, προκειμένου να διασφαλιστεί η συνεκτική εφαρμογή των απαιτήσεων της παρούσας οδηγίας ανεξαρτήτως των τεχνολογικών αλλαγών ότι η διαδικασία αυτή εφαρμόζεται μόνο σε χαρακτηριστικά που είναι απαραίτητα για την προσαρμογή του παραρτήματος σε νέες τεχνολογικές εξελίξεις, λαμβάνοντας υπόψη τις αλλαγές που παρατηρούνται στις απαιτήσεις της αγοράς και στη ζήτηση από πλευράς καταναλωτών ότι η Επιτροπή οφείλει να ενημερώνει δεόντως το Ευρωπαϊκό Κοινοβούλιο για την πρόθεσή της να εφαρμόσει την εν λόγω διαδικασία και ότι, άλλως, εφαρμόζεται η διαδικασία του άρθρου 100 Α της συνθήκης

(28) ότι, για να διευκολυνθεί η τήρηση των διατάξεων της παρούσας οδηγίας, πρέπει να προβλεφθεί ειδική ρύθμιση για την επεξεργασία δεδομένων που έχει ήδη αρχίσει την ημερομηνία έναρξης ισχύος των εθνικών νομοθετικών διατάξεων οι οποίες θεσπίζονται σύμφωνα με την παρούσα οδηγία,
ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

Άρθρο 1 Στόχος και πεδίο εφαρμογής
1. Η παρούσα οδηγία αποσκοπεί στην εναρμόνιση των διατάξεων των κρατών μελών οι

οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως δε το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, καθώς και στην ελεύθερη κυκλοφορία των δεδομένων αυτών και των τηλεπικοινωνιακών εξοπλισμών και υπηρεσιών στην Κοινότητα.
2. Οι διατάξεις της παρούσας οδηγίας εξειδικεύουν και συμπληρώνουν την οδηγία 95/46/ΕΚ για τους σκοπούς που αναφέρονται στην παράγραφο 1. Επιπλέον, οι εν λόγω διατάξεις παρέχουν προστασία των εννόμων συμφερόντων των συνδρομητών που είναι νομικά πρόσωπα.
3. Η παρούσα οδηγία δεν εφαρμόζεται στις δραστηριότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής της κοινοτικής νομοθεσίας, όπως οι δραστηριότητες που αναφέρονται στους τίτλους V και VI της συνθήκης για την Ευρωπαϊκή Ένωση, και σε καμία περίπτωση στις δραστηριότητες που αφορούν τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης και της οικονομικής ευημερίας του κράτους εφόσον οι δραστηριότητες συνδέονται με θέματα ασφάλειας του κράτους) και στις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου.

Άρθρο 2 Ορισμοί
Εκτός των ορισμών που περιλαμβάνονται στην οδηγία 95/46/ΕΚ, για τους σκοπούς της παρούσας οδηγίας νοούνται ως:
α) «συνδρομητής», κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών για την παροχή των υπηρεσιών αυτών
β) «χρήστης», κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό τηλεπικοινωνιακή υπηρεσία για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας
γ) «δημόσιο τηλεπικοινωνιακό δίκτυο», τα συστήματα μετάδοσης και, όπου δει, ο εξοπλισμός μεταγωγής και τα λοιπά μέσα που επιτρέπουν την μεταφορά σημάτων μεταξύ συγκεκριμένων τερματικών σημείων με τη χρήση καλωδίου, ραδιοκυμάτων, οπτικών ή άλλων ηλεκτρομαγνητικών μέσων, τα οποία χρησιμοποιούνται, εν μέρει ή εν όλω, για την παροχή διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών
δ) «τηλεπικοινωνιακές υπηρεσίες», οι υπηρεσίες των οποίων η παροχή συνίσταται εν όλω ή εν μέρει στη μετάδοση και περαιτέρω διαβίβαση σημάτων σε τηλεπικοινωνιακά δίκτυα, εξαιρουμένων των ραδιοφωνικών και τηλεοπτικών εκπομπών.

Άρθρο 3 Υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής
1. Η παρούσα οδηγία εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στα πλαίσια της παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών σε δημόσια τηλεπικοινωνιακά δίκτυα στην Κοινότητα, ιδίως μέσω του ψηφιακού δικτύου ενοποιημένων υπηρεσιών (ISDN) και των δημοσίων ψηφιακών κινητών δικτύων.
2. Τα άρθρα 8, 9 και 10 εφαρμόζονται στις γραμμές συνδρομητών που συνδέονται με ψηφιακά κέντρα και, όταν αυτό είναι τεχνικώς εφικτό και δεν συνεπάγεται δυσανάλογη οικονομική επιβάρυνση, σε γραμμές συνδρομητών που συνδέονται με αναλογικά κέντρα.
3. Τα κράτη μέλη κοινοποιούν στην Επιτροπή τις περιπτώσεις όπου είναι τεχνικώς ανέφικτο ή όπου απαιτείται δυσανάλογη επένδυση για να υπάρξουν οι προϋποθέσεις των άρθρων 8, 9 και 10.

Άρθρο 4 Ασφάλεια
1. Ο φορέας παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται

η ασφάλεια των υπηρεσιών του, και εφόσον χρειάζεται, από κοινού με το φορέα παροχής του δημοσίου δικτύου τηλεπικοινωνιών, όσον αφορά την ασφάλεια του δικτύου. Λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων και του κόστους εφαρμογής τους, τα μέτρα αυτά εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τον υπάρχοντα κίνδυνο.
2. Σε περίπτωση που υπάρχει ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δικτύου, ο φορέας που παρέχει διαθέσιμη στο κοινό τηλεπικοινωνιακή υπηρεσία οφείλει να ενημερώσει τους συνδρομητές για τον κίνδυνο αυτό και για όλες τις τυχόν δυνατότητες αποτροπής του, συμπεριλαμβανομένου και του σχετικού κόστους.

Άρθρο 5 Απόρρητο των επικοινωνιών
1. Τα κράτη μέλη κατοχυρώνουν, με εθνικούς κανόνες, το απόρρητο των επικοινωνιών που διενεργούνται μέσω του δημόσιου τηλεπικοινωνιακού δικτύου και των διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών. Ειδικότερα, απαγορεύουν την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης των επικοινωνιών από πρόσωπα πλην των χρηστών χωρίς τη συγκατάθεση των χρηστών στους οποίους αναφέρονται, εκτός αν υπάρχει σχετική νόμιμη άδεια, σύμφωνα με το άρθρο 14 παράγραφος 1.
2. Η παράγραφος 1 δεν επηρεάζει οποιαδήποτε επιτρεπόμενη από το νόμο μαγνητοφώνηση συνδιαλέξεων κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης συνδιαλέξεως στο πλαίσιο εμπορικών συναλλαγών.

