Κεφάλαιο 1

Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση

Δημήτρης Γκρίτζαλης

Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών
Πατησίων 76, Αθήνα 10434
email: dgrit@aueb.gr

Περίληψη

Στόχος του κεφαλαίου αυτού είναι να αποτελέσει ένα εύχρηστο κείμενο αναφοράς, που θα βοηθήσει τον αναγνώστη να κατανοήσει και να διασυνδέσει μεταξύ τους τις έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων και Υποδομών. Σημείωνεται ότι στις έννοιες που περιγράφονται δεν έχουν περιληφθεί αυτές της Κρυπτολογίας. *Ευχαριστώ τον Κ. Λαμπρινουδάκη για τη συνεισφορά του στην επιλογή των όρων της Ασφάλειας Υποδομών, το Σ. Κοκολάκη για τη συνεισφορά του στην απόδοση των όρων στην ελληνική γλώσσα, καθώς και τους φοιτητές του Μεταπτυχιακού Προγράμματος Σπουδών του Οικονομικού Πανεπιστημίου Αθηνών στα Πληροφορικά Συστήματα για τα γόνιμα σχόλια και τις παρατηρήσεις τους. Τέλος, ευχαριστώ την Ευρωπαϊκή Επιτροπή γιατί έθεσε στη διάθεσή μου τα αποτελέσματα σχετικών μελετών.*

1.1 Εισαγωγή

Στο παρόν κεφάλαιο περιγράφονται οι βασικότερες έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων και Υποδομών. Οι έννοιες αυτές θα χρησιμοποιηθούν στη συνέχεια για την ομαδοποίηση επιμέρους όρων-εννοιών της γνωστικής αυτής

περιοχής, για την περιγραφή των όρων αυτών, καθώς και για την εννοιολογική συσχέτισή τους.

Η Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών αφορά οντότητες και αντικείμενα που αξίζει να προστατευθούν. Ο,τι αξίζει να προστατευθεί ονομάζεται Αγαθό (Asset). Τα Αγαθά αξίζει να προστατευθούν επειδή έχουν Αξία (Value). Η Αξία τους μπορεί να μειωθεί αν υποστούν Ζημιά. Τα Αγαθά χρειάζονται προστασία μόνον αν υπάρχουν Κίνδυνοι (Dangers) που είναι μπορεί να τους προκαλέσουν Ζημιά (Harm). Ο Ιδιοκτήτης (Owner) ενός προστατευόμενου Αγαθού χρησιμοποιεί Μέσα Προστασίας (Safeguards) είτε για να μειώσει τον Κίνδυνο να προξενηθεί Ζημιά στο Αγαθό είτε για να μειώσει τις συνέπειές της.

Η χρήση Μέσων Προστασίας επιφέρει Κόστος. Δεδομένου ότι τα Μέσα Προστασίας δεν μπορούν να εγγυηθούν πλήρη ασφάλεια, το Κόστος τους πρέπει να αναλογεί στην Επισφάλεια (Hazard) του Αγαθού αυτού, καθώς και στις συνέπειες που θα έχει μια Ζημιά στον Ιδιοκτήτη του. Ο Ιδιοκτήτης είναι εκείνος που θα κρίνει, όταν θέτει το Στόχο Ασφάλειας (Infosec Goal), ποια είναι η πιο επωφελής ισορροπία ανάμεσα στο Κόστος, την Επισφάλεια και τις Συνέπειες. Ο Ιδιοκτήτης μπορεί, επίσης, να αναζητήσει Εξασφάλιση (Assurance) ότι ο Στόχος του θα επιτευχθεί με τα Μέσα Προστασίας που θα χρησιμοποιήσει.

Αφού τα αγαθά υπάρχουν για να αξιοποιούνται, ενδιαφέρον αποκτά η έννοια τόσο του Χρήστη όσο και του Ιδιοκτήτη τους. Κάθε αγαθό έχει Ιδιότητες (Attributes) που πρέπει να προστατευθούν. Οι Ζημιές μπορεί να προκληθούν από Κινδύνους και αφορούν Ζημιές όχι στα Αγαθά, αλλά στις Ιδιότητές τους. Οι ζημιές εκτιμούνται από τον Ιδιοκτήτη ή το Χρήστη. Ο Ιδιοκτήτης είναι αυτός που θα καθορίσει τους Στόχους, οι οποίοι προσδιορίζουν τη μέγιστη ανεκτή Ζημιά που οι Ιδιότητες μπορούν να υποστούν. Τα Μέσα Προστασίας αντιμετωπίζουν τους Κινδύνους αποτρέποντας τις Ζημιές και προστατεύουν τις Ιδιότητες και τα Αγαθά. Ο όρος Εξασφάλιση υπονοεί ότι τα Μέσα Προστασίας μπορούν να αντιμετωπίσουν τους Κινδύνους προστατεύοντας τα Αγαθά και τις Ιδιότητές τους από Ζημιές.

Ακολουθώντας την παραπάνω τακτική θα μπορούσαμε να κάνουμε μια περιδιάβαση στις περισσότερες έννοιες της γνωστικής περιοχής, αλλά δεν θα μπορούσαμε να αποκτήσουμε μια συστηματική εικόνα για το πως διασυνδέονται μεταξύ τους οι έννοιες αυτές. Ετσι, στη συνέχεια θα εργασθούμε διαφορετικά. Πιο συγκεκριμένα, οι έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων και Υποδομών θα ταξινομηθούν πρώτα σε ομάδες-δένδρα συναφών όρων και - στη συνέχεια - κάθε δένδρο θα αναλυθεί ξεχωριστά. Οι βασικές έννοιες-ρίζες των εννοιολογικών δένδρων είναι: *Αγαθά, Ιδιοκτήτες και Χρήστες, Ιδιότητες, Κίνδυνοι, Στόχοι, Εξασφάλιση, Μέσα Προστασίας*.

1.2 Αγαθά

Τα Αγαθά που μας ενδιαφέρουν είναι δύο ειδών, η Πληροφορία (ή τα Δεδομένα) και οι Υπολογιστικοί ή άλλοι Πόροι που χρησιμοποιούμε για να επεξεργασθούμε τις Πληροφορίες και τα Δεδομένα. Η ταξινόμηση αυτή είναι σημαντική επειδή οι Κίνδυνοι που αντιμετωπίζει ένα Αγαθό, η Ζημιά που μπορεί να προκληθεί, καθώς

και τα Μέσα Προστασίας για να αντιμετωπιστούν οι Κίνδυνοι και οι Ζημιές είναι διαφορετικά για κάθε είδος Αγαθού. Οι βασικές έννοιες που εντάσσονται στο δένδρο των Αγαθών είναι: Πληροφοριακό Σύστημα, Υπολογιστικό Σύστημα, Υ-πολογιστικό Συγκρότημα, Υπολογιστικοί Πόροι, Πληροφορίες, Δεδομένα.

Ενα Υπολογιστικό Συγκρότημα αποτελείται από Υπολογιστικούς Πόρους. Οι Πληροφορίες αποτελούνται από Δεδομένα που έχουν ένα νόημα και από την ερμηνεία που χρειάζονται για να αποδοθεί το νόημα αυτό στα Δεδομένα. Με δεδομένο περιβάλλον και σκοπό, το Υπολογιστικό Συγκρότημα γίνεται Υπολογιστικό Σύστημα.

Δεδομένα (Data)	Ενα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί.
Πληροφορία (Information)	Τα δεδομένα μαζί με την έννοια που τους αποδίδεται.

Οι έννοιες Πληροφοριακό Σύστημα, Υπολογιστικό Σύστημα και Υπολογιστικό Συ-γκρότημα συγκροτούν μία ιεραρχία όρων, στην οποία το Πληροφοριακό Σύστημα βρίσκεται στο υψηλότερο επίπεδο και το Υπολογιστικό Συγκρότημα στο χαμηλότερο. Ενα Υπολογιστικό Σύστημα ορίζεται μέσω του Υπολογιστικού Συγκροτήματος και ένα Πληροφοριακό Σύστημα ορίζεται μέσω του Υπολογιστικού Συστήματος.

Η ουσία της έννοιας Υπολογιστικό Συγκρότημα είναι ότι αποτελεί μόνο μία συλ-λογή από υπολογιστικά και άλλα στοιχεία (πχ. υλικό, λογισμικό, τηλεπικοινωνιακός εξοπλισμός κλπ.) τα οποία, ως σύνολο, είναι από μόνα τους ικανά να επεξεργασθούν Πληροφορίες (ή Δεδομένα) και να παράσχουν ένα επίπεδο λειτουργικότητας.

Η έννοια του Υπολογιστικού Συστήματος περιλαμβάνει, εκτός από τα τεχνικά συ-στατικά του, το λειτουργικό περιβάλλον και το σκοπό για τον οποίο το Υπολογιστικό Σύστημα υπάρχει. Το λειτουργικό περιβάλλον περιλαμβάνει και τους ανθρώπους που είναι απαραίτητοι για τη λειτουργία των τεχνικών μερών του συστήματος και που θεωρούνται ως Υπολογιστικοί Πόροι. Ο σκοπός του Υπολογιστικού Συστήματος εκφράζεται μέσω του λογισμικού εφαρμογών.

Η έννοια του Πληροφοριακού Συστήματος περιλαμβάνει όλα τα τεχνικά συστατικά του Υπολογιστικού Συγκροτήματος, το περιβάλλον στο οποίο λειτουργεί το σύστημα, το σκοπό (όλα μαζί συγκροτούν το Υπολογιστικό Σύστημα) και επιπλέον τις Πληροφορίες. Στο βαθμό που οι άνθρωποι είναι υπεύ-θυνοι για την μεταφορά της Πληροφορίας στο Υπολογιστικό Σύστημα, και συνεπώς εκτελούν λειτουργίες απαραίτητες για την πληρότητα και την ακρίβεια των Πληροφοριών, μπορεί να θεωρηθεί ότι αποτελούν μέρος του ίδιου του Πληρο-φοριακού Συστήματος.

Η έννοια των Υπολογιστικών Πόρων περιλαμβάνει κάθε στοιχείο του Υπολογιστικού Συστήματος, εκτός από τις Πληροφορίες ή τα Δεδομένα που διαχειρίζεται. Αντίθετα με το Υπολογιστικό Συγκρότημα, οι Υπολογιστικοί Πόροι

δεν είναι απαραίτητο να διαχειρίζονται τις Πληροφορίες από μόνοι τους, με την προϋπόθεση ότι θα μπορούν να το κάνουν με τη συνεργασία άλλων Υπολογιστικών Πόρων. Ενα Υπολογιστικό Συγκρότημα και ένα Υπολογιστικό Σύστημα είναι και τα δύο παραδείγματα Υπολογιστικών Πόρων. Ενα Πληροφοριακό Σύστημα δεν είναι Υπολογιστικός Πόρος.

