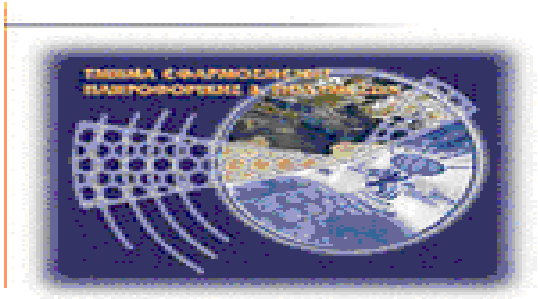
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Διαχείριση Πολιτικών Ασφαλείας σύμφωνα με το ISO 27001-27002

Γιώργος Χαβιαράς (ΑΜ:1223)

Ηράκλειο – 06/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

ΙΣΤΟΡΙΚΟ ΕΚΔΟΣΕΩΝ

Ημερομηνία	**Έκδοση**	**Συγγραφέας**	**Λεπτομέρειες**
2-11-2008	v1.0	Γιώργος Χαβιαρας	Ολοκλήρωση Κεφαλαίων 1,2,3
23-01-2008	v1.1	Γιώργος Χαβιαρας	Ολοκλήρωση Κεφαλαίου 4
7-05-2009	v1.2	Γιώργος Χαβιαρας	Ολοκλήρωση Κεφαλαίου 7 και Παραρτήματος
17-05-2009	v1.3	Γιώργος Χαβιαρας	Ολοκλήρωση Κεφαλαίου 6

Περιγραφή Πτυχιακής

Ένας οργανισμός για να έχει την δυνατότητα να πετύχει τους στόχους που έχει θέσει, πρέπει να διασφαλίσει την απαιτούμενη ασφάλεια των πληροφοριακών συστημάτων του καθώς και των ευαίσθητων δεδομένων (βάση νομικών υποχρεώσεων ή λόγω της φύσης του οργανισμού) που αποθηκεύονται η διακινούνται σε αυτή, στον μέγιστο βαθμό. 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 καταρχήν ασχολείται:

- Με την περιγραφή της διαδικασίας πιστοποίησης ενός οργανισμού βάση του προτύπου ISO27001 και κατά δεύτερο λόγο με αυτοματοποιημένες μεθόδους διαχείρισης στρατηγικών ασφάλειας.
- Εργαλεία δημιουργίας και διαχείρισης πολιτικών ασφαλείας. Όπως και ιστοσελίδες ή άλλες πηγές εύρεσης πολιτικών ασφαλείας.
- Καταγραφή των πολιτικών ασφάλειας που ορίζουν την ορθή χρήση της υποδομών ενός οργανισμού.
- Παρουσίαση πολιτικών και οδηγιών για εκπαίδευση και συνειδητοποίηση προσωπικού σε θέματα ασφαλείας.

Το αποτέλεσμα της πτυχιακής είναι δυνατό θα εφαρμοστεί στα πλαίσια του Τ.Ε.Ι 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.

Διάθρωση Πτυχιακής

Αριθμός κεφαλαίου	Τίτλος	Σύντομη περιγραφή
1	Εισαγωγή	Εισαγωγή πτυχιακής εργασίας
2	Διαδικασίες Πιστοποίησης Κατά ISO 27001	Οι διαδικασίες που πρέπει να ακολουθήσει ένας οργανισμός για να πάρει πιστοποίηση ISO.
3	Πηγές Πολιτικών Ασφαλείας, Συνοπτικά Παραδείγματα και Λίστα πολιτικών από την SANS.	Παρουσίαση πηγών στο Internet για εξεύρεση πολιτικών ασφαλείας, παρουσίαση συνοπτικών πολιτικών ασφαλείας και λίστα με πολιτικές από την SANS
4	Εργαλεία Δημιουργίας και Διαχείρισης Πολιτικών Ασφαλείας	Λίστα με ελεύθερα εργαλεία δημιουργίας και διαχείρισης πολιτικών ασφαλείας, συνοπτική παρουσίαση τους και παρουσίαση εργαλείων της Cisco.
5	Πολιτικές Ασφαλείας για το Κέντρο Ελέγχου και Διαχείρισης Δικτύου Τ.Ε.Ι Κρήτης	Παράθεση πολιτικών ασφαλείας για το Κέντρο Ελέγχου και Διαχείρισης Δικτύου ΤΕΙ Κρήτης
6	Εκπαίδευση και Συνειδητοποίηση πάνω στις Πολιτικές Ασφαλείας	Πολιτικές και οδηγίες για την εκπαίδευση υπαλλήλων ενός οργανισμού σε θέματα ασφαλείας
Παράρτημα	Πολιτικές Ασφαλείας στα Αγγλικά	Παρουσίαση πολιτικών ασφαλείας αυτούσιες στα αγγλικά.

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 ISO27001. The advantages for the organization are summarised in the followings:

- With the description of certification process of base on ISO27001 and incidentally with automated methods management of strategies safety
- Creation and management tools for security policies . As with web pages or other sources for finding policies
- Registration of policies for equitable use of infrastructures
- Presentation of policies and directives on training and awareness of personnel on security issues.

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.

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

Πίνακας Εικόνων

Πίνακας Πινάκων

Κεφάλαιο 1

Εισαγωγή

Από τη απαρχή της επιστήμης των υπολογιστών, η ασφάλεια των πληροφοριών που αυτοί επεξεργάζονταν ήταν ένα σημαντικό θέμα. Πόσο μάλλον όταν αυτές οι πληροφορίες μπορούσαν να κρίνουν ένα πόλεμο, την κούρσα για ανακάλυψη μιας τεχνολογίας, ή την αγορά ενός προϊόντος. Αναμφισβήτητα σήμερα, ο κίνδυνος είναι ακόμα πιο ορατός καθώς τα συστήματα εκτίθενται σε ευρύ φάσμα χρηστών και συνεπώς κινδύνων. Έτσι η πληροφορία όσο σημαντική και εάν είναι πρέπει να φυλάσσεται κατάλληλα και σωστά. 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.

Τις τελευταίες δεκαετίες τα περιουσιακά στοιχεία μίας εταιρίας προέρχονται κυρίως από άυλα στοιχεία. Αυτό σημαίνει ότι οι οργανισμοί είναι πιο ευάλωτοι σε απειλές ασφαλείας, λόγω της εξάρτησής τους σε πληροφοριακά συστήματα και υπηρεσίες. Επίσης λόγω της μεγάλης αύξησης των επιχειρήσεων έχουμε ως συνέπεια αυτές να γίνονται πιο ελκυστικός στόχος. Έτσι τα συστήματα των επιχειρήσεων πρέπει να είναι σε θέση να αντιμετωπίσουν διάφορες απειλές:απάτη με χρήση υπολογιστή, δολιοφθορά, κατασκοπεία ή και φυσικές καταστροφές.

Άρα ένας οργανισμός πρέπει να εξασφαλίσει την ακεραιτότητα τού και να εξασφαλίσει την συνοχή και την ασφάλεια των δεδομένων του με διάφορους μηχανισμούς, ελέγχους και διαδικασίες. Ο έλεγχος όμως έχει αρκετή δυσκολία λόγω :διασύνδεσης δημόσιων και ιδιωτικών δικτύων και διανεμημένης πληροφόρησης. 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. Και αναγνωρίζοντας τι έλεγχοι και απαιτήσεις ασφαλείας χρειάζονται σε έναν οργανισμό πάμε στο επόμενο στάδιο που είναι ο σχεδιασμός των πολιτικών ασφαλείας που απαιτούνται. Έτσι γίνεται κατανοητό ότι στην εποχή μας πρέπει να ακολουθείται και να εφαρμόζεται μία πολιτική ασφάλειας εδραιώνοντας έτσι την ασφάλεια σε κάθε δυνατό επίπεδο και παρέχοντας την απαιτούμενη προστασία στην επιχείρηση.

Κεφάλαιο 2

Διαδικασίες Πιστοποίησης Κατά ISO 27001[1]

Στη σημερινή εποχή, η πληροφορία πηγάζει από την επεξεργασία των ψηφιακά αποθηκευμένων δεδομένων σε πληροφοριακά συστήματα, στα οποία μπορούν να έχουν πρόσβαση πολλοί χρήστες από διάφορες γεωγραφικές περιοχές. Σε ένα τέτοιο λειτουργικό περιβάλλον εισάγονται κίνδυνοι μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες, εισαγωγής λανθασμένων δεδομένων, μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, καθώς και αλλοίωσης ή καταστροφής τους. Σε αυτό το κεφάλαιο παρουσιάζονται τα βήματα, οι διαδικασίες που πρέπει μια επιχείρηση, οργανισμός να ακολουθήσει ώστε να πιστοποιηθεί κατά ISO 27001. Ξεκινώντας από τον προσδιορισμό του λειτουργικού περιβάλλοντος δηλαδή καταγραφή της δραστηριότητας της επιχείρησης και της πληροφοριακής της δομής. Εξέτασης των ήδη υπαρχόντων δικλείδων ασφαλείας και προσδιορισμός του νομικού και κανονιστικού πλαισίου ασφαλείας. Στην συνέχεια η αξιολόγηση και η διαχείριση των κινδύνων και των αδυναμιών του οργανισμού. Και τέλος η ανάπτυξη του συστήματος διαχείρισης ασφαλείας πληροφοριών σαν αποτέλεσμα των παραπάνω ενεργειών.

Σχήμα 1: Αποτύπωση μεθοδολογικής προσέγγισης για την υλοποίηση του έργου.

[1] Τεχνική προσέγγιση για Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών από την Innova A.E

2.1 Προσδιορισμός Λειτουργικού Περιβάλλοντος

2.1.1 Καταγραφή Επιχειρηματικής Δραστηριότητας

Σκοπός του σταδίου αυτού είναι η συνοπτική καταγραφή της επιχειρηματικής δραστηριότητας του Οργανισμού. Η κατανόηση του περιβάλλοντος λειτουργίας και της γενικότερης κουλτούρας του Οργανισμού είναι απαραίτητη για την ανάπτυξη ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, το οποίο θα ανταποκρίνεται στις ανάγκες, προτεραιότητες, στόχους και τα χαρακτηριστικά λειτουργίας του.

Έτσι καταγράφεται το υπάρχον επιχειρηματικό λειτουργικό περιβάλλον και συγκεκριμένα το αντικείμενο και το εύρος των δραστηριοτήτων του Οργανισμού, οι υπηρεσίες που παρέχει, η οργανωτική του δομή, οι επιχειρηματικοί του στόχοι, οι συνεργασίες που διατηρεί και οι πιθανές απαιτήσεις της Διοίκησης αναφορικά με την ασφάλεια πληροφοριών.

Η μη δημιουργία του οδηγεί σε ένα μη λειτουργικό και αποτελεσματικό συστήματα ασφάλειας, ανίκανο να επιτύχει τους πρωταρχικούς στόχους για τους οποίους κρίθηκε επιτακτική η ανάπτυξή του.

2.1.2 Καταγραφή Πληροφοριακής Υποδομής

Σκοπός του σταδίου αυτού είναι η αναγνώριση και οριοθέτηση του λειτουργικού περιβάλλοντος και η καταγραφή των πληροφοριακών συστημάτων, τα οποία θα συμπεριληφθούν στη μελέτη ανάπτυξης συστήματος διαχείρισης ασφάλειας πληροφοριών. Η καταγραφή αυτή θα αφορά τους κρίσιμους πληροφοριακούς πόρους (information assets) και θα έχουν συμφωνηθεί με τον Οργανισμό.

Ο προσδιορισμός των κρίσιμων περιουσιακών στοιχείων (assets), τα οποία υπάρχουν στην συγκεκριμένη περιοχή ελέγχου και συνδέονται με τη συλλογή, επεξεργασία αποθήκευση και διακίνηση των πληροφοριών, αποτελούν σημαντική πληροφόρηση για την ορθή και αποτελεσματική αξιολόγηση των κινδύνων ασφάλειας πληροφοριών μίας συγκεκριμένης περιοχής. Ως εκ τούτου, είναι απαραίτητη η δημιουργία ενός καταλόγου στον οποίο περιλαμβάνονται όλοι οι πόροι, οι οποίοι συμμετέχουν στις διεργασίες της εν λόγω περιοχής ελέγχου και έχουν σχέση με την επεξεργασία των πληροφοριών. Ο συγκεκριμένος κατάλογος θα προσδιορίσει το εύρος, το αντικείμενο και το σχεδιασμό υλοποίησης της εκάστοτε αξιολόγησης κινδύνων. Κάθε τέτοιος πόρος έχει κάποια αξία για τον Οργανισμό, και ανάλογα με αυτήν τον προστατεύουμε αναλόγως.

2.1.3 Εξέταση Υφιστάμενων Οργανωτικών και Τεχνικών Δικλείδων Ασφάλειας

Σκοπός του σταδίου αυτού είναι η εξέταση και καταγραφή των υφιστάμενων δικλείδων ασφάλειας οι οποίοι έχουν υιοθετηθεί και εφαρμόζονται στον Οργανισμό, είτε αυτές είναι οργανωτικής είτε τεχνικής φύσης. Αυτό θα βοηθήσει σε μια αρχική εκτίμηση αδυναμιών και κινδύνων που διέπουν τον Οργανισμό, ώστε να δημιουργηθούν κατάλληλα εγχειρίδια ασφαλείας και να βοηθηθεί ο σχεδιασμός της αρχιτεκτονικής ασφαλείας του Οργανισμού.

2.1.4 Προσδιορισμός Νομικού και Κανονιστικού Πλαισίου Ασφάλειας Πληροφοριών

Σκοπός του σταδίου αυτού είναι ο προσδιορισμός του νομικού και κανονιστικού πλαισίου ασφάλειας πληροφοριών που διέπει το συγκεκριμένο χώρο που δραστηριοποιείται ο Οργανισμός, όπως αυτό ορίζεται από την ελληνική και ευρωπαϊκή νομοθεσία και νομολογία και τις αρμόδιες κανονιστικές αρχές.

Έτσι πραγματοποιείται ανάλυση του υφιστάμενου νομικού, θεσμικού και κανονιστικού πλαισίου όπως ορίζεται από την ελληνική και διεθνή νομοθεσία και νομολογία όσον αφορά στην ασφάλεια των πληροφοριών. Η ανάλυση καλύπτει διάφορες θεματικές ενότητες όπως προστασία δεδομένων προσωπικού χαρακτήρα, πνευματική ιδιοκτησία, ψηφιακές υπογραφές, άδειες χρήσης λογισμικού, ηλεκτρονικό εμπόριο κλπ.

2.2 Διαχείριση & Αξιολόγηση Κινδύνου

2.2.1 Προσδιορισμός Εύρους Αξιολόγησης Κινδύνου

Σε αυτή την φάση γίνεται προσδιορισμός και αξιολόγηση των κινδύνων ασφάλειας που αφορούν στους πληροφοριακούς πόρους και στις επιχειρηματικές διαδικασίες, όπως και τον προσδιορισμός της επίδρασης των κινδύνων αυτών στην καθημερινή λειτουργία του Οργανισμού, όσο και στην επίτευξη των στρατηγικών στόχων του. Τα αποτελέσματα από τα παραπάνω στάδια θα χρησιμοποιηθούν για την επιλογή των κατάλληλων δικλείδων ασφάλειας.

Στην συνέχεια γίνεται ο προσδιορισμός των πληροφοριακών συστημάτων τα οποία θα συμπεριληφθούν σε αυτή τη φάση. Και αφορά κρίσιμους πληροφοριακού πόρους (information assets) όπως αυτοί θα έχουν προκύψει πιο πάνω και θα έχουν συμφωνηθεί με τον Οργανισμό.

Συμφωνείται με τον Οργανισμό η ακριβής έκταση των ελέγχων, δηλαδή προσδιορίζονται & συμφωνούνται όλες οι περιοχές και τα πληροφοριακά συστήματα τα οποία θα συμπεριληφθούν στην αξιολόγηση των κινδύνου.

Και αναπτύσσεται το «Πλάνο Ελέγχων», το οποίο αποτελεί το σχέδιο στο οποίο προδιαγράφονται οι έλεγχοι που πρόκειται να πραγματοποιηθούν, το χρονικό διάστημα στο οποίο θα διεξαχθούν και το όνομα των ατόμων που πρόκειται να διενεργήσουν.

2.2.2 Ανάλυση Επιχειρηματικών Επιπτώσεων Ασφάλειας Πληροφοριών

Σκοπός του σταδίου της ανάλυσης επιχειρηματικών επιπτώσεων ασφάλειας είναι ο προσδιορισμός της κρισιμότητας που έχουν για τον Οργανισμό οι πληροφοριακοί πόροι και τα δεδομένα τα οποία επεξεργάζονται, διακινούνται και αποθηκεύονται στο εύρος της περιοχής ελέγχου. Επιπρόσθετα, η συγκεκριμένη διαδικασία χρησιμοποιείται προκειμένου να προσδιοριστεί η κρισιμότητα του αξιολογούμενου συστήματος για τον Οργανισμό. Η κρισιμότητα των πληροφοριών που αφορούν κάθε έναν από τους πόρους της υπό αξιολόγηση περιοχής, οι οποίοι συμμετέχουν στην επεξεργασία και διακίνηση των πληροφοριών, εκτιμάται προσδιορίζοντας την επίδραση που θα είχε για τον Οργανισμό η απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους. Η εν λόγω αξιολόγηση θεωρείται επιβεβλημένη κάθε φορά που αναπτύσσεται ή αγοράζεται νέα εφαρμογή και κάθε φορά που μεταβάλλεται το εύρος και ο σκοπός χρήσης της κάθε εφαρμογής.

Τέλος αξιολογείται η επίπτωση για τον Οργανισμό από πιθανή απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών που επεξεργάζεται κάθε πληροφοριακό σύστημα, με σκοπό να καταταχθούν τα πληροφοριακά συστήματα σύμφωνα με την κρισιμότητα των δεδομένων τους και να προσδιοριστούν οι εκάστοτε απαιτήσεις ασφάλειας.

2.2.3 Προσδιορισμός Απειλών Ασφάλειας

Σκοπός του σταδίου αυτού είναι ο εντοπισμός των κυριοτέρων απειλών ασφάλειας πληροφοριών που αφορούν στα δεδομένα και τις πληροφορίες της υπό αξιολόγηση περιοχής, ώστε να γίνουν κατανοητοί οι κίνδυνοι οι οποίοι είναι συνυφασμένοι με τη φύση των δραστηριοτήτων που υποστηρίζουν. Κατά την αρχική φάση του προσδιορισμού των απειλών ασφάλειας δημιουργείται κατάλογος, ο οποίος περιλαμβάνει τις εστίες απειλών, οι οποίες αφορούν στην εκάστοτε περιοχή ελέγχου και μπορούν να υποκινήσουν την εκδήλωση των απειλών ασφάλειας. Για τον πληρέστερο προσδιορισμό των παραπάνω, αναφέρεται και το κίνητρο, το οποίο θα μπορούσε να χρησιμοποιηθεί για την υποκίνηση της εκδήλωσης της απειλής.

Προσδιορίζονται οι απειλές στις οποίες είναι εκτεθειμένος ο Οργανισμός λόγω του εύρους δραστηριοτήτων και των υπηρεσιών που προσφέρει, οι πηγές προέλευσής τους, καθώς και η πιθανότητα εκδήλωσής τους. Ο προσδιορισμός αυτός στηρίζεται – εκτός των άλλων- στην ανάλυση των αποτελεσμάτων προηγούμενων φάσεων, στα

δίκτυα με τα οποία συνδέονται τα συστήματα του Οργανισμού, τα δεδομένα που αυτά αποθηκεύουν, επεξεργάζονται και διακινούν, τους τρόπους και τα επίπεδα πρόσβασης. Τα παραπάνω αποτελέσματα των απειλών αποτελούν τους κύριους κινδύνους της ασφάλειας πληροφοριών. Ο προσδιορισμός και η αξιολόγηση των κινδύνων αυτών αποτελεί αντικείμενο της διαδικασίας αξιολόγησης κινδύνων.

2.2.4 Εντοπισμός Αδυναμιών Ασφάλειας

Σκοπός του σταδίου αυτού, κατά το οποίο προσδιορίζονται οι αδυναμίες ασφάλειας που αφορούν στην περιοχή υπό εξέταση, είναι η δημιουργία λίστας με τις αδυναμίες, οι οποίες θα μπορούσαν να αποτελέσουν αντικείμενο εκμετάλλευσης από τις απειλές. Οι αδυναμίες ασφάλειας δεν προκύπτουν μόνο από την έλλειψη ή την αναποτελεσματικότητα των τεχνικών δικλείδων ασφάλειας, αλλά πηγάζουν από λάθη κατά τη σχεδίαση των συστημάτων (design vulnerabilities), από λανθασμένη υλοποίηση ενός σχεδιαστικά καλού συστήματος (implementation vulnerabilities), από λάθη κατά την παραμετροποίηση (configuration vulnerabilities), από μη τήρηση των προδιαγραφών ασφάλειας έτσι όπως αυτές προκύπτουν από την Πολιτική Ασφάλειας, τις πρότυπες οδηγίες ασφάλειας και τις διεθνείς πρακτικές ασφάλειας. Επίσης, αδυναμίες ασφάλειας προκύπτουν από την έλλειψη ή την αναποτελεσματικότητα δικλείδων ασφάλειας, οι οποίες αφορούν στην ασφαλή διαχείριση της πληροφορίας, είτε αυτή γίνεται από πληροφορικά συστήματα, είτε από ανθρώπινο παράγοντα.

Έλεγχος Τήρησης Προδιαγραφών Ασφάλειας (Gap Analysis)

Στα πλαίσια διενέργειας του συγκεκριμένου ελέγχου εξετάζεται η εναρμόνιση της ελεγχόμενης περιοχής με τις απαιτήσεις ασφάλειας του Οργανισμού, έτσι όπως αυτές προσδιορίζονται από τα ακόλουθα:

- Αρχές και στόχους του Οργανισμού
- Πολιτική Ασφάλειας του Οργανισμού
- Διαδικασίες Ασφάλειας (τεχνικού περιεχομένου και μη)
- Οδηγίες Ασφάλειας
- Νομικές, κανονιστικές και συμβατικές υποχρεώσεις
- Διεθνείς πρακτικές ασφάλειας οι οποίες εφαρμόζονται σε Οργανισμούς οι οποίοι
- Επεξεργάζονται δεδομένα της ίδιας ή και μεγαλύτερης κρισιμότητας με τον Οργανισμό
- Διεθνή πρότυπα ασφάλειας

Έλεγχος Τεχνικών Αδυναμιών (Vulnerability Assessment)

Η συγκεκριμένη ενότητα ελέγχων αφορά σε τεχνικές αδυναμίες ασφάλειας στην αρχιτεκτονική ασφάλειας, καθώς και σε όλους τους πληροφοριακούς πόρους και λογισμικό που αυτοί διαθέτουν. Είναι απόλυτα τεχνικής φύσεως και εξετάζει έμφυτες (εγγενείς) αδυναμίες της σχεδίασης ενός πληροφοριακού συστήματος ή μιας εφαρμογής (design vulnerabilities), είτε αυτές αφορούν λογισμικό είτε υλικό, αδυναμίες που οφείλονται σε λανθασμένη υλοποίηση ενός σχεδιαστικά καλού συστήματος (implementation vulnerabilities) και αδυναμίες που οφείλονται σε λάθη

παραμετροποίησης (configuration vulnerabilities) των συστημάτων ή διαχείρισής τους.

Έλεγχος Αποτελεσματικότητας Υφιστάμενων Δικλείδων Ασφάλειας (Controls Assessment)

Η συγκεκριμένη ενότητα ελέγχων αφορά την αποτελεσματικότητα των δικλείδων ασφάλειας τόσο σε οργανωτικό όσο και σε τεχνικό επίπεδο. Συγκεκριμένα, ελέγχεται η αποτελεσματικότητα των υφιστάμενων δικλείδων ασφάλειας που προστατεύουν τα πληροφοριακά συστήματα του Οργανισμού, η υλοποίηση ή όχι των δικλείδων ασφάλειας που κρίνονται απαραίτητες για το εκάστοτε λειτουργικό περιβάλλον και, τέλος, η παραμετροποίηση των πληροφοριακών συστημάτων και εφαρμογών.

2.2.5 Αξιολόγηση Πιθανότητας Εκμετάλλευσης Αδυναμιών Ασφάλειας

Η έννοια της απειλής είναι συνυφασμένη με την πιθανότητα εκδήλωσης μιας αδυναμίας ασφάλειας. Η πιθανότητα εκδήλωσης μιας αδυναμίας ασφάλειας είναι αποτέλεσμα της παρουσίας ή απουσίας των κατάλληλων δικλείδων ασφάλειας. Σε περίπτωση κατά την οποία υπάρχουν δικλείδες ασφάλειας, η πιθανότητα εκμετάλλευσης μιας αδυναμίας προκύπτει από την αξιολόγηση της αποτελεσματικότητας των εγκατεστημένων δικλείδων ασφάλειας, είτε αυτές είναι τεχνικές δικλείδες, είτε διαδικαστικές.

2.2.6 Εκτίμηση Κινδύνου Ασφάλειας Πληροφοριών

Σκοπός του σταδίου αυτού είναι η εκτίμηση του επιπέδου κινδύνου για κάθε ζεύγος απειλής και αδυναμίας ασφάλειας, όπως αυτά έχουν προκύψει από προηγούμενα στάδια της μεθοδολογίας, με σκοπό να προσδιοριστεί το συνολικό επίπεδο κινδύνου στο οποίο είναι εκτεθειμένος ο Οργανισμός. Η εκτίμηση του κινδύνου πραγματοποιείται συνδυάζοντας την κρισιμότητα των πληροφοριακών πόρων, των απειλών και των αδυναμιών ασφάλειας, ενώ αποτελεί την πυξίδα για την επιλογή των κατάλληλων δικλείδων ασφάλειας και την επίτευξη του επιθυμητού
επιπέδου ασφάλειας πληροφοριών.

Αξιολόγηση Αποτελεσμάτων & Εκτίμηση του Κινδύνου

Έχοντας ολοκληρώσει τους ελέγχους, απομένει η αξιολόγηση των αποτελεσμάτων και ο προσδιορισμός του κινδύνου για κάθε μία από τις αδυναμίες ασφάλειας που εντοπίσθηκαν. Ο κίνδυνος προκύπτει σύμφωνα με την παρακάτω σχέση:
Κίνδυνος = Πιθανότητα Εκμετάλλευσης Αδυναμίας (Απειλή) Χ Επίδραση της Απειλής Χ Αξία Πόρου

2.2.7 Σχέδιο Διαχείρισης Κινδύνου

Σκοπός του σταδίου αυτού είναι η ανάπτυξη ενός σχεδίου για τη διαχείριση του κινδύνου ασφάλειας πληροφοριών (information security risk management plan), με στόχο την ελαχιστοποίηση ή την εξάλειψη του κινδύνου που έχει εντοπιστεί. Στο πλαίσιο αυτό, προσδιορίζονται οι απαιτούμενες διορθωτικές ενέργειες, είτε αυτές είναι νέες δικλείδες ασφάλειας ή βελτιστοποίηση της αποτελεσματικότητας των υπαρχόντων, αξιολογούνται και τέλος, προτεραιότητα προς υλοποίηση. Δεδομένου ότι η ολοκληρωτική εξάλειψη του κινδύνου είναι πρακτικώς αδύνατη, επιλέγονται οι κατάλληλες διορθωτικές ενέργειες, το κόστος των οποίων είναι μικρότερο ή ίσο με το κόστος της πιθανής απώλειας σε περίπτωση που οι προτεινόμενες δικλείδες ασφάλειας δεν υλοποιούνταν και ο κίνδυνος είχε πραγματοποιηθεί. Η ευθύνη για την επιλογή αυτή έγκειται στην ανώτερη Διοίκηση και τα διευθυντικά στελέχη του Οργανισμού.

Προσδιορισμός Δικλείδων Ασφάλειας & Διορθωτικών Ενεργειών

Μελέτη των κινδύνων, οι οποίοι έχουν προσδιοριστεί και πρόταση δικλείδων ασφάλειας ελαχιστοποίησής τους, αναλόγως της κρισιμότητας των πληροφοριών που πρόκειται να προστατεύουν. Για κάθε κίνδυνο, προτείνονται οι κατάλληλες δικλείδες ασφάλειας σε οργανωτικό & τεχνικό επίπεδο.

2.2.8 Τεκμηρίωση και Παρουσίαση Αποτελεσμάτων

Σκοπός του τελευταίου σταδίου της μεθοδολογίας αξιολόγησης και διαχείρισης κινδύνου είναι η αναλυτική και ολοκληρωμένη τεκμηρίωση και παρουσίαση των αποτελεσμάτων των ελέγχων, της αξιολόγησης κινδύνου και της προτεινόμενης στρατηγικής διαχείρισης του κινδύνου ασφάλειας.

Στην Διοίκηση του Οργανισμού παρουσιάζεται μια σύνοψη με τα κύρια σημεία που εντοπίσθηκαν κατά τη διενέργεια των ελέγχων ασφάλειας πληροφοριών. Τα σημεία υψηλού κινδύνου ομαδοποιούνται και περιγράφονται χωρίς την τεχνική λεπτομέρεια. Η σύνοψη συμπληρώνεται από μία παρουσίαση, η οποία έχει σαν στόχο την κατανόηση των κυριότερων σημείων της αξιολόγησης και την επεξήγηση των δικλείδων ασφάλειας που πρέπει να υλοποιηθούν.