Άρθρο 6 Δεδομένα κίνησης και χρέωσης
1. Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία για την πραγματοποίηση κλήσεων και αποθηκεύονται από το φορέα παροχής τηλεπικοινωνιακού δικτύου ή/και διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας πρέπει να απαλείφονται ή να καθίστανται ανώνυμα κατά τη λήξη της κλήσης, με την επιφύλαξη των διατάξεων των παραγράφων 2, 3 και 4.
2. Για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων, επιτρέπεται να υποβάλλονται σε επεξεργασία τα δεδομένα που αναφέρονται στο παράρτημα. Η επεξεργασία αυτή επιτρέπεται μόνο έως το τέλος της περιόδου εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή.
3. Για την εμπορική προώθηση των τηλεπικοινωνιακών υπηρεσιών του, ο φορέας παροχής διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας μπορεί να επεξεργασθεί τα δεδομένα που αναφέρονται στην παράγραφο 2, εφόσον ο συνδρομητής δώσει τη συγκατάθεσή του.
4. Η επεξεργασία των δεδομένων κίνησης και χρέωσης πρέπει να περιορίζεται στα πρόσωπα τα οποία ενεργούν υπό την εποπτεία των φορέων παροχής των δημοσίων τηλεπικοινωνιακών δικτύων ή/και των διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών τα οποία ασχολούνται με τη διαχείριση των χρεώσεων ή της κίνησης, τις απαντήσεις σε ερωτήσεις πελατών, την ανίχνευση της απάτης και την εμπορική προώθηση των τηλεπικοινωνιακών υπηρεσιών του φορέα αυτή η επεξεργασία πρέπει να περιορίζεται στο απολύτως αναγκαίο για την εξυπηρέτηση των σκοπών αυτών.
5. Οι παράγραφοι 1, 2, 3 και 4 ισχύουν με την επιφύλαξη της δυνατότητας των αρμοδίων αρχών να ενημερώνονται για τα δεδομένα τα σχετικά με τη χρέωση ή την κίνηση σύμφωνα με την ισχύουσα νομοθεσία, με σκοπό την επίλυση διαφορών, ιδίως σχετικά με τη διασύνδεση ή τη χρέωση.

Άρθρο 7 Αναλυτική χρέωση
1. Οι συνδρομητές έχουν το δικαίωμα να λαμβάνουν μη αναλυτικούς λογαριασμούς.

2. Τα κράτη μέλη εφαρμόζουν εθνικές διατάξεις προκειμένου να συμβιβάσουν τα δικαιώματα των συνδρομητών που λαμβάνουν αναλυτικούς λογαριασμούς με την προστασία της ιδιωτικής ζωής των καλούντων χρηστών και των καλουμένων συνδρομητών, διασφαλίζοντας επί παραδείγματι ότι βρίσκονται στη διάθεση των χρηστών και των συνδρομητών αυτών επαρκείς εναλλακτικοί τρόποι επικοινωνίας ή πληρωμής.

Άρθρο 8 Ένδειξη της ταυτότητας και περιορισμός αναγνώρισης καλούσας και συνδεδεμένης γραμμής

1. Όταν παρέχεται η ένδειξη της ταυτότητας καλούσας γραμμής, ο καλών χρήστης πρέπει να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να εμποδίζει αυτή τη λειτουργία ανά κλήση. Ο καλών συνδρομητής πρέπει να έχει τη δυνατότητα αυτή ανά γραμμή.
2. Όταν παρέχεται ένδειξη της ταυτότητας καλούσας γραμμής, ο καλούμενος συνδρομητής πρέπει να έχει τη δυνατότητα, με απλά μέσα και ατελώς εφόσον κάνει λελογισμένη χρήση αυτής της λειτουργίας, να μην επιτρέπει την ένδειξη της ταυτότητας της καλούσας γραμμής για τις εισερχόμενες κλήσεις.
3. Όταν παρέχεται ένδειξη της ταυτότητας καλούσας γραμμής και η ένδειξη αυτή γίνεται πριν γίνει οριστικά η κλήση, ο καλούμενος συνδρομητής πρέπει να έχει τη δυνατότητα, με απλά μέσα, να μη δέχεται την εισερχόμενη κλήση όταν ο καλών χρήστης ή συνδρομητής δεν έχει επιτρέψει την ένδειξη της ταυτότητας της καλούσας γραμμής.
4. Όταν παρέχεται ένδειξη της ταυτότητας της συνδεδεμένης γραμμής, ο καλούμενος συνδρομητής πρέπει να έχει τη δυνατότητα να απαλείφει, με απλά μέσα και ατελώς, την ένδειξη της ταυτότητας της συνδεδεμένης γραμμής στον καλούντα χρήστη.
5. Οι διατάξεις της παραγράφου 1 ισχύουν επίσης όσον αφορά κλήσεις από την Κοινότητα προς τρίτες χώρες οι διατάξεις των παραγράφων 2, 3 και 4 ισχύουν επίσης και για τις εισερχόμενες κλήσεις που προέρχονται από τρίτες χώρες.
6. Τα κράτη μέλη εξασφαλίζουν ότι όταν παρέχεται ένδειξη της ταυτότητας καλούσας ή/και συνδεδεμένης γραμμής, οι φορείς παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών ενημερώνουν το κοινό σχετικά, όπως επίσης και για τις δυνατότητες που ορίζονται στις παραγράφους 1, 2, 3 και 4.

Άρθρο 9 Εξαιρέσεις

Τα κράτη μέλη διασφαλίζουν ότι υπάρχουν διαφανείς διαδικασίες που διέπουν τον τρόπο με τον οποίο ο φορέας παροχής δημόσιου τηλεπικοινωνιακού δικτύου ή/και διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας μπορεί να εξουδετερώνει τη δυνατότητα της μη αναγραφής της καλούσας γραμμής:
α) για περιορισμένο χρονικό διάστημα, τη αιτήσει συνδρομητή που ζητεί τον εντοπισμό κακοβούλων ή ενοχλητικών κλήσεων στην περίπτωση αυτή, σύμφωνα με το εθνικό δίκαιο τα δεδομένα που περιέχουν την αναγνώριση της ταυτότητας του καλούντος συνδρομητή αποθηκεύονται και είναι διαθέσιμα από το φορέα παροχής δημόσιου τηλεπικοινωνιακού δικτύου ή/και διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας
β) επί τη βάσει της ανά γραμμή απάλειψης για οργανισμούς που ασχολούνται με τις κλήσεις άμεσης επέμβασης και είναι αναγνωρισμένα από τα κράτη μέλη, όπως οι διωκτικές αρχές, οι υπηρεσίες πρώτων βοηθειών και οι πυροσβεστικές υπηρεσίες, ώστε να δίδεται απάντηση στις κλήσεις αυτές.