Υπολογιστικό Συγκρότημα (IT Assembly)	Συλλογή υπολογιστικού υλικού, λογισμικού, τηλεπικοινωνιακού εξοπλισμού ή άλλων υπολογιστικών εξαρτημάτων που χρησιμοποιείται για τη διαχείριση πληροφοριών.
Υπολογιστικό Σύστημα (IT System)	Υπολογιστικό Συγκρότημα εγκατεστημένο σε συγκεκριμένη τοποθεσία, με συγκεκριμένο λειτουργικό περιβάλλον, που ανταποκρίνεται σε συγκεκριμένο σκοπό.
Πληροφοριακό Σύστημα (Information System)	Υπολογιστικό Συγκρότημα μαζί με τις πληροφορίες που διαχειρίζεται.
Υπολογιστικός Πόρος (IT Resource)	Οτιδήποτε αξιοποιείται από ένα υπολογιστικό σύστημα για να διαχειριστεί πληροφορίες.

Η Εφαρμογή είναι ένας συνδυασμός Υπολογιστικών Πόρων και Πληροφοριών.

Εφαρμογή (Application)	Πληροφορίες, λογισμικό και διαδικασίες που έχουν σχεδιαστεί για την επίτευξη συγκεκριμένων στόχων.

Το Υπολογιστικό Αντικείμενο χαρακτηρίζει κάθε μέρος ενός συνόλου που αποτελείται από: Υπολογιστικό Συγκρότημα, Υπολογιστικό Σύστημα, Πληροφοριακό Σύστημα, Υπολογιστικό Εξάρτημα (IT component) και Υπολογιστικό Προϊόν (IT product).

Υπολογιστικό Αντικείμενο (IT Object)	Υπολογιστικό συγκρότημα ή υπολογιστικό σύστημα ή πληροφοριακό σύστημα ή υπολογιστικό εξάρτημα ή προϊόν.
Αξία (Value)	Σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.

Αγαθό (Asset) Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία.

1.3 Ιδιοκτήτης και Χρήστης

Αν τα Αγαθά έχουν Αξία, τότε ανήκουν σε κάποιον και θα χρησιμοποιηθούν για κάποιο σκοπό. Αυτό εισάγει τις έννοιες του Ιδιοκτήτη και του Χρήστη. Ούτε οι Ι-διοκτήτες ούτε οι Χρήστες είναι απαραίτητο να είναι φυσικά πρόσωπα (πχ. ο Χρήστης μπορεί να είναι διεργασία). Η αστική έννοια της ιδιοκτησίας συνεπάγεται ότι ο Χρήστης έχει το δικαίωμα να καθορίζει τον τρόπο διαχείρισης των Αγαθών.

Ιδιοκτήτης (Owner) Πρόσωπο που κατέχει ή είναι υπεύθυνο για ένα αγαθό και που έχει το δικαίωμα να καθορίσει πώς μπορεί να χρησιμοποιηθεί, να μεταβληθεί ή να διατεθεί το αγαθό αυτό.

Αναφέρονται, επίσης, οι (αυτονόητοι) όροι: Ιδιοκτήτης Πληροφοριών (Information Owner) και Ιδιοκτήτης Συστήματος (System Owner). Η έννοια του Ιδιοκτήτη εισάγει την έννοια της Εξουσιοδότησης.

Εξουσιοδότηση (Authorisation) Αδεια που παρέχεται από έναν ιδιοκτήτη για κάποιο σκοπό.

Εξουσιοδοτημένος (Authorised) Με την άδεια του ιδιοκτήτη για κάποιο σκοπό.

Μη Εξουσιοδοτημένος (Unauthorised) Χωρίς την άδεια του ιδιοκτήτη για κάποιο σκοπό.

Εκτός από τους Ιδιοκτήτες, τα Αγαθά τα αξιοποιουν και Χρήστες (που μπορεί να είναι ή να μην είναι τα ίδια πρόσωπα με τους Ιδιοκτήτες).

Χρήστης (User) Προσωπο ή διεργασία που χρησιμοποιεί ολόκληρο ή μέρος του πληροφοριακού συστήματος.

1.4 Ιδιότητες

Δεν έχει νόημα να υπάρχουν Αγαθά αν δεν μπορούν να χρησιμοποιηθούν για να εκπληρωθεί κάποιος σκοπός. Τα περισσότερα Αγαθά που έχουν σχέση με τα Πληροφοριακά Συστήματα χρησιμοποιούνται για να παράσχουν κάποιου είδους Υπηρεσίες.

Υπηρεσία (Service) Σύνολο λειτουργιών που παρέχονται σε ένα χρήστη από ένα υπολογιστικό σύστημα.

Συχνά απαιτείται συνεχής παροχή Υπηρεσιών στους Εξουσιοδοτημένους Χρήστες, καθώς και προστασία τους από τους Μη Εξουσιοδοτημένους. Για να αξιοποιηθεί ένα Αγαθό από ένα Χρήστη, πρέπει ο Χρήστης να μπορεί να το προσπελάσει. Υπάρχουν δύο είδη Προσπέλασης: Προσπέλαση Πληροφορίας και Προσπέλαση Συστήματος.

Προσπέλαση (Access)	Η δυνατότητα μιας οντότητας να αξιοποιεί πληροφορίες ή υπολογιστικούς πόρους, στο πλαίσιο ενός πληροφοριακού συστήματος.
Προσπέλαση Πληροφορίας (Information Access)	Η δυνατότητα κάποιου να χρησιμοποιεί συγκεκριμένες πληροφορίες ενός πληροφοριακού συστήματος.
Προσπέλαση Συστήματος (System Access)	Η δυνατότητα κάποιου να χρησιμοποιεί υπολογιστικούς πόρους στο πλαίσιο ενός πληροφοριακού συστήματος.

Συχνά πρέπει να εξουσιοδοτήσουμε ορισμένους χρήστες για κάποια μορφή Προσπέλασης, αλλά - ταυτόχρονα - να αρνηθούμε την εξουσιοδότηση αυτή σε άλλους. Ετσι, υπάρχουν δύο προσεγγίσεις της προστασίας των Ιδιοτήτων των Αγαθών που βασίζονται στην εξασφάλιση ότι οι Χρήστες: α) μπορούν να κάνουν με τα Αγαθά μόνον ό,τι έχουν Εξουσιοδοτηθεί, β) έχουν περιοριστεί να κάνουν μόνον ό,τι έχουν Εξουσιοδοτηθεί. Τα Αγαθά χωρίζονται σε Πληροφορίες (ή Δεδομένα) και σε Υπολογιστικούς Πόρους. Οι πράξεις, τις οποίες ένας Ιδιοκτήτης επιθυμεί να δώσει τη δυνατότητα στους χρήστες να εκτελούν ή όχι, διαφέρουν ανάλογα με το είδος των Αγαθών. Οι Ιδιότητες μπορούν να ταξινομηθούν σε σχέση με το αν αφορούν Πληροφορίες, Υπολογιστικούς Πόρους ή και τα δύο. Οι Ιδιότητες και η ταξινόμησή τους, σύμφωνα με το παραπάνω πλαίσιο, παρουσιάζονται στον Πίνακα 1.1.

	Περιορίζουν	***Επιτρέπουν***	***Ουδέτεροι/Μικτοί***
Πληροφορία	Εμπιστευτικότητα Ακεραιότητα Αυθεντικότητα	Διαθεσιμότητα Πληροφοριών Εγκυρότητα	Προσπέλαση Πληροφοριών Ασφάλεια Πληροφοριών
Υπολογιστικοί Πόροι		Διαθεσιμότητα Συστήματος	Προσπέλαση Συστήματος Ασφάλεια Υπολογιστικού Συστήματος
Πληροφοριακό Σύστημα		Διαθεσιμότητα	Προσπέλαση Ασφάλεια Πληροφοριακών Συστημάτων

Πίνακας 1.1: *Ταξινόμηση των ιδιοτήτων των αγαθών*

Οι έννοιες που σχετίζονται με τις Ιδιότητες των Πληροφοριών/Δεδομένων είναι η Ασφάλεια Πληροφοριών, η Διαθεσιμότητα Πληροφοριών, η Εγκυρότητα, η Εμπι-

στευτικότητα, η Ασφάλεια, η Αυθεντικότητα και η Ακεραιότητα. Τρεις από αυτές τις έννοιες (Ακεραιότητα, Αυθεντικότητα, Εγκυρότητα) αφορούν την αποφυγή Μη Εξουσιοδοτημένης/μη επιθυμητής δραστηριότητας του Χρήστη. Η Εγκυρότητα ορίζεται υπό την οπτική γωνία εκείνων που χρησιμοποιούν τις Πληροφορίες του συστήματος. Αυτοί που ενδιαφέρονται για την πληρότητα και την ακρίβειά τους, λόγω των αποφάσεων που πρέπει να λάβουν, είναι οι Χρήστες που διαβάζουν την Πληροφορία.

Η πληρότητα (completeness) και ακρίβεια (accuracy) μιας Πληροφορίας αποτελεί ευθύνη του Ιδιοκτήτη Πληροφοριών καθώς και εκείνων στους οποίους έχει αναθέσει την ευθύνη αυτή. Οι τελευταίοι έχουν τη δυνατότητα να διαβάζουν τις Πληροφορίες, αλλά και να τις τροποποιούν. Ο Ιδιοκτήτης Πληροφοριών ενδιαφέρεται να εκτελούνται μόνον Εξουσιοδοτημένες τροποποιήσεις και μόνο μετά τον έλεγχο της πληρότητας και ακρίβειάς τους. Τα κριτήρια του Ιδιοκτήτη για την πληρότητα και την ακρίβεια μπορεί να είναι λιγότερο αυστηρά από αυτά ορισμένων Χρηστών. Στις περιπτώσεις που ο Ιδιοκτήτης αντιπροσωπεύει όλους τους Χρήστες, η Εγκυρότητα είναι το άθροισμα Ακεραιότητας και Αυθεντικότητας.

Ακεραιότητα (Integrity)	Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.
Αυθεντικότητα (Authenticity)	Αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.
Εγκυρότητα (Validity)	Απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.

Η Ακεραιότητα και η Αυθεντικότητα είναι περιοριστικές έννοιες, ενώ η Εγκυρότητα αφορά παροχή δυνατοτήτων. Η Εμπιστευτικότητα ακολουθεί την οπτική γωνία του Ιδιοκτήτη που ενδιαφέρεται για την αποτροπή της Μη Εξουσιοδοτημένης αποκάλυψης Πληροφοριών. Η Διαθεσιμότητα Πληροφοριών αναφέρεται σε Χρήστη και Ιδιοκτήτη και αφορά την εξασφάλιση ότι μόνο Εξουσιοδοτημένοι Χρήστες μπορούν να λάβουν μέρος σε συγκεκριμένες δραστηριότητες.

Διαθεσιμότητα Πληροφοριών (Information Availability)	Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες.
Εμπιστευτικότητα (Confidentiality)	Αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους.

Η Ασφάλεια Πληροφοριών περιλαμβάνει όλες τις πρωτεύουσες ιδιότητες της Πληροφορίας που χρειάζονται προστασία. Η έννοια της Ασφάλειας είναι πιο περιορισμένη αφού καλύπτει μόνο την έννοια της Εξουσιοδότησης (δεν καλύπτει την ακρίβεια και την πληρότητα).