2.3 Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (κατά ISO27001)

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών αποτελεί μέρος του ευρύτερου συστήματος διαχείρισης ενός Οργανισμού και αφορά στη θεμελίωση, υλοποίηση, λειτουργία, έλεγχο τήρησης, συντήρηση και βελτίωση της ασφάλειας πληροφοριών ενός Οργανισμού. Η υλοποίησή του ακολουθεί προσέγγιση βασισμένη στους επιχειρηματικούς κινδύνους του Οργανισμού (risk based approach).

Το Σ.Δ.Α.Π αποτελεί ένα πλαίσιο αρχών με σκοπό την επίτευξη και στη συνέχεια τη διατήρηση του επιθυμητού επιπέδου ασφάλειας πληροφοριών ενός Οργανισμού. Είναι ένα είδος σχεδίου / οδηγού στον οποίο προσδιορίζεται το επιθυμητό επίπεδο ασφάλειας πληροφοριών. Το Σ.Δ.Α.Π οφείλει και πρέπει να είναι εναρμονισμένο με τους αντικειμενικούς στόχους του Οργανισμού και να είναι ανάλογο της κρισιμότητας των επιχειρηματικών πληροφοριών. Ένα τέτοιο πλαίσιο αρχών προσδιορίζει το σύνολο των συμπεριφορών, διεργασιών και πρακτικών τα οποία συνηγορούν στην υλοποίηση του επιθυμητού επιπέδου ασφάλειας πληροφοριών (με σχέση με τις απαιτήσεις Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των πληροφοριών του Οργανισμού). Χρησιμοποιώντας τους επιχειρηματικούς στόχους σαν κριτήριο, οι οργανισμοί μπορούν να προσδιορίσουν το επιθυμητό επίπεδο ασφάλειας και να το τοποθετήσουν σε μία κλίμακα μέτρησης, στο ενδιάμεσο της απόστασης ανάμεσα στο υφιστάμενο επίπεδο ασφάλειας και στο ιδεατό (όπως αυτό προσδιορίζεται από πρότυπα και τις διεθνείς πρακτικές).

Όπως όλα τα συστήματα διαχείρισης (management systems), το Σ.Δ.Α.Π περιλαμβάνει τον προσδιορισμό οργανωτικής δομής και υπευθυνοτήτων, πολιτικών, διαδικασιών, προτύπων και οδηγιών ασφάλειας πληροφοριών. Ο σχεδιασμός και υλοποίηση ενός Σ.Δ.Α.Π επηρεάζεται από τις επιχειρηματικές απαιτήσεις και τους αντικειμενικούς στόχους του Οργανισμού, τους κινδύνους που προκύπτουν από την απώλειας της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των πληροφοριών, τις απαιτήσεις ασφάλειας πληροφοριών, τις διεργασίες και τον τρόπο λειτουργίας, το μέγεθος και τη δομή ενός Οργανισμού.

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών αποτελείται από ένα δομημένο σύνολο εντύπων διαφορετικών βαθμίδων, το οποίο περιλαμβάνει Πολιτικές, Πρότυπα, Διαδικασίες και Οδηγίες. Μέσα από τα έντυπα προσδιορίζονται οι βασικές προδιαγραφές και ταυτόχρονα απαιτήσεις ασφάλειας των Πληροφοριών του Οργανισμού, καθώς και οι διαδικασίες υλοποίησης των προδιαγραφών αυτών.

Στο παραπάνω πλαίσιο αναπτύσσονται τα ακόλουθα:

Οργανωτικό Πλαίσιο Ασφάλειας Πληροφοριών – Θέτει τις προϋποθέσεις για τη δημιουργία ενός πλαισίου εργασίας, μέσω του ορισμού ρόλων και αρμοδιοτήτων ως προς την ασφάλεια, το οποίο υποστηρίζει το συντονισμό και τον έλεγχο της υλοποίησης και εφαρμογής των πολιτικών, διαδικασιών, προτύπων και οδηγιών ασφάλειας πληροφοριών.

Πολιτική Ασφάλειας Πληροφοριών – Αντικατοπτρίζει τις θέσεις της Διοίκησης για την Ασφάλεια Πληροφοριών του Οργανισμού. Η πολιτική ασφάλειας καθορίζει τους κανόνες μέσα από τους οποίους επιτυγχάνεται το επιθυμητό επίπεδο ασφάλειας πληροφοριών.

Επιμέρους Πολιτικές Ασφάλειας Πληροφοριών (ανά θεματική ενότητα) – Προσδιορίζουν τους κανόνες ασφάλειας, σύμφωνα με τους οποίους τα πληροφοριακά συστήματα εγκαθίστανται, σχεδιάζονται, λειτουργούν και συντηρούνται.

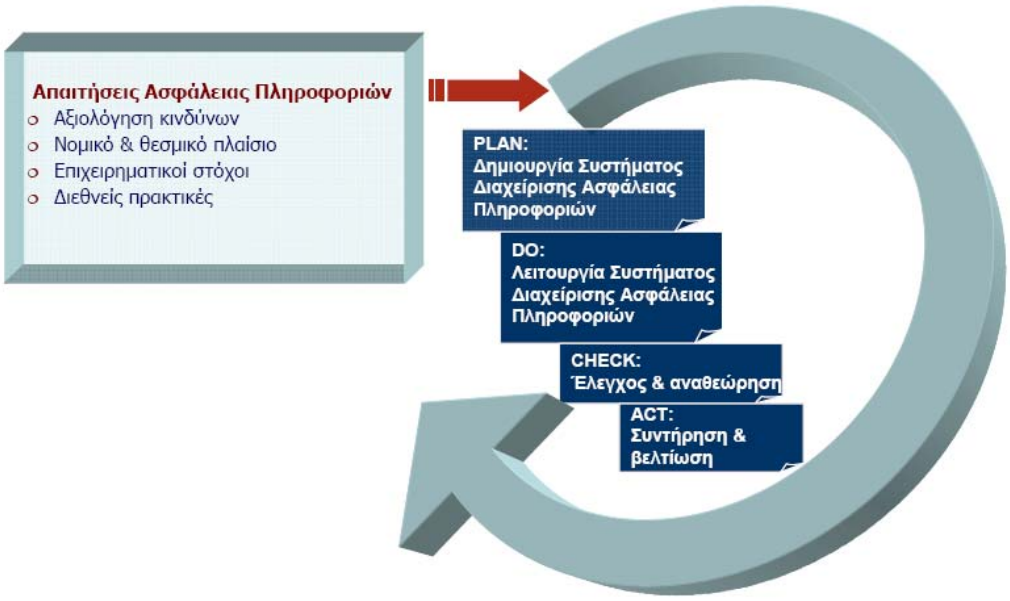
Διαδικασίες Ασφάλειας Πληροφοριών – Προσδιορίζουν με λεπτομέρεια τον τρόπο με το οποίο υλοποιούνται οι απαιτήσεις ασφάλειας πληροφοριών, κατά την καθημερινή λειτουργία του Οργανισμού.

Τεχνολογικά Πρότυπα Ασφάλειας – Λεπτομερή έντυπα τα οποία αντιστοιχίζουν (μεταφράζουν) τις γενικές προδιαγραφές ασφάλειας της Πολιτικής σε συγκεκριμένες απαιτήσεις και κανόνες που αφορούν στους πληροφοριακούς πόρους και στις διεργασίες διαχείρισης του Οργανισμού.

Τεχνικά Πρότυπα Ασφάλειας - Λεπτομερή έντυπα τα οποία καθορίζουν τις βέλτιστες πρακτικές που πρέπει να ακολουθούνται για την ασφαλή ανάπτυξη των πληροφοριακών συστημάτων συγκεκριμένων κατασκευαστών, ορίζοντας τις ελάχιστες αποδεκτές ρυθμίσεις ασφάλειας τους (baseline security configuration).

Οδηγίες Ασφάλειας Πληροφοριών - Αφορούν στην ασφαλή διαχείριση και παραμετροποίηση των βασικών λειτουργικών πλατφόρμων πληροφοριακών συστημάτων του Οργανισμού.

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών διαμορφώνεται σύμφωνα με τις ανάγκες ασφάλειας του Οργανισμού, όπως αυτές προσδιορίζονται από την αρχική αξιολόγηση κρισιμότητας των δεδομένων και των επιπτώσεων για τον Οργανισμό από πιθανή απώλεια της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των πληροφοριών που διαχειρίζεται, από την αξιολόγηση των κινδύνων που είναι συνυφασμένοι με τη λειτουργία του, από το ισχύον Νομικό, Θεσμικό και Κανονιστικό πλαίσιο και σύμφωνα με τα διεθνή πρότυπα και τις διεθνείς πρακτικές ασφάλειας πληροφοριών (ISO/IEC17799, ISO13335, COBIT).



Σχήμα 2:Κύκλος ζωής Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Έτσι σκοπός της συγκεκριμένης φάσης του έργου είναι ο σχεδιασμός ενός αποτελεσματικού Σ.Δ.Α.Π, προσαρμοσμένο στις ανάγκες και απαιτήσεις ασφάλειας πληροφοριών του Οργανισμού, καθώς και η ανάπτυξη του βασικού κορμού αυτού. Στα πλαίσια της συγκεκριμένης φάσης σχεδιάζεται το Σ.Δ.Α.Π της εταιρίας και ταυτόχρονα αναπτύσσεται ο βασικός του κορμός σύμφωνα με τις απαιτήσεις του προτύπου ISO27001, προκειμένου το συγκεκριμένο Σ.Δ.Α.Π να μπορεί να πιστοποιηθεί στην αμέσως επόμενη φάση του έργου.

2.3.1 Σχεδιασμός ΣΔΑΠ

Στα πλαίσια της συγκεκριμένης ενέργειας γίνεται σχεδίαση και προτείνει ολοκληρωμένο σύστημα διαχείρισης ασφάλειας πληροφοριών (Σ.Δ.Α.Π) για τον Οργανισμό έτσι όπως αυτό προκύπτει από:

- Το υφιστάμενο λειτουργικό & επιχειρηματικό περιβάλλον
- Τους κινδύνους ασφάλειας της εταιρείας
- Τις απαιτήσεις της Διοίκησης για την Ασφάλειας Πληροφοριών
- Τις ιδιαιτερότητες λειτουργίας της εταιρίας
- Τις απαιτήσεις αποτελεσματικότητας
- Τις απαιτήσεις του προτύπου ISO27001
- Ο σχεδιασμός του Σ.Δ.Α.Π ξεκινά με το προσδιορισμό των απαιτήσεων ασφάλειας και η ευθυγράμμισή τους με τις επιχειρηματικές απαιτήσεις και τους στόχους της Οργανισμού.

Έχοντας προσδιορίσει τις απαιτήσεις ασφάλειας πληροφοριών του Οργανισμού ακολουθεί η φάση «Ανάπτυξη Εγχειριδίου Ασφάλειας Πληροφοριών» το οποίο αφορά στην τεκμηρίωση των διαδικασιών, κανόνων και πολιτικών, οι οποίες θα υποδείξουν τις κατάλληλες δικλείδες ασφάλειας, η τήρηση των οποίων διαμορφώνει το επιθυμητό επίπεδο ασφάλειας των πληροφοριών.

Διαμορφώνονται κανόνες και προδιαγραφές ασφάλειας, η τήρηση των οποίων διαμορφώνει το απαιτούμενο επίπεδο Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των δεδομένων, ανάλογο της κρισιμότητάς τους για τον Οργανισμό στον οποίο απευθύνονται. Δημιουργείται ένα σύνολο δομημένων πολιτικών και κανόνων ασφάλειας (το οποίο αποτελεί το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών) σύμφωνα με τους οποίους πληροφοριακά συστήματα και υπηρεσίες εγκαθίστανται, σχεδιάζονται, λειτουργούν και συντηρούνται.

Κατά το στάδιο αυτό διαμορφώνονται τα ακόλουθα:

- Πολιτική ασφάλειας πληροφοριών
- Επιμέρους πολιτικές ασφάλειας πληροφοριών
- Διαδικασίες ασφάλειας
- Τεχνολογικά πρότυπα ασφάλειας
- Τεχνικά πρότυπα ασφάλειας για τις βασικότερες λειτουργικές πλατφόρμες
- Οδηγίες ασφάλειας πληροφοριών

Υποστηρικτικά έντυπα που βοηθούν στη λειτουργικότητα και υλοποίηση των όσων προσδιορίζονται στο Εγχειρίδιο Ασφάλειας Πληροφοριών. Τα παραπάνω αποτελούν το Εγχειρίδιο Ασφάλειας Πληροφοριών (Information Security Manual) το οποίο αποτελείται από μία σειρά από έντυπα που αναθεωρούνται συνεχώς, καθώς αλλάζει η εγκατεστημένη τεχνολογική βάση, μεταβάλλονται οι επιχειρηματικές δραστηριότητες του Οργανισμού και αλλάζουν οι απαιτήσεις ασφάλειας.

Τα έντυπα που απαρτίζουν το Εγχειρίδιο Ασφάλειας Πληροφοριών δεν είναι όλα στο ίδιο επίπεδο. Αποτελούν μέρος μιας δομής πυραμίδας η οποία έχει στην κορυφή της τις βασικές αρχές για την ασφάλεια πληροφοριών έτσι όπως αυτές προσδιορίζονται από τη Διοίκηση του Οργανισμού.

Σχήμα 3:Διάγραμμα προσέγγισης υλοποίησης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Η «καρδιά» του Εγχειριδίου Ασφάλειας Πληροφοριών (και κατ' επέκταση το κεντρικό σημείο του Σ.Δ.Α.Π) είναι η Πολιτική Ασφάλειας, η οποία αποτυπώνει τη φιλοσοφία και βούληση του Οργανισμού για την ασφάλεια των δεδομένων της σε σχέση με την Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα που κρίνει ότι αυτά έχουν ανάγκη. Η πολιτική ασφάλειας είναι ο μηχανισμός που επιτρέπει τον προσδιορισμό και την υλοποίηση των αντικειμενικών στόχων της ασφάλειας πληροφοριών. Αποτελεί τις βασικές αρχές που όλοι στον Οργανισμό οφείλουν να τηρούν. Η Πολιτική Ασφάλειας συμπληρώνεται από επιμέρους πολιτικές, οι οποίες καλύπτουν εκτενέστερα περιοχές υψηλής κρισιμότητας για τον Οργανισμό.

Το επόμενο επίπεδο του Εγχειριδίου Ασφάλειας Πληροφοριών είναι οι πρότυπες οδηγίες ασφάλειας ή πρότυπα, τα οποία δεν εκφράζουν γενικούς κανόνες και αρχές, όπως η πολιτική ασφάλειας, αλλά προσδιορίζουν συγκεκριμένες πρακτικές και δικλείδες ασφάλειας για συγκεκριμένες επιχειρηματικές διεργασίες και τεχνολογίες, όπως για παράδειγμα η ασφάλεια των λειτουργικών συστημάτων που χρησιμοποιούνται στον Οργανισμό, η ασφάλεια του ηλεκτρονικού ταχυδρομείου, η πρόσβαση σε δεδομένα και εφαρμογές, η ασφάλεια του δικτύου. Τα πρότυπα αντιστοιχίζουν τις γενικές προδιαγραφές ασφάλειας της Πολιτικής, σε συγκεκριμένες απαιτήσεις και κανόνες που αφορούν στους πληροφοριακούς πόρους και στις διεργασίες διαχείρισης του Οργανισμού.

Τελευταίο επίπεδο του Εγχειριδίου Ασφάλειας Πληροφοριών είναι οι διαδικασίες ασφάλειας, οι οποίες καθοδηγούν το προσωπικό του Οργανισμού σε θέματα ασφάλειας κατά την καθημερινή τους εργασία και διεκπεραίωση των καθηκόντων τους (περιλαμβάνουν θέματα όπως διαβάθμιση της διακινούμενης πληροφορίας, τα backup, αλλαγή των password σημαντικών λογαριασμών, διαδικασία παροχής πρόσβασης σε συστήματα και εφαρμογές).

Όλες οι πολιτικές και οδηγίες ασφάλειας είναι προσαρμοσμένες στις ανάγκες του Οργανισμού, έτσι ώστε να είναι αποτελεσματικές και να επιφέρουν το επιθυμητό αποτέλεσμα.

Η τελευταία φάση υλοποίησης του Σ.Δ.Α.Π είναι η «Υλοποίηση Πολιτικής και Δικλείδων Ασφάλειας». Αφορά στην παροχή των απαραίτητων εργαλείων για την υλοποίηση των όσων προδιαγράφονται στο Εγχειρίδιο Ασφάλειας Πληροφοριών». Στα πλαίσια της συγκεκριμένης φάσης, σχεδιάζεται η αρχιτεκτονική ασφάλειας του Οργανισμού, επιλέγεται ο εξοπλισμός ασφάλειας που κρίνεται απαραίτητος για το υφιστάμενο λειτουργικό περιβάλλον, διαμορφώνονται τα Σχέδια Ασφάλειας για τα κύρια Πληροφοριακά Συστήματα του Οργανισμού και πραγματοποιείται εκπαίδευση του προσωπικού.

2.3.2 Προσδιορισμός εύρους πιστοποίησης

Στα πλαίσια της συγκεκριμένης ενέργειας σε συνεργασία με την ομάδα έργου του Οργανισμού θα προσδιορίσει το εύρος – έκταση του Σ.Δ.Α.Π.

Η συγκεκριμένη απόφαση δεν επηρεάζει την αποτελεσματικότητα καθώς και την ανάπτυξη του Σ.Δ.Α.Π, είναι όμως σημαντική διότι επηρεάζει συγκεκριμένες απαιτήσεις τεκμηρίωσης του προτύπου όπως:

- Έκταση Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS scope)
- Μητρώο καταγραφής περιουσιακών στοιχείων (asset registry)
- Εμβέλεια εφαρμοσιμότητας προτύπου (scope of applicability)

Ο προσδιορισμός του εύρους πιστοποίησης επηρεάζει το εύρος εφαρμογής του προτύπου στην εταιρεία και κατ' επέκταση προσδιορίζει τις απαιτήσεις από τη πλευρά του φορέα πιστοποίησης σχετικά με τεκμηρίωση, αρχεία και λοιπά αποδεικτικά στοιχεία εφαρμογής του προτύπου.

2.3.3 Ανάπτυξη Σ.Δ.Α.Π

Στα πλαίσια της συγκεκριμένης ενέργειας αναπτύσσεται ο βασικός κορμός του Σ.Δ.Α.Π του Οργανισμού ο οποίος περιλαμβάνει τα ακόλουθα:

Ανάπτυξη τεκμηρίωση που αφορά στο πρότυπο:

- Έκταση Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS scope)
- Μητρώο καταγραφής περιουσιακών στοιχείων (asset registry)
- Εμβέλεια εφαρμοσιμότητας προτύπου (scope of applicability)
- Μεθοδολογία αξιολόγησης κινδύνων

- Οργάνωση Ασφάλειας Πληροφοριών
- Σύνταξη κυρίου τεύχους Πολιτικής Ασφάλειας
- Σύνταξη υποστηρικτικών διαδικασιών ασφάλειας πληροφοριών
- Σύνταξη βασικών προτύπων ασφάλειας πληροφοριών (information security standards)

Οργάνωση Ασφάλειας Πληροφοριών

Σε αυτήν την φάση τίθενται οι προϋποθέσεις για τη δημιουργία ενός πλαισίου εργασίας, μέσω του ορισμού ρόλων και αρμοδιοτήτων ως προς την ασφάλεια, το οποίο υποστηρίζει το συντονισμό και τον έλεγχο της υλοποίησης και εφαρμογής της πολιτικής και των υποστηρικτικών διαδικασιών, καθώς και του σχεδίου έκτακτης ανάγκης.

Πολιτική Ασφάλειας Πληροφοριών

Στη φάση αυτή συντάσσεται το κείμενο της πολιτικής ασφάλειας. Επίσης, συντάσσονται οι διαδικασίες που υποστηρίζουν την πολιτική στα σημεία όπου χρειάζεται να είναι πιο λεπτομερής.

Το κύριο τεύχος της Πολιτικής Ασφάλειας που θα αναπτυχθεί θα πλήρη τις προδιαγραφές όπως αυτές ορίζονται από το πρότυπο ISO27001 αλλά και τις ευρύτερες ανάγκες ασφάλειας πληροφοριών της εταιρείας.

Τα βασικά χαρακτηριστικά της πολιτικής ασφαλείας είναι τα παρακάτω:

- Απαιτεί συμμόρφωση από το προσωπικό του οργανισμού. Το έγγραφο της πολιτικής θα πρέπει να είναι στη διάθεση όλου του προσωπικού.
- Εκφράζει γενικότερες απόψεις ή αρχές του οργανισμού.
- Είναι σαφής ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της και εφαρμόσιμη από άποψη κόστους.
- Είναι γενικεύσιμη ώστε η εφαρμογή της να είναι επεκτάσιμη σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα του οργανισμού.
- Είναι απαλλαγμένη από μη απαραίτητους τεχνικούς όρους και ειδικευμένες αναφορές ώστε να μην καθίσταται δύσκολη στην εφαρμογή της και εξαρτημένη από τεχνολογικές επιλογές καθώς και να μην τροποποιείται συχνά, παρά μόνο όταν συμβαίνουν σημαντικές αλλαγές στα εξής:
    1. Στην οργανωτική δομή και στην κουλτούρα του οργανισμού
    2. Στις απαιτήσεις ασφαλείας
    3. Στις τεχνολογικές εξελίξεις.

Η πολιτική ασφάλειας που θα αναπτυχθεί θα καλύπτει τουλάχιστον τις ακόλουθες θεματικές ενότητες:

1. Οργάνωση Ασφάλειας
2. Ταξινόμηση και Έλεγχος Πόρων
3. Ασφάλεια Προσωπικού
4. Φυσική και Περιβαλλοντολογική Ασφάλεια
5. Διαχείριση Τηλεπικοινωνιών και Λειτουργιών

6. Έλεγχος Πρόσβασης
7. Ασφάλεια κατά την Ανάπτυξη Συστημάτων
8. Διαχείριση Συνέχειας Δραστηριοτήτων
9. Συμμόρφωση.

Σύνταξη Διαδικασιών Ασφάλειας Πληροφοριών

Στα πλαίσια της ενέργειας αυτής αναπτύσσονται οι αναλυτικές διαδικασίες οι οποίες θα υποστηρίξουν την πολιτική ασφάλειας. Οι επιμέρους διαδικασίες θα προεκτείνουν το τεύχος της πολιτικής κάθετα, παρέχοντας εξειδικευμένες και λεπτομερείς οδηγίες. Οι διαδικασίες είναι δομημένες, αναλυτικές και συμπληρώνουν την πολιτική ασφάλειας, καθώς ορίζουν βήμα προς βήμα τον τρόπο με τον οποίο θα διεκπεραιωθούν οι απαιτούμενες ενέργειες για την διεκπεραίωση ορισμένων κρίσιμων για την ασφάλεια λειτουργιών.

Σύνταξη βασικών προτύπων ασφάλειας πληροφοριών

Τα εγχειρίδια προτύπων και οδηγιών ασφάλειας είναι τεχνικής φύσεως και σχεδιάζονται έτσι ώστε να προσδιορίσουν τα απαραίτητα τεχνολογικά μέτρα ασφάλειας, προκειμένου να διατηρήσουν υπό οποιεσδήποτε συνθήκες το επιθυμητό επίπεδο ασφάλειας. Τα πρότυπα και οι οδηγίες αφορούν σε συγκεκριμένα τεχνολογικά θέματα, καλύπτοντας όλες τις απαιτήσεις ασφάλειας, παραμένοντας όμως αρκετά γενικά έτσι ώστε να μπορούν να εφαρμοστούν σε διαφορετικά πληροφοριακά συστήματα-περιβάλλοντα, ανεξαρτήτως κατασκευαστή. Παράλληλα αναπτύσσονται και τεχνικά πρότυπα με σκοπό να ορίσουν τα απαραίτητα τεχνολογικά μέτρα ασφάλειας, προκειμένου να διατηρήσουν υπό οποιεσδήποτε συνθήκες το επιθυμητό επίπεδο ασφάλειας.

2.3.4 Προτάσεις Τεχνικής υλοποίησης απαιτήσεων προτύπου ISO27001

Στα πλαίσια της συγκεκριμένης ενέργειας θα προταθεί, όπου κρίνεται αναγκαίο, τεχνικές δικλείδες ασφάλειας οι οποίες απορρέουν από τη από την εφαρμογή του προτύπου ISO 27001.

2.3.5 Εκπαίδευση – Προετοιμασία Πιστοποίησης

Η αποτελεσματική εφαρμογή ενός Σ.Δ.Α.Π, καθώς και η αποτελεσματική εφαρμογή του προτύπου ISO27001, απαιτεί τη επικοινωνία και κατανόηση της Πολιτικής Ασφάλειας και των κανόνων / διαδικασιών εφαρμογής αυτής. Σκοπός της συγκεκριμένης φάσης του έργου είναι η διεξαγωγή ενός κύκλου εκπαίδευσης. Η εκπαίδευση αυτή αποσκοπεί στη μεταφορά της απαιτούμενης τεχνογνωσίας στο προσωπικό του Πανεπιστημίου, ώστε να μπορεί να αντεπεξέλθει στις διαρκώς αυξανόμενες ανάγκες ασφάλειας και στο μακροχρόνιο στόχο να διαθέτει ανθρώπινο δυναμικό το οποίο θα έχει τόσο επίγνωση της έννοιας και των απαιτήσεων συμμόρφωσης με την πολιτική ασφάλειας.

Κεφάλαιο 3

Πήγες Πολιτικών Ασφαλείας

Σε αυτό το κεφάλαιο θα ασχοληθούμε γενικά με πολιτικές ασφάλειας. Θα δούμε διάφορες πηγές από το Internet. Μερικά συνοπτικά παραδείγματα πολιτικών ασφαλείας. Και μια λίστα με πολιτικές που την SANS.

3.1 Πηγές Πολιτικών Ασφαλείας από το Internet

Στο Web υπάρχουν πολλές πήγες όπου μπορούμε να βρούμε πολιτικές ασφαλείας για πληροφοριακά συστήματα. Μερικές αξιοσημείωτα site περιγράφονται παρακάτω. Η www.sans.org ενός οργανισμού παγκοσμίου εμβέλειας όπου ασχολείται με εκπαίδευση, πιστοποίηση και έρευνα πάνω σε θέματα ασφάλειας πληροφοριών. Έχουμε το www.cert.org ένα κέντρο έρευνας με μελέτες πάνω σε αδυναμίες ασφάλειας στο Internet, σε μακροχρόνιες αλλαγές ασφάλειας στα δικτυωμένα συστήματα και ανάπτυξη πληροφοριών και την κατάρτισης για βελτίωση της ασφάλειας. Το www.ISO27001.org οπού υπάρχουν τα ISO της σειράς 27000 που ασχολούνται θέματα ασφάλειας πληροφοριών. Επίσης έχουμε τα:
http://www.information-security-policies-and-standards.com
http://www.securityauditor.net
http://www.upenn.edu/computing/policy/

3.2 Συνοπτικά Παραδείγματα Πολιτικών Ασφαλείας

Παρακάτω παρατίθεται μια σειρά από πολιτικές ασφαλείας που μπορεί να εφαρμοστούν σε έναν οργανισμό.

3.2.1Ownership of assets

Έλεγχος

Όλες οι πληροφορίες και τα περιουσιακά στοιχεία που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών πρέπει να ανήκουν από ένα οριζόμενο μέρος της οργάνωσης.

Οδηγός Υλοποίησης

Ο υπεύθυνος των περιουσιακών αυτών πρέπει να είναι αρμόδιος να:

- εξασφαλίσει ότι οι πληροφορίες και τα περιουσιακά στοιχεία που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών να είναι όπως πρέπει απόρρητες.
- καθορίζοντας και περιοδικά ανανεώνοντας τους περιορισμούς και διαβαθμίσεις πρόσβασης , που λαμβάνονται υπόψη από τις εφαρμόσιμες πολιτικές ελέγχου πρόσβασης.

Ιδιοκτησία μπορεί να προσδιοριστεί σε:

a) επιχειρησιακή διαδικασία.
b) ένα καθορισμένο σύνολο δραστηριοτήτων.
c) μια εφαρμογή ή
d) ένα καθορισμένο σύνολο δεδομένων

Άλλες πληροφορίες

Οι επαναλαμβανόμενες εργασίες μπορούν να μεταβιβαστούν, π.χ. σε έναν επιστάτη που φροντίζει το περιουσιακό στοιχείο σε καθημερινή βάση, αλλά η ευθύνη παραμένει στον ιδιοκτήτη.

Σε σύνθετα συστήματα πληροφοριών μπορεί να είναι χρήσιμο να υποδειχθούν ομάδες στοιχείων τα οποία ενεργούν από κοινού για να παρέχουν μια ιδιαίτερη λειτουργία σαν υπηρεσία. Σε αυτήν την περίπτωση ο ιδιοκτήτης της υπηρεσίας είναι αρμόδιος για την παράδοση της, συμπεριλαμβανομένης της λειτουργίας των στοιχείων της, τα οποία την παρέχουν.

3.2.2 Acceptable use of assets

Έλεγχος

Κανόνες για την αποδεκτή χρήση των πληροφοριών και των περιουσιακών στοιχείων που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών πρέπει να αναγνωριστούν, να τεκμηριωθούν και να υλοποιηθούν.