Άρθρο 10 Αυτόματη προώθηση κλήσεων

Τα κράτη μέλη διασφαλίζουν ότι κάθε συνδρομητής έχει, ατελώς και μέσω απλού τεχνικού μέσου, τη δυνατότητα να σταματά τις αυτόματα προωθούμενες κλήσεις στην τερματική συσκευή του από τρίτους.

Άρθρο 11 Τηλεφωνικοί κατάλογοι συνδρομητών

1. Τα δεδομένα προσωπικού χαρακτήρα που περιέχονται στους έντυπους ή ηλεκτρονικούς καταλόγους συνδρομητών, τα οποία βρίσκονται στη διάθεση του κοινού ή μπορούν να ληφθούν μέσω των υπηρεσιών πληροφοριών καταλόγου, πρέπει να περιορίζονται στα απαραίτητα για την αναγνώριση της ταυτότητας συγκεκριμένου συνδρομητή, εκτός εάν ο συνδρομητής έχει δώσει τη ρητή συγκατάθεσή του για τη δημοσίευση συμπληρωματικών δεδομένων προσωπικού χαρακτήρα. Ο συνδρομητής δικαιούται, άνευ επιβαρύνσεως και εφόσον το ζητεί, να μην συμπεριλαμβάνεται σε έντυπο ή ηλεκτρονικό κατάλογο, να δηλώνει ότι δεν επιτρέπει τη χρησιμοποίηση των προσωπικών του στοιχείων για απευθείας εμπορική προώθηση, να ζητά να παραλείπεται η διεύθυνσή του εν μέρει και να μην επιτρέπει να υπάρχει αναφορά που να αποκαλύπτει το φύλο του, εφόσον τούτο είναι γλωσσικά εφικτό.

2. Παρά την παράγραφο 1, τα κράτη μέλη δύνανται να επιτρέψουν στο φορέα παροχής της υπηρεσίας να χρεώνει το συνδρομητή που επιθυμεί να μην αναφέρονται τα στοιχεία του στον κατάλογο, υπό τον όρο ότι η χρέωση δεν αποτελεί αντικίνητρο για την άσκηση αυτού του δικαιώματος, και ότι, λαμβάνοντας υπόψη τις απαιτήσεις για την ποιότητα του δημοσίου καταλόγου υπό το πρίσμα της καθολικής υπηρεσίας, περιορίζεται στο πραγματικό κόστος του φορέα παροχής της υπηρεσίας για την προσαρμογή και ενημέρωση της καταστάσεως των συνδρομητών των οποίων τα στοιχεία δεν θα εγγραφούν στο δημόσιο κατάλογο.

3. Τα δικαιώματα που παρέχονται σύμφωνα με την παράγραφο 1 ισχύουν για τους συνδρομητές που είναι φυσικά πρόσωπα. Τα κράτη μέλη οφείλουν επίσης να εξασφαλίζουν, στο πλαίσιο του κοινοτικού δικαίου και των εφαρμοστέων εθνικών νομοθεσιών, ότι τα έννομα συμφέροντα των συνδρομητών που δεν είναι φυσικά πρόσωπα σε ό,τι αφορά την αναγραφή των στοιχείων τους σε δημόσιους καταλόγους προστατεύονται επαρκώς.

Άρθρο 12 Μη ζητηθείσες κλήσεις

1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (αυτομάτων συσκευών κλήσεως) ή συσκευών τηλεομοιοτυπίας (φαξ) για σκοπούς απ' ευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους.

2. Τα κράτη μέλη λαμβάνουν τα ενδεδειγμένα μέτρα προκειμένου να εξασφαλίζεται ατελώς ότι οι μη ζητηθείσες κλήσεις με σκοπό την απ' ευθείας εμπορική προώθηση με μέσα εκτός των προβλεπομένων στην παράγραφο 1, δεν επιτρέπονται χωρίς τη συγκατάθεση των ενδιαφερομένων συνδρομητών ή όταν πρόκειται για συνδρομητές οι οποίοι δεν επιθυμούν να λαμβάνουν αυτές τις κλήσεις η σχετική επιλογή καθορίζεται από την εθνική νομοθεσία.

3. Τα δικαιώματα που παρέχονται σύμφωνα με τις παραγράφους 1 και 2 ισχύουν για τους συνδρομητές που είναι φυσικά πρόσωπα. Τα κράτη μέλη οφείλουν επίσης να εξασφαλίζουν, στο πλαίσιο του κοινοτικού δικαίου και των εφαρμοστέων εθνικών νομοθεσιών, ότι τα έννομα συμφέροντα των συνδρομητών που δεν είναι φυσικά πρόσωπα σε ό,τι αφορά τις μη ζητηθείσες κλήσεις προστατεύονται επαρκώς.

Άρθρο 13 Τεχνικά χαρακτηριστικά και τυποποίηση

1. Κατά την εφαρμογή των διατάξεων της παρούσας οδηγίας, τα κράτη μέλη διασφαλίζουν, με την επιφύλαξη των διατάξεων των παραγράφων 2 και 3, ότι καμία υποχρεωτική απαίτηση σχετικά με ειδικά τεχνικά χαρακτηριστικά δεν επιβάλλεται στις τερματικές συσκευές ή στον άλλο τηλεπικοινωνιακό εξοπλισμό, η οποία θα μπορούσε να

παρακωλύσει τη διάθεση εξοπλισμού στην αγορά ή την ελεύθερη κυκλοφορία του εξοπλισμού αυτού στα κράτη μέλη ή μεταξύ των κρατών μελών.
2. Όταν η εφαρμογή ορισμένων διατάξεων της παρούσας οδηγίας μπορεί να επιτευχθεί μόνο βάσει ειδικών τεχνικών χαρακτηριστικών, τα κράτη μέλη ενημερώνουν σχετικά την Επιτροπή, σύμφωνα με τις διαδικασίες που προβλέπονται στην οδηγία 83/189/ΕΟΚ (), η οποία προβλέπει διαδικασία πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών.
3. Κατά περίπτωση, η Επιτροπή διασφαλίζει την εκπόνηση κοινών ευρωπαϊκών προτύπων για την εφαρμογή των ειδικών τεχνικών χαρακτηριστικών, σύμφωνα με την κοινοτική νομοθεσία που αφορά την προσέγγιση των νομοθεσιών των κρατών μελών σχετικά με τον τηλεπικοινωνιακό τερματικό εξοπλισμό, συμπεριλαμβανομένης της αμοιβαίας αναγνώρισης της συμμόρφωσης του εξοπλισμού αυτού, και με την απόφαση 8/95/ΕΟΚ του Συμβουλίου, της 22ας Δεκεμβρίου 1986, για την τυποποίηση στον τομέα της τεχνολογίας των πληροφοριών και των τηλεπικοινωνιών (8).