Ασφάλεια (Security)	Προστασία της διαθεσιμότητας πληροφοριών, της ακεραιότητας και της εμπιστευτικότητας.
Ασφάλεια Πληροφοριών (Information Security)	Διασφάλιση εμπιστευτικότητας, εγκυρότητας, αυθεντικότητας, ακεραιότητας και διαθεσιμότητας πληροφοριών.

Η Εγκυρότητα περιλαμβάνει την Ακεραιότητα και την Αυθεντικότητα, έτσι ώστε η Ασφάλεια Πληροφοριών να είναι ο συνδυασμός των εννοιών: Εμπιστευτικότητα, Διαθεσιμότητα Πληροφοριών, Εγκυρότητα.

Υπάρχουν δύο έννοιες που αφορούν στην προστασία των Ιδιοτήτων των Υπολογιστικών Πόρων: Διαθεσιμότητα Συστήματος και Ασφάλεια Υπολογιστικού Συστήματος. Η Διαθεσιμότητα Συστήματος επιδιώκει να εξασφαλίσει στον Εξουσιοδοτημένο Χρήστη τη δυνατότητα να μπορεί να χρησιμοποιεί τους Υπολογιστικούς Πόρους. Παράλληλα, η Ασφάλεια Υπολογιστικού Συστήματος επιδιώκει να εξασφαλίσει στο Χρήστη ότι μπορεί όχι μόνο να χρησιμοποιεί το Υπολογιστικό Σύστημα, αλλά ότι το Σύστημα αυτό μπορεί να λειτουργεί σωστά.

Διαθεσιμότητα Συστήματος (System Availability)	Αποτροπή της μη διάθεσης υπολογιστικών πόρων σε εξουσιοδοτημένους χρήστες.
Ασφάλεια Υπολογιστικού Συστήματος (IT System Security)	Διασφάλιση διαθεσιμότητας συστήματος και ασφάλειας πληροφοριών, καθώς και των παραμέτρων που αποτελούν τμήμα του υπολογιστικού συστήματος.
Ασφάλεια Πληροφοριακού Συστήματος (Information System Security)	Ασφάλεια πληροφοριών και υπολογιστικού συστήματος για δεδομένο πληροφοριακό σύστημα.
Διαθεσιμότητα (Availability)	Αποφυγή καθυστερήσεων στην εξουσιοδοτημένη προσπέλαση πληροφοριών ή υπολογιστικών πόρων.

1.5 Ζημιά

Ζημιά είναι ο περιορισμός μιας ή περισσοτέρων από τις Ιδιότητες των Αγαθών που χρήζουν προστασίας. Παραδείγματα Ζημιάς αποτελούν η "Απώλεια Εμπιστευτικότητας" και η "Απώλεια Διαθεσιμότητας". Οι έννοιες που είναι σχετικές με τη Ζημιά μπορεί να κατανεμηθούν σε εκείνες που έχουν σχέση περισσότερο με τους Κινδύνους και σε εκείνες που έχουν σχέση περισσότερο με τους Στόχους. Υπάρχουν πέντε πρωτεύοντες όροι που ομαδοποιούνται όπως δείχνει ο Πίνακας 1.2. Οι όροι αυτοί θα περιγραφούν στο πλαίσιο της ομάδας των Κινδύνων και της ομάδας των Στόχων.

Συναφείς με Κίνδυνο	Συναφείς με Στόχο
Ρήγμα Ασφάλειας	Επίπτωση Συνολική Επικινδυνότητα
Παραβίαση	Απομένουσα Συνολική Επικινδυνότητα Απομένουσα Επισφάλεια

Πίνακας 1.2: *Ταξινόμηση του δένδρου της έννοιας Ζημιά*

1.6 Κίνδυνοι

Η έννοια του Κινδύνου σχετίζεται με ο,τι μπορεί να προξενήσει Ζημιά σε μια ιδιότητα ενός Αγαθού. Υμφανή είδη Ζημιών υπάρχουν δύο όροι σχετικοί με τη Ζημιά και τους Κινδύνους: Ρήγμα Ασφάλειας και Παραβίαση. Ρήγμα Ασφάλειας θεωρείται η απώλεια μιας τουλάχιστον από τις Ιδιότητες: Ακεραιότητα, Διαθεσιμότητα Πληροφοριών, Εμπιστευτικότητα. Η έννοια της Παραβίασης είναι πιο ευρεία από το Ρήγμα Ασφάλειας γιατί αφορά στον περιορισμό της Ασφάλειας Πληροφοριακών Συστημάτων.

Ρήγμα Ασφάλειας (Breach of Security) — Μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή απόκρυψη πληροφοριών.

Παραβίαση (Violation) — Γεγονός κατά το οποίο περιορίστηκαν κάποιες από τις αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.

Οι Κίνδυνοι οφείλονται σε Απειλές που είναι εξωγενείς σε σχέση με τα Αγαθά που προστατεύονται, καθώς και σε Αδυναμίες που είναι ενδογενώς αδύνατα σημεία των Αγαθών που προστατεύονται. Η Απειλή είναι μία πιθανή πράξη ή ένα γεγονός που μπορεί να προκαλέσει Ζημιά σε ένα Αγαθό. Η Αδυναμία είναι ένα χαρακτηριστικό ενός Αγαθού που μπορεί να επιτρέψει σε μία Απειλή να ζημιώσει είτε το ίδιο, είτε κάποιο άλλο Αγαθό. Μία Απειλή μπορεί να προκαλέσει Ζημιά μόνο αν μπορεί να εκμεταλλευθεί μία Αδυναμία.

Απειλή (Threat) — Ο,τι μπορεί να περιορίσει την ασφάλεια ενός πληροφοριακού συστήματος.

Αδυναμία (Vulnerability) — Χαρακτηριστικό ενός πληροφοριακού συστήματος που μπορεί να επιτρέψει να συμβεί μία παραβίαση.

Ακόμα και όταν υπάρχει ένας συνδυασμός Απειλής και Αδυναμίας, δεν θα προκύπτει απαραιτήτως κάποια Παραβίαση. Η διαπίστωση αυτή οδηγεί στις έννοιες Επισφάλεια και Περιστατικό. Επισφάλεια είναι η πιθανότητα να προκύψει

μία Ζημιά λόγω του συνδυασμού μιας ή περισσότερων Απειλών-Αδυναμιών. Ενα Περιστατικό μπορεί ή όχι να αποτελεί Απειλή, η οποία μπορεί να οδηγήσει ή όχι σε Παραβίαση.

Επισφάλεια (Hazard)	Πιθανότητα να συμβεί μία παραβίαση.
Περιστατικό (Incident)	Γεγονός που συνέβη ενδεχομένως εξαιτίας μιας απειλής.

Οι Απειλές και οι Αδυναμίες μπορεί να είναι σκόπιμες ή τυχαίες, ανθρώπινες ή όχι. Οι Σκόπιμες Απειλές και Αδυναμίες προέρχονται από ανθρώπους, αλλά οι Απειλές και οι Αδυναμίες που προέρχονται από ανθρώπους δεν είναι όλες σκόπιμες.

Φυσική Απειλή (Physical Threat)	Απειλή, οι συνέπειες της οποίας μπορούν να επιφέρουν φυσική ζημιά σε ένα πληροφοριακό σύστημα.
Ανθρώπινη Απειλή (Human Threat)	Απειλή που προέρχεται από ανθρώπινες ενέργειες.
Τυχαία Απειλή (Accidental Threat)	Απειλή που προκύπτει από ενέργειες που δεν προϋποθέτουν κακή πρόθεση.
Σκόπιμη Απειλή (Deliberate Threat)	Απειλή που προϋποθέτει κακή πρόθεση.
Ανθρώπινη Αδυναμία (Human Vulnerability)	Αδυναμία που προκύπτει από ανθρώπους που αποτελούν μέρος του υπολογιστικού συστήματος.
Τεχνική Αδυναμία (Technical Vulnerabilty)	Αδυναμία που πηγάζει από τη δυσλειτουργία ενός τεχνικού συστατικού ενός υπολογιστικού συστήματος.
Τεχνική Απειλή (Technical Threat)	Απειλή που οφείλεται σε δυσλειτουργία που συνέβη εκτός των ορίων του υπολογιστικού συστήματος.

1.7 Στόχοι

Οι Κίνδυνοι δεν προκαλούν πάντα ζημιές στις Ιδιότητες των Αγαθών και η προστασία των Αγαθών κοστίζει στους Ιδιοκτήτες τους. Η Ασφάλεια των Πληροφοριών πρέπει να επιτυγχάνεται είτε μειώνοντας τις συνέπειες των Κινδύνων είτε μειώνοντας την πιθανότητα να προκαλέσουν Ζημιά στα Αγαθά (Πληροφορίες, Δεδομένα, Υπολογιστικοί Πόροι). Αυτό πρέπει να επιτευχθεί με αποδεκτό κόστος.

Κόστος (Cost) Πόροι που απαιτούνται για την πραγματοποίηση μιας ενέργειας.

Ο Στόχος σχετίζεται με το συμβιβασμό μεταξύ Κόστους και προστασίας των Αγαθών, η οποία επιτυγχάνεται με χρήση Μέσων Προστασίας.

Μέσο Προστασίας (Safeguard) Μέτρο σχεδιασμένο για να εμποδίσει μία παραβίαση είτε να μειώσει τις επιπτώσεις της.

Τα Μέσα Προστασίας επιδιώκουν να εμποδίσουν τις Παραβιάσεις και ταυτόχρονα να αντιμετωπίσουν τις συνέπειές τους. Αν ούτε οι συνέπειες μιας Παραβίασης, ούτε η πιθανότητα να συμβεί είναι υψηλές, τότε ο Ιδιοκτήτης ενδέχεται να μην επιθυμεί να αναλάβει σημαντικό Κόστος με αντάλλαγμα την προστασία των Αγαθών. Αν οι συνέπειες της παραβίασης είναι αξιοσημείωτες, τότε ο Ιδιοκτήτης θα συμφωνήσει να αναλάβει κάποιο κόστος για να τις μειώσει. Ετσι εισάγεται η έννοια της Επίπτωσης:

Επίπτωση (Impact) Απώλεια μίας αξίας, η αύξηση του κόστους ή άλλη ζημία που μπορεί να προκύψει ως συνέπεια μιας παραβίασης.

Επικινδυνότητα (Risk) Συνδυασμός επίπτωσης με επισφάλεια.

Στην πράξη, αυτό που ενδιαφέρει τον Ιδιοκτήτη δεν είναι η Επικινδυνότητα που προκύπτει από ένα συνδυασμό Απειλής-Αδυναμίας, αλλά το σύνολο της Επικινδυνότητας, καθώς και το Κόστος που απαιτείται για να περιοριστεί αυτή σε αποδεκτά επίπεδα. Αυτό εισάγει την έννοια της Συνολικής Επικινδυνότητας.

Συνολική Επικινδυνότητα (Overall Risk) Σύνολο όλων των επικινδυνοτήτων.

Η Συνολική Επικινδυνότητα μπορεί να υπολογιστεί πριν ή μετά τη χρήση των Μέσων Προστασίας. Ως συνέπεια αυτού εμφανίζονται δύο έννοιες: Απομένουσα Συνολική Επικινδυνότητα και Απομένουσα Επισφάλεια.