Οδηγός Υλοποίησης

Όλοι οι υπάλληλοι, οι ανάδοχοι έργων και οι χρήστες τρίτων ομάδων πρέπει να ακολουθήσουν τους κανόνες για την αποδεκτή χρήση των πληροφοριών και των περιουσιακών στοιχείων που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών, συμπεριλαμβάνοντας:

a) κανόνες για τις χρήσεις ηλεκτρονικού ταχυδρομείου και Internet.
b) οδηγίες για τη χρήση των κινητών συσκευών, ειδικά για τη χρήση έξω από τις εγκαταστάσεις του οργανισμού.

Συγκεκριμένες κανόνες ή οδηγίες πρέπει να παρέχονται από τους σχετικούς διαχειριστές. Οι υπάλληλοι, οι ανάδοχοι έργων και οι χρήστες τρίτων ομάδων χρησιμοποιώντας ή έχοντας την πρόσβαση στα περιουσιακά στοιχεία του οργανισμού πρέπει να γνωρίζουν τα όρια που υπάρχουν για τη χρήση των πληροφοριών και περιουσιακών στοιχείων που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών και πόρων. Πρέπει να είναι υπεύθυνοι για τη χρήση οποιωνδήποτε πόρους επεξεργασίας πληροφοριών, και οποιασδήποτε χρήσης τους που πραγματοποιείται έξω από το οργανισμό γίνεται κάτω από την ευθύνη τους.

3.3 Λίστα πολιτικών από την SANS

1. Acceptable Encryption Policy
2. Acceptable Use Policy
3. Acquisition Assessment Policy
4. Analog / ISDN Line Policy
5. Anti-Virus Process Policy
6. Application Service Provider Policy
7. Audit Vulnerability Scanning Policy
8. Automatically Forwarded Email Policy
9. Backup Policy
10. Bluetooth Device Security Policy
11. Certification and Accreditation Policy
12. Cryptography Policy
13. Communications Policy
14. Data Classification Policy
15. Database Credentials Coding Policy
16. Dial-in Access Policy
17. Disaster Recovery Policy
18. DMZ Security Policy
19. DMZ Lab Security Policy
20. E-mail Policy
21. E-mail Retention
22. Ethics Policy
23. Extranet Policy
24. Identification and Authentication Policy
25. Information Data Ownership Policy
26. Information Sensitivity Policy
27. Information System Audit Logging Requirements
28. Internal Lab Security Policy
29. Internet DMZ Equipment Policy
30. Lab Anti-Virus Policy
31. Network Security Policy
32. Password Protection Policy
33. Personal Communication Device
34. Personnel Security Policy
35. Physical Security Policy
36. Privacy Policy
37. Remote Access Policy
38. Removable Media Policy
39. Remote Access - Mobile Computing and Storage Devices
40. Resource Utilization Security Policy
41. Risk Assessment Policy
42. Router Security Policy
43. Security Awareness Policy
44. Security Training Policy
45. Server Security Policy
46. Server Malware Protection Policy
47. Telecommuting/Teleworking Securiti Policy
48. The Third Party Network Connection Agreement
49. User Data Protection Policy

50. VPN Security Policy
51. Wireless Communication Policy

Α/Α	Πολιτική / Περιγραφή Πολιτικής	Link
1.	**Acceptable Encryption Policy** Ο σκοπός αυτής της πολιτικής είναι να παράσχει καθοδήγηση για τα όρια χρήσης κρυπτογράφησης από αλγορίθμους που έχουν λάβει την ουσιαστική δημόσια επισκόπηση και έχουν αποδειχθεί ότι είναι αποτελεσματικοί. Επιπλέον, αυτή η πολιτική παρέχει την κατεύθυνση για να εξασφαλίσει ότι οι ομοσπονδιακοί κανονισμοί ακολουθούνται, και η νομική εξουσία εκχωρείται για τη διάδοση και χρήση των τεχνολογιών κρυπτογράφησης έξω από τις Ηνωμένες Πολιτείες.	**http://www.sans.org/resources/policies/Acceptable_Encryption_Policy.pdf**
2.	**Acceptable Use Policy** Στόχος της πολιτικής αυτής είναι να καθορίσει την αποδεκτή χρήση υπολογιστικού εξοπλισμού ενός οργανισμού. Οι κανόνες της είναι σε θέση να προστατεύσουν τον οργανισμό και τους υπαλλήλους. Μη αποδεκτή χρήση μπορεί να οδηγήσει σε επίθεση κακοηθών προγραμμάτων, έκθεση του δικτύου και νομικά προβλήματα.	**http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf**
3	**Acquisition Assessment Policy** Η πολιτική αυτή έχει σαν στόχο να καθιερώσει τις ευθύνες του οργανισμού πιστοποίησης σχετικά με την ιδιοκτησία του οργανισμού, και να καθορίσουν τις	**http://www.sans.org/resources/policies/Aquisition_Assessment_Policy.pdf**

	ελάχιστες απαιτήσεις ασφάλειας βάση αξιολόγησης της εταιρίας πιστοποίησης.	
4	**Analog / ISDN Line Policy** Η παρούσα πολιτική μιλάει για αποδεκτές χρήσεις, πολιτικές και διαδικασίες έγκρισης αναλογικών και γραμμών ISDN. Αυτή η πολιτική καλύπτει δύο ευδιάκριτες χρήσεις των γραμμών αναλογικών /ISDN: γραμμές που πρόκειται να συνδεθούν μόνο για την χρήση fax, και γραμμές που πρόκειται να συνδεθούν με τους υπολογιστές.	**http://www.sans.org/resources/policies/Analog_Line_Policy.pdf**
5	**Anti-Virus Process Policy** Καθορίζει τις οδηγίες για την αποτελεσματική μείωση της απειλής των ιών υπολογιστών σε ένα δίκτυο του οργανισμού. Συγκεκριμένα καθορίζει διαδικασίες που τηρούνται σε επίπεδο Η/Υ, δικτύου ώστε τα παραπάνω να μην εκτεθούν και εκθέσουν τα δεδομένα που περιέχουν ή διακινούν.	**http://www.sans.org/resources/policies/Anti-virus_Guidelines.pdf**
6	**Application Service Provider Policy** Αυτή η πολιτική καθορίζει τις ελάχιστες απαιτήσεις ασφάλειας πληροφοριών που πρέπει να έχει ένας παροχέας εφαρμογών υπηρεσιών ώστε να αναλάβει κάποιο έργο ενός οργανισμού.	**http://www.sans.org/resources/policies/Application_Service_Providers.pdf**
7	**Audit Vulnerability Scanning Policy** Καθορίζει τις απαιτήσεις και παρέχει την αρχή στην ομάδα ασφάλειας πληροφοριών για να διεξαγάγει τους ελέγχους και τις αξιολογήσεις του κινδύνου για να εξασφαλίσει ακεραιότητα των πληροφοριών και πόρων, για να ερευνήσει τα γεγονότα, για	**http://www.sans.org/resources/policies/Audit_Policy.pdf**

	να εξασφαλίσει προσαρμογή στις πολιτικές ασφάλειας ή στη παρακολούθηση της δραστηριότητα χρηστών, συστημάτων όπου απαιτείται.	
8	**Automatically Forwarded Email Policy** Στόχος αυτής είναι να αποτρέψει την αναρμόδια ή αμελή κοινοποίηση των ευαίσθητων πληροφοριών της επιχείρησης, λόγω αυτόματης προώθησης e-mail από υπαλλήλους, εργολάβους κ.τ.λ. .	**http://www.sans.org/resources/policies/Automatically_Forwarded_Email_Policy.pdf**
9	**Backup Policy** Η πολιτική αυτή μιλάει για το πως θα διατηρηθεί η ακεραιότητα και η διαθεσιμότητα των πληροφοριών και εγκαταστάσεων επεξεργασίας πληροφοριών. Τακτικές διαδικασίες πρέπει να καθιερωθούν για να εφαρμόσουν τη συμφωνηθείσα backup πολιτική και στρατηγική για την δημιουργία εφεδρικών αντιγράφων των δεδομένων και την έγκαιρη αποκατάστασή τους.	**http://its.uncg.edu/Policy_Manual/Computer_Backup/**
10	**Bluetooth Device Security Policy** Αυτή η πολιτική παρέχει κανόνες για ασφαλέστερες λειτουργίες συσκευών Bluetooth. Προστατεύει την επιχείρηση από την απώλεια προσωπικών αναγνωρίσιμων πληροφοριών (PII) και ιδιόκτητων δεδομένων ενός οργανισμού. Συγκεκριμένα εστιάζει στην έκδοση του πρωτοκόλλου Bluetooth που πρέπει να χρησιμοποιείται, στα pin και στο πως ζευγάρια συσκευών πρέπει να	**http://www.sans.org/resources/policies/bluetooth_security_policy.pdf**

	συνδέονται, ακροάσεις ασφαλείας για αυτές τις συσκευές, μέτρα ασφαλείας στις συσκευές, μη εξουσιοδοτημένη χρήση και ευθύνες του χρήστη.	
11	**Certification and Accreditation Policy** Η πολιτική αυτή καθορίζει τις απαιτήσεις για τη εγγύηση μέσω της υιοθέτησης ενός καθορισμένου με σαφήνεια μοντέλου κύκλου ζωής για όλα τα βήματα της ανάπτυξης, συμπεριλαμβανομένων των διαδικασιών και των πολιτικών επανόρθωσης αδυναμιών, της σωστής χρήσης των εργαλείων, των τεχνικών, των διαδικασιών, και των μέτρων βασικών γραμμών ασφάλειας που χρησιμοποιούνται για να προστατεύσουν το περιβάλλον ανάπτυξης.	**http://www.tess-llc.com/Certification%20&%20Accreditation%20PolicyV4.pdf**
12	**Cryptography Policy** Ο σκοπός αυτής της πολιτικής είναι να διευκρινιστεί ότι η αξία των πληροφοριών ενός οργανισμού βρίσκεται στη διαθεσιμότητά της, αλλά να προστατευθούν οι πληροφορίες που πρέπει να γίνουν απρόσιτες σε όλους εκτός από εκείνους που εξουσιοδοτούνται κατάλληλα. Επίσης περιγράφει τη κρυπτογραφία ως εργαλείο για ένα ευρύ φάσμα αναγκών και απαιτήσεων του προγράμματος ασφάλειας πληροφοριών ενός οργανισμού.	**http://www.tess-llc.com/Cryptography%20PolicyV4.pdf**
13	**Communications Policy** Η πολιτική αυτή μιλάει για την εμπιστευτικότητα, ακεραιότητα, και διαθεσιμότητα των πληροφοριών του οργανισμού	**http://www.tess-llc.com/Communications%20PolicyV4.pdf**

	που μεταδίδονται μέσα από ένα δίκτυο επικοινωνιών, που χρησιμοποιεί τις επικοινωνίες ή τα συστήματα δικτύου.	
14	**Data Classification Policy** Αυτή η πολιτική εκφράζει την ανάγκη για ασφαλή αποθήκευση των δεδομένων και την ταξινόμηση τους σύμφωνα με την μυστικότητά τους.	**http://www.sans.org/resources/policies/DB_Credentials_Policy.pdf**
15	**Database Credentials Coding Policy** Αυτή η πολιτική εκφράζει την ανάγκη για ασφαλή αποθήκευση και ανάκτηση ονομάτων χρηστών και κωδικών πρόσβασης βάσεων δεδομένων (δηλ., πιστοποιητικά βάσεων δεδομένων) προς χρήση από ένα πρόγραμμα που έχει πρόσβαση σε μια βάση δεδομένων που τρέχει σε δίκτυο ενός οργανισμού.	**http://www.sans.org/resources/policies/DB_Credentials_Policy.pdf**
16	**Dial-in Access Policy** Ο σκοπός της πολιτικής αυτής είναι να προστατεύσει ενός οργανισμού τις ηλεκτρονικές πληροφορίες να εκτεθούν ακούσια από εξουσιοδοτημένα άτομα που χρησιμοποιούν dial-in συνδέσεις.	**http://www.sans.org/resources/policies/Dial-in_Access_Policy.pdf**
17	**Disaster Recovery Policy** Καθορίζει ένα σχέδιο που εξετάζει τα βήματα που πρέπει να λαμβάνονται για να διατηρηθούν οι κρίσιμες λειτουργίες σε περίπτωση απωλειών, ανωμαλιών, ή καταστροφών που επηρεάζουν τα συστήματα πληροφοριών ενός οργανισμού.	**http://www.nchica.org/hipaaresources/Security/UAB17.doc**
18	**DMZ Security Policy** Αυτή η πολιτική εγκαθιδρύει τις απαιτήσεις ασφαλείας πληροφοριών για τα δίκτυα	**http://www.sans.org/resources/policies/DMZ_Lab_Security_Policy.pdf**

	και τον εξοπλισμό των εργαστηρίων ενός οργανισμού που βρίσκονται στην λεγόμενη αποστρατικοποιημένη ζώνη "De-Militarized Zone" (DMZ). Η απαρέγκλιτη τήρηση αυτών των απαιτήσεων θα ελαχιστοποιήσει τον πιθανό κίνδυνο από ζημία στη δημόσια εικόνα που προκαλείται από την αναρμόδια χρήση πόρων του οργανισμού και την απώλεια ευαίσθητων, εμπιστευτικών στοιχείων της επιχείρησης και πνευματικής ιδιοκτησίας.	
19	**DMZ Lab Security Policy** Ομοίως με την παραπάνω πολιτική	**http://www.sans.org/resources/policies/DMZ_Lab_Security_Policy.pdf**
20	**E-mail Policy** Η πολιτική αυτή εστιάζει στο να αποτρέψει την αμαύρωση της δημόσιας εικόνας ενός οργανισμού. Επειδή όταν το ηλεκτρονικό ταχυδρομείο φεύγει προς το ευρύ κοινό θα εμφανίσει εκείνο το μήνυμα ως επίσημη δήλωση από το οργανισμό αυτό. Συγκεκριμένα εστιάζει στις περιπτώσεις μη-εγκριμένης χρήσης, προσωπικής χρήσης και στην παρακολούθηση του ηλεκτρονικού ταχυδρομείου.	**http://www.sans.org/resources/policies/Email_Policy.pdf**
21	**E-mail Retention** Η πολιτική διατήρησης ηλεκτρονικού ταχυδρομείου προορίζεται να βοηθήσει τους υπαλλήλους να καθορίσουν εάν οι πληροφορίες που στέλνονται ή που παραλαμβάνονται με ηλεκτρονικό ταχυδρομείο πρέπει να διατηρηθούν και για πόσο καιρό. Οι πληροφορίες που καλύπτονται σε αυτές τις	**http://www.sans.org/resources/policies/email_retention.pdf**

	οδηγίες περιλαμβάνουν, αλλά δεν περιορίζονται, σε πληροφορίες που είτε καταχωρούνται είτε μοιράζονται μέσω του ηλεκτρονικού ταχυδρομείου είτε των εφαρμογών άμεσων μηνυμάτων.	
22	**Ethics Policy** Ο σκοπός για αυτήν την πολιτική ηθικής είναι να καθιερωθεί ένας πολιτισμός της ειλικρίνειας, της εμπιστοσύνης και της ακεραιότητας στις επιχειρησιακές πρακτικές. Η αποτελεσματική ηθική είναι μια ομαδική προσπάθεια που περιλαμβάνει τη συμμετοχή και την υποστήριξη του κάθε υπάλληλου.	**http://www.sans.org/resources/policies/Ethics_Policy.pdf**
23	**Extranet Policy** Η παρούσα πολιτική περιγράφει υπό ποιες προϋποθέσεις τρίτες οργανώσεις θα συνδέονται με τα δίκτυα ενός οργανισμού με σκοπό να πραγματοποιήσουν συναλλαγές τον οργανισμό αυτό. Συγκεκριμένα για την συμφωνία με τους τρίτους οργανισμούς, τον λόγο σύνδεσης, προεπισκόπηση ασφάλειας και τις διαδικασίες συνδέσεις.	**http://www.sans.org/resources/policies/Extranet_Policy.pdf**
24	**Identification and Authentication Policy** Ο σκοπός αυτής της πολιτικής είναι να καθιερώσει μια πολιτική για τη χρήση και την επέκταση ποικίλων λύσεων ελέγχου πρόσβασης για να εξασφαλίσει την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα των πληροφοριακών περιουσιακών στοιχείων. Αυτή η πολιτική είναι να	**http://www.tess-llc.com/Identification%20&%20Authentication%20PolicyV4.pdf**

	διατηρηθεί ένα επαρκές επίπεδο ασφάλειας για να προστατευθούν τα οικονομικά στοιχεία και τα συστήματα πληροφοριών από την αναρμόδια πρόσβαση.	
25	**Information Data Ownership Policy** Ο σκοπός αυτής της πολιτικής ιδιοκτησίας πληροφοριών είναι να παρασχεθεί μια πολιτική για την προστασία των πληροφοριών. Αυτή η πολιτική επιτρέπει σε κάποιο υπεύθυνο ή manager ενός οργανισμού να μεταβιβάσει τις ευθύνες και την υπευθυνότητα για τις πληροφορίες σε υφιστάμενα στελέχη του. Επίσης εγκαθιδρύει ρόλους, τις ευθύνες, και τη υπευθυνότητα που απαιτούνται για να διαχειριστούν κατάλληλα και να προστατευθούν οι πληροφορίες.	**http://www.tess-llc.com/Information%20Data-Ownership%20PolicyV4.pdf**
26	**Information Sensitivity Policy** Η πολιτική ευαισθησίας πληροφοριών προορίζεται να βοηθήσει τους υπαλλήλους να καθορίσουν ποιες πληροφορίες μπορούν να αποκαλυφθούν στους μη-υπαλλήλους, καθώς επίσης και τη σχετική ευαισθησία των πληροφοριών που δεν πρέπει να αποκαλυφθούν έξω από τον οργανισμό χωρίς τη κατάλληλη έγκριση. Οι πληροφορίες που καλύπτονται σε αυτές τις οδηγίες περιλαμβάνουν, αλλά δεν περιορίζονται, σε πληροφορίες που είτε αποθηκεύονται είτε μοιράζονται μέσω οποιωνδήποτε μέσων.	**http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf**

27	**Information System Audit Logging Requirements** Η παρούσα πολιτική προσπαθεί να αντιμετωπίσει το ζήτημα για τις καταγραφές ελέγχου με τον προσδιορισμό συγκεκριμένων απαιτήσεων για τα συστήματα πληροφοριών πρέπει να υπάρχουν προκειμένου να παραχθούν οι κατάλληλες καταγραφές ελέγχου και να ενσωματωθεί με μια διοικητική λειτουργία για τις καταγραφές ελέγχου.	**http://www.sans.org/resources/policies/info_sys_audit.pdf**
28	**Internal Lab Security Policy** Αυτή η πολιτική καθιερώνει τις απαιτήσεις για την ασφάλεια πληροφοριών για τα εργαστήρια του οργανισμού ώστε να εξασφαλιστεί ότι εμπιστευτικές πληροφορίες και τεχνολογίες δεν θα αποκαλυφθούν, και ότι οι υπηρεσίες παραγωγής και άλλα ενδιαφέροντα του οργανισμού προστατεύονται από τις δραστηριότητες εργαστηρίων.	**http://www.sans.org/resources/policies/Internal_Lab_Security_Policy.pdf**
29	**Internet DMZ Equipment Policy** Ο σκοπός αυτής της πολιτικής είναι να καθοριστούν τα πρότυπα που ανταποκρίνονται σε όλο τον εξοπλισμό που ανήκει ή/ και που χρησιμοποιείται από στο όνομα ενός οργανισμού και είναι τοποθετημένος εξωτερικά από τα firewall οργανισμού. Αυτά τα πρότυπα έχουν ως σκοπό να ελαχιστοποιήσουν την πιθανή έκθεση του οργανισμού από την απώλεια ευαίσθητων ή εμπιστευτικών δεδομένων , πνευματικής ιδιοκτησίας, ζημίας στη δημόσια εικόνα	**http://www.sans.org/resources/policies/Internet_DMZ_Equipment_Policy.pdf**

	κ.λπ., η οποία μπορεί να προκύψει από την αναρμόδια χρήση πόρων του οργανισμού.	
30	**Lab Anti-Virus Policy** Καθορίζει τις απαιτήσεις που πρέπει να καλυφτούν από όλους τους υπολογιστές που συνδέονται με δίκτυα εργαστηρίων ενός οργανισμού για να εξασφαλιστεί η αποτελεσματική ανίχνευση και πρόληψη ιών.	**http://www.sans.org/resources/policies/Lab_Anti-Virus_Policy.pdf**
31	**Network Security Policy** Για να εξασφαλίσει την προστασία των πληροφοριών στα δίκτυα και την προστασία των υποδομών υποστήριξης. Η ασφαλής διαχείριση των δικτύων, που μπορεί να εκταθεί τα οργανωτικά όρια του οργανισμού, απαιτεί την προσεκτική εκτίμηση στη ροή πληροφοριών, τις νομικές επιπτώσεις, τον έλεγχο, και την προστασία.	**http://www.sans.org/resources/policies/Ethics_Policy.pdf**
32	**Password Protection Policy** 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. Συγκεκριμένα εστιάζει σε οδηγίες δημιουργίας δυνατών κωδικών, προτύπων για την προστασία τους, και Passphrases.	**http://www.sans.org/resources/policies/Password_Policy.pdf**
33	**Personal Communication Device** Η παρούσα πολιτική περιγράφει τις απαιτήσεις της ασφαλείας πληροφοριών για τις προσωπικές συσκευές επικοινωνίας και για το Voicemail ενός οργανισμού. Εστιάζει στη χρήση αυτών	**http://www.sans.org/resources/policies/Personal_Communication_Device.pdf**

	των συσκευών, στο πρωτόκολλο Bluetooth, στην περίπτωση απώλειας ή κλοπής και τέλος στο Voicemail.	
34	**Personnel Security Policy** 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.	**http://www.datasecuritypolicies.com/wp-content/uploads/2007/04/generic-personnel-security-policy.pdf**
35	**Physical Security Policy** 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.	**http://www.tessllc.com/Physical%20Security%20PolicyV4.pdf**
36	**Privacy Policy** Η πολιτική αυτή έχει σαν στόχο να παρέχει τη διαβεβαίωση στους επισκέπτες, πελάτες, υπαλλήλους και λοιπά άτομα που ένας οργανισμός έχει προσωπικά δεδομένα ότι οι πληροφορίες αυτές δεν θα γίνουν αντικείμενο κατάχρησης.	**http://www.cbe.uidaho.edu/wegman/404/PRIVACY%20POLICY%20IVI%20Generic.htm**
37	**Remote Access Policy**	**http://www.sans.org/resources/policies/**

	Ο σκοπός αυτής της πολιτικής είναι να καθοριστούν τα πρότυπα για τη σύνδεση του δικτύου του ενός οργανισμού με οποιοδήποτε άλλο δίκτυο ή απομακρυσμένο υπολογιστή. Αυτά τα πρότυπα έχουν ως σκοπό να ελαχιστοποιήσουν την πιθανή έκθεση από τις ζημίες που μπορούν να προκύψουν από την αναρμόδια χρήση των πόρων του.	**Remote_Access_Policy.pdf**
38	**Removable Media Policy** Η πολιτική αυτή έχει σαν στόχο να ελαχιστοποιήσει τον κίνδυνο απώλειας ή την έκθεση των ευαίσθητων πληροφοριών που διατηρείται από στον οργανισμό και για να μειώσει τον κίνδυνο από κακοήθη κώδικα, τις μολύνσεις στους υπολογιστές που χρησιμοποιούνται από τον οργανισμό.	**http://www.sans.org/resources/policies/Removable_Media.pdf**
39	**Remote Access - Mobile Computing and Storage Devices** Σκοπός αυτής της πολιτικής είναι να καθιερώσει έναν εξουσιοδοτημένη μέθοδο για τον έλεγχο κινητών υπολογιστών και συσκευών αποθήκευσης που περιέχουν ή έχουν πρόσβαση σε πηγές πληροφοριών του οργανισμού. Συγκεκριμένα κατανέμει ρόλους και ευθύνες, δημιουργεί διαδικασίες για αίτηση χρήσης τέτοιων συσκευών ή σε περίπτωση κλοπής.	**http://www.sans.org/resources/policies/Remote_Access.pdf**
40	**Resource Utilization Security Policy** Ο σκοπός αυτής της πολιτικής είναι να μεγιστοποιηθεί η διαθεσιμότητα των πληροφοριών ενός	**http://www.tess-llc.com/Resource%20Utilization%20PolicyV4.pdf**

	οργανισμού. Οι αποτυχίες μεταξύ του τελικού χρήστη και των επιθυμητών στοιχείων πρέπει να εξουδετερωθούν. Αυτή η πολιτική ανακουφίζει τις αποτυχίες μεταξύ των τελικών χρηστών με την εφαρμογή και τη διατήρηση ενός υψηλού επιπέδου ανοχής βλαβών, χωρίς παραγωγή των τεράστιων κύριων επενδύσεων.	
41	**Risk Assessment Policy** Η πολιτική αυτή καθορίζει τις απαιτήσεις και παρέχει την εξουσία για την ομάδα ασφάλειας πληροφοριών να προσδιορίσει, αξιολογεί, και να αποκαταστήσει τους κινδύνους για μια υποδομή πληροφοριών του οργανισμού που χρησιμοποιείται για τις επιχειρησιακές του ανάγκες .	**http://www.sans.org/resources/policies/Risk_Assessment_Policy.pdf**
42	**Router Security Policy** Η παρούσα πολιτική περιγράφει μια απαραίτητη ελάχιστη διαμόρφωση ασφάλειας για όλους τους δρομολογητές και τους κατανεμητές που συνδέουν το δίκτυο του οργανισμού ή άλλα δίκτυα που συνδέονται σε αυτόν.	**http://www.sans.org/resources/policies/Router_Security_Policy.pdf**
43	**Security Awareness Policy** Αυτή η πολιτική καθορίζει τις ευθύνες και τους ρόλους για την εμφύσηση της συνειδητοποίησης ασφάλειας πληροφοριών μεταξύ όλων των ιδιοκτητών, των διευθυντών, των φορέων παροχής υπηρεσιών και των χρηστών των πηγών πληροφοριών.	**http://lits.ollusa.edu/LITSNavBar/Policies/SecurityAwarenessPolicy.shtml**
44	**Security Training Policy** Ο σκοπός της πολιτικής κατάρτισης ασφάλειας είναι να περιγραφούν οι απαιτήσεις	**http://www.cis.tamuk.edu/help/policies/1_170_Security%20Training%20Policy.pdf**

	που εξασφαλίζουν ότι κάθε χρήστης των πηγών πληροφοριών του Οργανισμού έχει επαρκή εκπαίδευση πάνω σε ζητήματα ασφάλειας υπολογιστών.	
45	**Server Security Policy** 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.	**http://www.sans.org/resources/policies/Server_Security_Policy.pdf**
46	**Server Malware Protection Policy** Ο σκοπός αυτής της πολιτικής είναι να ορίσει που συστήματα server απαιτούνται ώστε να έχουμε εφαρμογές anti-virus ή anti-spyware. Συγκεκριμένα μιλάει για ποίες καταστάσεις θα έχουμε anti-virus και anti-spyware , σε περίπτωση που mail server πώς πρέπει να προστατευθεί και ποίες εξαιρέσεις έχουμε.	**http://www.sans.org/resources/policies/Server_Malware_Protection_Policy.pdf**
47	**Telecommuting/Teleworking Securiti Policy** Καθορίζει την πολιτική για το teleworking που καλύπτει τα ζητήματα ασφάλειας απασχόλησης καθώς επίσης και πληροφοριών. Συγκεκριμένα τι είναι teleworking, τους στόχους, κριτήρια, υποχρεώσεις, επικοινωνία με το κέντρο της εργασίας κ.λ.π. .	**http://www.womans-work.com/teleworking_policy.htm**
48	**The Third Party Network Connection Agreement** Καθορίζει τα πρότυπα και τις	**http://www.sans.org/resources/policies/Third_Party_Agreement.pdf**

	απαιτήσεις, συμπεριλαμβανομένων των νομικών απαιτήσεων, που απαιτούνται προκειμένου να διασυνδεθεί ένα δίκτυο άλλου οργανισμού στο δίκτυο παραγωγής ενός οργανισμού. Αυτή η συμφωνία πρέπει να υπογραφεί από αμφότερα τα συμβαλλόμενα μέρη.	
49	**User Data Protection Policy** Καθορίζει τις απαιτήσεις για τους ελέγχους πρόσβασης, ελάχιστα προνόμια, ακεραιότητα κ.λπ. για να εξασφαλίσει τα προσωπικά δεδομένα. Αναλύει πως οι υπάλληλοι πρέπει να είναι σε θέση να ασκήσουν την ευελιξία στο χειρισμό και την προστασία των δεδομένων.	**http://www.tess-llc.com/User%20Data%20Protection%20PolicyV4.pdf**
50	**VPN Security Policy** Ο σκοπός αυτής της πολιτικής είναι να ορίσει τις οδηγίες για σύνδεση στο δίκτυο του οργανισμού μέσω του Virtual Private Network(VPN).	**http://www.sans.org/resources/policies/Virtual_Private_Network.pdf**
51	**Wireless Communication Policy** Αυτή η πολιτική καθορίζει τις συνθήκες τις οποίες πρέπει να πληροί 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.	**http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf**

Πίνακας 1:Λίστα πολιτικών ασφαλείας από την SANS

Κεφάλαιο 4

Εργαλεία Δημιουργίας και Διαχείρισης Πολιτικών Ασφαλείας

Στο κεφάλαιο αυτό θα εξετάσουμε εργαλεία που μας επιτρέπουν να δημιουργήσουμε και να διαχειριστούμε πολιτικές ασφαλείας. Θα δούμε μια λίστα με κάποια εργαλεία από το Internet και θα κάνουμε μία συνοπτική παρουσίαση μερικών εργαλείων

4.1 Λίστα Εργαλείων Δημιουργίας και Διαχείρισης Πολιτικών Ασφαλείας.