Άρθρο 14 Επέκταση του πεδίου εφαρμογής ορισμένων διατάξεων της οδηγίας 95/46/ΕΚ
1. Τα κράτη μέλη δύνανται να λαμβάνουν νομοθετικά μέτρα για να περιορίσουν την εμβέλεια των υποχρεώσεων και δικαιωμάτων που προβλέπονται στα άρθρα 5 και 6 και στο άρθρο 8 παράγραφοι 1, 2, 3 και 4, εφόσον ο περιορισμός αυτός αποτελεί αναγκαίο μέτρο για τη διαφύλαξη της ασφάλειας του κράτους, της εθνικής άμυνας, της δημόσιας ασφάλειας, καθώς και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών παραβάσεων ή της άνευ αδείας χρησιμοποίησης του τηλεπικοινωνιακού συστήματος, όπως προβλέπεται στο άρθρο 13 παράγραφος 1 της οδηγίας 95/46/ΕΚ.
2. Οι διατάξεις του κεφαλαίου ΙΙΙ της οδηγίας 95/46/ΕΚ περί ενδίκων μέσων, ευθύνης και κυρώσεων ισχύουν όσον αφορά τις εθνικές διατάξεις που θεσπίζονται δυνάμει της παρούσας οδηγίας και όσον αφορά τα ατομικά δικαιώματα που απορρέουν από την παρούσα οδηγία.
3. Η ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία έχει συσταθεί δυνάμει του άρθρου 29 της οδηγίας 95/46/ΕΚ, εκτελεί τα καθήκοντα που προβλέπονται στο άρθρο 30 της προαναφερθείσας οδηγίας, όσον αφορά επίσης την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών και των εννόμων συμφερόντων στον τομέα των τηλεπικοινωνιών που αποτελεί το αντικείμενο της παρούσας οδηγίας.
4. Η Επιτροπή, επικουρούμενη από την επιτροπή που έχει συσταθεί με το άρθρο 31 της οδηγίας 95/46/ΕΚ, καθορίζει τις τεχνικές λεπτομέρειες του παραρτήματος σύμφωνα με την οριζόμενη στο εν λόγω άρθρο διαδικασία. Η επιτροπή αυτή συγκαλείται ειδικά για τα θέματα που καλύπτει η παρούσα οδηγία.

Άρθρο 15 Εφαρμογή της οδηγίας
1. Τα κράτη μέλη θέτουν σε ισχύ τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν με την παρούσα οδηγία όχι αργότερα από τις 24 Οκτωβρίου 1998.
Κατά παρέκκλιση του πρώτου εδαφίου, τα κράτη μέλη θέτουν σε ισχύ τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν με το άρθρο 5 της παρούσας οδηγίας όχι αργότερα από τις 24 Οκτωβρίου 2000.
Τα μέτρα αυτά όταν θεσπίζονται από τα κράτη μέλη, περιέχουν αναφορά στην παρούσα οδηγία ή συνοδεύονται από την αναφορά αυτή κατά την επίσημη δημοσίευσή τους. Οι λεπτομέρειες της αναφοράς αυτής καθορίζονται από τα κράτη μέλη.
2. Κατά παρέκκλιση του άρθρου 6 παράγραφος 3, δεν απαιτείται συγκατάθεση όσον

αφορά την επεξεργασία δεδομένων που έχει ήδη αρχίσει κατά την ημερομηνία έναρξης ισχύος των εθνικών διατάξεων που θεσπίζονται δυνάμει της παρούσας οδηγίας. Στις περιπτώσεις αυτές, οι συνδρομητές ενημερώνονται για την επεξεργασία αυτή και, εφόσον δεν εκφράσουν την αντίθεσή τους εντός χρονικού διαστήματος που θα οριστεί από τα κράτη μέλη, θεωρείται ότι έδωσαν τη συγκατάθεσή τους.
3. Το άρθρο 11 δεν ισχύει για εκδόσεις καταλόγων που έχουν κυκλοφορήσει πριν από την έναρξη ισχύος των εθνικών διατάξεων οι οποίες θεσπίζονται δυνάμει της παρούσας οδηγίας.
4. Τα κράτη μέλη ανακοινώνουν στην Επιτροπή τα κείμενα των διατάξεων εσωτερικού δικαίου που θεσπίζουν στον τομέα που διέπεται από την παρούσα οδηγία.

Άρθρο 16 Αποδέκτες
Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Βρυξέλλες, 15 Δεκεμβρίου 199.
Για το Ευρωπαϊκό Κοινοβούλιο
Ο Πρόεδρος
J. M. GIL-ROBLES
Για το Συμβούλιο
Ο Πρόεδρος
J.-C. JUNCKER

Προστασία πνευματικών δικαιωμάτων βάσεων δεδομένων

Πώς ορίζεται και τι περιλαμβάνει η νομική κατοχύρωση των δικαιωμάτων που απορρέουν από τη δημιουργία και διάθεση βάσεων δεδομένων; Σε ποιες περιπτώσεις επιτρέπεται η αναπαραγωγή τους και ποια είναι τα δικαιώματα του δημιουργού; Θα αναλύσουμε τα παραπάνω ζητήματα, στο πλαίσιο της Κοινοτικής νομοθεσίας.

Τι είναι βάση δεδομένων;

Βάση δεδομένων (database) είναι η συλλογή έργων, δεδομένων ή άλλων ανεξάρτητων στοιχείων, που είναι οργανωμένα με συστηματικό ή μεθοδικό τρόπο και προσιτά με ηλεκτρονικά ή άλλα μέσα.

Πώς προστατεύονται οι βάσεις δεδομένων;

Οι βάσεις δεδομένων, σύμφωνα με το άρθρο 3 της Οδηγίας 96/9, αποτελούν πνευματικά δημιουργήματα και ως εκ τούτου προστατεύονται βάσει του δικαιώματος του δημιουργού (πνευματική ιδιοκτησία).

Η προστασία αυτή εκτείνεται και στο περιεχόμενο μιας βάσης δεδομένων;

Η προστασία μιας βάσης δεδομένων, βάσει του δικαιώματος του δημιουργού, δεν εκτείνεται στο περιεχόμενό της. Έτσι, δεν θίγει το δικαίωμα του δημιουργού, τα συγγενικά ή άλλα δικαιώματα ή υποχρεώσεις που υφίστανται επί των δεδομένων, των έργων ή άλλων στοιχείων που είναι ενσωματωμένα στη βάση αυτή.

Ποιος θεωρείται δημιουργός μιας βάσης δεδομένων;

Δημιουργός μιας βάσης δεδομένων είναι το πρόσωπο ή η ομάδα προσώπων που την έχουν δημιουργήσει. Σύμφωνα με το άρθρο 4 της Οδηγίας 96/9, δημιουργός μπορεί να είναι και εταιρία, εφόσον κάτι τέτοιο επιτρέπεται από τη νομοθεσία του κράτους-μέλους, ωστόσο η οδηγία αυτή δεν έχει ενσωματωθεί ακόμα στην ελληνική νομοθεσία.