Απομένουσα Συνολική Επικινδυνότητα (Residual Overall Risk) Συνολική επικινδυνότητα που απομένει μετά την εγκατάσταση των μέσων προστασίας.

Απομένουσα Επισφάλεια (Residual Hazard)	Επισφάλεια που απομένει μετά την εγκατάσταση των μέσων προστασίας.

Με συνδυασμό των εννοιών Απομένουσα Επισφάλεια και Απομένουσα Συνολική Επικινδυνότητα προκύπτουν οι έννοιες: Απαιτήσεις και Αντικειμενικοί Σκοποί. Η Απαίτηση αφορά τις προδιαγραφές απόδοσης του Πληροφοριακού Συστήματος ενώ ο Αντικειμενικός Σκοπός αφορά τον Ιδιοκτήτη.

Απαίτηση (Requirement)	Τα επίπεδα αυθεντικότητας, διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας που πρέπει να διασφαλίζει ένα Πληροφοριακό Σύστημα.
Αντικειμενικός Σκοπός (Objective)	Μέγιστη απομένουσα συνολική επικινδυνότητα την οποία αποδέχεται ο ιδιοκτήτης των πληροφοριών.

1.8 Εξασφάλιση

Για να προλαμβάνουμε Παραβιάσεις ή να μειώνουμε τις επιπτώσεις τους χρειάζεται Εξασφάλιση ότι τα Μέτρα Προστασίας που υιοθετούμε είναι τα κατάλληλα γι' αυτό.

Εξασφάλιση (Assurance)	Εμπιστοσύνη ότι ένας αντικειμενικός σκοπός ή μία απαίτηση επιτυγχάνονται.

Η χρήση ανάλυσης είναι κρίσιμος παράγοντας για την Εξασφάλιση. Η ανάλυση αυτή μπορεί να βασίζεται: α) στην απόδειξη ότι οι λειτουργίες που υποστηρίζονται από ένα Υπολογιστικό Αντικείμενο γίνονται με βάση τις προδιαγραφές, β) σε δειγματοληπτικό έλεγχο ότι οι λειτουργίες του Υπολογιστικού Αντικειμένου είναι οι αναμενόμενες, γ) σε επιθεώρηση της ανάπτυξης και λειτουργίας του Υπολογιστικού Αντικειμένου. Κατά τη διαδικασία Εξασφάλισης υπάρχουν τρία ερωτήματα που πρέπει να απαντηθούν: α) λειτουργούν τα Μέσα Προστασίας σύμφωνα με τις προδιαγραφές; β) είναι αποτελεσματικά; γ) είναι κατάλληλα; Η πρώτη από τις ερωτήσεις μπορεί να απαντηθεί μόνον αν οι προδιαγραφές της λειτουργίας των Μέσων Προστασίας είναι ορθές. Αν ως μέθοδος ανάλυσης χρησιμοποιείται η απόδειξη, τότε οι προδιαγραφές πρέπει να είναι σαφείς και εισάγονται οι έννοιες: Τυπικός και Τυπική Μέθοδος Προδιαγραφών.

Τυπικός (Formal)	Ακριβής και σαφής, μαθηματικός ή συμβολικός.
Τυπική Μέθοδος Προδιαγραφών (Formal Method of Specification)	Αυστηρή περιγραφή των αναγκαίων χαρακτηριστικών.

Μέθοδοι προσδιορισμού προδιαγραφών είναι η (ημιτυπικής μορφής) Γλώσσα Προσδιορισμού Απαιτήσεων και τα Πρότυπα. Το Πρότυπο είναι ένα κριτήριο επίτευξης της Εξασφάλισης μέσω της επιθεώρησης.

Γλώσσα Προσδιορισμού Απαιτήσεων (Claims Language)	Υποσύνολο μιας φυσικής γλώσσας που χρησιμοποιείται για να μειώσει τις ασάφειες στην περιγραφή των αναγκών και των προσδοκώμενων λειτουργιών ενός μέσου προστασίας.
Πρότυπο (Standard)	Μέθοδοι και δράσεις που επιτρέπουν τη συνεπή αντιμετώπιση των ζητημάτων που προκύπτουν σε ένα πεδίο.
Τυπική Επαλήθευση (Formal Verification)	Τυπική απόδειξη ότι ένα πληροφοριακό σύστημα ή τα συστατικά του έχουν τα επιθυμητά χαρακτηριστικά.
Απόδειξη Προγράμματος (Program Proving)	Διαδικασία χρησιμοποίησης αποδείξεων, βασισμένων σε ένα πλήρες Τυπικό επιχείρημα, για να αποδειχθεί ότι ένα πρόγραμμα διαθέτει τα επιθυμητά χαρακτηριστικά.
Ελεγχος Λογισμικού (Software Testing)	Διαδικασία ελέγχου, με δοκιμές με αντιπροσωπευτικά δεδομένα, ότι το λογισμικό διαθέτει τα χαρακτηριστικά που έχουν προδιαγραφεί.
Δοκιμή Συμμόρφωσης (Conformance Testing)	Διαδικασία κατά την οποία αποδεικνύεται ότι ένα υπολογιστικό αντικείμενο ή ένα συστατικό του είναι σύμφωνα με ένα πρότυπο.
Στοιχεία Ελέγχου (Audit Trail)	Ενδείξεις που επιτρέπουν την επιθεώρηση της λειτουργίας των στοιχείων ενός πληροφοριακού συστήματος.
Ελεγχος Ασφάλειας (Audit of Security)	Ανεξάρτητη και με προκαθορισμένο σκοπό επιθεώρηση της ασφάλειας ενός πληροφοριακού συστήματος.

Αυστηρή απόδειξη μπορεί να υπάρξει μόνο για ένα τεχνικό Μέσο Προστασίας περιορισμένης λειτουργικότητας. Οταν είναι δυνατόν να υπάρξει κάτι τέτοιο, αυτό προσδίδει στα Μέσα Προστασίας την ιδιότητα της Ορθότητας. Η Ορθότητα αντιμετωπίζει μόνο το ζήτημα της συμμόρφωσης με τις προδιαγραφές και όχι το ζήτημα της Αποτελεσματικότητας και καταλληλότητας των Μέσων Προστασίας.

Ορθότητα (Correctness)	Απόδειξη της υποστηριζόμενης λειτουργικότητας.
Αποτελεσματικότητα (Effectiveness)	Βαθμός ικανοποίησης των απαιτήσεων ενός μέσου προστασίας.

Σκοπός του ελέγχου είναι η εκτίμηση της Αποτελεσματικότητας. Σκοπός της Αξιολόγησης είναι η εκτίμηση της Ορθότητας και της Αποτελεσματικότητας.

Αξιολόγηση (Evaluation)	Αποτίμηση ενός υπολογιστικού αντικειμένου, σε σχέση με προκαθορισμένα κριτήρια.

Τα προκαθορισμένα κριτήρια σχετίζονται άμεσα με την Ορθότητα και με την Αποτελεσματικότητα. Η Αξιολόγηση δεν περιορίζεται στην ανάλυση με τη μέθοδο της απόδειξης ή του ελέγχου. Η επιθεώρηση της κατασκευής ενός Υπολογιστικού Αντικειμένου είναι πολλές φορές σημαντικό κομμάτι της όλης διαδικασίας. Ειδικότερα, το Περιβάλλον Ανάπτυξης μπορεί να δείξει αν χρησιμοποιήθηκαν διαδικασίες επαρκείς για την ορθότητα του υπολογιστικού αντικειμένου ή όχι.

Περιβάλλον Ανάπτυξης (Development Environment)	Εργαλεία, διαδικασίες και μέθοδοι που χρησιμοποιήθηκαν κατά την ανάπτυξη και συντήρηση ενός μέρους ή όλου του υπολογιστικού συστήματος.

Οταν τα Υπολογιστικά Αντικείμενα πρόκειται να ελεγχθούν, να επιθεωρηθούν ή να Αξιολογηθούν εμφανίζεται ο ρόλος του ελεγκτή. Αν ο ελεγκτής δεν είναι αποδεκτός, το επίπεδο της Εξασφάλισης θα είναι χαμηλό. Για να επιτευχθούν υψηλά επίπεδα Εξασφάλισης απαιτείται η ουσιαστική καταξίωση και τυπική αναγνώριση προσώπων ή φορέων ελέγχου. Αυτό οδηγεί στην έννοια της Διαπίστευσης Εργαστηρίου.

Διαπίστευση Εργαστηρίου (Laboratory Accreditation)	Δημόσια και ευρέως αποδεκτή αναγνώριση ότι το εργαστήριο ικανοποιεί συγκεκριμένα κριτήρια και επιτρέπεται να πραγματοποιεί συγκεκριμένες λειτουργίες.

Το αποτέλεσμα μιας θετικής εκτίμησης περιγράφεται με δύο διαφορετικούς όρους. Αν πρόκειται για θετική Αξιολόγηση αναφέρεται ως η Πιστοποίηση. Αν πρόκειται για την ευρύτερη εκτίμηση ενός Πληροφοριακού Συστήματος, που περιλαμβάνει τον έλεγχο της καταλληλότητας των Μέσων Προστασίας, αναφέρεται ως Πιστοποίηση Συστήματος. Το τελικό αποτέλεσμα μιας θετικής εκτίμησης ονομάζεται Αποδοχή.

Πιστοποίηση (Certification)	Επιβεβαίωση αναγνωρισμένου φορέα ότι οι ιδιότητες ασφάλειας ενός υπολογιστικού αντικειμένου έχουν υποστεί αξιολόγηση και ικανοποιούν τα αναγκαία κριτήρια.
Πιστοποίηση Συστήματος (System Accreditation)	Διαδικασία επιβεβαίωσης αναγνωρισμένου φορέα, ότι ένα πληροφοριακό σύστημα πληροί τους αντικειμενικούς του σκοπούς και μπορεί να αξιοποιηθεί για συγκεκριμένες χρήσεις, σε συγκεκριμένες συνθήκες.
Αποδοχή (Acceptance)	Διαδικασία κατά την οποία αναγνωρίζεται ότι μέρος ή ολόκληρο το πληροφοριακό σύστημα έχει μεταπέσει από ένα στάδιο του κύκλου ζωής στο επόμενο.

1.9 Μέσα Προστασίας

Ενας Ιδιοκτήτης πρέπει να εκπονήσει ένα γενικό σχέδιο ασφάλειας για να πετύχει τους Αντικειμενικούς Σκοπούς του. Από αυτό θα εξαχθούν αναλυτικότερα σχέδια που καθορίζουν τα συγκεκριμένα Μέσα Προστασίας που θα χρησιμοποιηθούν και τον τρόπο που θα υλοποιηθούν. Το σύνολο των γενικών σχεδίων ονομάζεται Στρατηγική.

Στρατηγική (Strategy)	Σχέδιο πραγματοποίησης των αντικειμενικών σκοπών κάποιων πληροφοριακών συστημάτων.

Η Στρατηγική καθορίζει τόσο τις Απαιτήσεις ενός Πληροφοριακού Συστήματος, όσο και το πώς αυτές θα ικανοποιηθούν από τα διοικητικά μέτρα και τα Μέσα Προστασίας. Στο υψηλότερο επίπεδο διοικητικών μέτρων είναι η Πολιτική.