Σε αυτήν την παράγραφο παρουσιάζουμε μια λίστα με εργαλεία διαχείρισης πολιτικών ασφαλείας και κάνουμε μια συνοπτική παρουσίαση τους.

A/A	Toolkit	Link
1	Cisco Security Policy Builder	http://www.ciscowebtools.com/spb/
2	UCISA Information Security Toolkit	http://www.ucisa.ac.uk/Home/members/activities/ist.aspx
3	HIMSS Privacy & Security Toolkit	http://www.himss.org/ASP/privacySecurityTree.asp?faid=78&tid=4#PSToolkit#PSToolkit
4	ICC CUSTOMS SECURITY TOOLKIT	http://www.iccwbo.org/policy/customs/id1208/index.html
5	Gender and Security Sector Reform Toolkit	http://www.osce.org/item/29669.html
6	Zone Labs security management toolkit	http://www.networkworld.com/news/2002/0205zlabs.html
7	Information Shield	http://www.informationshield.com/securitypolicysolutions.html
8	CONTROL-IT Toolkit	http://citt.privacyresources.org/
9	ISO 17999 Toolkit	http://www.17799-toolkit.com/17799policies.htm
10	SSi Network Security Management	http://www.secured-networking.com/network_security_management.htm
11	Callio Toolkit 17799	http://www.sofotex.com/Callio-Toolkit-17799-download_L20800.html
12	Disaster Recovery Toolkit	http://www.businesscontinuityworld.com/access.htm
13	IBM Tivoli Security Policy Manager	http://www-01.ibm.com/software/tivoli/products/security-policy-mgr/

Πίνακας 2:Λίστα εργαλείων δημιουργίας και διαχείρισης πολιτικών ασφαλείας.

Cisco Security Policy Builder: Παρουσιάζεται πιο αναλυτικά παρακάτω.

UCISA Information Security Toolkit : Είναι ένα toolkit, το οποίο φτιάχτηκε για την δημιουργία policies, για οργανισμούς ανωτάτης εκπαίδευσης της Βρετανίας. Βασίζεται στο βρετανικό standard BS 7799. Το toolkit αυτό χωρίζει τις πολιτικές στις σε κατηγόριες. Πολιτικές σχετικά με τον οργανισμό, σχετικά με την χρήση πληροφοριών και συστημάτων πληροφοριών και προαιρετικές σχετικά με κρυπτογραφία , teleworking και mobile computing.

HIMSS Privacy & Security Toolkit: Είναι ένα σύνολο πολιτικών ασφαλείας και διαχείρισης προσωπικών δεδομένων για την Healthcare Information and Management Systems Society(HIMSS). Με αυτό σύνολο εργαλείων της HIMSS ένας οργανισμός υγείας πρέπει να είναι σε θέση να προγραμματίσει, να εφαρμόσει, και να αξιολογήσει τις διαδικασίες επιτήρησης προσωπικών δεδομένων και ασφάλειας που κλιμκώνονται στις οργανωτικές ανάγκες τους.

ICC CUSTOMS SECURITY TOOLKIT: Είναι ένα εργαλείο από την International Chamber of Commerce που έχει σαν σκοπό την εφαρμογή διαφανών, απλοποιημένών και εναρμονισμένων πολιτικών για τα τελωνεία. Είναι και ιδιαίτερα χρήσιμο για μια γρήγορη εκτίμηση της ποιότητας της τελωνειακής διαχείρισης ασφάλειας.

Gender and Security Sector Reform Toolkit: Αυτή η ομάδα εργαλείων αναπτύχθηκε από κοινού από το ODIHR, the UN International Research and Training Institute for the Advancement of Women (UN-INSTRAW), και το Geneva Centre for the Democratic Control of Armed Forces (DCAF), ως μια απάντηση στην ανάγκη για ενημέρωση και την ανάλυση σχετικά με το φύλο και η μεταρρύθμιση του τομέα της ασφάλειας (M.T.A). Απευθύνεται σε MTA χάραξης πολιτικής, επαγγελματίες και ερευνητές, στο πλαίσιο των εθνικών κυβερνήσεων, θεσμικών οργάνων του τομέα της ασφάλειας, τις διεθνείς και περιφερειακές οργανώσεις και οργανώσεις της κοινωνίας των πολιτών.

Zone Labs security management toolkit: Η κονσόλα διαχείρισης πολιτικής επιτρέπει στους διαχειριστές να προωθήσουν agent λογισμικού, οι οποίοι περιλαμβάνουν το Zone Labs firewall Zone Alarm Pro , μέχρι και σε 2000 σε υπολογιστές. Το ZoneAlarm Pro firewall / VPN μπορεί να μπλοκάρει την εισερχόμενες ή εξερχόμενες συνδέσεις, και μπορεί να φιλτράρει περιεχόμενο, όπως τα συνημμένα ηλεκτρονικού ταχυδρομείου.

Information Shield: Είναι μία πηγή για πολιτικές ασφάλειας πληροφοριών από τον εμπειρογνώμονα και συμβούλου πολιτικών ασφάλειας, Charles Cresson Wood, CISA, CISSP και που χρησιμοποιούνται από πάνω από 7000 οργανώσεις παγκοσμίως. Περιλαμβάνει πάνω από 1350 προ-γραπτές πολιτικές ασφάλειας πληροφοριών, κάθε μια με τα ειδικά σχόλια, που οργανώνονται μέσα στο πλαίσιο ασφάλειας του ISO 17799. Επίσης περιέχει τη συμβουλή από ειδήμονες για την οικοδόμηση και τη διατήρηση ενός αποτελεσματικού πολιτικού προγράμματος ασφάλειας πληροφοριών και περιλαμβάνει πλήρη δείγματα έγγράφων πολιτικών ασφάλειας.

CONTROL-IT Toolkit: Είναι ένα σύνολο εργαλείων που παρέχει μια ολόκληρη σειρά πηγών για να σας βοηθήσει να εξετάσετε και να εφαρμόσετε το COBIT(Control Objectives for Information and related Technology). Χωρίζετε στις παρακάτω κατηγορίες : HIGH LEVEL SECURITY POLICY FRAMEWORK, DETAILED SECURITY POLICY FRAMEWORK, AUDIT COMPLIANCE CHECKLIST KIT, THE COBIT COMPLIANCE PLAN, THE IT AND SECURITY GLOSSARY, SUPPORT RESOURCES.

ISO 17999 Toolkit: Το σύνολο εργαλείων του ISO 27000 περιλαμβάνει ένα πλήρες και περιεκτικό σύνολο εκατοντάδων πολιτικών ασφάλειας σύμφωνα με το 27002/17799. Αυτές έχουν δοκιμαστεί, και εξεταστεί και είναι αυτήν την περίοδο σε χρήση σε εκατοντάδες οργανώσεισε περισσότερες από 40 χώρες.

SSi Network Security Management: SonicWALL Global Management System (GMS) επιτρέπει σε διανεμημένες επιχειρήσεις και τους φορείς παροχής υπηρεσιών να κατορθώσουν να διαχειριστούν χιλιάδες συσκευές ασφάλειας Διαδικτύου και υπηρεσίες ασφάλειας από μια κεντρική θέση για να μειώσουν τις ανάγκες επάνδρωσης, να επιταχύνουν την επέκταση, και τις χαμηλότερες διοικητικές δαπάνες ασφάλειας.

Callio Toolkit 17799: Αυτή η ομάδα εργαλείων αποτελείται από μια σειρά εγγράφων, εργαλείων, και άλλων αντικειμένων που συγκεντρώνονται με μόνο σκοπό να γίνει αντιληπτό το πρότυπο και να γίνουν αντιληπτές οι βασικές προϋποθέσεις του. Το σετ εργαλείων αυτο περιέχει:Εισαγωγή στο ISO 17799/ BS 7799, module επεξεργασίας κινδύνου, αποσπάσματα από τα ISO 17799/ BS 7799, σετ ελέγχου, εργαλείο δημιουργίας πολιτικών, και πρότυπα εφαρμογής.

Disaster Recovery Toolkit: Είναι μια συλλογή εγγράφων και αντικειμένων με σκοπό να βοηθήσουν στην εξασφάλιση συνοχής σε περίπτωση καταστροφής ή σοβαρού γεγονότος. Περιλαμβάνει ερωτηματολόγιο ελέγχου για σχέδιο αποκατάστασης καταστροφής, ανάλυσης επιχειρησιακού αντίκτυπου. Λίστα πίνακα ελέγχου, πλαίσιου και μια ενεργειών για την αποκατάσταση καταστροφής. Ερωτήσεις και καθοδήγηση εγγράφων ανάλυσης εξάρτησης.

IBM Tivoli Security Policy Manager: Παρουσιάζεται πιο αναλυτικά παρακάτω.

4.2 IBM Tivoli Security Policy Manager

IBM® Tivoli® Security Policy Manager παρέχει λύσεις για να καλύψει τις ανάγκες ασφάλειας ιδιόκτητων εφαρμογών και υπηρεσιών Web. Ενισχύει την πρόσβαση εφαρμογών, διευκολύνουν τη συμμόρφωση, και υποστηρίζουν τη λειτουργική διαχείριση πέρα από την υποδομή πληροφοριών. Ειδικότερα:

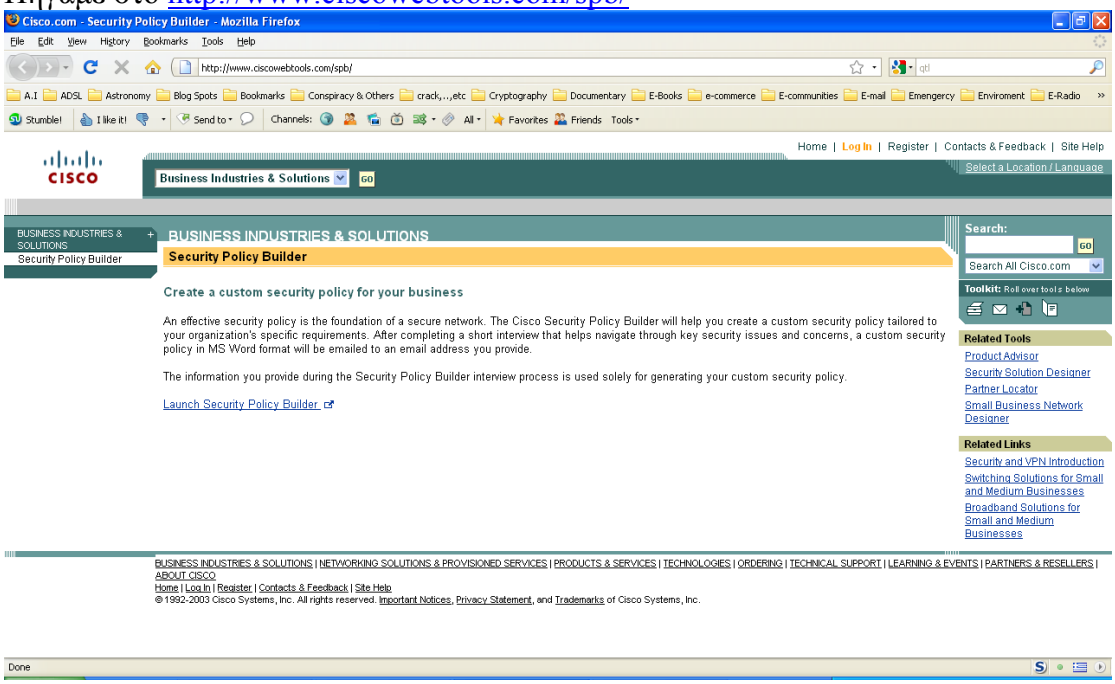
- Ανακαλύψτε και εισάγετε τις υπηρεσίες από registries και τις εφαρμογές.
- Εισάγετε τους ρόλους εφαρμογών και ενσωματώστε με στο υπάρχον σύστημα.
- Ο διαχειριστής , μετασχηματίζει, διαχειρίζεται και διανέμει τις
- πολιτικές ασφάλειας.
- Επιβολή πολιτικών στα πολλαπλά σημεία επιβολής χρησιμοποιώντας τις runtime υπηρεσίες ασφάλειας.
- Ελαχιστοποιήστε τις λειτουργικές ανεπάρκειες και την ευπάθεια σχετικές με τις εξουσιοδοτήσεις και την πολιτική διαχείριση ασφάλειας SOA.
- Διαχειριστείτε τις πολιτικές ασφάλειας SOA και τις εξουσιοδοτήσεις καθ' όλη τη διάρκεια του κύκλου ζωής της πολιτικής, από τη δημιουργία και έκδοση στην επιβολή και την ενημέρωση.
- Επιβάλατε τις πολιτικές στο runtime, που ενισχύει τη στάση ασφάλειας της οργάνωσής σας.
- Άμεσες αλλαγές και έλεγχος πολιτικών κεντρικά, για γρηγορότερη και αποτελεσματική συμμόρφωση σε νέες ή πιό αυστηρές απαιτήσεις επιβολής.
- Χρήση εργαλείων διαχείρισης πολιτικών ομόσπονδων μεταξύ τους για να βοηθήσει γεφυρωθεί το χάσμα μεταξύ των προσεγγίσεων επιχειρήσιακών και τεχνολογιών πληροφοριών πολιτικών ασφάλειας.
- Ενεργοποίηση σε end-to-end έγκριση εφαρμογής χρησιμοποιώντας εύκαμπτη πολιτική διαχείρισης και τις αποφάσεις για τις πολιτικές βασισμένες σε πρότυπα.
- Υποστηρίζει ένα ευρύ σύνολο πλατφορμών, συμπεριλαμβανομένης της IBM AIX®, περιβαλλόντων Red Hat Enterprise Linux®, Microsoft® Windows®, και Solaris.

4.3 Cisco Security Policy Designer & Security Solution Designer

4.3.1 Cisco Security Policy Designer

Ο Cisco Security Policy Builder θα βοηθήσει να δημιουργηθεί μια συνηθισμένη πολιτική ασφάλειας που προσαρμόζεται στις συγκεκριμένες απαιτήσεις ενός οργανισμού. Μετά από την ολοκλήρωση μιας σύντομης συνέντευξης που οι οδηγίες πλοηγούν στα βασικά ζητήματα ασφάλειας , μια πολιτική ασφάλειας με τη μορφή MS-WORD θα σταλθεί μήνυμα με ηλεκτρονικό ταχυδρομείο σε μια διεύθυνση ηλεκτρονικού ταχυδρομείου που θα δοθεί.

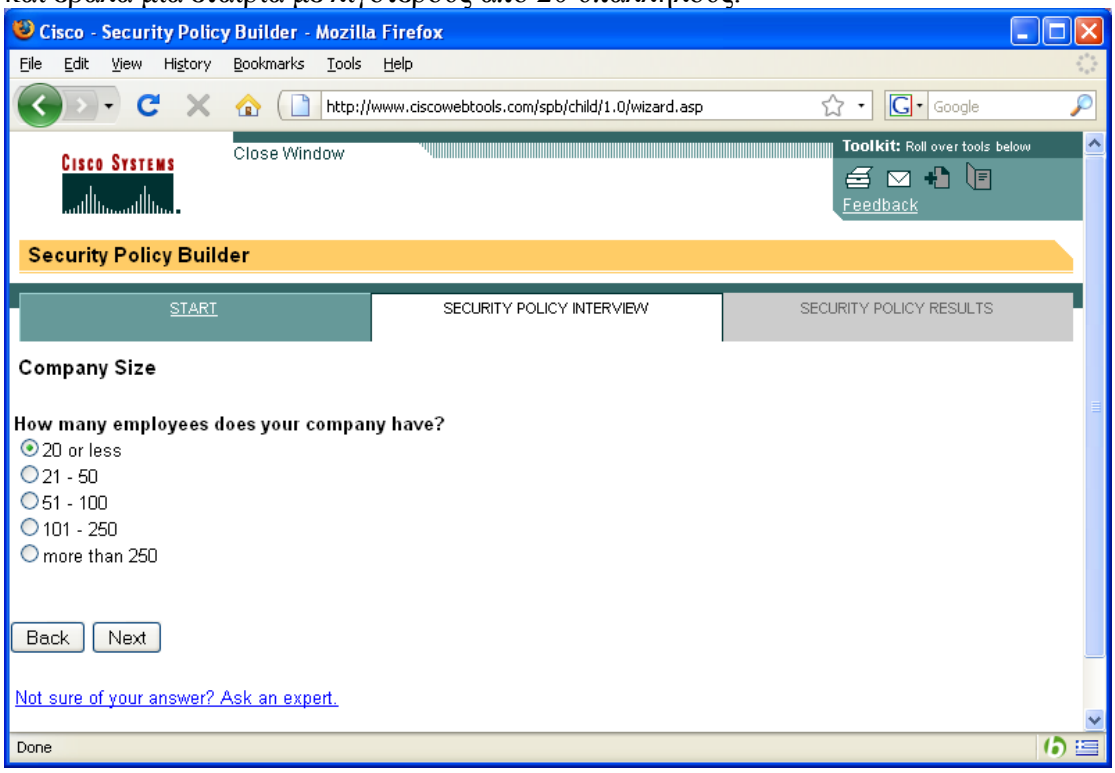
Πήγαμε στο http://www.ciscowebtools.com/spb/



Εικόνα 1:Cisco Builder:Αρχική οθόνη του Security Policy Builder της Cisco

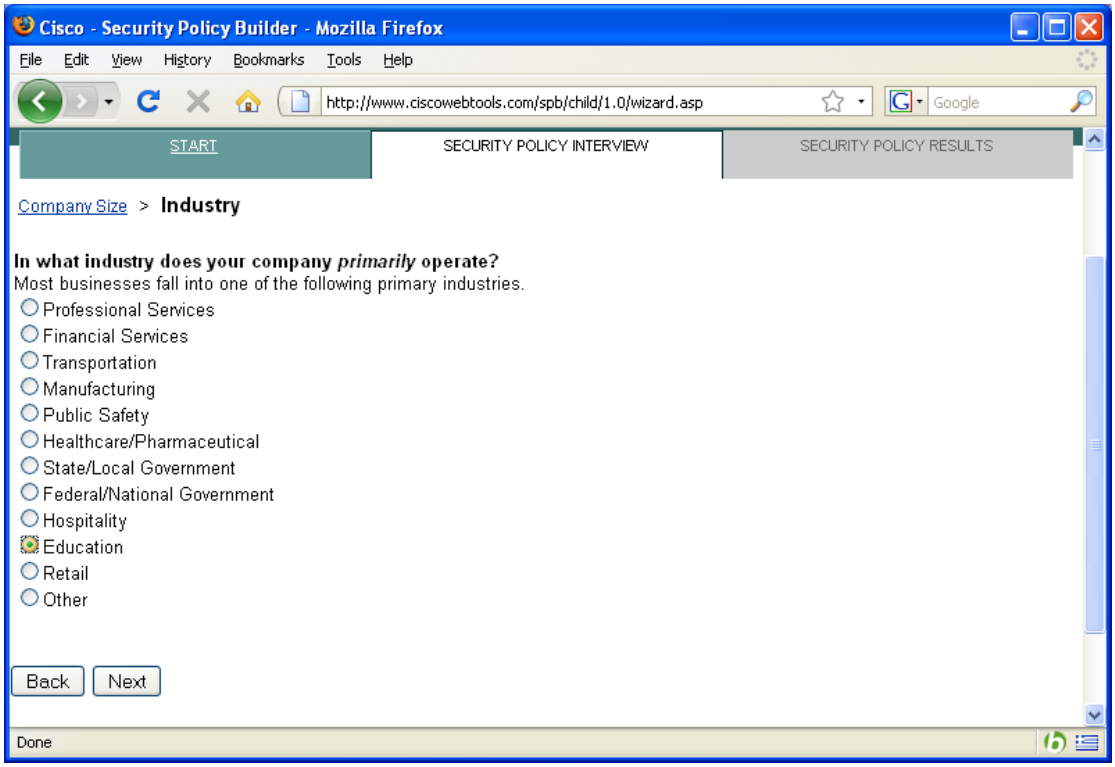
Εικόνα 2: Cisco Builder: Εκκίνηση του Security Policy Builder

και έβαλα μια εταιρία με λιγότερους από 20 υπαλλήλους.



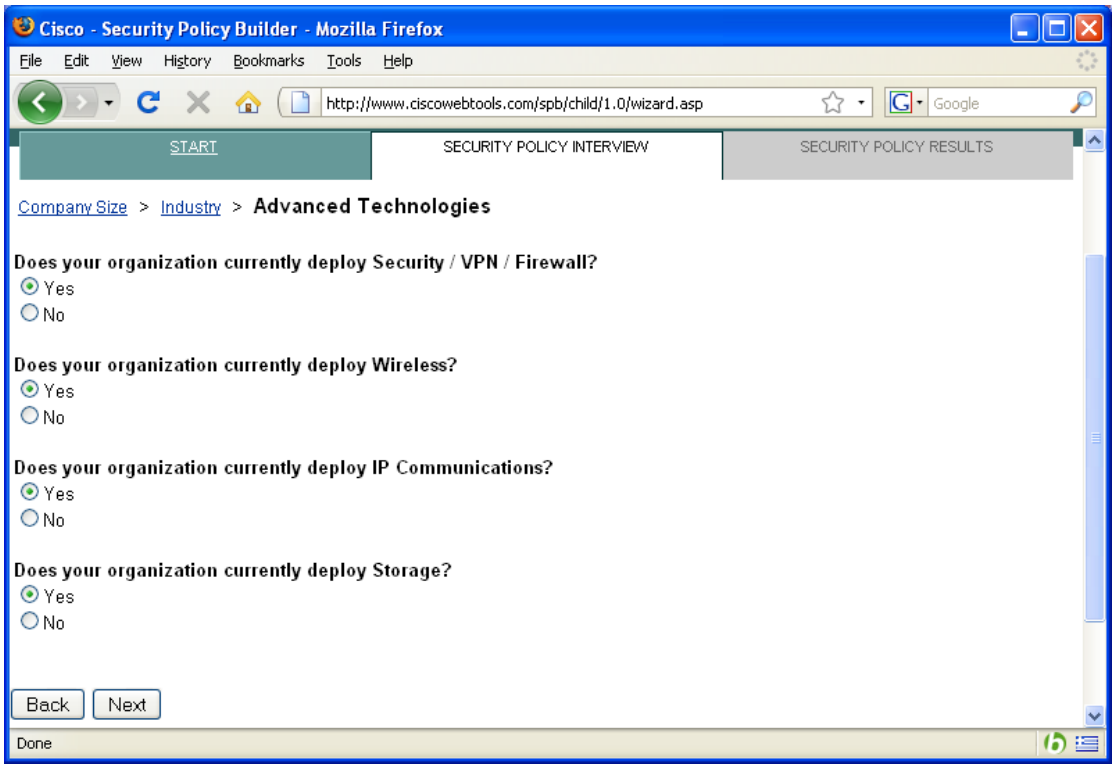
Εικόνα 3: Cisco Builder: Company Size

Μετά βάλαμε τομέας λειτουργίας την παιδεία.



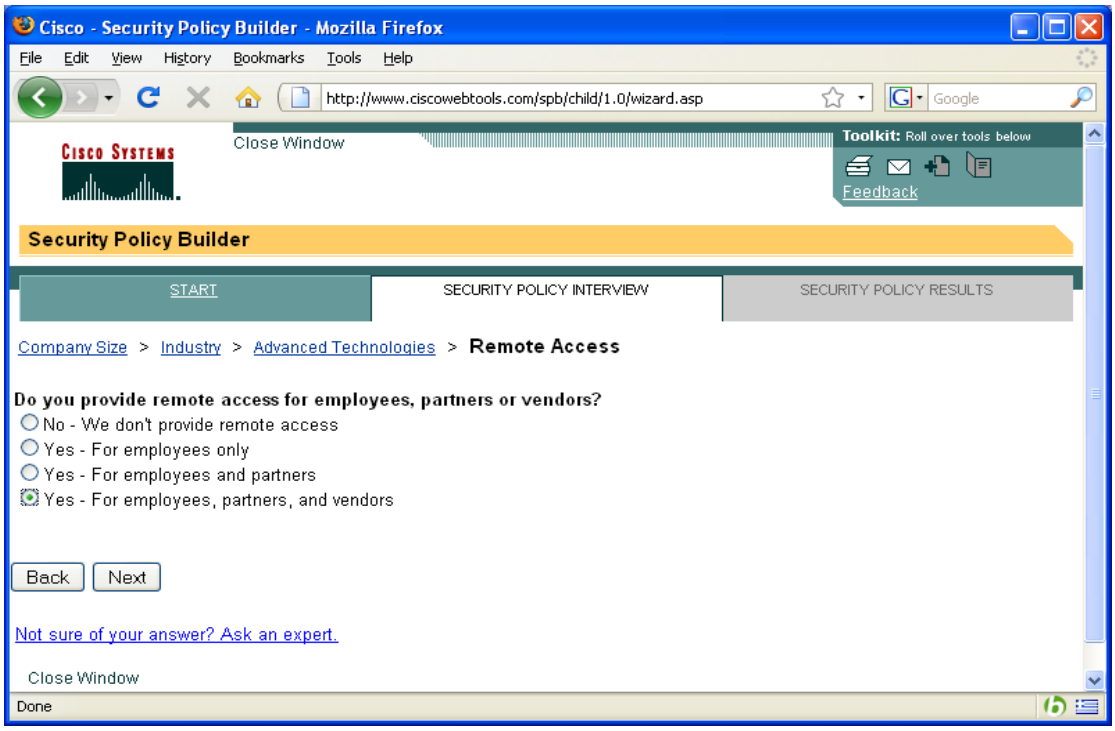
Εικόνα 4: Cisco Builder: Επιλογή τομέα δραστηριότητας

Στην συνέχεια ορίσαμε ότι έχει αναπτυγμένα Security/VPN/Firewall, IP Communications , wireless και Storage. Από την στιγμή που έχουμε ένα οργανισμό εκπαίδευσης θέλουμε επικοινωνίες με IP(Internet),wireless,και ασφάλεια από την στιγμή που έχουμε ευαίσθητα δεδομένα.



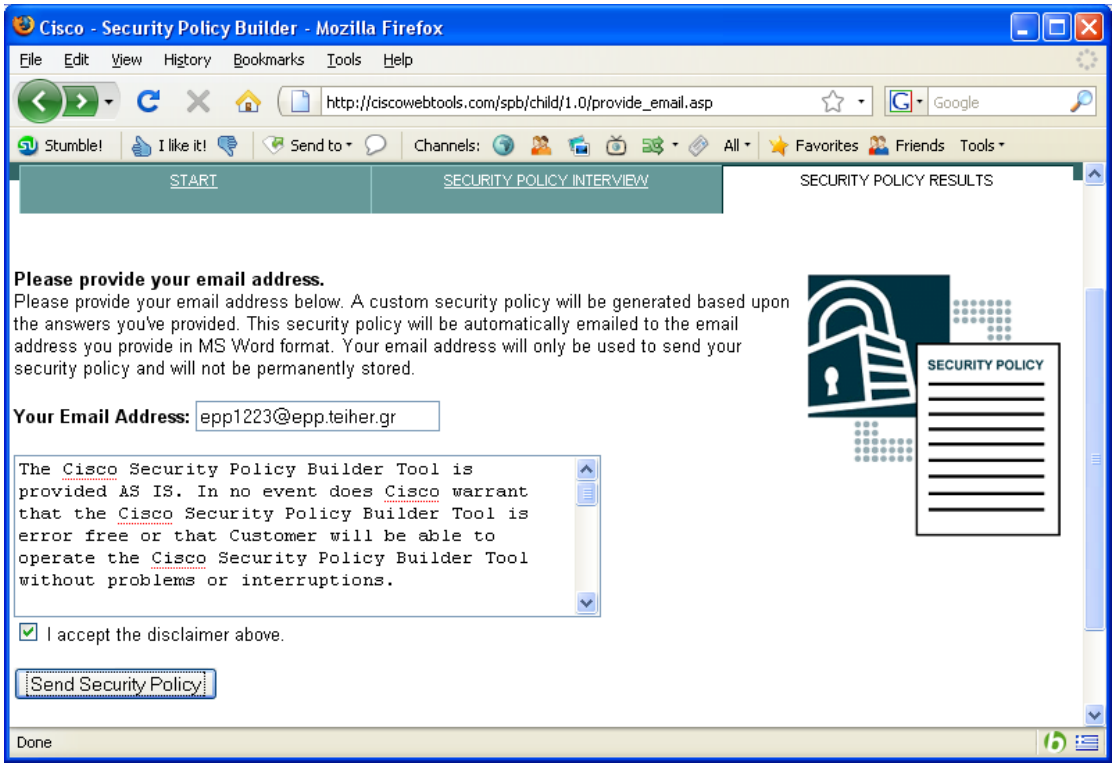
Εικόνα 5: Cisco Builder: Επιλογή τεχνολογιών του Οργανισμού

Μετά όρισα απομακρυσμένη πρόσβαση για προμηθευτές, συνεργάτες και υπαλλήλους. Εάν βάζαμε παράδειγμα μόνο υπάλληλους θα είχαμε επιθυμία για μεγαλύτερη ασφάλεια άρα μικρότερο ρίσκο από απειλές / επιθέσεις. Όσο μεγαλύτερος είναι ο κύκλος των χρηστών που θα έχουν πρόσβαση στα συστήματα του οργανισμού τόσο μεγαλώνει ο κίνδυνος από επιθέσεις.