Μπορεί το κράτος να θέσει περιορισμούς στις παραπάνω πράξεις του δημιουργού;

Το κράτος μπορεί να περιορίσει τα παραπάνω αποκλειστικά δικαιώματα του δημιουργού στις εξής περιπτώσεις:
α) Όταν πρόκειται για αναπαραγωγή μη ηλεκτρονικής βάσης δεδομένων για ιδιωτικούς σκοπούς.
β) Όταν πρόκειται για χρήση αποκλειστικά για εκπαιδευτικούς ή ερευνητικούς σκοπούς, εφόσον αναφέρεται η πηγή, στο βαθμό που η χρήση αυτή δικαιολογείται από τον επιδιωκόμενο μη εμπορικό σκοπό.
γ) Όταν πρόκειται για χρήση λόγω δημόσιας ασφάλειας ή για τους σκοπούς διοικητικής ή δικαστικής διαδικασίας.

Τις παραπάνω επιτρεπόμενες πράξεις μπορεί να τις ενεργεί ο νόμιμος χρήστης μιας βάσης δεδομένων, και πότε;

Ο νόμιμος χρήστης μιας βάσης δεδομένων ή αντιγράφων της μπορεί να εκτελέσει οποιαδήποτε από τις παραπάνω πράξεις, εφόσον είναι αναγκαίες για την πρόσβαση στο περιεχόμενό της, και την κανονική χρησιμοποίησή της χωρίς να απαιτείται άδεια του δημιουργού της βάσης.

Τι είναι εξαγωγή και τι επαναχρησιμοποίηση μιας βάσης δεδομένων;

Εξαγωγή είναι η μόνιμη ή προσωρινή μεταφορά του συνόλου ή ουσιώδους μέρους του περιεχομένου βάσης δεδομένων σε άλλο υπόθεμα, με οποιοδήποτε μέσο ή σε οποιαδήποτε μορφή. Επαναχρησιμοποίηση είναι η πάσης μορφής διάθεση στο κοινό του συνόλου ή ουσιώδους μέρους του περιεχομένου της βάσης με διανομή αντιγράφων, εκμίσθωση, μετάδοση με άμεση επικοινωνία ή με άλλο τρόπο.

Πώς προστατεύεται ο δημιουργός έναντι τρίτων;

Ο δημιουργός μιας βάσης δεδομένων έχει το δικαίωμα να απαγορεύει την εξαγωγή και επαναχρησιμοποίηση του συνόλου ή ουσιώδους μέρους μιας βάσης δεδομένων, εφόσον γίνονται με σκοπό την εκμετάλλευση. Επίσης, μπορεί να απαγορεύσει την εξαγωγή ή επαναχρησιμοποίηση και επουσιωδών μερών της βάσης, εφόσον θίγονται αδικαιολόγητα τα νόμιμα συμφέροντά του.

γίνονται με σκοπό την εκμετάλλευση. Επίσης, μπορεί να απαγορεύσει την εξαγωγή ή επαναχρησιμοποίηση και επουσιωδών μερών της βάσης, εφόσον θίγονται αδικαιολόγητα τα νόμιμα συμφέροντά του.

Πόσο διαρκεί η προστασία αυτή;

Ο δημιουργός της βάσης έχει το παραπάνω δικαίωμα της απαγόρευσης από την ολοκλήρωση της κατασκευής της βάσης και για 15 έτη μετά την 1η Ιανουαρίου του έτους που έπεται της ημερομηνίας ολοκλήρωσης.
Αν η βάση έχει τεθεί στη διάθεση του κοινού προτού περάσει η 15ετία, η διάρκεια της προστασίας βάσει αυτού του δικαιώματος λήγει 15 έτη μετά την 1η Ιανουαρίου του έτους που έπεται της ημερομηνίας κατά την οποία η βάση τέθηκε για πρώτη φορά στη διάθεση του κοινού.
Οποιαδήποτε ουσιώδης τροποποίηση του περιεχομένου της βάσης δεδομένων δημιουργεί νέο δικαίωμα προστασίας, που ισχύει για 15 χρόνια.

Ο νόμιμος χρήστης μιας βάσης μπορεί να προβαίνει σε εξαγωγή ή επαναχρησιμοποίηση της;

Ο νόμιμος χρήστης βάσης δεδομένων μπορεί να εξάγει ή να επαναχρησιμοποιεί μόνο τα επουσιώδη μέρη του περιεχομένου της, για οποιονδήποτε σκοπό, και εφόσον η βάση έχει τεθεί στη διάθεση του κοινού με οποιονδήποτε τρόπο. Δεν μπορεί όμως με τις πράξεις αυτές να θίγει την κανονική εκμετάλλευση της βάσης ή τα νόμιμα συμφέροντα του δημιουργού.

Πότε ο νόμιμος χρήστης μπορεί να εξάγει ή να επαναχρησιμοποιεί ουσιώδες μέρος της βάσης;

Σε τρεις περιπτώσεις ο νόμιμος χρήστης της βάσης δεδομένων που έχει τεθεί στη διάθεση του κοινού με οποιονδήποτε τρόπο, μπορεί να εξάγει ή να επαναχρησιμοποιεί ουσιώδη μέρη του περιεχομένου της χωρίς την άδεια του δημιουργού:
α) Όταν πρόκειται για εξαγωγή του περιεχομένου μη ηλεκτρονικής βάσης δεδομένων, εφόσον αυτό γίνεται για ιδιωτικό σκοπό.
β) Όταν πρόκειται για εξαγωγή με εκπαιδευτικούς ή ερευνητικούς σκοπούς, εφόσον αναφέρεται η πηγή και στο βαθμό που αυτό δικαιολογείται από τον επιδιωκόμενο μη εμπορικό σκοπό.
γ) Όταν πρόκειται για εξαγωγή ή επαναχρησιμοποίηση για λόγους δημόσιας ασφάλειας ή για σκοπούς διοικητικής ή δικαστικής διαδικασίας.