Πολιτική (Policy)	Περιγραφή του συνόλου των κανόνων, μέτρων και διαδικασιών που καθορίζουν τα φυσικά, διαδικαστικά και άλλα μέτρα ασφάλειας που λαμβάνονται κατά τη διαχείριση και προστασία των αγαθών.

Η Πολιτική περιλαμβάνει γενικές συστάσεις που ονομάζονται Οδηγίες. Οι Οδηγίες καλύπτουν, μεταξύ άλλων, την προσδοκώμενη συμπεριφορά των ατόμων σε έναν οργανισμό και το πώς θα παρασχεθεί σε αυτά Ενημέρωση. Επίσης περιλαμβάνει τις διαδικασίες στελέχωσης του οργανισμού, τις διαδικασίες που θα ακολουθηθούν πριν το Πληροφοριακό Σύστημα λάβει Αποδοχή, καθώς και πώς θα ελέγχονται οι αλλαγές και τροποποιήσεις (Ελεγχος Μεταβολών).

Οδηγίες (Guidelines)	Υποδείξεις για τις ενδεικνυόμενες ενέργειες, διαδικασίες, μεθόδους, εξοπλισμό ή πρότυπα, που πρέπει να χρησιμοποιούνται σε συγκεκριμένες περιστάσεις.
Ενημέρωση (Awareness)	Γνώση ζητημάτων ασφάλειας πληροφοριακών συστημάτων και υποδομών, καθώς και των επιπτώσεών τους.
Πολιτική Προσωπικού (Personnel Policy)	Οδηγίες που καθορίζονται από ένα φορέα για να συμβάλουν στην εξασφάλιση ότι το προσωπικό συμπεριφέρεται με τρόπο συμβατό με τους επιδιωκόμενους σκοπούς.
Έλεγχος Μεταβολών (Configuration Control)	Διαδικασίες που ελέγχουν και καταγράφουν τις μεταβολές των συστατικών ενός πληροφοριακού συστήματος.

Η Στρατηγική ορίζει το βαθμό στον οποίο τα Μέσα Προστασίας πρέπει να ικανοποιούν τις Απαιτήσεις, καθώς και το βαθμό στον οποίο η Επισφάλεια θα είναι αποδεκτή ή ποια μέσα μείωσης των Επιπτώσεων της Παραβίασης θα χρησιμοποιηθούν.

Ο σκοπός των Μέσων Προστασίας είναι να εξασφαλίσουν ότι οι Αντικειμενικοί Σκοποί θα επιτευχθούν. Υπάρχουν τρεις ταξινομήσεις των συναφών με τα Μέσα Προστασίας όρων, με βάση: α) πότε ένα Μέσο Προστασίας ενεργοποιείται, β) τη φύση του Αγαθού και των Ιδιοτήτων που προστατεύει και γ) τα τεχνικά και άλλα μέσα με τα οποία υλοποιείται. Τα Μέσα Προστασίας μπορούν να δράσουν ως εξής: α) σταματώντας την Απειλή πριν πραγματοποιηθεί ή μειώνοντας την πιθανότητα να πραγματοποιηθεί, β) παρέχοντας παθητική αντίσταση στην Απειλή, γ) προσφέροντας ενεργητική αντίσταση στην Απειλή, δ) μειώνοντας την ευπάθεια των Πληροφοριών ή των Υπολογιστικών Αντικειμένων και ε) μειώνοντας την Επίπτωση στον οργανισμό.

Πρόληψη (Prevention)	Αποτροπή της κατάληξης μίας πραγματικής ή πιθανής απειλής σε παραβίαση.

Προληπτικό Μέτρο (Preventive Measure)	Μέτρο που αποσκοπεί στην πρόληψη μίας απειλής συγκεκριμένου τύπου.
Ανίχνευση (Detection)	Διαπίστωση της εμφάνισης ενός περιστατικού ή μίας παραβίασης.
Ανιχνευτική Διαδικασία (Detective Control)	Ανίχνευση παραβίασης και υιοθέτηση των κατάλληλων ενεργειών αποκατάστασης.
Περιορισμός Συνεπειών (Damage Limitation)	Περιορισμός των επιπτώσεων μίας παραβίασης, μέσω κατάλληλων ενεργειών.

Η Πρόληψη και τα Προληπτικά Μέτρα δρουν πριν τα συμβάντα, είτε σταματώντας τις Απειλές πριν πραγματοποιηθούν, είτε μειώνοντας τις Αδυναμίες. Η Ανίχνευση και οι Ανιχνευτικές Διαδικασίες δρουν μετά τα συμβάντα. Τα μέτρα Περιορισμού των Συνεπειών δρούν μετά την Παραβίαση. Τα απλούστερα Προληπτικά Μέτρα είναι εκείνα που περιορίζουν την Προσπέλαση στα Αγαθά ώστε αυτή να γίνεται μόνο από Εξουσιοδοτημένους Χρήστες. Οι περιορισμοί Προσπέλασης για τους Υπολογιστικούς Πόρους, ονομάζονται Ελεγχος Προσπέλασης Συστήματος ενώ για τις Πληροφορίες ονομάζεται Ελεγχος Προσπέλασης Πληροφοριών.

Ελεγχος Προσπέλασης Συστήματος (System Access Control)	Περιορισμός της προσπέλασης στο σύστημα μόνο σε εξουσιοδοτημένους χρήστες.
Ελεγχος Προσπέλασης Πληροφοριών (Information Access Control)	Περιορισμός της προσπέλασης στις πληροφορίες μόνο εξουσιοδοτημένων χρηστών.

Υπάρχουν δύο όροι που αφορούν τήρηση Εμπιστευτικότητας μέσω του περιορισμού της Προσπέλασης Πληροφοριών: Ελεγχος Ανάγνωσης και Ασφάλεια Εκπομπών.

Ελεγχος Ανάγνωσης (Read Access Control)	Ελεγχος προσπέλασης πληροφοριών για τη μεταφορά πληροφοριών ή δεδομένων από ένα πληροφοριακό σύστημα.
Ασφάλεια Εκπομπών (Emanation Security)	Ελεγχος των ανεπιθύμητων ηλεκτρομαγνητικών, ακουστικών ή ηλεκτρικών σημάτων που εκπέμπονται από τον υπολογιστικό εξοπλισμό.

Ο όρος που περιγράφει το μηχανισμό Ελέγχου Προσπέλασης Πληροφοριών που είναι σχεδιασμένος για να διαφυλάξει την Ακεραιότητα είναι ο Ελεγχος Εγγραφής.

Ελεγχος Εγγραφής (Write Access Control)	Ελεγχος προσπέλασης που αφορά τη μεταβολή των δεδομένων ενός πληροφοριακού συστήματος.

Εκτός από τον έλεγχο της Προσπέλασης, που σχεδιάζεται με σκοπό να περιορίσει τις Ζημιές από τους Χρήστες, άλλο βασικό Προληπτικό Μέτρο για την προστασία των Πληροφοριών και των Υπολογιστικών Πηγών είναι η Φυσική Προστασία.

Φυσική Προστασία (Physical Protection)	Συσκευές και διαδικασίες που προστατεύουν τα συστατικά ενός πληροφοριακού συστήματος και τις σχετικές υποδομές από ζημιές που προκύπτουν από φυσικές απειλές.

Τα Προληπτικά Μέτρα αποθαρρύνουν όσους μπορούν να απειλήσουν το Πληροφοριακό Σύστημα και ενισχύουν τους μηχανισμούς που επιτρέπουν τον εντοπισμό των ευθυνών σε περιπτώσεις Περιστατικών ή Παραβιάσεων. Η βασική σχετική έννοια είναι η Απονομή Ευθυνών.

Απονομή Ευθυνών (Accountability)	Διαδικασία ανάληψης της ευθύνης, από φυσικά πρόσωπα, για τις συνέπειες μιας πράξης.

Τα μέτρα Ανίχνευσης αποσκοπούν είτε στον εντοπισμό της εμφάνισης Περιστατικών και Παραβιάσεων τη στιγμή που συμβαίνουν είτε στη διαπίστωση ότι ένα Περιστατικό ή μία Παραβίαση έχει ήδη συμβεί. Ο δεύτερος τύπος Ανίχνευσης είναι γνωστός ως Επίβλεψη και υπάρχει Ανίχνευση Περιστατικών και Ανίχνευση Παραβιάσεων.

Επίβλεψη (Monitoring)	Διαδικασία ανίχνευσης συνεχούς λειτουργίας, σχεδιασμένη να αναγνωρίζει περιστατικά και παραβιάσεις.
Ανίχνευση Περιστατικών (Incident Detection)	Εντοπισμός ενός περιστατικού.
Ανίχνευση Παραβιάσεων (Violation Detection)	Εντοπισμός μιας παραβίασης.

Η Διαθεσιμότητα Πληροφοριών βασικά προστατεύεται με Μέτρα Προστασίας. Η απώλεια Διαθεσιμότητας των Πληροφοριών οφείλεται στην: α) απώλεια της Διαθεσιμότητας Συστήματος του Υπολογιστικού Συστήματος που αποθηκεύει ή επεξεργάζεται τις Πληροφορίες, β) αποτυχία της διαδικασίας Ελέγχου Ανάγνωσης ή Ελέγχου Εγγραφής, που έχει ως αποτέλεσμα το Πληροφοριακό Σύστημα να θεωρήσει ως Εξουσιοδοτημένο Χρήστη έναν Μη Εξουσιοδοτημένο Χρήστηκαι γ) απώλεια της Ακεραιότητας της Πληροφορίας. Το κύριο Μέσο Προστασίας που χρησιμοποιείται για τη Διαθεσιμότητα Συστήματος είναι γνωστό ως Ανοχή σε Σφάλματα.

Ανοχή σε Σφάλματα (Fault Tolerance)	Δυνατότητα ενός πληροφοριακού συστήματος να διατηρεί το επίπεδο ασφάλειας, παρά τις αστοχίες συστατικών του.

Βασικά Μέσα Προστασίας για τον Περιορισμό των Συνεπειών είναι: Μεταβίβαση Επικινδυνότητας, Ανάκαμψη, Σχέδιο Συνέχειας, Εφεδρικό Αντίγραφο Πληροφοριών.

Μεταβίβαση Επικινδυνότητας (Risk Transfer)	Μέτρα που αποσκοπούν στη μείωση των επιπτώσεων, μέσω της μεταβίβασής τους σε άλλο φορέα.
Ανάκαμψη (Recovery)	Αποκατάσταση της λειτουργίας ενός πληροφοριακού συστήματος σε επιθυμητό επίπεδο, μετά από κάποια αστοχία.
Σχέδιο Συνέχειας (Continuity Plan)	Περιγραφή των ενεργειών που απαιτούνται για να επιτευχθεί ανάνηψη μετά από μία μείζονα παραβίαση.
Εφεδρικό Αντίγραφο Πληροφοριών (Information Back Up)	Αντίγραφο των πληροφοριών που χρησιμοποιείται για να επιτευχθεί ανάκαμψη.