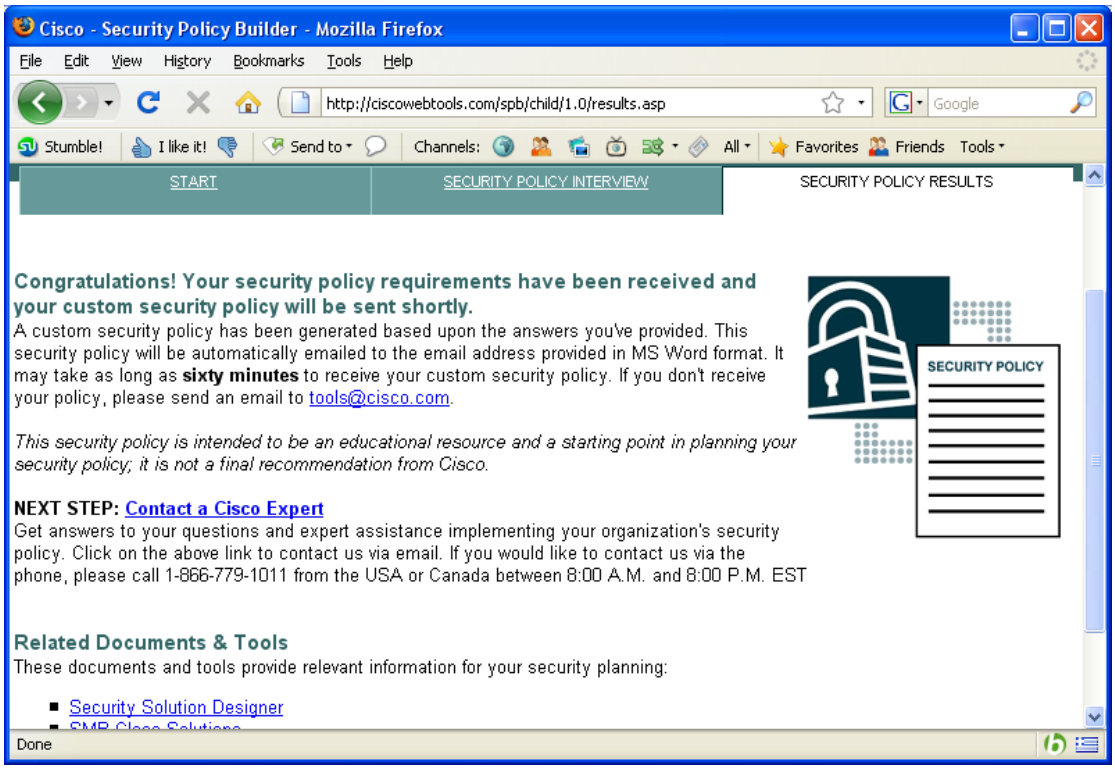


Εικόνα 6: Cisco Builder: Επιλογή τύπου Remote Access

Τέλος η Cisco μου έφτιαξε μια πολιτική και την έστειλε σε email.



Εικόνα 7: Cisco Builder: Εισαγωγή e-mail για αποστολή και αποδοχή του diclaimer.



Εικόνα 8: Cisco Builder: Μήνυμα επιτυχούς αποστολής.

4.3.2 Παραδείγματα Πολιτικών από την Cisco

Εδώ παραθέτουμε συνοπτικά μερικές από τις πολιτικές που περιέχει το έγγραφο που παράχθηκε από την παραπάνω διαδικασία:

Email and Communications Activities

Σκοπός

Η πολιτική καθορίζει τα πρότυπα για τη διεύθυνση των επικοινωνιών μέσα στο σύστημα ηλεκτρονικού ταχυδρομείου δικτύων. Αυτά τα πρότυπα ελαχιστοποιούν την πιθανή έκθεση από τα εκούσια μηνύματα και τις συνδέσεις ηλεκτρονικού ταχυδρομείου. Οι ζημίες περιλαμβάνουν την απώλεια ευαίσθητων ή εμπιστευτικών στοιχείων επιχείρησης ή πνευματικής ιδιοκτησίας, τη ζημία στη δημόσια εικόνα, τη ζημία στα κρίσιμα εσωτερικά συστήματα, και την ακούσια έκθεση υπαλλήλων στο ακατάλληλο περιεχόμενο ή το υλικό.

1. Στέλνοντας τα εκούσια μηνύματα ηλεκτρονικού ταχυδρομείου, συμπεριλαμβανομένης της αποστολής του "junk mail" ή άλλου υλικού διαφήμισης στα άτομα που δεν ζήτησαν συγκεκριμένα τέτοιο υλικό (ηλεκτρονικό ταχυδρομείο spam).
2. Οποιαδήποτε μορφή της παρενόχλησης μέσω του ηλεκτρονικού ταχυδρομείου, του τηλεφώνου, ή της σελιδοποίησης, είτε μέσω της γλώσσας, της συχνότητας, είτε του μεγέθους των μηνυμάτων.
3. Αναρμόδια χρήση, ή τροποποίησης των πληροφοριών επικεφαλίδων ηλεκτρονικού ταχυδρομείου.
4. Ζητώντας το ηλεκτρονικό ταχυδρομείο για οποιαδήποτε άλλη διεύθυνση ηλεκτρονικού ταχυδρομείου, εκτός από αυτήν του λογαριασμού χρήστη, με την πρόθεση για να παρενοχλήσει ή να συλλέξει τις απαντήσεις.
5. Δημιουργία ή διαβίβαση "επιστολών αλυσίδων" ή "Ponzi" ή άλλων σχεδίων "πυραμίδων" οποιουδήποτε τύπου.
6. Χρησιμοποιώντας το εκούσιο ηλεκτρονικό ταχυδρομείο που δημιουργείται από τα δίκτυα ή άλλους φορείς παροχής υπηρεσιών Internet /intranet /extranet εξ ονόματος, ή για να διαφημίσει, οποιαδήποτε υπηρεσία που φιλοξενείται ή που συνδέεται μέσω του δικτύου.
7. Ταχυδρόμηση των ίδιων ή παρόμοιων μη- επιχειρησιακών-σχετικών μηνυμάτων στους μεγάλους αριθμούς ομάδων πληροφόρησης USENET (ομάδα πληροφόρησης spam).

Επιβολή
Οποιοσδήποτε υπάλληλος που παραβιάζει αυτήν την πολιτική μπορεί να είναι υπαγόμενος σε πειθαρχική ενέργεια, μέχρι και συμπεριλαμβανομένης τη λήξη της απασχόλησης.

Anti-Virus Policy

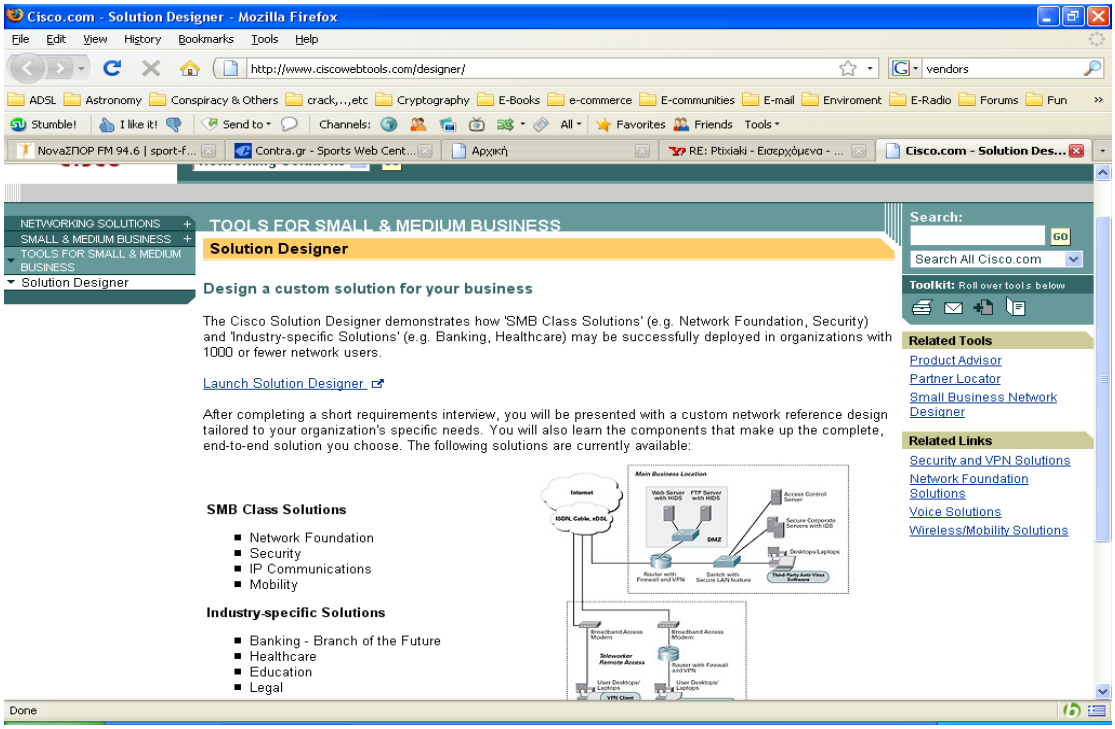
Σκοπός

Η πολιτική καθορίζει τα πρότυπα για την προστασία του δικτύου από οποιαδήποτε απειλή σχετική με ιούς, worms ή trojan horse. Αυτά τα πρότυπα ελαχιστοποιούν την πιθανή έκθεση από τις ζημίες που μπορούν να προκύψουν από και μη προστατευμένο δίκτυο. Οι ζημίες μπορούν να περιλάβουν την απώλεια ευαίσθητων ή εμπιστευτικών στοιχείων επιχείρησης ή πνευματικής ιδιοκτησίας, τη ζημία στη δημόσια εικόνα, τη ζημία στα κρίσιμα εσωτερικά συστήματα, κ.λπ..

1. Πάντα να εκτελείτε το πρότυπο, υποστηριζόμενο λογισμικό antivirus. Κατεβάστε και τρέξτε την παρούσα έκδοση, όπως επίσης και ενημερώσεις όταν αυτές γίνονται διαθέσιμες.
2. Μην ανοίξτε ποτέ οποιασδήποτε αρχεία ή μακροεντολές που συνδέονται με ένα ηλεκτρονικό ταχυδρομείο από μια άγνωστη, ύποπτη, πηγή. Διαγράψτε αυτές τις συνδέσεις αμέσως, κατόπιν αδειάστε τα απορρίμματα σας.
3. Διαγράψτε spam, junk ηλεκτρονικό ταχυδρομείο σας χωρίς προώθηση, ανάλογα με τη πολιτική αποδεκτής χρήσης.
4. Μην κατεβάζετε ποτέ τα αρχεία από τις άγνωστες ή ύποπτες πηγές.
5. Αποφύγετε τον άμεση πρόσβαση ανάγνωσης-γραφής σε δίσκο εκτός αν υπάρχει απολύτως μια επιχειρησιακή απαίτηση να κάνει έτσι.
6. Πάντα ανιχνεύστε μια floppy δισκέτα από μια άγνωστη πηγή για ιούς πριν την χρήση.
7. Τακτική αποθήκευση κρίσιμων διαμορφώσεων δεδομένων και συστημάτων σε ασφαλή θέση.
8. Εάν τα test εργαστηρίων έχουν conflicts με τα antivirus, τρέξτε το scanner του antivirus για να εξασφαλιστεί ένα καθαρό σύστημα, θέστε εκτός λειτουργίας το λογισμικό, και τρέξτε έπειτα τη δοκιμή εργαστηρίων. Μετά από τη δοκιμή εργαστηρίων, τρέξτε το antivirus. Όταν το antivirus τίθεται εκτός λειτουργίας, μην τρέξτε οποιεσδήποτε εφαρμογές που θα μπορούσαν να μεταφέρουν έναν ιό, π.χ., διανομή ηλεκτρονικού ταχυδρομείου ή αρχείων.
9. Οι νέοι ιοί ανακαλύπτονται σχεδόν κάθε ημέρα. Περιοδικά ελέγξτε την πολιτική antivirus επιχείρησης και αυτόν τον συνιστώμενο κατάλογο διαδικασιών για τις αναπροσαρμογές.

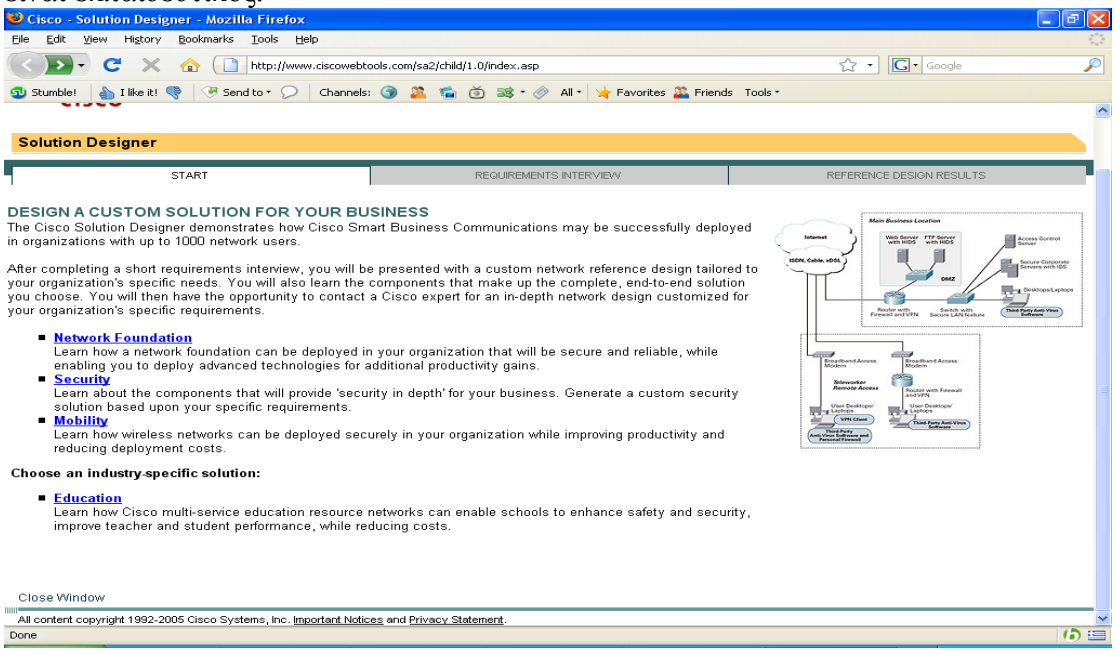
4.3.3 Cisco Security Solution Designer

Το Security Solution Designer καταδεικνύει πώς μέσω θεμελιωδών κλάσεων λύσης δικτύων S.M.B(Server Message Block) μπορεί να επεκταθεί επιτυχώς σε οργανώσεις με 1.000 ή λιγότερους χρήστες δικτύου. Μετά αφού ολοκληρώσετε μια σύντομη συνέντευξη απαιτήσεων, θα παρουσιαστεί ένα σχέδιο αναφοράς δικτύου που προσαρμόζεται στις συγκεκριμένες ανάγκες της οργάνωσής σας. Θα μάθετε επίσης τα συστατικά που αποτελούν την πλήρη, end to end λύση που εσείς επιλέξατε.



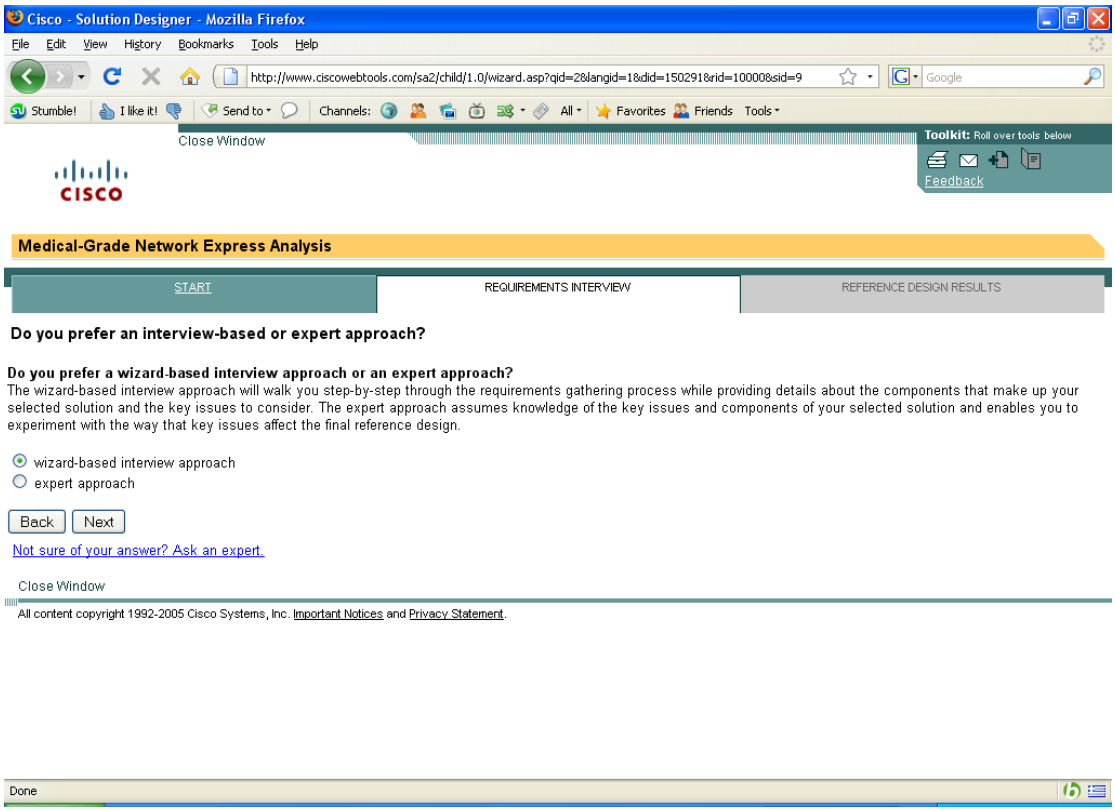
Εικόνα 9:Ο Security Solution Designer της Cisco.

Στην συνέχεια στην αρχή του designer επιλέξαμε Education επειδή ο οργανισμός μας είναι εκπαιδευτικός.

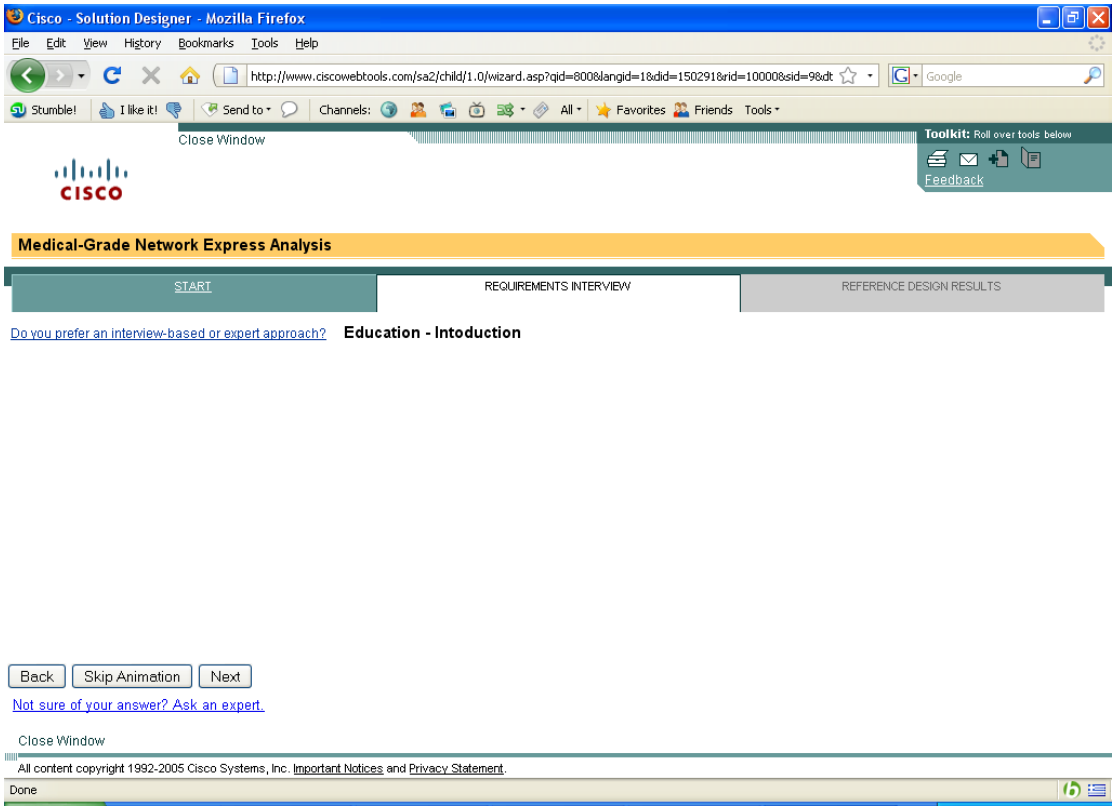


Εικόνα 10: Cisco Designer: Επιλογή τομέα δραστηριοποίησης του οργανισμού

Στην συνέχεια ο designer ρωτά εάν θέλουμε ένα wizard-based interview approach ή ένα expert approach. Επέλεξα το wizard-based interview approach.

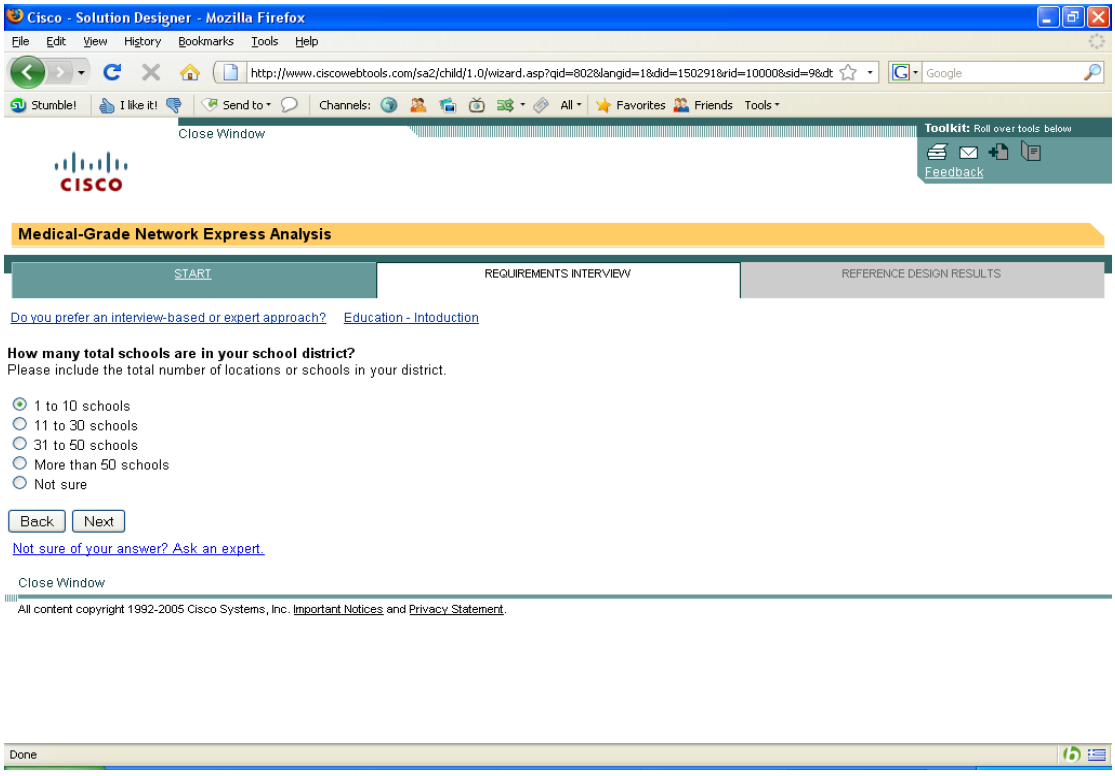


Εικόνα 11: Cisco Designer: Επιλογή τρόπου προσέγγισης του interview για τον Security Solution Designer



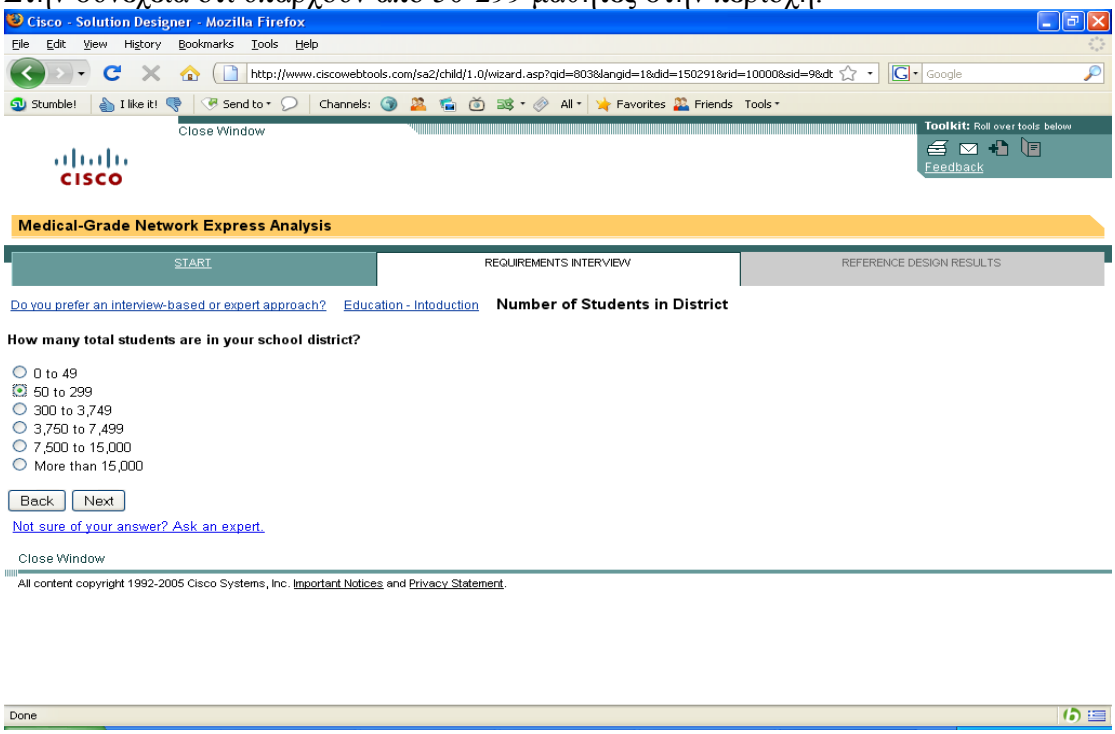
Εικόνα 12: Cisco Designer: Επιβεβαίωση τρόπου προσέγγισης.

Μετά βάλαμε 1 to 10 schools στην ερώτηση πόσα σχολεία υπάρχουν στην περιοχή του οργανισμού.



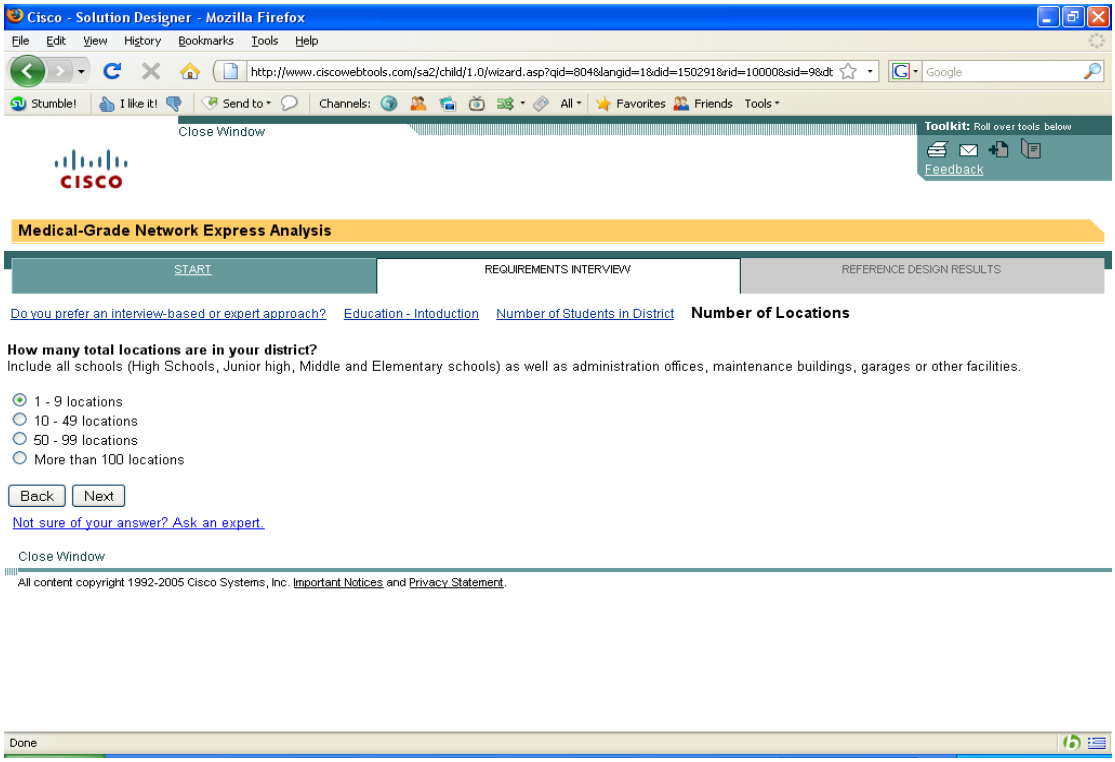
Εικόνα 13: Cisco Designer: Επιλογή αριθμού σχολείων που υπάρχουν στην περιοχή του οργανισμού.