Νομοθεσία	
ΟΔΗΓΙΑ 96/9/ΕΟΚ	ΤΟΥ ΕΥΡΩΠΑΙΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 11ης Μαρτίου 1996 σχετικά με τη νομική προστασία των βάσεων δεδομένων
Πνευματική Ιδιοκτησία: Λίστα Νομικών κειμένων	
Νόμος 2121.1993	Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα.
Ν. 3057/2002	Εναρμόνιση του νόμου 2121/1993 με την Οδηγία 2001/29/ΕΚ.
Ν. 3183/2003	Κύρωση της Συνθήκης του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για τις εκτελέσεις και τα φωνογραφήματα
Ν. 3184/2003	Κύρωση της Συνθήκης του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για την πνευματική ιδιοκτησία
Υπουργικές Αποφάσεις	
Υ.Α. 2170/2003	Υπουργική απόφαση 2170/2003 - Χορήγηση έγκρισης λειτουργίας Οργανισμού Συλλογικής Διαχείρισης με την επωνυμία "ΟΡΓΑΝΙΣΜΟΣ ΣΥΛΛΟΓΙΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΜΟΥΣΙΚΩΝ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ - Η ΑΥΤΟΔΙΑΧΕΙΡΙΣΗ - ΑΣΤΙΚΟΣ ΣΥΝΕΤΑΙΡΙΣΜΟΣ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΕΥΘΥΝΗΣ"
Κοινοτικές Οδηγίες	
Κανονισμός (ΕΚ)1383/2003	Για την παρέμβαση των τελωνειακών αρχών έναντι εμπορευμάτων που είναι ύποπτα ότι παραβιάζουν ορισμένα δικαιώματα πνευματικής ιδιοκτησίας.
Οδηγία 2001/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου	Για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας
Οδηγία 93/98/ΕΟΚ του Συμβουλίου	Περί εναρμονίσεως της διάρκειας προστασίας του δικαιώματος πνευματικής ιδιοκτησίας και ορισμένων συγγενών δικαιωμάτων

ΠΑΡΑΡΤΗΜΑ

4.1 ΥΠΟΔΕΙΓΜΑΤΙΚΕΣ ΕΡΩΤΗΣΕΙΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

Μέσω των ακόλουθων ερωτήσεων στο προσωπικό, μπορούμε να αποκτήσουμε μία γενική εικόνα για τα λειτουργικά χαρακτηριστικά του οργανισμού. Οι ερωτήσεις αυτές θα πρέπει να αναπτυχθούν βάσει του πληροφοριακού συστήματος που χρησιμοποιείται από τον οργανισμό. Οι απαντήσεις που θα λάβουμε, εκτός του ότι θα συμβάλουν στην κατανόηση του συστήματος, θα συνεισφέρουν επίσης στην διαδικασία εκτίμησης επικινδυνότητας.

- Ποιοι είναι επικυρωμένοι χρήστες;
- Ποιος είναι ο σκοπός του οργανισμού;
- Ποιος είναι ο σκοπός του συστήματος σε σχέση με την αποστολή;
- Πόσο σημαντικό είναι το σύστημα στην αποστολή του οργανισμού;
- Ποια είναι η απαίτηση διαθεσιμότητας του συστήματος;
- Τι είδους πληροφορία παράγεται, καταναλώνεται, επεξεργάζεται, αποθηκεύεται και ανακτάται από το σύστημα;
- Πόσο σημαντική είναι η πληροφορία στην αποστολή του οργανισμού;
- Ποια ροή ακολουθεί η πληροφορία;
- Τι είδους πληροφορία επεξεργάζεται και αποθηκεύεται στο σύστημα (πχ. Οικονομική, προσωπική, έρευνας και ανάπτυξης, ιατρική, εντολών και ελέγχου);
- Ποια είναι το επίπεδο ευαισθησίας (ή ταξινόμησης) της πληροφορίας;
- Ποια από τις πληροφορίες που διαχειρίζεται το σύστημα δεν θα πρέπει να αποκαλυφθεί και σε ποιον;
- Που συγκεκριμένα επεξεργάζεται και αποθηκεύεται η πληροφορία;
- Ποια είναι τα είδη αποθήκευσης της πληροφορίας;
- Ποιες είναι οι απαιτήσεις για της διαθεσιμότητα και την ακεραιότητα της πληροφορίας;
- Ποια θα ήταν η επίδραση στην αποστολή του οργανισμού εάν το σύστημα ή η πληροφορία δεν ήταν αξιόπιστη;
- Πόσος είναι ο χρόνος μη λειτουργίας του συστήματος που μπορεί να αντέξει ο οργανισμός; Τι συσχέτιση θα είχε αυτός ο χρόνος με τον χρόνο επιδιόρθωσης του συστήματος; Σε τι άλλες εναλλακτικές επιλογές επεξεργασίας ή επικοινωνίας θα μπορούσε να έχει πρόσβαση ο χρήστης;
- Θα μπορούσε μία δυσλειτουργία του συστήματος να έχει ως αποτέλεσμα τον τραυματισμό;

4.2 Η "ΟΙΚΟΓΕΝΕΙΑ" ΤΩΝ ΠΡΟΤΥΠΩΝ ISO 27000

Η σειρά των ISO/IEC 27000 (που είναι επίσης γνωστή ως 'ISMS Family of Standards' ή 'ISO27k' για συντομία) περιλαμβάνει τα πρότυπα ασφάλειας πληροφοριών που εκδίδονται από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC).

Η σειρά παρέχει τις καλύτερες συστάσεις πάνω στη διαχείριση της ασφάλειας πληροφοριών, τους κινδύνους και τους ελέγχους που πραγματοποιούνται για τα Information Security Management System (ISMS). Στην πραγματικότητα αυτά τα πρότυπα καλύπτουν πολλά περισσότερα από την εμπιστευτικότητα και τεχνικά θέματα ασφαλείας. Όλοι οι οργανισμοί ενθαρρύνονται να εκτιμήσουν τους κινδύνους της ασφάλειας πληροφοριών, έπειτα να εφαρμόσουν τους κατάλληλους ελέγχους ασφάλειας πληροφοριών σύμφωνα με τις ανάγκες τους, χρησιμοποιώντας καθοδήγηση και συστάσεις όπου κρίνεται απαραίτητο.

Τα πρότυπα εφαρμόζονται σε οργανισμούς κάθε είδους και μεγέθους. Προς το παρόν, τρία από τα πρότυπα είναι διαθέσιμα ενώ πολλά ακόμη είναι υπό ανάπτυξη.

- ISO/IEC 27001 – Το πρότυπο με το οποίο οι οργανισμοί μπορούν να πιστοποιηθούν για την Information Security Management System (ISMS). (εκδόθηκε το 2005)
- ISO/IEC 27002 – Το πρότυπο με καλές συμβουλές πάνω στα ISMS (στο παρελθόν ήταν γνωστό ως το ISO 17799 και πριν από αυτό ήταν το BS 7799 Part 1 (η τελευταία επισκόπηση έγινε το 2005, και έπειτα μετονομάστηκε σε ISO/IEC 27002:2005 τον Ιούλιο του 2007)
- ISO/IEC 27006 – Ένας οδηγός για την διαδικασία πιστοποίησης/δήλωσης (εκδόθηκε το 2007)

Υπό σχεδιασμό βρίσκονται τα ακόλουθα πρότυπα:

- ISO/IEC 27000 – Μία εισαγωγή για την οικογένεια των προτύπων ISMS, και επιπλέον λεξικό με τους συνηθισμένους όρους.
- ISO/IEC 27003 – Ένας οδηγός εφαρμογής του ISMS.
- ISO/IEC 27004 – Ένα πρότυπο για τις μετρήσεις διαχείρισης της ασφάλειας πληροφοριών.
- ISO/IEC 27005 – Ένα πρότυπο για την διαχείριση των κινδύνων ασφαλείας των πληροφοριών.
- ISO/IEC 27007 – Ένας οδηγός για τον διαχειριστικό έλεγχο των ISMS (επικεντρώνεται στα συστήματα διοίκησης).
- ISO/IEC 27008 – Ένας οδηγός για τον διαχειριστικό έλεγχο της ασφάλειας πληροφοριών (Επικεντρώνεται στους ελέγχους ασφαλείας).
- ISO/IEC 27011 – Ένας οδηγός εφαρμογής ISMS για την βιομηχανία των τηλεπικοινωνιών (είναι επίσης γνωστό ως X.1051).
- ISO/IEC 27031 – Μία ειδίκευση για την ICT ετοιμότητα για τις επιχειρηματικές δραστηριότητες.
- ISO/IEC 27032 – Ένας οδηγός για την ασφάλεια στο διαδίκτυο.