Μέχρι τώρα έχουν ομαδοποιηθεί τα Μέσα Προστασίας, αλλά δεν έχει εξεταστεί ο τρόπος λειτουργίας τους, ο οποίος ονομάζεται Μηχανισμός.

Μηχανισμός (Mechanism)	Τρόπος υλοποίησης ενός μέσου προστασίας.

Οι Μηχανισμοί που χρησιμοποιούνται για τον έλεγχο της Προσπέλασης των Πληροφοριών και των Υπολογιστικών Πόρων μπορούν να ομαδοποιηθούν με βάση τις έννοιες Λογικός Ελεγχος Προσπέλασης και Φυσικός Ελεγχος Προσπέλασης. Ο Φυσικός Ελεγχος Προσπέλασης χρησιμοποιείται για τον έλεγχο της Προσπέλασης Συστήματος και μπορεί να ελέγξει την Προσπέλαση Πληροφοριών μόνο μέσα από τον έλεγχο της Προσπέλασης των Υπολογιστικών Πόρων που χρειάζονται για την ανάγνωση ή την επεξεργασία των Πληροφοριών. Ο Λογικός Ελεγχος Προσπέλασης χρησιμοποιείται για τον έλεγχο της Προσπέλασης Πληροφοριών, παρά το γεγονός ότι είναι δυνατόν να χρησιμοποιηθούν Μηχανισμοί Λογικού Ελέγχου Προσπέλασης για τον έλεγχο των συσκευών που χρησιμοποιούνται για το Φυσικό Ελεγχο Προσπέλασης.

Λογικός Ελεγχος Προσπέλασης (Logical Access Control)	Ελεγχος προσπέλασης πληροφοριών που βασίζεται στις λειτουργικότητες του υπολογιστικού συστήματος.
Φυσικός Ελεγχος Προσπέλασης (Physical Access Control)	Ελεγχος της φυσικής προσπέλασης στα αγαθά.

Οι Μηχανισμοί Λογικού Ελέγχου Προσπέλασης εξακριβώνουν την Ταυτότητα του Χρήστη που επιχειρεί πρόσβαση ή εκτέλεση των διεργασιών Ταυτοποίησης Χρήστη και Ελέγχου Αυθεντικότητας Χρήστη και αποφαίνονται αν η Προσπέλαση είναι Εξουσιοδοτημένη, χρησιμοποιώντας Χαρακτηριστικά που επισυνάπτονται στις Πληροφορίες. Γνωστή μέθοδος Αυθεντικοποίησης Χρήστη είναι η χρήση Συνθηματικών.

Ταυτότητα (Identity)	Χαρακτηρισμός που επισυνάπτεται στο χρήστη και είναι μοναδικός για κάθε υπολογιστικό σύστημα.
Ταυτοποίηση Χρήστη (User Identification)	Διαδικασία αναγνώρισης της ταυτότητας ενός χρήστη από ένα Υπολογιστικό Σύστημα.
Ελεγχος Αυθεντικότητας Χρήστη (User Authentication)	Διαδικασία επαλήθευσης του ισχυρισμού ενός Χρήστη ότι κατέχει μία συγκεκριμένη ταυτότητα.
Χαρακτηριστικό (Label)	Σύμβολοσειρά που επισυνάπτεται σε ένα αρχείο και επιτρέπει έλεγχο ανάγνωσης και εγγραφής.

Συνθηματικό (Password)	Εμπιστευτική συμβολοσειρά που χρησιμοποιείται για τον ελεγχο της αυθεντικότητας του χρήστη.
Ευαίσθητη Πληροφορία (Sensitive Information)	Πληροφορία της οποίας η αποκάλυψη, τροποποίηση ή παρακράτηση χωρίς εξουσιοδότηση μπορεί να προκαλέσει απώλεια ή ζημιά.
Ευαισθησία (Sensitivity)	Μέτρο σπουδαιότητας που αποδίδεται σε πληροφορίες, προκειμένου να δηλωθεί η ανάγκη προστασίας τους.
Διαβάθμιση (Classification)	Μέλος ενός πεπερασμένου συνόλου ιεραρχημένων επιπέδων με το οποίο χαρακτηρίζεται μία πληροφορία.
Βαθμός Εξουσιοδότησης (Clearance)	Ιδιότητα που επιτρέπει σε ένα χρήστη να προσπελαύνει πληροφορίες μέχρις ενός επιπέδου διαβάθμισης.
Διάκριση Καθηκόντων (Separation of Duties)	Διαδικασία που καθορίζει ότι μόνο συγκεκριμένα πρόσωπα επεξεργάζονται ευαίσθητες πληροφορίες.

Η Διάκριση Καθηκόντων μπορεί να υλοποιηθεί επιτρέποντας σε Εξουσιοδοτημένους Χρήστες να Προσπελαύνουν υποσύνολα Πληροφοριών και όχι ολόκληρη την Πληροφορία ή χρησιμοποιώντας μεθόδους Ελέγχου Προσπέλασης Συστήματος.

Ο κύριος Μηχανισμός υλοποίησης της Απονομής Ευθυνών είναι η Καταγραφή Δραστηριοτήτων.

Καταγραφή Δραστηριοτήτων (Activity Logging)	Δυνατότητα ενός πληροφοριακού συστήματος που επιτρέπει στις δραστηριότητες του συστήματος να συσχετιστούν με συγκεκριμένες οντότητες.

Ο κυριότερος Μηχανισμός με τον οποίο υλοποιείται η Ανοχή σε Σφάλματα είναι ο Πλεονασμός.

Πλεονασμός	Παραγωγή αντιγράφων κρίσιμων συστατικών ενός πληροφοριακού συστήματος ώστε να περιορίζονται οι

(Redundancy) επιπτώσεις μιας αστοχίας.

Ο κυριότερος Μηχανισμός Ανάκαμψης είναι η χρήση Ημερολογίου Κίνησης που επιτρέπει την αποκατάσταση των Πληροφοριών ή του Πληροφοριακού Συστήματος όπως ήταν πριν τη ζημιά.

Ημερολόγιο Κίνησης (Transaction Log) Εγγραφές που επιτρέπουν την ανίχνευση των μεταβολών των δεδομένων.

Τα υψηλά επίπεδα Ασφάλειας Πληροφοριακού Συστήματος επιτυγχάνονται με τη συνεργασία διαφόρων Μέσων Προστασίας. Το δένδρο των Μέσων Προστασίας περιλαμβάνει όρους όπως την Τάξη Λειτουργικότητας, τον Οδηγό και τους Βασικούς Ελέγχους, οι οποίοι είναι ανεξάρτητοι από τη φύση των Υπολογιστικών Πόρων και των Ιδιοτήτων των Αγαθών υπό προστασία. Από την άλλη πλευρά, οι Γενικοί Ελεγχοι, οι Ελεγχοι Εφαρμογής και το Πρωτόκολλο εξαρτώνται από τη φύση των Υπολογιστικών Πόρων που προστατεύονται.

Τάξη Λειτουργικότητας (Functionality Class) Προκαθορισμένο σύνολο μέσων προστασίας που περιγράφεται με γενικό τρόπο.

Μορφότυπος (Profile) Επιλεγμένο και προκαθορισμένο υποσύνολο επιλογών που προσφέρονται από ένα πρότυπο και επιτρέπει τη διαμόρφωση των μέσων προστασίας.

Βασικοί Ελεγχοι (Baseline Controls) Διαδικασίες ελέγχου που αποβλέπουν στη διασφάλιση ενός ελάχιστου επιπέδου προστασίας.

Γενικοί Ελεγχοι (General Controls) Διαδικασίες ελέγχου που μπορούν να εφαρμοστούν σε πολλά πληροφοριακά συστήματα ταυτόχρονα, όταν αυτά μοιράζονται υπολογιστικούς πόρους.

Ελεγχοι Εφαρμογής (Application Controls) Ειδικές διαδικασίες ελέγχου ενός πληροφοριακού συστήματος που διασφαλίζουν ότι κάποια εφαρμογή δεν έχει τροποιηθεί χωρίς εξουσιοδότηση.

Πρωτόκολλο (Protocol) Σύνολο συμβατικών ρυθμίσεων που ορίζουν τη μορφή και τις διαδικασίες ανταλλαγής δεδομένων μεταξύ επικοινωνούντων υπολογιστικών συγκροτημάτων.

Κατανεμημένη Ασφάλεια (Distributed Security)	Η ασφάλεια ενός πληροφοριακού συστήματος που κατανέμεται σε διασυνδεδεμένα συστήματα τα οποία πρέπει να συνεργαστούν για να ικανοποιήσουν τις απαιτήσεις.

Οι Ελεγχοι Εφαρμογής υλοποιούνται με λογισμικό και με διαδικασίες που βρίσκονται μέσα στην Εφαρμογή. Μερικές από αυτές τις διαδικασίες θα εκτελούνται από Χρήστες (ανθρώπους), γιαυτό είναι πέρα από τα όρια του Υπολογιστικού Συστήματος.

Τα Πρωτόκολλα χρησιμοποιούνται για να επιτευχθεί η Ασφάλεια Πληροφοριών σε διαφορετικά, αλλά επικοινωνούντα, περιβάλλοντα. Τα Πρωτόκολλα αντιπροσωπεύουν συνεργαζόμενους Μηχανισμούς και Μέσα Προστασίας που αποβλέπουν κυρίως στην εξασφάλιση της Ακεραιότητας των Πληροφοριών που μεταδίδονται. Στο περιβάλλον αυτό υπάρχουν Υπηρεσίες Ελέγχου Αυθεντικότητας Χρήστη που ελέγχουν τις ταυτότητες αποστολέα και παραλήπτη. Ετσι εμφανίζονται οι όροι Ελεγχος Αυθεντικότητας Μηνύματος και Επιβεβαίωση.

Ελεγχος Αυθεντικότητας Μηνύματος (Message Authentication)	Επαλήθευση ότι ένα μήνυμα διαβιβάστηκε, χωρίς να τροποποιηθεί, από ένα συγκεκριμένο αποστολέα στον επιδιωκόμενο παραλήπτη.
Επιβεβαίωση (Μη αποποίηση ευθύνης) (Non Repudiation)	Αμοιβαία αυθεντικοποίηση αποστολής και παραλαβής δεδομένων από ένα υπολογιστικό συγκρότημα

1.10 Ασφάλεια Υποδομών

Η Ασφάλεια Υποδομών αποτελεί αναπόσπαστο τμήμα της γενικότερης εννοιολογικής προσέγγισης του ζητήματος της Ασφάλειας. Για την παροχή ασφάλειας σε υποδομές τύπου κτιριακής εγκατάστασης εγκατάσταση χρησιμοποιούνται τρεις κυρίως τεχνολογίες: Συστήματα Περιμετρικής Ασφάλειας (Perimeter Intrusion Detection Systems), Κλειστά Κυκλώματα Τηλεόρασης (Closed Circuit TV) και Συστήματα Ελέγχου Φυσικής Προσπέλασης (Access Control Systems).

Σύστημα Περιμετρικής Ασφάλειας (Perimeter Intrusion Detection Systems)	Τα συστήματα που επιδιώκουν να εντοπίζουν τις απόπειρες μη εξουσιοδοτημένης πρόσβασης σε μια εγκατάσταση και να ειδοποιούν το αρμόδιο προσωπικό.