Στην συνέχεια ότι υπάρχουν από 50-299 μαθητές στην περιοχή.



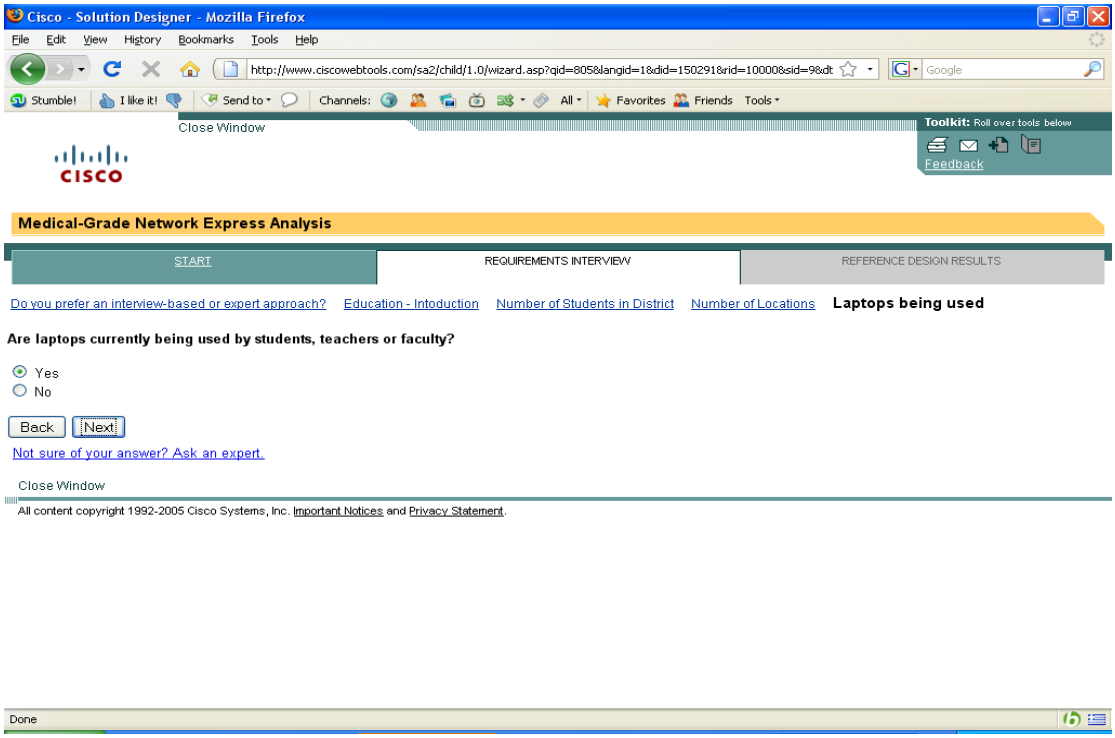
Εικόνα 14: Cisco Designer: Επιλογή αριθμού μαθητών στην περιοχή του οργανισμού

Μετά ρωτάει σχετικά με τις εγκαταστάσεις το σχολείων αυτών διαλέξαμε 1-9.



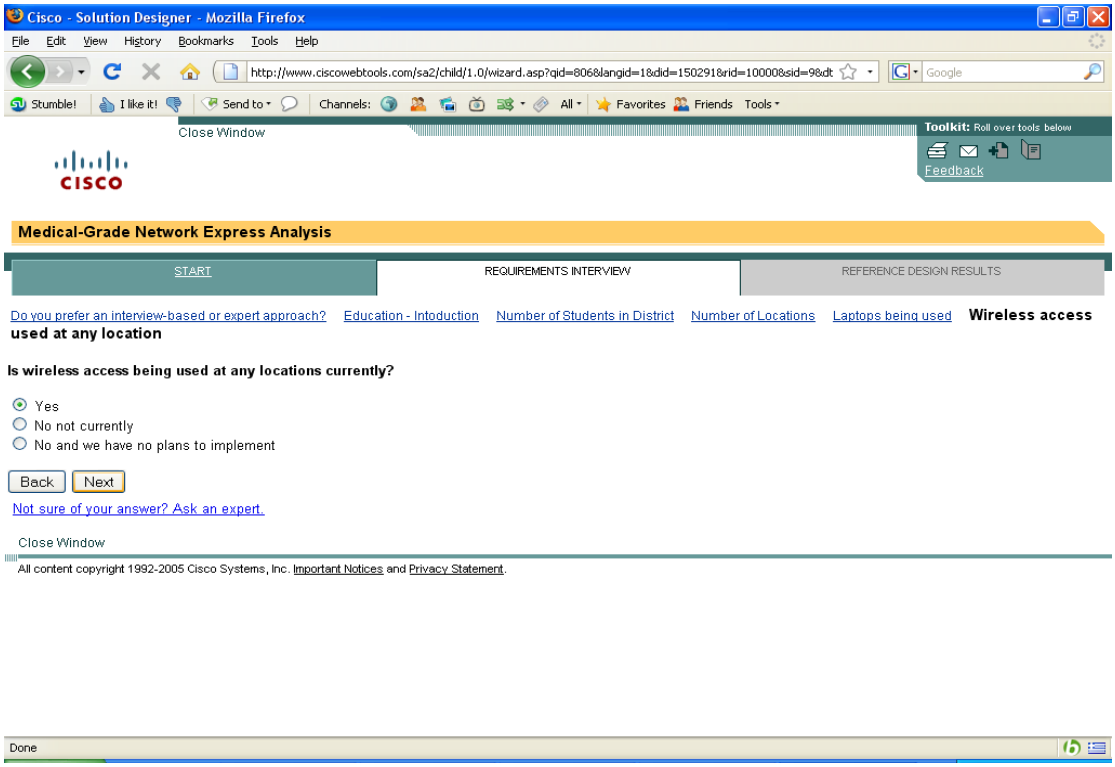
Εικόνα 15: Cisco Designer: Επιλογή αριθμού εγκαταστάσεων στην περιοχή του οργανισμού.

Στην συνέχεια ρωτάει εάν προσωπικό, μαθητές και καθηγητές έχουν laptop. Απάντησα ναι.



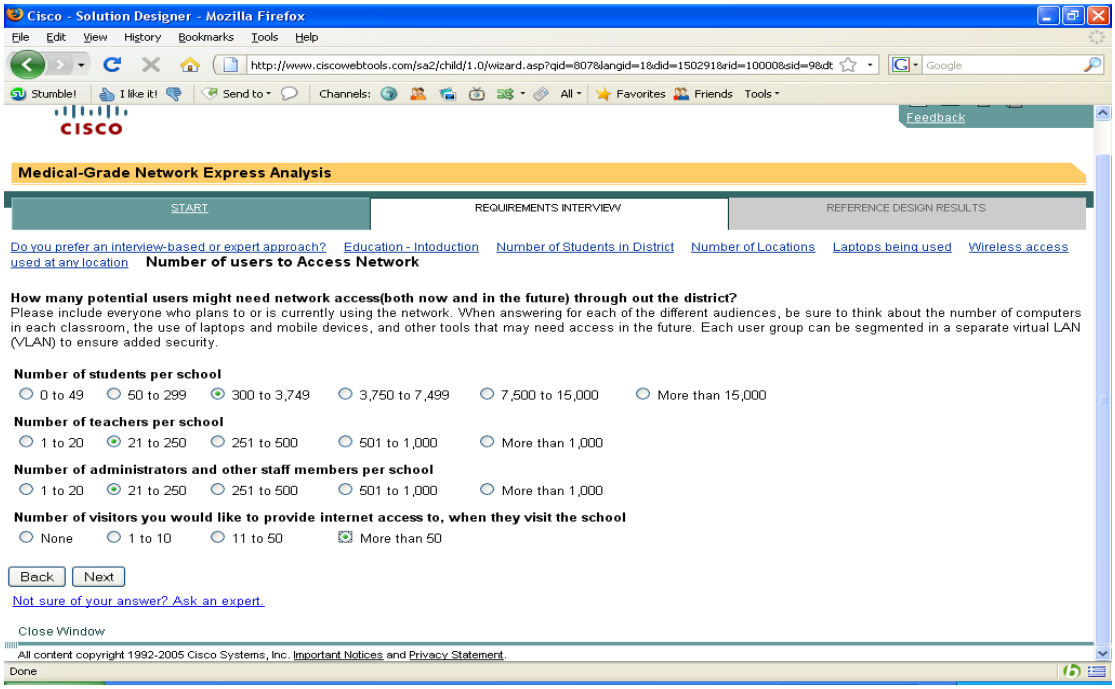
Εικόνα 16: Cisco Designer: Ερώτηση εάν το προσωπικό ,οι μαθητές και το διδακτικό προσωπικό χρησιμοποιούν laptop.

Μετά ρωτάει για πρόσβαση σε wireless από οποιοδήποτε σημείο έβαλα ναι.



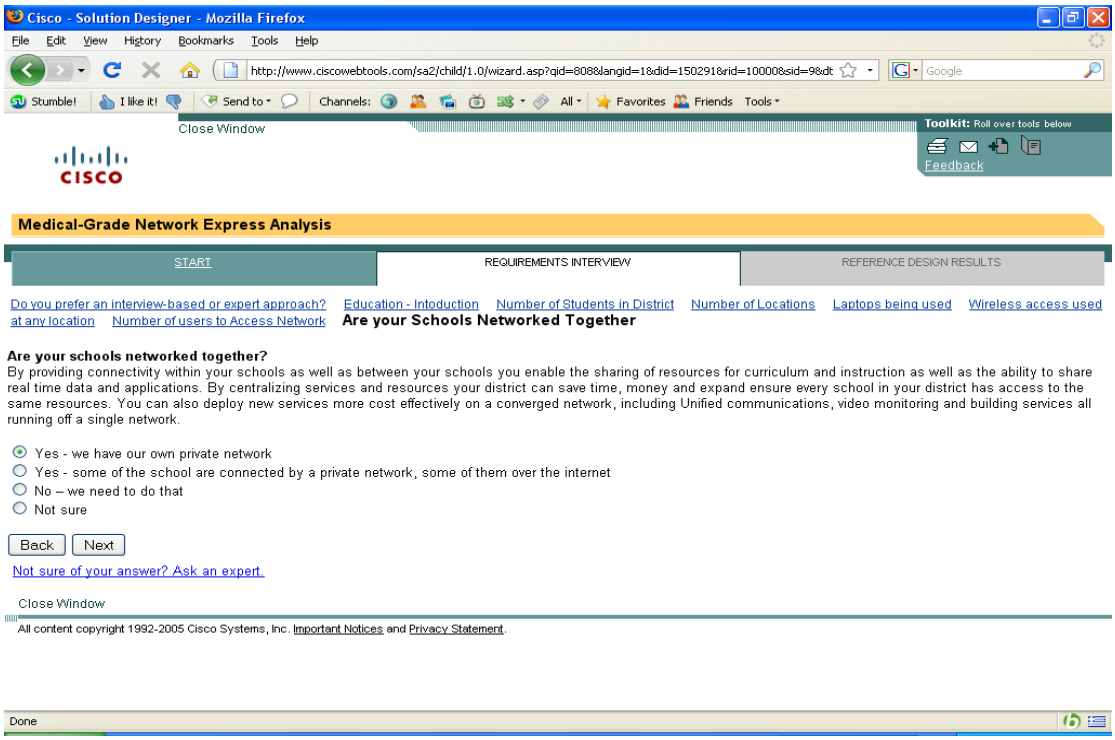
Εικόνα 17: Cisco Designer: Wireless network access positions .

Παρακάτω ρωτάει για μελλοντικούς χρήστες στο δίκτυο του οργανισμού ανά μαθητές, καθηγητές, προσωπικό, επισκέπτες. Επέλεξα τα παρακάτω:



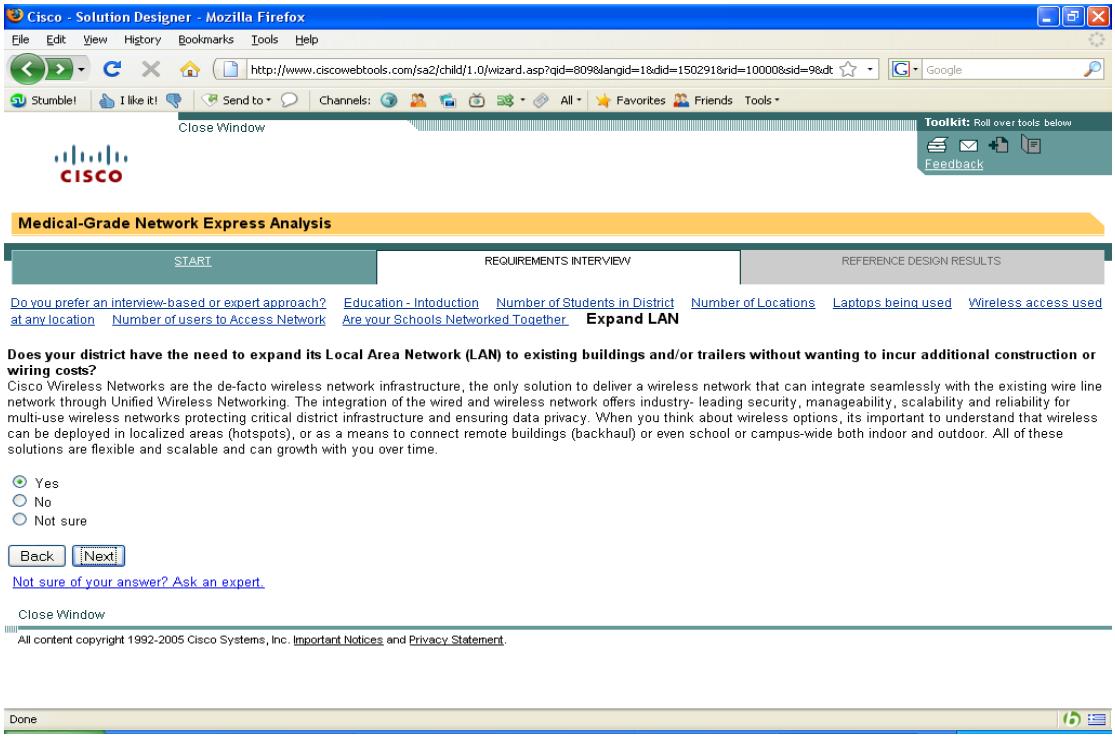
Εικόνα 18: Cisco Designer: Ερώτηση για τον αριθμό μελλοντικών χρηστών στο δίκτυο του οργανισμού

Μετά ρωτάει εάν τα σχολεία είναι συνδεμένα. Απάντησα ναι.



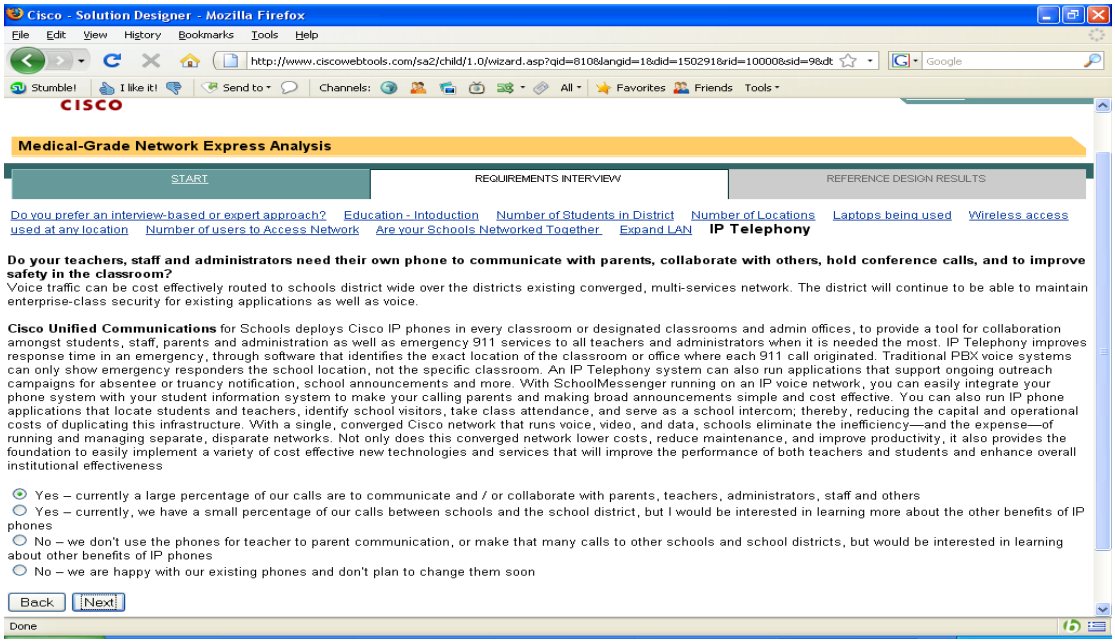
Εικόνα 19: Cisco Designer: Ερώτηση για το εάν τα σχολεία είναι συνδεμένα.

Στην συνέχεια ρώτα εάν θέλουμε επέκταση του δικτύου χωρίς επιπλέον κόστη. Επιλέξαμε ναι.



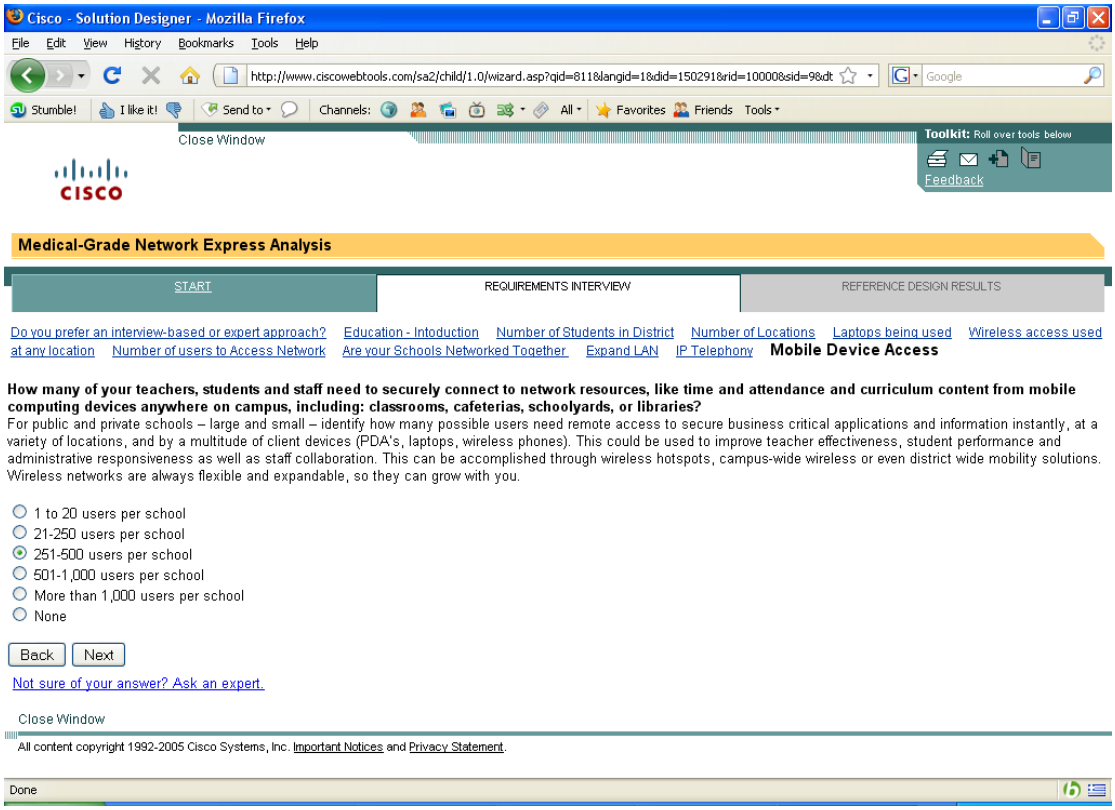
Εικόνα 20: Cisco Designer: Ερώτηση για την επέκταση του δικτύου χωρίς επιπλέον κόστη.

Στην συνέχεια ρωτάει εάν θα χρησιμοποιείται IP telephony από κάθε ένα από το προσωπικό για πάσης φύσεως ανάγκη (εκπαιδευτική, έκτακτη, κτλ). Επιλέξαμε ναι.



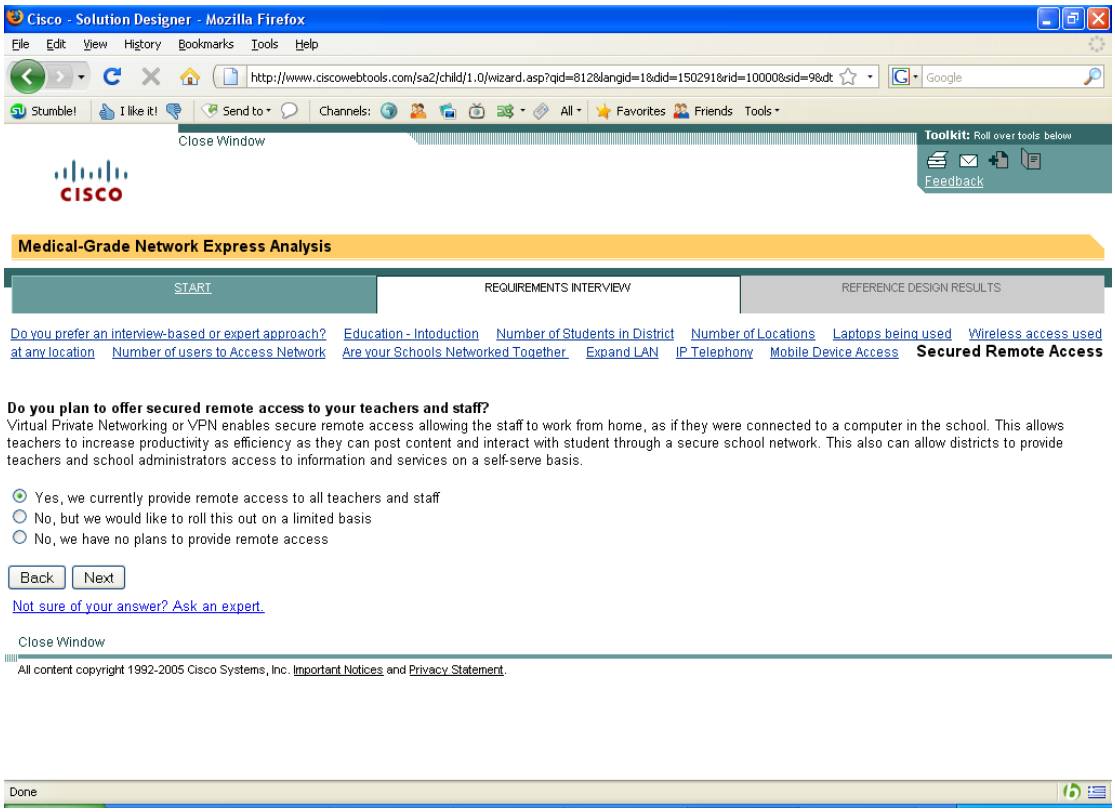
Εικόνα 21: Cisco Designer: IP telephony από κάθε ένα από το προσωπικό για πάσης φύσεως ανάγκη.

Μετά ρωτάει σχετικά με mobile computing devices access από οπουδήποτε στο campus πόσοι user ανά σχολείο.



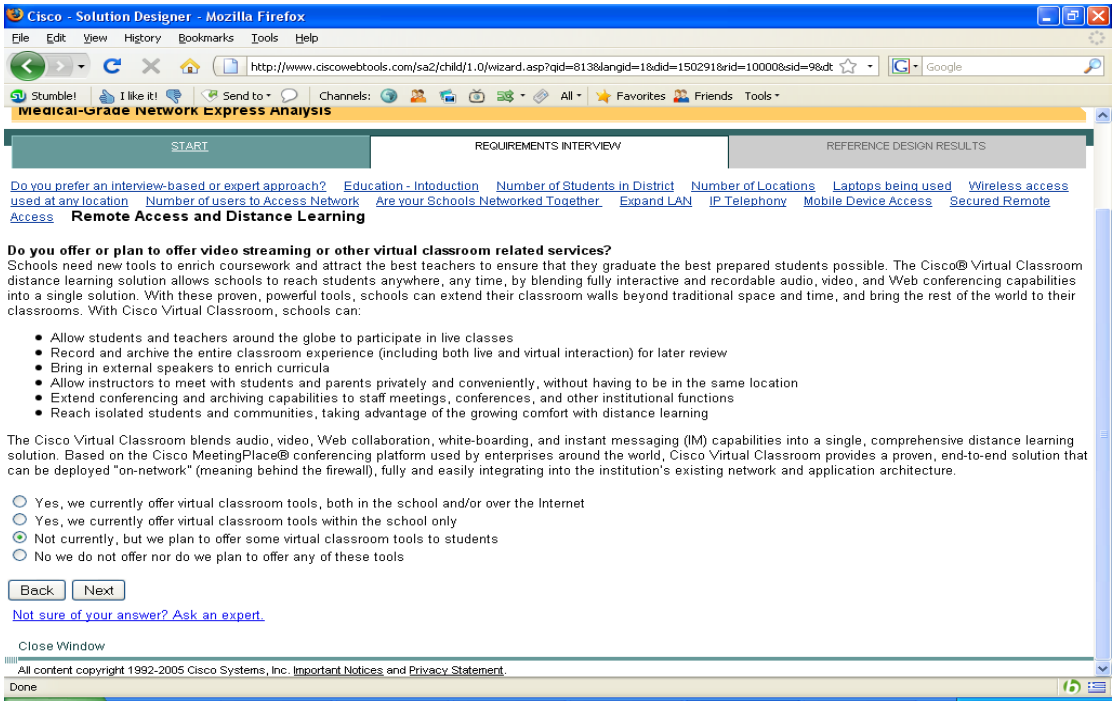
Εικόνα 22: Cisco Designer: Mobile computing devices access από οπουδήποτε στο campus και πόσοι user ανά σχολείο.

Στην συνέχεια ρωτάει για ασφαλή remote access από το προσωπικό.



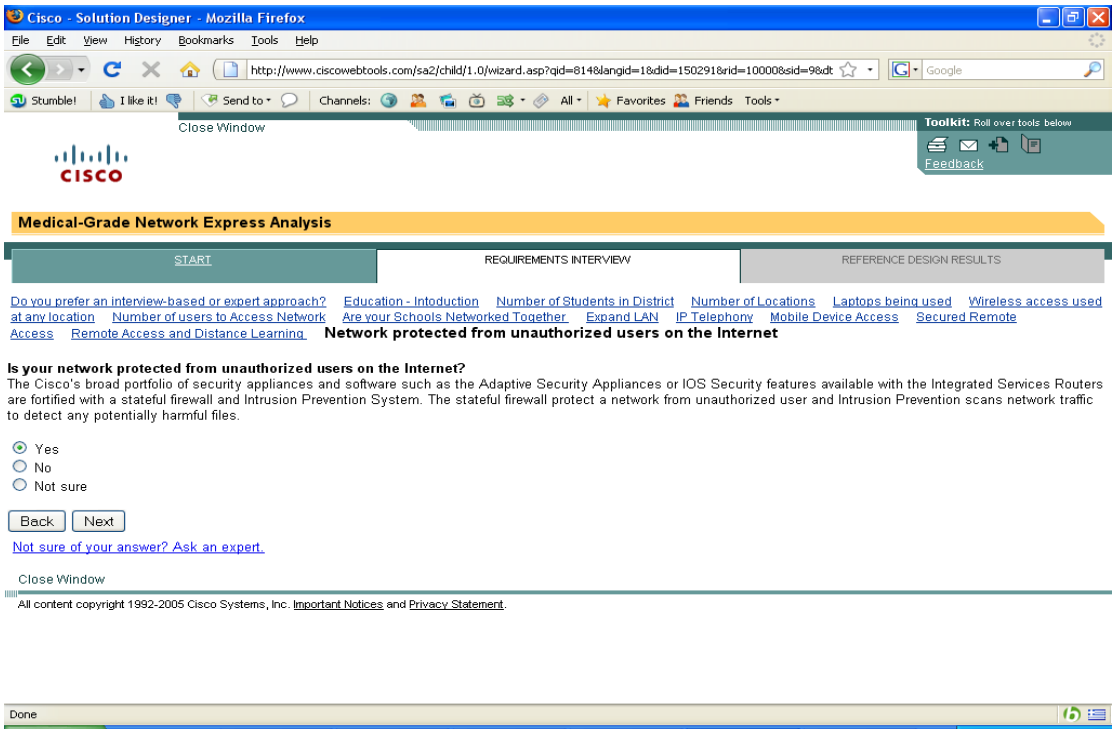
Εικόνα 23: Cisco Designer: Ασφαλή remote access από το προσωπικό.

Μετά ρωτάει εάν θα προσφέρεται υπηρεσία video streaming για εκπαιδευτικούς σκοπούς και έβαλα Not currently, but we plan to offer some virtual classroom tools to students.