- ISO/IEC 27033 – Δικτυακή ασφάλεια των πληροφοριακών συστημάτων, ένα πρότυπο με πολλές ενότητες το οποίο είναι στην παρούσα φάση γνωστό ως ISO/IEC 18028:2006.
- ISO/IEC 27034 – Ένας οδηγός για την εφαρμογή ασφαλείας.

ISO/IEC 27001

Το ISO/IEC 27001 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) το οποίο εκδόθηκε τον Οκτώβρη του 2005 από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Το πλήρες του όνομα είναι ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements αλλά για λόγους συντομίας αναφερόμαστε σε αυτό με το "ISO 27001".

Πρόκειται να χρησιμοποιηθεί σε συνδυασμό με το ISO/IEC 27002, the Code of Practice for Information Security Management, το οποίο βρίσκεται στην λίστα των σκοπών ελέγχου ασφαλείας και συνιστά ένα εύρος συγκεκριμένων ελέγχων ασφαλείας. Οι οργανισμοί οι οποίο θα εφαρμόσουν ένα ISMS σύμφωνα με την καλύτερη πρακτική συμβουλή στο ISO/IEC 27002 είναι πιθανότατα ταυτόχρονα καλυμμένοι για τις απαιτήσεις του ISO/IEC 27001 αλλά η επικύρωση με το δίπλωμα είναι καθαρά προαιρετική.

Η πιστοποίηση με το πρότυπο ISO/IEC 27001, συνήθως εμπεριέχει μία διαδικασία με τρία βήματα:

- Στο πρώτο βήμα γίνεται μία ανασκόπηση της ύπαρξης και της πληρότητας σημαντικών εγγράφων όπως η πολιτική ασφαλείας του οργανισμού, Statement of Applicability (SoA) and Risk Treatment Plan (RTP).
- Στο δεύτερο βήμα γίνεται ένας λεπτομερείς, σε βάθος έλεγχος για την ύπαρξη και την αποτελεσματικότητα των ελέγχων ασφάλειας που δηλώνονται στο SoA και στο RTP, καθώς επίσης και τα υποστηρικτικά τους έγγραφα.
- Στο τρίτο βήμα πραγματοποιείται μία επανεκτίμηση για να επιβεβαιώσει ότι ο οργανισμός ο οποίος έχει ήδη πιστοποιηθεί, παραμένει συμμορφωμένος με το πρότυπο. Η συντήρηση της πιστοποίησης περιέχει περιοδικές ανασκοπήσεις και επανεκτιμήσεις για να επιβεβαιωθεί ότι το ISMS συνεχίζει να λειτουργεί όπως έχει καθοριστεί.

ISO/IEC 27002

Το ISO/IEC 27002 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) το οποίο εκδόθηκε από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC) ως το ISO/IEC 17799:2005 και έπειτα αριθμήθηκε ως το ISO/IEC 27002:2005 τον Ιούλιο του 2007, φέρνοντας το στην σειρά των προτύπων ISO/IEC 27000. Έχει τον τίτλο Information technology -- Security techniques – Code of practice for information security management. Το παρόν πρότυπο είναι μία επανάληψη της πρώτης έκδοσης που δημοσιεύτηκε από την ISO/IEC το 2000, αλλά ήταν μία λέξη προς λέξη αντιγραφή του British Standard (BS) 7799-1:1999.

Το ISO/IEC 27002 παρέχει βελτιωμένες συστάσεις για την διαχείριση της ασφάλειας πληροφοριών για την αρχικοποίηση, την εφαρμογή ή την συντήρηση των Information Security Management Systems (ISMS). Συνοπτικά, η ασφάλεια πληροφοριών καθορίζεται μέσα στο πρότυπο από το ακόλουθο κείμενο:
Η συντήρηση της εμπιστευτικότητας (διασφαλίζοντας ότι η πρόσβαση στην πληροφορία γίνεται μόνο απ' όσους έχουν εξουσιοδοτηθεί για να έχουν πρόσβαση), η ακεραιότητα (ασφαλίζοντας την ακρίβεια και την πληρότητα της πληροφορίας και των μεθόδων επεξεργασίας) και την διαθεσιμότητα (εξασφαλίζοντας ότι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στην πληροφορία που σχετίζεται με τα αγαθά, όταν απαιτείται).

Μετά το εισαγωγικό μέρος, το πρότυπο περιέχει τις ακόλουθες κύριες ενότητες:

1. Εκτίμηση Επικινδυνότητας
2. Πολιτική ασφαλείας – διοικητική καθοδήγηση
3. Οργανωτική ασφάλεια
4. Διαχείριση Αγαθών – ταξινόμηση των πληροφοριακών αγαθών
5. Ασφάλεια Προσωπικού
6. Φυσική και περιβαλλοντολογική ασφάλεια
7. Διαχείριση επικοινωνιών και διεργασιών
8. Έλεγχος πρόσβασης – περιορισμός των δικαιωμάτων πρόσβασης σε δίκτυα, συστήματα, εφαρμογές και δεδομένα
9. Απόκτηση, ανάπτυξη και συντήρηση των πληροφοριακών συστημάτων
10. Διαχείριση περιστατικών ασφαλείας πληροφοριών
11. Διαχείριση της επιχειρηματικής συνέχειας – προστασία, συντήρηση, και ανάρρωση των ευαίσθητων επιχειρηματικών διαδικασιών και συστημάτων
12. Συμμόρφωση – διασφάλιση της συμμόρφωσης με τις πολιτικές ασφαλείας, τα πρότυπα, το νόμο και τους κανονισμούς

ISO/IEC 27006

Το ISO/IEC 27006 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC ISMS standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Η έκδοση του 2007 έχει τίτλο Information technology - Security techniques – Requirements for bodies providing audit and certification of information security management systems.

Το ISO/IEC 27006 προσφέρει οδηγίες για την λειτουργική πιστοποίησης/ δήλωση των Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών.