Η λειτουργία αυτών των συστημάτων στηρίζεται, κυρίως, σε Καλώδια Αισθητήρων (Sensor Cables), σε Επαγωγικά Καλώδια (Inductive Cables), σε Ανιχνευτές Δεσμών Υπέρυθρων Ακτίνων (Infrared Beam Detectors) και σε Μικροκυματικούς Ανιχνευτές (Microwave Detectors).

Καλώδιο Αισθητήρων	Καλώδιο που τοποθετείται στην περίφραξη της περι-

(Sensor Cables)	μέτρου και επιτρέπει την ανίχνευση προσπαθειών εισβολής

Γνωστοί τύποι αισθητήρων είναι οι αισθητήρες δόνησης (vibration sensors), οι αισθητήρες αδράνειας (inertia sensors) και οι αισθητήρες κρούσης (shock sensors).Υπάρχει δυνατότητα καθορισμού ορίων δραστηριότητας (activity thresholds), καθώς και ενεργοποίησης συναγερμού (alarm signal) στην περίπτωση που διαπιστώνεται δραστηριότητα που υπερβαίνει τα προαναφερόμενα όρια.

Επαγωγικό Καλώδιο (Inductive Cables)	Καλώδιο που τοποθετείται στην περίμετρο μιας εγκατάστασης και επιτρέπει την ανίχνευση προσπαθειών εισβολής μέσω της μεταβολής του επαγωγικού πεδίου.
Ανιχνευτής Υπέρυθρων Ακτίνων (Infrared Beam Detectors)	Φράγματα ενεργητικών υπέρυθρων ακτίνων που επιτρέπουν την προστασία τμημάτων της περιμέτρου μιας εγκατάστασης.
Μικροκυματικός Ανιχνευτής (Microwave Detectors)	Συσκευή ανίχνευσης μιας απόπειρας εισβολής από την περίμετρο μιας εγκατάστασης, με εντοπισμό χωρικών διαφοροποιήσεων.

Για την αξιοποίηση των τεχνολογιών αυτών λαμβάνονται υπόψη τα συγκεκριμένα χαρακτηριστικά της εγκατάστασης και οι τοπογραφικές ιδιαιτερότητες της περιμέτρου, δεδομένου ότι τα Περιμετρικά Συστήματα Ασφάλειας επιτρέπουν τη λειτουργική διαίρεση της περιμέτρου σε αυτόνομες ζώνες επιτήρησης, έτσι ώστε σε περίπτωση συναγερμού να είναι δυνατόν να εντοπιστεί το σημείο από όπου προκλήθηκε.

Πέραν των συνήθων συσκευών επιτήρησης και ελέγχου, ένα Σύστημα Περιμετρικής Ασφάλειας έχει τη δυνατότητα διαχείρισης και συσκευών ήπιας καταστολής (πχ. ηχητικές συσκευές, προβολείς κλπ.). Ο έλεγχος των συσκευών αυτών γίνεται σε πραγματικό χρόνο με καλή απόκριση και αποτελέσματα. Η γεωγραφική κατανομή, το πλήθος και το είδος των ελεγχόμενων συσκευών δεν επηρεάζει τη συνολική απόδοση του συστήματος. Τα Συστήματα Περιμετρικής Ασφάλειας έχουν δυνατότητα διασύνδεσης με συστήματα CCTV, ώστε σε περίπτωση συναγερμού από την περίμετρο να υπάρχει η δυνατότητα οπτικού ελέγχου του χώρου από όπου προήλθε ο συναγερμός.

Κλειστό Κύκλωμα Τηλεόρασης (Closed Circuit TV - CCTV)	Σύστημα που παρέχει τη δυνατότητα κεντρικής εποπτείας και καταγραφής των δραστηριοτήτων που λαμβάνουν χώρα σε μια εγκατάσταση.

Το κλειστό κύκλωμα τηλεόρασης έχει στόχο: α) τη συνεχή οπτική επιτήρηση της περιμέτρου των εγκαταστάσεων με κάμερες, β) την επιλεκτική οπτική επιτήρηση εσωτερικών σημείων των εγκαταστάσεων με τηλεχειριζόμενες κάμερες και γ) την οπτική εποπτεία επιλεγμένων καταστάσεων ή συναγερμών. Οι λειτουργίες CCTV ελέγχονται μέσω εξειδικευμένου λογισμικού, το οποίο εκτελείται σε υπολογιστή που είναι εγκατεστημένος σε κατάλληλο Κέντρο Ελέγχου. Οι βασικές δυνατότητες του λογισμικού του CCTV είναι οι εξής:

- Εμφάνιση της εικόνας που λαμβάνεται από κάθε κάμερα στην οθόνη υπολογιστή.
- Δυνατότητα επιλογής εικόνας που προέρχεται από κάποια συγκεκριμένη κάμερα.
- Δυνατότητα εγκατάστασης πλέγματος οθονών (video-wall). Η συχνότητα εναλλαγής και η επιλογή κάμερας για κάθε οθόνη είναι προγραμματιζόμενη.
- Δυνατότητα καταγραφής εικόνας σε ψηφιακό VCR.

Το λογισμικό υποστήριξης του CCTV μπορεί να αναβαθμιστεί αποκτώντας δυνατότητα ανίχνευσης της κίνησης, έτσι ώστε αν ανιχνευθεί κίνηση σε προκαθορισμένο χώρο και χρόνο να ενεργοποιηθεί σήμα συναγερμού. Στην περίπτωση αυτή επιλέγεται αυτόματα για εμφάνιση η εικόνα που προέρχεται από την κάμερα που εποπτεύει το χώρο από όπου έχει προκληθεί ο συναγερμός.

Έλεγχος Φυσικής Προσπέλασης (Access Control System)	Σύστημα που παρέχει τη δυνατότητα αυθεντικοποίησης ατόμων, μέσω μαγνητικών, ψηφιακών ή έξυπνων καρτών που τα άτομα αυτά κατέχουν.

Τα Συστήματα Ελέγχου της Φυσικής Προσπέλασης βασίζονται στην παροχή δικαιωμάτων πρόσβασης προσώπων σε συγκεκριμένους χώρους. Αυτό συχνά πραγματοποιείται με ψηφιακές κάρτες που κατέχουν τα εξουσιοδοτημένα πρόσωπα. Η ανάγνωση των ψηφιακών καρτών γίνεται από καρταναγνώστες είτε εισάγοντας τις κάρτες στον αναγνώστη είτε με την μέθοδο της προσέγγισης εξ αποστάσεως (contactless).

Συνήθης πρακτική για την ολοκλήρωση των συστημάτων ασφάλειας μιας εγκατάστασης είναι η δημιουργία ενός Κέντρου Ελέγχου Ασφάλειας (Security Control Room).

Κέντρο Ελέγχου Ασφάλειας (Security Control Room)	Κατάλληλα προστατευόμενος χώρος μιας εγκατάστασης, από όπου εποπτεύεται ολόκληρη ή τμήμα της εγκατάστασης για λόγους ασφαλείας, με αξιοποίηση εξοπλισμού και αρμόδιου προσωπικού.

Ο εξοπλισμός που εγκαθίσταται στο Κέντρο Ελέγχου Ασφάλειας είναι ο ακόλουθος:

- Σύστημα Περιμετρικής Ασφάλειας: Υπολογιστής με λογισμικό παραμετροποίησης, ελέγχου και διαχείρισης των συναγερμών του συστήματος περιμετρικής ασφάλειας. Στον υπολογιστή απεικονίζεται χάρτης της περιμέτρου.
- Κλειστό Κύκλωμα Τηλεόρασης: α) Υπολογιστής με λογισμικό παραμετροποίησης, ελέγχου και διαχείρισης συναγερμών, β) ηλεκτρονικός εξοπλισμός για τη συλλογή και διαχείριση των οπτικών σημάτων, γ) πολλαπλή οθόνη εμφάνισης της εικόνας από τις κάμερες, δ) εικονοκαταγραφέας (VCR) για αποθήκευση εικόνας.
- Σύστημα Ελέγχου Φυσικής Πρόσβασης: Υπολογιστής με εξειδικευμένο λογισμικό παραμετροποίησης, ελέγχου και διαχείρισης συναγερμών που παράγει το σύστημα.

Παράρτημα Α - Απόδοση Αγγλικών όρων στην Ελληνική γλώσσα

A	
Acceptance	Αποδοχή
Access	Προσπέλαση
Access Control System	Σύστημα Ελέγχου Προσπέλασης
Accidental Threat	Τυχαία Απειλή
Accountability	Απονομή Ευθυνών
Activity Logging	Καταγραφή Δραστηριοτήτων
Application	Εφαρμογή
Application Controls	Ελεγχοι Εφαρμογής
Asset	Αγαθό
Assurance	Εξασφάλιση
Audit of Security	*Ελεγχος Ασφάλειας*
Audit Trail	Στοιχεία Ελέγχου
Authenticity	Αυθεντικότητα
Authorisation	Εξουσιοδότηση
Authorised	Εξουσιοδοτημένος
Availability	Διαθεσιμότητα
Awareness	Ενημέρωση
B	
Baseline Controls	Βασικοί Ελεγχοι
Breach of Security	Ρήγμα Ασφάλειας
C	
Classification	Διαβάθμιση
Certification	Πιστοποίηση
Claims Language	Γλώσσα Προσδιορισμού Απαιτήσεων
Clearance	Βαθμός Εξουσιοδότησης
Closed Circuit TV	Κλειστό Κύκλωμα Τηλεόρασης
Confidentiality	Εμπιστευτικότητα
Configuration Control	Ελεγχος Μεταβολών
Conformance Testing	Δοκιμή Συμμόρφωσης
Continuity Plan	Σχέδιο Συνέχειας
Correctness	Ορθότητα
Cost	Κόστος

D

Damage Limitation	Περιορισμός Συνεπειών (Φθορών)
Data	Δεδομένα
Deliberate Threat	Σκόπιμη Απειλή
Detection	Ανίχνευση
Detective Controls	Ανιχνευτική Διαδικασία
Development Environment	Περιβάλλον Ανάπτυξης
Distributed Security	Κατανεμημένη Ασφάλεια

E

Effectiveness	Αποτελεσματικότητα
Emanation Security	Ασφάλεια Εκπομπών
Evaluation	Αξιολόγηση

F

Fault Tolerance	Ανοχή Σφαλμάτων
Formal	Τυπικός
Formal Method of Specification	Τυπική Μέθοδος Προδιαγραφών
Formal Verification	Τυπική Επαλήθευση
Functionality Class	Τάξη Λειτουργικότητας

G

General Controls	Γενικοί Ελεγχοι
Guidelines	Οδηγίες

H

Hazard	Επισφάλεια
Human Threat	Ανθρώπινη Απειλή
Human Vulnerability	Ανθρώπινη Αδυναμία (Αλωσιμότητα)