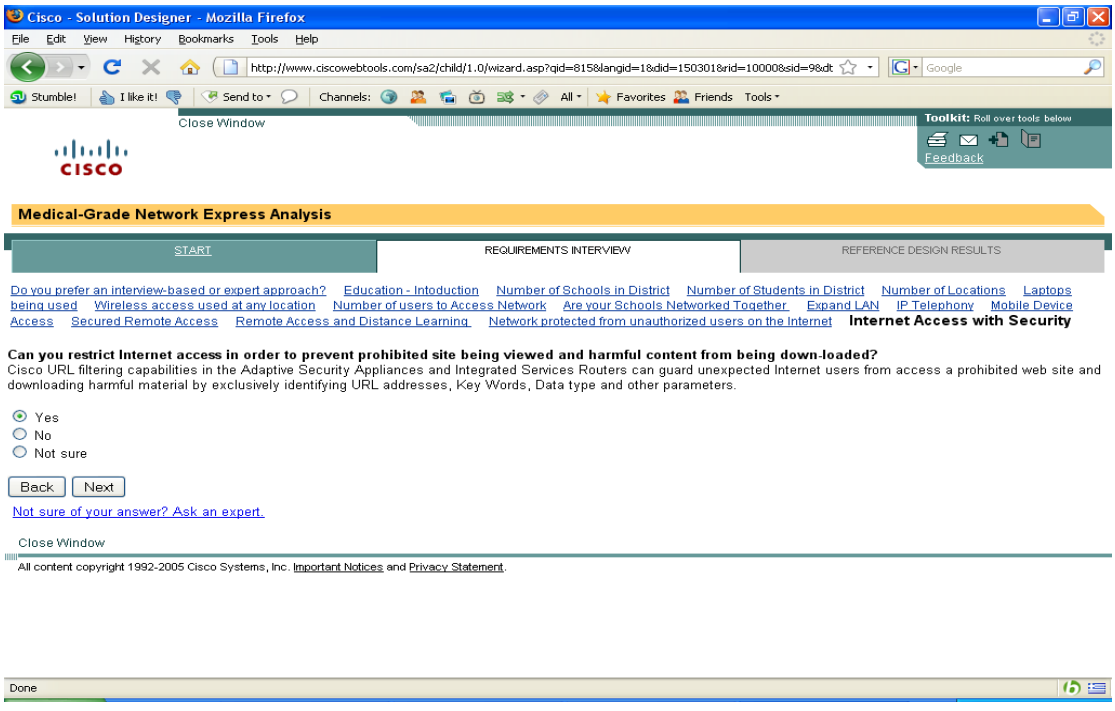
Εικόνα 24: Cisco Designer: Video streaming για εκπαιδευτικούς σκοπούς.

Ρωτάει επίσης εάν υπάρχει προστασία από μη εξουσιοδοτημένους χρηστές. Απαντήσαμε ναι.



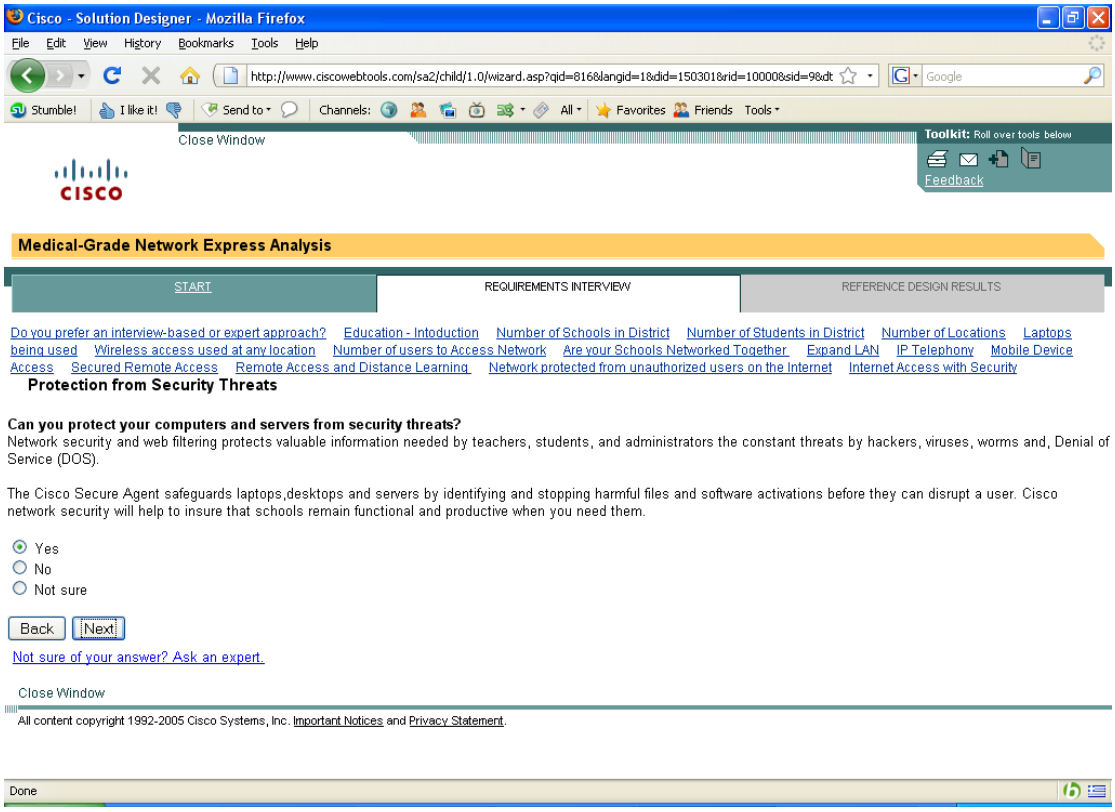
Εικόνα 25: Cisco Designer: Προστασία από μη εξουσιοδοτημένους χρηστές.

Στην συνέχεια ρωτάει εάν θα απαγορεύεται η πρόσβαση στο Internet σε κάποια site ή να αποφευχθεί το κατέβασμα κακοήθους κώδικα. Επιλέγουμε ναι .



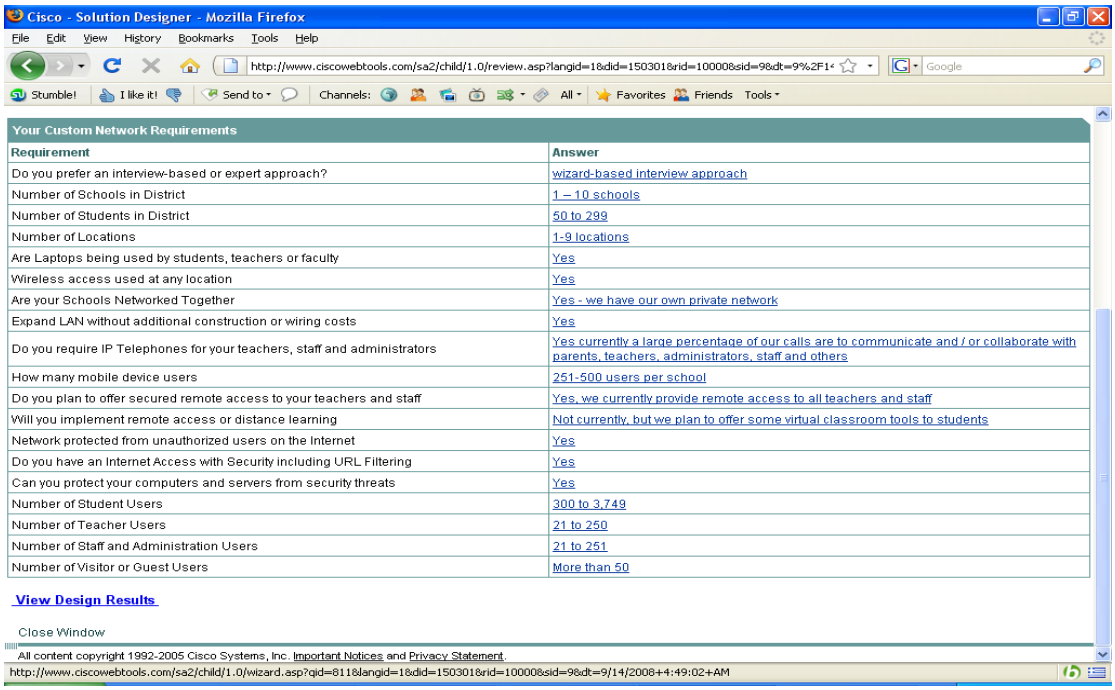
Εικόνα 26: Cisco Designer: Απαγόρευση πρόσβασης στο Internet σε κάποια site ή να αποφυγή κατέβασματος κακοήθους κώδικα.

Η επόμενη ερώτηση είναι εάν μπορούμε να προστατεύσουμε υπολογιστές και servers από απειλές και απαντάμε ναι.



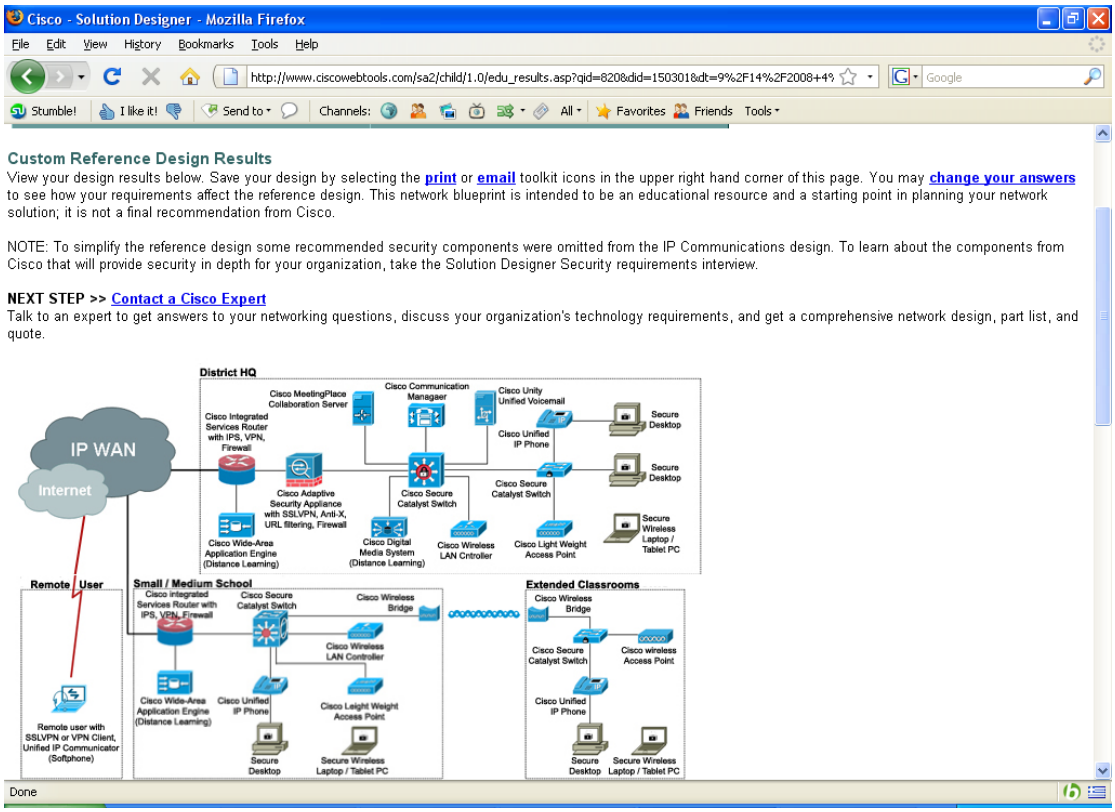
Εικόνα 27: Cisco Designer: Προστασία υπολογιστών και servers από απειλές

Στην συνέχεια μου εμφανίζει όλες τις απαιτήσεις που είχα παραπάνω.

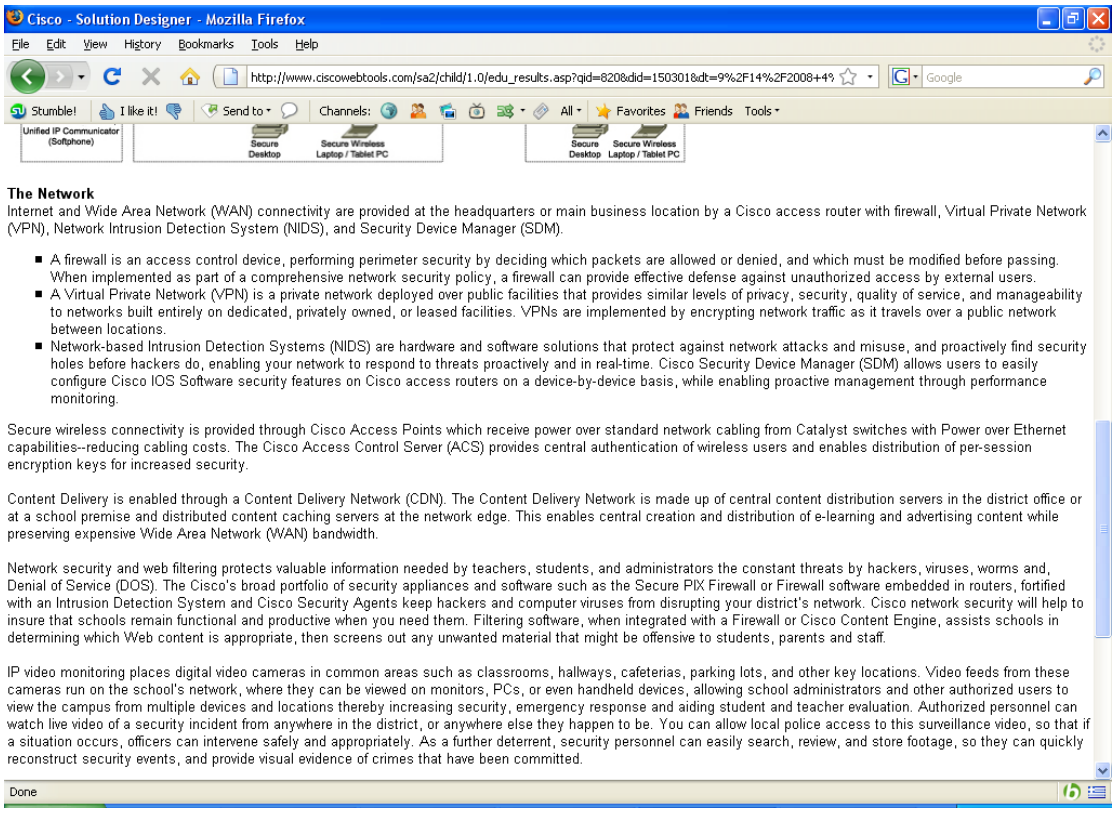


Εικόνα 28: Cisco Designer: Εμφάνιση όλων των απαιτήσεων που θέσαμε παραπάνω.

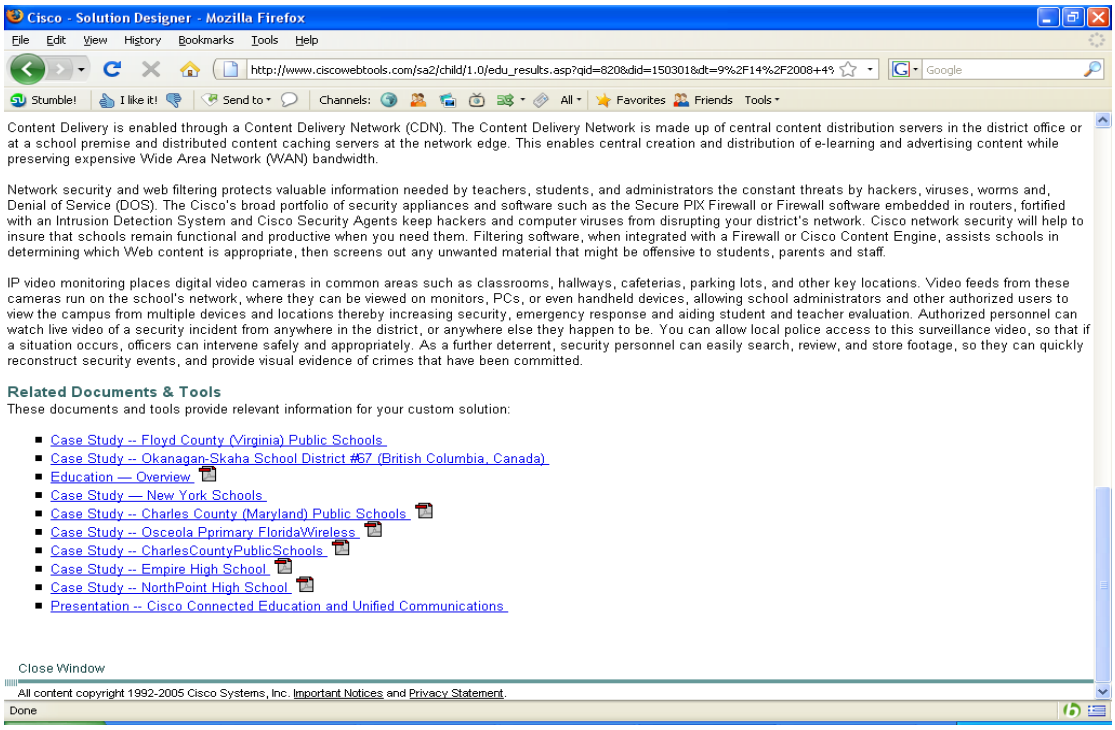
Μετά μου δείχνει τα αποτελέσματα.



Εικόνα 29: Cisco Designer: Solution Diagram.



Εικόνα 30: Cisco Designer: Network Solution.



Εικόνα 31: Cisco Designer: Related Documents & Tools.

Από τα αποτελέσματα του Cisco Security Solution Designer βλέπουμε πως αυτός ο wizard επικεντρώνεται σε πιο πρακτικά ζητήματα ασφαλείας σε ένα οργανισμό. Σχεδιάζει την δομή του δικτύου, επικεντρώνεται σε πιο συγκεκριμένα θέματα του δικτύου και την ασφάλεια τους και προτείνει λύσεις.

Συμπεράσματα

Τα 2 wizard που είδαμε παραπάνω είναι πολύ χρήσιμα εργαλεία για την σχεδίαση πολιτικών ασφάλείας και ασφάλειας δικτύου. Καθώς μέσα από μικρές interviews, σε σύντομο χρόνο μπορεί να έχουμε λύσεις πάνω σε θέματα ασφαλείας. Όμως μπορεί αυτά τα εργαλεία να είναι χρήσιμα δεν είναι όμως και πλήρη.

Συγκεκριμένα:

Το policy που παράχθηκε από το Security Policy Builder της Cisco,επικεντρώνεται σε 8 πτυχές από άποψη ασφάλειας ενός πληροφοριακού συστήματος. Email-communications activities, antivirus, identity, password, encryption, remote access, Virtual Private Network, Extranet policies. Βλέπουμε ότι σε αριθμό δεν έχουμε πολλές πολιτικές λόγω του μεγέθους και των απαιτήσεων του οργανισμού. Έχει πολύ λιγότερα policies σε σχέση με της SANS το Security Policy Project.Αυτά τα policies είναι ίδια με της SANS. Γενικά συμπεραίνουμε ότι είναι κατάλληλο policy για το μέγεθος του οργανισμού που θα εφαρμοστεί.

Ενώ το αποτελέσματα από το Security Solution Designer είναι επαρκή μόνο για οργανισμό μέχρι 1000 και δεν εμβαθύνει σε πολλά θέματα ασφάλειας δικτύου.

Κεφάλαιο 5

Πολιτικές Ασφαλείας Για Το Κέντρο Έλεγχου Και Διαχείρισης Δικτύου Τ.Ε.Ι Κρήτης

Οι πολιτικές με * είναι από την πτυχιακή της Αλεξάκη Ευφροσύνης με τίτλο "Καταγραφή Πολιτικών Ασφάλειας σύμφωνα με το πρότυπο ISO27002". Οι πολιτικές με & είναι στα πλαίσια και της προαναφερθείσας πολιτικής και αυτής εδώ.

5.1 Acceptable Encryption Policy[2]

Σκοπός

Ο σκοπός αυτής της πολιτικής είναι να παράσχει καθοδήγηση για τα όρια χρήσης κρυπτογράφησης από αλγορίθμους που έχουν λάβει την ουσιαστική δημόσια επισκόπηση και έχουν αποδειχθεί ότι είναι αποτελεσματικοί. Επιπλέον, αυτή η πολιτική παρέχει την κατεύθυνση για να εξασφαλίσει ότι οι κανονισμοί ακολουθούνται, και η νομική εξουσία εκχωρείται για τη διάδοση και χρήση των τεχνολογιών κρυπτογράφησης έξω από τις Ηνωμένες Πολιτείες.

Εμβέλεια

Η πολιτική ισχύει για όλους τους υπαλλήλους και συνεργάτες.

Πολιτική

Οι αποδεδειγμένοι, πρότυποι αλγόριθμοι όπως DES, Blowfish, RSA, RC5 και ο IDEA πρέπει να χρησιμοποιηθούν ως βάση για τις τεχνολογίες κρυπτογράφησης. Αυτοί οι αλγόριθμοι αντιπροσωπεύουν το πραγματικό κρυπτογράφημα που χρησιμοποιείται σε μια εγκεκριμένη εφαρμογή. Παράδειγμα , το PGP χρησιμοποιεί έναν συνδυασμό του IDEA και της RSA ή Diffie- Hellman, το SSL χρησιμοποιεί την κρυπτογράφηση RSA. Το κλειδί συμμετρικού κρυπτογραφικού συστήματος πρέπει να είναι τουλάχιστον 56 bit. Τα συμμετρικά κρυπτογραφικά συστήματα πρέπει να είναι ενός μήκους που παράγει την ισοδύναμη δύναμη. Οι απαιτήσεις του μήκους κλειδιού του οργανισμού θα αναθεωρούνται ετησίως και θα αναβαθμίζονται ως εκεί που η τεχνολογία το επιτρέπει. Η χρήση των ιδιόκτητων αλγορίθμων κρυπτογράφησης δεν επιτρέπεται για οποιοδήποτε σκοπό, εκτός αν αναθεωρείται από τους καταρτισμένους εμπειρογνώμονες έξω από τον εν λόγω οργανισμό. Επίσης η εξαγωγή των τεχνολογιών κρυπτογράφησης περιορίζεται από την Αμερικάνικη κυβέρνηση. Κάτοικοι χώρες εκτός Η.Π.Α πρέπει να είναι ενήμεροι για τους νόμους περί τεχνολογιών κρυπτογράφησης στην χώρα που αυτοί κατοικούν.

[2] http://www.sans.org/resources/policies/Acceptable_Encryption_Policy.pdf

Επιβολή

Οποιοσδήποτε υπάλληλος έχει βρεθεί να παραβιάσει την πολιτική αυτή είναι υπαγόμενος σε πειθαρχική ενέργεια συμπεριλαμβανόμενης και της λήξης της απασχόλησης.

5.2 Acceptable Use Policy[3&]

Κανόνες

Οι κανόνες για την αποδεκτή χρήση των πληροφοριών και των περιουσιακών στοιχείων που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών πρέπει να προσδιοριστούν, να τεκμηριωθούν, και να εφαρμοστούν.

Καθοδήγηση Υλοποίησης

Όλοι οι υπάλληλοι, οι ανάδοχοι και οι τρίτοι χρήστες πρέπει να ακολουθήσουν τους κανόνες για την αποδεκτή χρήση των πληροφοριών και των προτερημάτων που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών, που περιλαμβάνουν:

a) Κανόνες για τις χρήσεις ηλεκτρονικού ταχυδρομείου και Διαδικτύου.
b) Οδηγίες για τη χρήση των κινητών συσκευών, ειδικά για τη χρήση έξω από τις εγκαταστάσεις της οργάνωσης.

Οι συγκεκριμένες κανόνες ή οι οδηγίες πρέπει να παρασχεθούν από τη σχετικούς διαχειριστές. Οι υπάλληλοι, οι ανάδοχοι και οι τρίτοι χρήστες χρησιμοποιώντας ή έχοντας την πρόσβαση στα προτερήματα του οργανισμού πρέπει να γνωρίζουν τα όρια που υπάρχουν για τη χρήση τους πληροφοριών και προτερημάτων του οργανισμού που συνδέονται με τις εγκαταστάσεις επεξεργασίας πληροφοριών, και τα στοιχεία συμπεριφοράς. Πρέπει να είναι αρμόδιοι για τη χρήση οποιωνδήποτε πηγών επεξεργασίας πληροφοριών, και οποιασδήποτε χρήσης τους που πραγματοποιείται κάτω από την ευθύνη τους έξω από τον οργανισμό.

[3] Από το έγγραφο του ISO 27002

5.3 Analog/ISDN Line Security Policy[4]

Σκοπός

Το παρόν έγγραφο εξηγεί για τις αναλογικές και γραμμές ISDN αποδεκτές χρήσεις και πολιτικές και διαδικασίες έγκρισης. Αυτή η πολιτική καλύπτει δύο ευδιάκριτες χρήσεις των γραμμών αναλογικών /ISDN: γραμμές που πρόκειται να συνδεθούν μόνο για την χρήση fax, και γραμμές που πρόκειται να συνδεθούν με τους υπολογιστές.

Εμβέλεια

Αυτή η πολιτική καλύπτει μόνο εκείνες τις γραμμές που πρόκειται να συνδεθούν με ένα εσωτερικό σημείου κτιρίου του οργανισμού και περιοχές δοκιμής. Δεν αναφέρεται στις γραμμές ISDN/ αναλογικές που συνδέονται με τα σπίτια υπαλλήλων, τα τηλέφωνα υπολογιστών γραφείου P.B.X (private branch exchange), και εκείνες τις γραμμές που χρησιμοποιούνται από τον πάροχο για την έκτακτη ανάγκη και τους μη-εταιρικούς λόγους πληροφόρησης.

Πολιτική

<u>Σενάρια και Επιπτώσεις</u>

Υπάρχουν δύο σημαντικά σενάρια που περιλαμβάνουν την κατάχρηση αναλογικών γραμμών, ενάντια στην οποία προσπαθούμε να προφυλαχθούμε μέσω αυτής της πολιτικής. Το πρώτο είναι ένας εισβολέας που καλεί ένα σύνολο αναλογικών αριθμών γραμμών με την ελπίδα της σύνδεσης με έναν υπολογιστή που έχει συνδεμένο ένα modem. Εάν το modem απαντήσει (και οι περισσότεροι υπολογιστές έχουν σήμερα διαμορφωμένη αυτόματη-απάντηση) από μέσα από τις εγκαταστάσεις του οργανισμού, κατόπιν υπάρχει η δυνατότητα παραβίασης του εσωτερικού δικτύου μέσω εκείνου του υπολογιστή, χωρίς ίχνη. Η ελάχιστη ζημία, είναι οι πληροφορίες που φυλάσσονται σε εκείνο τον υπολογιστή να αποκαλυφθούν. Αυτό οδηγεί ενδεχομένως στην απώλεια μεγάλων χρηματικών ποσών λόγω των εταιρικών πληροφοριών.

Το δεύτερο σενάριο είναι η απειλή από οποιοδήποτε έχει φυσική σε εγκαταστάσεις του οργανισμού και όντας σε θέση να χρησιμοποιήσει ένα laptop εξοπλισμένο με modem ή έναν υπολογιστή γραφείου. Σε αυτήν την περίπτωση, ο εισβολέας θα είναι σε θέση να συνδεθεί με εμπιστευμένο δίκτυο μέσω της σύνδεσης Ethernet του Η/Υ, και να συνδεθεί έπειτα σε ένα μη επιτηρούμενο site χρησιμοποιώντας το modem, με τη δυνατότητα να διοχετεύσει πληροφορίες του οργανισμού σε μια άγνωστη θέση. Αυτό θα μπορούσε ενδεχομένως να οδηγήσει στη σημαντική απώλεια ζωτικής σημασίας πληροφοριών.
Συγκεκριμένες διαδικασίες για την αποφυγή κινδύνων ασφάλειας έμφυτους σε κάθε ένα από αυτά τα σενάρια ακολουθούν.

[4] http://www.sans.org/resources/policies/Analog_Line_Policy.pdf

Μηχανές Τηλε-ομοιότυπου

Σαν κανόνας, τα παρακάτω εφαρμόζονται σε περίπτωση αιτήματος για fax και αναλογικής τηλεφωνικής γραμμής:

- Οι γραμμές fax πρέπει να χρησιμοποιούνται μόνο για υπηρεσιακή χρήση.
- Κανένα fax δεν θα εγκαθίσταται για προσωπική χρήση.
- Καμία τηλεφωνική σύνδεση δεν θα εγκαθίσταται σε προσωπικό δωμάτιο.
- Η μηχανή fax πρέπει να τοποθετηθεί σε μια κεντρική διοικητική περιοχή που έχει σχεδιαστεί για υπηρεσιακή χρήση, και μακριά από άλλο εξοπλισμό Η/Υ.
- Ένας υπολογιστής που είναι σε θέση να δημιουργήσει σύνδεση fax απαγορεύεται να χρησιμοποιήσει μια αναλογική γραμμή για αυτόν το λόγο.

Αποποιούνται των παραπάνω κανόνων για αναλογικές γραμμές σε χρήση fax όσοι μετά από ανασκόπηση του αιτήματος, βάση της επιχειρησιακής ανάγκης εκτιμώντας το επίπεδο ευαισθησίας και ασφαλείας της στάσης του αιτήματος.