- Το πρότυπο περιέχει τις ακόλουθες ενότητες:
- Σκοπός
- Normative references
- Όροι και ορισμοί
- Αρχές
- Γενικές απαιτήσεις
- Κατασκευαστικές απαιτήσεις
- Απαιτήσεις πηγών
- Απαιτήσεις πληροφοριών
- Απαιτήσεις διαδικασιών

- Απαιτήσεις διαχείρισης συστημάτων

ISO/IEC 27000

Το ISO/IEC 27000 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC ISMS standards ('ISO/IEC 27000 series'). Αυτός ο αριθμός που έχει κατοχυρωθεί για το νέο διεθνές πρότυπο, το οποίο προς το παρόν έχει τον τίτλο: "Information technology - Security techniques - Information security management systems - Overview and vocabulary". Το πρότυπο είναι γνωστό ανεπίσημα ως το "ISO 27000".

Το πρότυπο είναι υπό ανάπτυξη από το Joint Technical Committee (JTC1) του International Organization for Standardization και την International Electrotechnical Commission.

Το ISO 27000 θα παρέχει μία γενική εικόνα των προτύπων που σχετίζονται με την οικογένεια προτύπων του ISO/IEC 27000 Information Security Management Systems (ISMS) και θα παρέχει ομοιομορφία και συνοχή των σημαντικών όρων και ορισμών (λεξιλόγιο) που χρησιμοποιούνται στην οικογένεια του ISMS.

Η ασφάλεια πληροφοριών, όπως πολλά τεχνικά θέματα, αναπτύσσεται με μία πολύπλοκη ορολογία. Το αρνητικό είναι ότι μόνο λίγοι συγγραφείς μπαίνουν στην διαδικασία να καθορίσουν επακριβώς τι εννοούν, μία προσέγγιση η οποία είναι μη-αποδεκτή καθώς οδηγεί σε σύγχυση και απαξιεί την επίσημη πιστοποίηση.

Η παρούσα έκδοση δεν έχει ακόμη δημοσιοποιηθεί, υπολογίζεται ότι αυτό θα γίνει περίπου το 2008 και στοχεύει στους χρήστες των προτύπων της σειράς ISO/IEC 27000-information security management standards.

ISO/IEC 27003

Το ISO/IEC 27003 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC ISMS standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών που στην παρούσα φάση είναι υπό ανάπτυξη από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Ο τρέχων τίτλος του είναι Security techniques – Information Security Management system οδηγίες εφαρμογής.

Ο σκοπός του ISO/IEC 27003 είναι να παρέχει βοήθεια και καθοδήγηση στην εφαρμογή ενός ISMS (Information Security Management System). Η έκδοση του δεν αναμένεται μέχρι το τέλος του 2008 ή στις αρχές του 2009.

Το προτεινόμενο πρότυπο αρχικά περιείχε τις ακόλουθες ενότητες

- Εισαγωγή
- Σκοπός
- Όροι και ορισμοί
- CSFs (Critical success factors)
- Οδηγίες στην προσέγγιση διαδικασιών
- Οδηγίες για την χρησιμοποίηση PDCA
- Οδηγίες για την Διαδικασία Σχεδιασμού
- Οδηγίες για την Διαδικασία Δραστηριοτήτων
- Οδηγίες για την Διαδικασία Ελέγχου

- Οδηγίες για την Διαδικασία Δράσης
- Συνεργασία μέσα στον οργανισμό

ISO/IEC 27004

Το ISO/IEC 27004 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC ISMS standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών που στην παρούσα φάση είναι υπό ανάπτυξη από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Ο τρέχων τίτλος του είναι Information technology - Security techniques -- Information security management measurements.

Ο σκοπός του ISO/IEC 27004 είναι να βοηθήσει τους οργανισμούς να μετρήσουν και να αναφέρουν την αποτελεσματικότητα των συστημάτων διαχείρισης της ασφάλειας πληροφοριών, καλύπτοντας παράλληλα την διαδικασία διαχείρισης της ασφάλειας και τους ελέγχους. Η έκδοση του δεν αναμένεται μέχρι το 2008.

ISO/IEC 27005

Το ISO/IEC 27005 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC ISMS standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών το οποίο βρίσκεται υπό ανάπτυξη από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Ο τρέχων τίτλος του είναι Information technology - Security techniques -- Information security risk management.

Ο σκοπός του ISO/IEC 27005 είναι να παράσχει τεχνικές για την εκτίμηση επικινδυνότητας της ασφάλειας πληροφοριών και διαχείριση κινδύνων ασφαλείας της τεχνολογίας των επικοινωνιών. Αυτό το πρότυπο εκδόθηκε τον Ιούνιο του 2008.

ISO/IEC 27007

Το ISO/IEC 27007 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC ISMS standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών το οποίο βρίσκεται υπό ανάπτυξη από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Ο τρέχων τίτλος του είναι Security techniques -- Guidelines for Information security management systems auditing.

Ο σκοπός του ISO/IEC 27007 είναι να παρέχει καθοδήγηση εξουσιοδοτημένη πιστοποίηση για τα Information Security Management Systems ενάντια στο ISO/IEC 27001. Η έκδοση του δεν αναμένεται μέχρι το 2009.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Risk Management Guide for Information Technology Systems, **Recommendations of the National Institute of Standards and Technology** Gary Stoneburner, Alice Goguen, and Alexis Feringa
- INFORMATION SECURITY, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8930, Ron Ross ,Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner
- European Network and Information Security Agency http://www.enisa.europa.eu
- The free Encyclopedia http://www.wikipedia.com
- Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών http://www.adae.gr
- Επίσημος κόμβος της "Εκπαιδευτικής Στήριξης του Δικτυωθείτε" http://www.go-online.gr
- SANS Institute, The SANS Security Policy Project, http://www.sans.org/resources/policies
- SANS Institute, InfoSec Acceptable Use Policy, 2006, http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf
- SANS Institute, Development of an Effective Communications Use Policy, Jul. 2001, https://www2.sans.org/reading_room/whitepapers/policyissues/485.php
- CISCO Systems, Acceptable Use Policy Template, Nov. 2006, http://www.first.org/resources/guides/aup_generic.doc
- Entanet, Acceptable Use Policy, http://www.enta.net/Policies/Acceptable_Use_Policy
- SurfControl, How to Write an Acceptable Use Policy, http://www.surfcontrol.com/uploadedfiles/AUP_Booklet_10011_uk.pdf
- http://www.rusecure.co.uk/
- http://www.noc.ntua.gr/binary/pdf/PolitikiXrisis.pdf
- http://www.acci.gr/ecomm/legal/pdf/reg_632%20.pdf
- http://www.netaction.gr/terms.asp
- http://www.forthnet.gr/templates/policy.html
- International Standard ISO/IEC 27002 Information Technology, code of practice for information security management
- http://www.lawnet.gr Legal Search Engines