I

Identity	Ταυτότητα
Impact	Επίπτωση
Incident	Περιστατικό
Incident Detection	Ανίχνευση Περιστατικών
Inductive Cables	Επαγωγικά Καλώδια
Information	Πληροφορία
Information Access Control	Ελεγχος Προσπέλασης Πληροφοριών
Information Availability	Διαθεσιμότητα Πληροφοριών
Information Back Up	Εφεδρικό Αντίγραφο Πληροφοριών
Information Owner	Ιδιοκτήτης Πληροφορίας

Information Security	Ασφάλεια Πληροφοριών
Information System	Πληροφοριακό Σύστημα
Information Systems Security	Ασφάλεια Πληροφοριακών Συστημάτων
Information Access	Προσπέλαση Πληροφορίας
Infrared Beam Detectors	Ανιχνευτές Υπέρυθρων Ακτίνων
Installation Security	Ασφάλεια Εγκαταστάσεων
Integrity	Ακεραιότητα
IT Assembly	Υπολογιστικό Συγκρότημα
IT Object	Υπολογιστικό Αντικείμενο
IT Resource	Υπολογιστικός Πόρος
IT System	Υπολογιστικό Σύστημα
IT System Security	Ασφάλεια Υπολογιστικού Συστήματος

L

Label	Χαρακτηριστικό
Laboratory Accreditation	Διαπίστευση Εργαστηρίου
Logical Access Control	Λογικός Έλεγχος Προσπέλασης

M

Mechanism	Μηχανισμός
Message Authentication	Ελεγχος Αυθεντικότητας Μηνύματος
Microwave Detectors	Μικροκυματικοί Ανιχνευτές
Monitoring	Επίβλεψη

N

Non Repudiation	Επιβεβαίωση (Μη αποποίηση ευθύνης)

O

Objective	Αντικειμενικός Σκοπός
Overall Risk	Συνολική Επικινδυνότητα
Owner	Ιδιοκτήτης

P

Password	Συνθηματικό
Personnel Policy	Πολιτική Προσωπικού
Physical Access Control	Φυσικός Έλεγχος Προσπέλασης
Physical Protection	Φυσική Προστασία
Physical Threat	Φυσική Απειλή
Perimeter Intrusion Detection Systems	Συστήματα Περιμετρικης Ασφάλειας

Policy	Πολιτική
Prevention	Πρόληψη
Preventive Measure	Προληπτικό Μέτρο
Profile	Οδηγός
Program Proving	Απόδειξη Προγράμματος
Protocol	Πρωτόκολλο

R

Read Access Control	Ελεγχος Ανάγνωσης
Recovery	Ανάκαμψη
Redundancy	Πλεονασμός
Requirement	Απαίτηση
Residual Hazard	Απομένουσα Επισφάλεια
Residual Overall Risk	Απομένουσα Συνολική Επικινδυνότητα
Risk	Επικινδυνότητα
Risk Transfer	Μεταβίβαση Επικινδυνότητας

S

Safeguard	Μέσο Προστασίας
Security	Ασφάλεια
Security Control Center	Κέντρο Ελέγχου Ασφάλειας
Sensitive Information	Ευαίσθητη Πληροφορία
Sensitivity	Ευαισθησία
Sensor Cables	Καλώδια Αισθητήρων
Separation of Duties	Διάκριση Καθηκόντων
Service	Υπηρεσία
Software Testing	Ελεγχος Λογισμικού
Standard	Πρότυπο
Strategy	Στρατηγική
System Access	Προσπέλαση Συστήματος
System Access Control	Ελεγχος Προσπέλασης Συστήματος
System Accreditation	Πιστοποίηση Συστήματος
System Availability	Διαθεσιμότητα Συστήματος
System Owner	Ιδιοκτήτης Συστήματος

T

Technical Threat	Τεχνική Απειλή
Technical Vulnerability	Τεχνική Αδυναμία
Threat	Απειλή
Transaction Log	Ημερολόγιο Κίνησης

U

Unauthorised	Μη Εξουσιοδοτημένος
User	Χρήστης
User Authentication	Ελεγχος Αυθεντικότητας Χρήστη
User Identification	Ταυτοποίηση Χρήστη

V

Validity	Εγκυρότητα
Value	Αξία
Violation	Παραβίαση
Violation Detection	Ανίχνευση Παραβιάσεων
Vulnerability	Αδυναμία

W

Write Access Control	Έλεγχος Εγγραφής

Παράρτημα Β - Απόδοση Ελληνικών όρων στην Αγγλική γλώσσα

Α

Αγαθό	Asset
Αδυναμία	Vulnerability
Ακεραιότητα	Integrity
Ανάκαμψη	Recovery
Ανθρώπινη Αδυναμία	Human Vulnerability
Ανθρώπινη Απειλή	Human Threat
Ανίχνευση	Detection
Ανίχνευση Παραβιάσεων	Violation Detection
Ανίχνευση Περιστατικών	Incident Detection
Ανιχνευτική Διαδικασία	*Detective Control*
Ανιχνευτές Υπέρυθρων Ακτίνων	Infrared Beam Detectors
Ανοχή Σφαλμάτων	Fault Tolerance
Αντικειμενικός Σκοπός	Objective
Αξία	Value
Αξιολόγηση	Evaluation
Απαίτηση	Requirement
Απειλή	Threat
Απόδειξη Προγράμματος	Program Proving
Αποδοχή	Acceptance
Απομένουσα Επισφάλεια	Residual Hazard
Απομένουσα Συνολική Επικινδυνότητα	Residual Overall Risk
Απονομή Ευθυνών	Accountability
Αποτελεσματικότητα	Effectiveness
Ασφάλεια	Security
Ασφάλεια Εγκαταστάσεων	Installation Security
Ασφάλεια Εκπομπών	Emanation Security
Ασφάλεια Πληροφοριακών Συστημάτων	Information Systems Security
Ασφάλεια Πληροφοριών	Information Security
Ασφάλεια Υπολογιστικού Συστήματος	IT System Security
Αυθεντικότητα	Authenticity

Β

Βαθμός Εξουσιοδότησης	Clearance

Βασικοί Έλεγχοι	Baseline Controls

Γ

Γενικοί Έλεγχοι	General Controls
Γλώσσα Προσδιορισμού Απαιτήσεων	Claims Language

Δ

Δεδομένα	Data
Διαβάθμιση	Classification
Διαθεσιμότητα	Availability
Διαθεσιμότητα Πληροφοριών	Information Availability
Διαθεσιμότητα Συστήματος	System Availability
Διάκριση Καθηκόντων	Separation of Duties
Διαπίστευση Εργαστηρίου	Laboratory Accreditation
Δοκιμή Συμμόρφωσης	Conformance Testing

Ε

Εγκυρότητα	Validity
Ελεγχοι Εφαρμογής	Application Controls
Ελεγχος Ανάγνωσης	Read Access Control
Ελεγχος Ασφάλειας	Audit of Security
Ελεγχος Αυθεντικότητας Μηνύματος	Message Authentication
Ελεγχος Αυθεντικότητας Χρήστη	User Authentication
Ελεγχος Εγγραφής	Write Access Control
Ελεγχος Λογισμικού	Software Testing
Ελεγχος Μεταβολών	Configuration Control
Ελεγχος Προσπέλασης Πληροφοριών	Information Access Control
Ελεγχος Προσπέλασης Συστήματος	System Access Control
Ελεγχος Φυσικής Προσπέλασης	Access Control System
Εμπιστευτικότητα	Confidentiality
Ενημέρωση	Awareness
Εξασφάλιση	Assurance
Εξουσιοδοτημένος	Authorised
Εξουσιοδότηση	Authorization
Επαγωγικά Καλώδια	Inductive Cables
Επιβεβαίωση	Non Repudiation
Επίβλεψη	Monitoring
Επικινδυνότητα	Risk
Επίπτωση	Impact

Επισφάλεια	Hazard
Ευαισθησία	Sensitivity
Ευαίσθητη Πληροφορία	Sensitive Information
Εφαρμογή	Application
Εφεδρικό Αντίγραφο Πληροφοριών	Information Back Up

Η

Ημερολόγιο Κίνησης	Transaction Log

Ι

Ιδιοκτήτης	Owner
Ιδιοκτήτης Πληροφορίας	Information Owner
Ιδιοκτήτης Συστήματος	System Owner

Κ

Καταγραφή Δραστηριοτήτων	Activity Logging
Κατανεμημένη Ασφάλεια	Distributed Security
Καλώδια Αισθητήρων	Sensor Cables
Κέντρο Ελέγχου Ασφάλειας	Security Control Center
Κλειστό Κύκλωμα Τηλεόρασης	Closed Circuit TV
Κόστος	Cost

Λ

Λογικός Έλεγχος Προσπέλασης	Logical Access Control

Μ

Μέσο Προστασίας	Safeguard
Μεταβίβαση Επικινδυνότητας	Risk Transfer
Μη Εξουσιοδοτημένος	Unauthorised
Μηχανισμός	Mechanism
Μικροκυματικοί Ανιχνευτές	Microwave Detectors

Ο

Οδηγίες	Guidelines
Οδηγός	Profile
Ορθότητα	Correctness

Π

Παραβίαση	Violation
Περιβάλλον Ανάπτυξης	Development Environment

Περιορισμός Συνεπειών	Damage Limitation
Περιστατικό	Incident
Πιστοποίηση	Certification
Πιστοποίηση Συστήματος	System Accreditation
Πλεονασμός	Redundancy
Πληροφορία	Information
Πληροφοριακό Σύστημα	Information System
Πολιτική	Policy
Πολιτική Προσωπικού	Personnel Policy
Προληπτικό Μέτρο	Preventive Measure
Πρόληψη	Prevention
Προσπέλαση	Access
Προσπέλαση Πληροφορίας	Information Access
Προσπέλαση Συστήματος	System Access
Πρότυπο	Standard
Πρωτόκολλο	Protocol

Ρ

Ρήγμα Ασφάλειας	Breach of Security

Σ

Σκόπιμη Απειλή	Deliberate Threat
Στοιχεία Ελέγχου	Audit Trail
Στρατηγική	Strategy
Συνθηματικό	Password
Συνολική Επικινδυνότητα	Overall Risk
Σύστημα Περιμετρικής Ασφάλειας	Perimeter Intrusion Detection System
Σχέδιο Συνέχειας	Continuity Plan

Τ

Τάξη Λειτουργικότητας	Functionality Class
Ταυτότητα	Identity
Ταυτοποίηση Χρήστη	User Identification
Τεχνική Αδυναμία	Technical Vulnerability
Τεχνική Απειλή	Technical Threat
Τυπική Επαλήθευση	Formal Verification

Τυπική Μέθοδος Προδιαγραφών	Formal Method of Specification
Τυπικός	Formal
Τυχαία Απειλή	Accidental Threat

Υ

Υπηρεσία	Service
Υπολογιστικό Αντικείμενο	IT Object
Υπολογιστικός Πόρος	IT Resource
Υπολογιστικό Συγκρότημα	IT Assembly
Υπολογιστικό Σύστημα	IT System

Φ

Φυσική Απειλή	Physical Threat
Φυσική Προστασία	Physical Protection
Φυσικός Έλεγχος Προσπέλασης	Physical Access Control

Χ

Χαρακτηριστικό	Label
Χρήστης	User