Η χρήση μιας γραμμής αναλογικής/ ISDN fax εξαρτάται από την πλήρη συμμόρφωση του αιτούμενου με τις απαιτήσεις που εμφανίζονται λίστα παρακάτω. Αυτές οι απαιτήσεις είναι ευθύνη του εξουσιοδοτημένου χρήστη να τις επιβάλει πάντα:

- Η γραμμή fax χρησιμοποιείται όπως προσδιορίζεται στο αίτημα.
- Μόνο εξουσιοδοτημένα άτομα να χρησιμοποιήσουν τη γραμμή έχουν πρόσβαση σε αυτήν.
- Όταν δεν είναι σε χρήση, η γραμμή πρέπει να αποσυνδεθεί από τον υπολογιστή.
- Όταν είναι χρήση η γραμμή , ο υπολογιστής πρέπει να αποσυνδεθεί από το εσωτερικό δίκτυο.
- Η γραμμή θα χρησιμοποιηθεί απλώς για επιχειρησιακούς λόγους, και όχι για προσωπικούς λόγους.
- Ότι υλικό έχει κατέβει από το Διαδίκτυο, και εισάγεται στα συστήματα και τα δίκτυα του οργανισμού πρέπει να εξετάζεται από εγκεκριμένο anti-virus πρόγραμμα που πρέπει να κάνει τις τακτικές αναβαθμίσεις.

Σύνδεση Η/Υ σε αναλογική γραμμή

Γενική πολιτική είναι ότι τα αιτήματα για τους υπολογιστές ή άλλες ευφυείς συσκευές που συνδέονται με γραμμές αναλογικές ή ISDN από μέσα από τον οργανισμό δεν θα εγκριθούν για λόγους ασφάλειας. Οι αναλογικές και ISDN γραμμές αντιπροσωπεύουν μια σημαντική απειλή ασφάλειας, και οι ενεργές διεισδύσεις έχουν προωθηθεί μέσα από τέτοιες γραμμές από hacker. Αποποίηση στην παραπάνω πολιτική θα χορηγείται σε περίπτωση ανά περίπτωση βάση. Οι γραμμές αντικατάστασης, όπως λόγω μετακίνησης, εκπίπτουν στην κατηγορία νέες γραμμές. Θα εξεταστούν επίσης σε περίπτωση ανά περίπτωση βάση.

<u>Αίτηση για Αναλογική/ISDN γραμμή</u>

Αφού έχει εγκριθεί από τον διαχειριστή, το άτομο που ζητά μια αναλογική /γραμμή ISDN πρέπει να παρέχει τις ακόλουθες πληροφορίες στον τηλεπικοινωνιακό φορέα:

- Μια λεπτομερής επιχειρησιακή αναφορά γιατί άλλες διαθέσιμες ασφαλείς συνδέσεις δεν μπορούν να χρησιμοποιηθούν.
- Ο επιχειρησιακός σκοπός για τον οποίο η αναλογική γραμμή πρόκειται να χρησιμοποιηθεί.
- Το λογισμικό και το υλικό που συνδέονται με τη γραμμή και που χρησιμοποιούνται από τη γραμμή.
- Ποιες εξωτερικές συνδέσεις ο αιτούμενος επιθυμεί να έχει πρόσβαση.

Η επιχειρησιακή αναφορά πρέπει να απαντά σε κάποια από τα παρακάτω ερωτήματα:

- Ποιες επιχειρησιακές ανάγκες θα διεξάγονται μέσω αυτής της γραμμής;
- Γιατί ένας υπολογιστής με δυνατότητα σύνδεσης στο Internet του είναι ανίκανος να εκπληρώσει τις ίδιες εργασίες με μία αναλογική γραμμή;
- Γιατί η υπάρχουσες προσβάσεις για συνδιαλέξεις είναι ανίκανες να εκπληρώσουν τις εργασίες μίας αναλογικής γραμμής;

Επιπλέον, ο αιτών πρέπει να προετοιμαστεί να απαντήσει στις ακόλουθες συμπληρωματικές ερωτήσεις σχετικές με το σχεδιάγραμμα ασφάλειας του αιτήματος:

- Οι μηχανές που χρησιμοποιούν τις αναλογικές γραμμές είναι φυσικά αποσυνδεμένες από το εσωτερικό δίκτυο;
- Πού θα τοποθετηθεί η αναλογική γραμμή; Σε γραφείο ή ένα εργαστήριο;
- Απαιτείται συνδιάλεξη από έξω προς το οργανισμό;
- Πόσες γραμμές ζητούνται, και πόσοι άνθρωποι θα χρησιμοποιήσουν τη γραμμή;
- Πόσο συχνά η γραμμή θα χρησιμοποιηθεί; Μία φορά την εβδομάδα, 2 ώρες ανά ημέρα...;
- Ποία είναι η πιο πρόωρη ημερομηνία η γραμμή μπορεί να τερματιστεί από την υπηρεσία;
- Η γραμμή πρέπει να τερματιστεί όταν δεν είναι πλέον σε χρήση.
- Ποια άλλα μέσα θα χρησιμοποιηθούν για να εξασφαλίσουν τη γραμμή από την μη εξουσιοδοτημένη χρήση;
- Είναι αυτή μια γραμμή αντικατάστασης από μια παλαιά θέση; Ποιος ήταν ο σκοπός της αρχικής γραμμής;
- Ποίοι τύποι πρωτοκόλλων θα υποστηρίζονται από τη γραμμή;
- Θα εγκατασταθεί ένα εγκεκριμένο anti-virus από το <όνομα οργανισμού> στα μηχανήματα που χρησιμοποιούν αναλογική γραμμή;

Ο αιτών πρέπει να χρησιμοποιήσει το έντυπο αιτήματος αναλογικών /γραμμών ISDN για να αντιμετωπίσει αυτά τα ζητήματα και να υποβάλει ένα αίτημα.

Εφαρμογή

Οποιοσδήποτε υπάλληλος που βρέθηκε για να έχει παραβιάσει αυτήν την πολιτική μπορεί να του επιβληθεί πειθαρχική ενέργεια, και συμπεριλαμβανομένης και τη λήξη της απασχόλησης.

5.4 Anti-Virus Process[5]*

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.

Εμβέλεια

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 άγνωστο, 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.

[5] http://www.sans.org/resources/policies/Anti-virus_Guidelines.pdf

- 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.

5.5 Backup Policy[6]

Σκοπός

Για να διατηρηθεί η ακεραιότητα και η διαθεσιμότητα των πληροφοριών και των εγκαταστάσεων επεξεργασίας πληροφοριών. Τακτικές διαδικασίες πρέπει να καθιερωθούν για να εφαρμόσουν τη συμφωνηθείσα backup πολιτική και στρατηγική για την δημιουργία εφεδρικών αντιγράφων των δεδομένων και την έγκαιρη αποκατάστασή τους.

Έλεγχος

Τα εφεδρικά αντίγραφα πληροφοριών και λογισμικού πρέπει να δημιουργούνται και να εξετάζονται τακτικά σύμφωνα με τη πολιτική για backup.

Οδηγίες Υλοποίησης

Επαρκείς εφεδρικές εγκαταστάσεις πρέπει να παρασχεθούν για να εξασφαλίσουν ότι όλες οι πληροφορίες και το λογισμικό μπορούν να ανακτηθούν μετά από μια καταστροφή ή μια αποτυχία ενός μέσου αποθήκευσης.

Τα παρακάτω στοιχεία πρέπει να ληφθούν υπόψη για την δημιουργία των εφεδρικών πληροφοριών:

1) Πρέπει να καθοριστεί το απαραίτητο επίπεδο των εφεδρικών πληροφοριών.
2) Ακριβή και πλήρη πρακτικά των εφεδρικών αντιγράφων και των γραπτών διαδικασιών αποκατάστασης πρέπει να παραχθούν.
3) Η έκταση και η συχνότητα δημιουργίας των αντιγράφων ασφαλείας πρέπει να αντικατοπτρίζει τις επιχειρησιακές ανάγκες του οργανισμού, τις απαιτήσεις ασφαλείας των πληροφοριών που θα γίνουν αντίγραφα, και την κρισιμότητα των πληροφοριών αυτών.
4) Τα αντίγραφα πρέπει να αποθηκευτούν σε μια απομακρυσμένη θέση, σε ικανοποιητική απόσταση για να αποφύγουν οποιαδήποτε ζημία από μια καταστροφή επί της κύριας τοποθεσίας του οργανισμού.
5) Στα αντίγραφα ασφαλείας πρέπει να υπάρχει το απαιτούμενο επίπεδο φυσικής και περιβαλλοντικής ασφαλείας σύμφωνα με τα πρότυπα της κύριας τοποθεσίας του οργανισμού. Ο έλεγχος που υπάρχει στα μέσα στην κύρια τοποθεσία πρέπει να επεκταθεί στο χώρο των αντιγράφων ασφαλείας.
6) Τα αντίγραφα ασφαλείας πρέπει να ελέγχονται συχνά ώστε να μπορούμε να βασιστούμε σε αυτά σε κάποια έκτακτη ανάγκη.
7) Οι διαδικασίες ανάκτησης πρέπει να ελέγχονται συχνά για να διασφαλίσουμε την αποτελεσματικότητα τους και να ολοκληρώνονται σε χρόνο που απαιτείται από τις λειτουργικές διαδικασίες για ανάκτηση.
8) Σε περιπτώσεις που χρειαζόμαστε εμπιστευτικότητα, τα αντίγραφα ασφαλείας θα προστατεύονται με κρυπτογραφικά μέσα.

Οι διακανονισμοί για αντίγραφα ασφαλείας για μεμονωμένα συστήματα πρέπει να εξετάζονται τακτικά για να εξασφαλίσουν ότι καλύπτουν τις απαιτήσεις των

[6] Από το έγγραφο του ISO 27002

σχεδίων επιχειρησιακής συνοχής. Για ζωτικής σημασίας συστήματα οι διακανονισμοί για αντίγραφα ασφαλείας πρέπει να καλύπτουν τις πληροφορίες, εφαρμογές και δεδομένα των συστημάτων αυτών ώστε να γίνει πλήρη ανάκτηση τους σε περίπτωση κάποιας καταστροφής.

Η περίοδος διατήρησης για τις απαραίτητες επιχειρησιακές πληροφορίες, και επίσης οποιαδήποτε απαίτηση για αρχείο αντιγράφων που διατηρούνται μόνιμα πρέπει να καθοριστούν.

Άλλες πληροφορίες

Οι διακανονισμοί για αντίγραφα ασφαλείας μπορούν να αυτοματοποιηθούν για διευκόλυνση των διαδικασιών αντιγραφής και ανάκτησης.

5.6 Certification and Accreditation Policy[7]

Πολιτική

Αυτή η πολιτική καθορίζει τις απαιτήσεις για τη διαβεβαίωση μέσω της υιοθέτησης ενός καθορισμένου με σαφήνεια μοντέλου κύκλου της ζωής για όλα τα βήματα της ανάπτυξης, συμπεριλαμβανομένων των διαδικασιών και των πολιτικών επανόρθωσης αδυναμιών, της σωστής χρήσης των εργαλείων, των τεχνικών, των διαδικασιών, και των μέτρων βασικών γραμμών ασφάλειας που χρησιμοποιούνται για να προστατεύσουν το περιβάλλον ανάπτυξης. Παρατείνει ευθύνες για να εξασφαλιστεί ότι η ευαίσθητη εφαρμογή επεξεργασίας πληροφοριών και τα γενικά συστήματα υποστήριξης καλύπτουν τις απαιτήσεις ασφάλειας και συμμορφώνονται με τους νόμους και τις οδηγίες για την ασφάλεια συστημάτων πληροφοριών.

Η διαδικασία κύκλου ζωής πιστοποίησης και διαπίστευσης χρησιμεύει για να εξασφαλιστεί ότι οι λειτουργίες ασφάλειας ενός αναπτυγμένου συστήματος ικανοποιούν τις ανάγκες ότι για το σύστημα και οι πληροφορίες του, και ότι αποφάσεις εφαρμογής γίνονται με την πλήρη εκτίμηση των παραγόντων ασφάλειας. Ο όρος σύστημα θα χρησιμοποιηθεί σε όλη αυτήν την πολιτική για να αναφερθεί σε οποιαδήποτε γενικό σύστημα υποστήριξης ή ευαίσθητη εφαρμογή επεξεργασίας πληροφοριών που αναπτύσσεται για τη λειτουργία μέσα σε ένα οργανισμό. Αυτή η έννοια ισχύει εάν το σύστημα είναι ένα πλήρες σύστημα υπολογιστών και επικοινωνιών με το υλικό του ή είναι μια νέα εφαρμογή που οργανώνεται σε μια υπάρχουσα πλατφόρμα.

Εμβέλεια

<u>Διαπίστευση</u>

Η διαπίστευση είναι η επίσημη διοικητική έγκριση για να ενεργοποιηθεί ένα σύστημα. Μια διαπίστευση χορηγεί κανονικά την έγκριση για ένα σύστημα για να λειτουργήσει για μια συγκεκριμένη χρονική περίοδο, καθορισμένου περιβάλλοντος, και με τα καθορισμένα μέτρα ασφάλειας και άλλους κατάλληλους περιορισμούς.
Ο διαπιστευτής αποδέχεται τυπικά την ευθύνη ασφάλειας για το σύστημα και δηλώνει ότι οι μηχανισμοί προστασίας ενάντια σε καταστροφή, ή την αναρμόδια τροποποίηση είναι επαρκείς. Δεδομένου ότι κανένα σύστημα πληροφοριών δεν είναι πάντα συνολικά ασφαλές, η πιστοποίηση τεκμηριώνει την κρίση του διαπιστευτής ότι τα οφέλη για το σύστημα αξίζουν τους υπόλοιπους κινδύνους που περιλαμβάνονται. Ανώτερο στέλεχος (κάτοχος δεδομένων) θα λάβει την παρούσα απόφαση διαπίστευσης.

<u>Πιστοποίηση</u>

Η πιστοποίηση είναι η περιεκτική ανάλυση των πτυχών ασφάλειας του συστήματος για να καθιερώσει το βαθμό στον οποίο το σύστημα καλύπτει τις απαιτήσεις

[7] http://www.tess-llc.com/Certification%20&%20Accreditation%20PolicyV4.pdf

ασφάλειάς του. Είναι μια αξιολόγηση του κινδύνου εφαρμογής που παράγει μια τεχνική άποψη και ενισχυτικές πληροφορίες. Ο διαπιστευτής στη λήψη της απόφασης χρησιμοποιεί την προκύπτουσα τεκμηρίωση. Για να κάνει μια τέτοια κρίση, Ο διαπιστευτής χρειάζεται τις αξιόπιστες πληροφορίες για το σύστημα. Αυτές οι πληροφορίες περιλαμβάνουν τις πιθανές απειλές ή τους τρόπους που το σύστημα μπορεί να χρησιμοποιηθεί κατ' άσχημο τρόπο, οι συγκεκριμένοι τομείς του συστήματος ή στοιχεία, οι οποίες χρειάζονται την προστασία, οι μηχανισμοί που χρησιμοποιούνται για να παρέχουν την προστασία, και πόσο καλά εκείνοι οι μηχανισμοί λειτουργούν. Αυτό είναι το σημείο της πιστοποίησης.

Αξιολόγηση και δοκιμή ευπάθειας

Μία ομάδα θα εκτελέσει και τις δοκιμές μονάδων και τις δοκιμές αποδοχής, και θα πιστοποιήσει ότι οι έλεγχοι ασφάλειας είναι επαρκείς για τις ανάγκες ασφάλειας.

1. Τα στοιχεία της δοκιμής κάλυψης θα εμφανίσουν την αντιστοιχία μεταξύ των δοκιμών που προσδιορίζονται στην τεκμηρίωση δοκιμής και του δικτύου όπως περιγράφεται στη λειτουργικό προσδιορισμό.
2. Η κάλυψη δοκιμής αυστηρά θα καταδείξει ότι όλα τα interface του δικτύου που προσδιορίζεται στη λειτουργική προδιαγραφή έχουν εξεταστεί εντελώς.
3. Η σε βάθος ανάλυση θα καταδείξει ότι οι δοκιμές που προσδιορίζονται στην τεκμηρίωση δοκιμής είναι επαρκείς για να καταδείξουν ότι το δίκτυο λειτουργεί σύμφωνα με το ευαίσθητο υψηλού επιπέδου και του χαμηλού επιπέδου σχέδιο του.
4. Τα σχέδια δοκιμής θα προσδιορίσουν τις λειτουργίες ασφάλειας που εξετάζονται και θα περιγράψουν το στόχο των δοκιμών που εκτελούνται.
5. Ο υπεύθυνος για την ανάπτυξη θα εξετάσει και θα τεκμηριώσει ότι μια συστηματική μέθοδος χρησιμοποιήθηκε για να προσδιορίσει τα συγκεκαλυμμένα κανάλια για κάθε πολιτική ελέγχου ροής πληροφοριών.
6. Η δοκιμή θα προσδιορίσει τους διακριτικούς τρόπους λειτουργίας του δικτύου (συμπεριλαμβανομένης της λειτουργίας μετά από την αποτυχία ή το λειτουργικό σφάλμα), των συνεπειών και των επιπτώσεών τους στη διατήρηση της ευαίσθητης λειτουργίας.
7. Μια ποσοτική ή στατιστική ανάλυση της συμπεριφοράς ασφάλειας θα προσδιορίσει οποιαδήποτε ευπάθεια που θα μπορούσε να παρακάμψει, να απενεργοποιήσει, ή να αλλοιώσει μια λειτουργία ή έναν μηχανισμό
8. Μια δοκιμή διείσδυσης, βασισμένη στην ανάλυση ευπάθειας, θα καθορίσει την ικανότητα επιτυχίας των πρόσθετων προσδιορισμένων ευπαθειών στο προοριζόμενο περιβάλλον.

* Περισσότερα στο:
http://www.tess-llc.com/Certification%20&%20Accreditation%20PolicyV4.pdf

5.7 Dial-In Access Policy[8]

Σκοπός

Ο σκοπός της πολιτικής αυτής είναι να προστατεύσει τις ηλεκτρονικές πληροφορίες του οργανισμού εάν εκτεθούν ακούσια από εξουσιοδοτημένα άτομα που χρησιμοποιούν dial-in συνδέσεις.

Εμβέλεια

Ορισμός της σωστής dial-in πρόσβασης και χρήσης από εξουσιοδοτημένα άτομα.

Πολιτική

Οι υπάλληλοι και εξουσιοδοτημένες ομάδες τρίτων μπορούν να χρησιμοποιούν dial-in συνδέσεις για να αποκτούν πρόσβαση στο δίκτυο του οργανισμού. Οι dial-in συνδέσεις πρέπει να είναι αυστηρά ελεγχόμενες και με κωδικό μίας χρήσης για πιστοποίηση.

Είναι ευθύνη των υπαλλήλων με δικαιώματα εισερχόμενης πρόσβασης να διασφαλίσουν ότι αυτή η εισερχόμενη σύνδεση δεν θα χρησιμοποιείται από άτομα εκτός οργανισμού για αποκτήσουν πρόσβαση σε πόρους πληροφοριών συστήματος αυτού.

Ένας υπάλληλος με προνόμια εισερχόμενης πρόσβασης πρέπει να έχει επίγνωση ότι η σύνδεση μεταξύ της τοποθεσίας του και του οργανισμού είναι κυριολεκτικά προέκταση του δικτύου του οργανισμού και παρέχει δυνητικό μονοπάτι σε ευαίσθητες πληροφορίες του οργανισμού. Οι υπάλληλοι ή άτομα εξουσιοδοτημένων ομάδων τρίτων πρέπει να πάρουν όλα τα απαραίτητα μέτρα για την προστασία της περιουσίας του οργανισμού.

Αναλογικές και μη G.S.M ψηφιακές κινητές συσκευές δεν πρέπει να χρησιμοποιούνται για να συνδεθούν στο δίκτυο του οργανισμού καθώς το σήμα τους μπορεί εύκολα να ανιχνευτεί ή και να καταληφθεί από μη εξουσιοδοτημένα άτομα. Μόνο G.S.M ψηφιακές κινητές συσκευές κρίνονται ασφαλής για σύνδεση με το δίκτυο του οργανισμού.*

Σημείωση: Εισερχόμενων προσβάσεων λογαριασμοί κρίνονται σαν αναγκαίοι. Η δραστηριότητα τους παρακολουθείται και εάν ένας τέτοιος λογαριασμός δεν χρησιμοποιείται για περίοδο 6 μηνών θα λήγει και δεν θα λειτουργεί πλέον. Εάν στην συνέχεια απαιτηθεί η πρόσβαση αυτή, το άτομο που την ζητά πρέπει να αιτηθεί μια καινούρια.

[8] http://www.sans.org/resources/policies/Dial-in_Access_Policy.pdf

Επιβολή

Οποιοσδήποτε υπάλληλος έχει βρεθεί να παραβιάσει την πολιτική αυτή είναι υπαγόμενος σε πειθαρχική ενέργεια συμπεριλαμβανόμενης και της λήξης της απασχόλησης.

5.8 Disaster Recovery Policy[9]

Σκοπός

Το σχέδιο έκτακτης ανάγκης εξετάζει τα μέτρα που λαμβάνονται για να διατηρήσουν τις κρίσιμες λειτουργίες σε περίπτωση απωλειών, τις δυσλειτουργιών, ή καταστροφών που επηρεάζουν τα συστήματα πληροφοριών. Κατά ανάπτυξη των απαιτήσεων για ένα σχέδιο έκτακτης ανάγκης, πρόνοια για το περιοδικό backup των δεδομένων, διαθεσιμότητα των κρίσιμων εγκαταστάσεων από κοινού με τις συγκεντρωμένες λειτουργίες του τηλεφωνικού παρόχου, και την καταστροφή διαδικασίες αποκατάστασης θα ληφθούν υπόψη.

Για να ικανοποιηθούν οι απαιτήσεις του σχεδίου έκτακτης ανάγκης, τα ακόλουθα στοιχεία θα περιληφθούν στο σχέδιο αυτό:

a. Στρατηγικές και διαδικασίες για να εξασφαλίσει τα συστήματα πληροφοριών.
b. Περιοδική δοκιμή-αποκατάσταση για να εξασφαλίσει βιωσιμότητα των σχεδίων αποκατάστασης.
c. Διαδικασίες για αποθήκευση και να ανάκτηση τα μέσα από την offsite αποθήκευση που εξασφαλίζει τη διαθεσιμότητα εκείνων των μέσων.
d. Διαδικασίες για να ελέγξει τις λειτουργίες υπολογιστών και δικτύων για να μετριάσει τις διακοπές.
e. Εργαλεία αποκατάστασης και offsite εγκαταστάσεις για να υποστηρίξει την έγκαιρη αποκατάσταση σε περίπτωση καταστροφής.

Πολιτική και Διαδικαστικά Πρότυπα

<u>Διαδικαστικά Πρότυπα για Εφεδρικά Δεδομένα</u>

1. Κάθε σχολείο, τμήμα, και κέντρο θα καθιερώσουν τις διαδικασίες για σε μια έκτακτη ανάγκη ή άλλο περιστατικό (παραδείγματος χάριν, πυρκαγιά, βανδαλισμός, διακοπή του συστήματος, και φυσική καταστροφή) που μπορούν να βλάψουν τα συστήματα που περιέχουν ηλεκτρονικές προστατευμένες/ εμπιστευτικές πληροφορίες.
2. Κάθε σχολείο, τμήμα, και κέντρο θα τεκμηριώσουν τις διαδικασίες για δημιουργία και συντήρηση ανακτήσιμων ακριβών αντιγράφων των ηλεκτρονικών προστατευμένων /εμπιστευτικών πληροφοριών τους
3. Κάθε σχολείο, τμήμα, και κέντρο θα έχει μια προστατευμένη offsite θέση για την καταχώρηση των εφεδρικών μέσων τους.
4. Οι διαδικασίες και τα μέσα θα εξεταστούν για την ακρίβεια και την ακεραιότητα των αποθηκευμένων δεδομένων τους.
5. Κάθε σχολείου, τμήματος, και κέντρου οι διαδικασίες εφεδρικών δεδομένων θα περιλαμβάνουν τις τεκμηριωμένες ηλεκτρονικές συμβάσεις ονομασίας.
6. Κάθε σχολείου, τμήματος, και κέντρου το σχέδιο αποκατάστασης καταστροφής θα περιλαμβάνει τις τεκμηριωμένες ηλεκτρονικές σκιώδης πολιτικές και τις διαδικασίες.

[9] http://www.nchica.org/hipaaresources/Security/UAB17.doc

7. Κάθε σχολείου, τμήματος, και κέντρου το σχέδιο αποκατάστασης καταστροφής θα περιλαμβάνει τις τεκμηριωμένες ηλεκτρονικές ημερολογιακές εγγραφές για τις πολιτικές και τις διαδικασίες.
8. Κάθε σχολείου, τμήματος, και κέντρου το σχέδιο αποκατάστασης καταστροφής θα περιλαμβάνει τεκμηριωμένα δεδομένα που αντανακλούν πολιτικές και διαδικασίες.

Σχέδιο Αποκατάστασης Καταστροφής –Πρότυπα Πολιτικής

1. Κάθε σχολείου, τμήματος, και κέντρου το σχέδιο αποκατάστασης καταστροφής θα περιλαμβάνει την τεχνολογία που απαιτείται για την offsite αποθήκευση.
2. Κάθε σχολείου, τμήματος, και κέντρου το σχέδιο αποκατάστασης καταστροφής θα περιλαμβάνει ένα φυσικό σχεδιάγραμμα (π.χ. blue print) της offsite δυνατότητας αποθήκευσης.
3. Κάθε σχολείου, τμήματος, και κέντρου το σχέδιο αποκατάστασης καταστροφής θα περιλαμβάνει ένα λογικό σχεδιάγραμμα (π.χ. διάγραμμα συνδετικότητας και καλωδίωσης) της offsite δυνατότητας αποθήκευσης.
4. Κάθε σχολείου, τμήματος, και κέντρου το σχέδιο αποκατάστασης καταστροφής θα περιλαμβάνει τις διαδικασίες εναλλαγής μέσων για την offsite αποθήκευση.

* Περισσότερα στο:
http://www.nchica.org/hipaaresources/Security/UAB17.doc

5.9 DMZ Security Policy[10]

Σκοπός

Αυτή η πολιτική εγκαθιδρύει τις απαιτήσεις ασφαλείας πληροφοριών για τα δίκτυα και τον εξοπλισμό των εργαστηρίων του οργανισμού που βρίσκονται στην λεγόμενη αποστρατικοποιημένη ζώνη "De-Militarized Zone" (DMZ). Η απαρέγκλιτη τήρηση αυτών των απαιτήσεων θα ελαχιστοποιήσει τον πιθανό κίνδυνο από ζημία στη δημόσια εικόνα που προκαλείται από την αναρμόδια χρήση πόρων του οργανισμού και την απώλεια ευαίσθητων/ εμπιστευτικών στοιχείων και πνευματικής ιδιοκτησίας.

Εμβέλεια

Δίκτυα και συσκευές εργαστηρίων (που περιλαμβάνουν αλλά που δεν περιορίζονται στους δρομολογητές, switchers, κ.λ.π.) που συνδέονται στο Internet και είναι τοποθετημένα έξω από τα Internet firewall του οργανισμού θεωρούνται μέρος των εργαστηρίων DMZ και υπόκεινται σε αυτήν την πολιτική. Αυτό περιλαμβάνει τα εργαστήρια DMZ στην κύρια τοποθεσία του φορέα παροχής υπηρεσιών Διαδικτύου (I.S.P) και απομακρυσμένες θέσεις. Όλος ο υπάρχων και μελλοντικός εξοπλισμός, που εμπίπτει στο πεδίο αυτής της πολιτικής, πρέπει να διαμορφωθεί σύμφωνα με τα αναφερόμενα έγγραφα. Αυτή η πολιτική δεν εφαρμόζεται σε εργαστήρια που υπάρχουν εσωτερικά του Internet firewall του οργανισμού.

Πολιτική

<u>Ιδιοκτησία και Ευθύνες</u>

1. Όλα τα νέα εργαστήρια DMZ πρέπει να παρουσιάσουν μια επιχειρησιακή δικαιολόγηση με την επικύρωση επιχειρησιακής μονάδας σε επίπεδο αντιπροέδρου. Η εταιρία ασφαλείας πρέπει να κρατήσει τις επιχειρησιακές δικαιολογίες στο αρχείο.
2. Οι οργανισμοί που έχουν στην ιδιοκτησία τους τα εργαστήρια αυτά είναι υπεύθυνοι για τον διορισμό διευθυντών για τα εργαστήρια, σημείων επαφής (Point of Contact), και εφεδρικά P.O.C για κάθε εργαστήριο. Η ιδιοκτήτες των εργαστηρίων πρέπει να κρατάνε ενήμερα τα P.O.C με την Εταιρία.(η εταιρία που συνεργάζεται πάνω σε θέματα διαχείρισης συστήματος). Οι διευθυντές των εργαστηρίων ή αντικαταστατές πρέπει είναι διαθέσιμοι για έκτακτη ανάγκη οποιαδήποτε ώρα.
3. Αλλαγές στις συνδέσεις ή και στον σκοπό ύπαρξης των DMZ εργαστηρίων και εγκατάσταση νέων DMZ εργαστηρίων πρέπει να απαιτούνται από το οργανισμό και να εγκρίνονται από την εταιρία ασφαλείας.
4. Όλες οι συνδέσεις από παρόχους υπηρεσιών Internet πρέπει να συντηρούνται από το οργανισμό.
5. Ο οργανισμός πρέπει να διατηρεί συσκευές firewall ανάμεσα στα DMZ και στο Internet.
6. Ο οργανισμός και η εταιρία ασφαλείας έχουν το δικαίωμα να διακόψουν κάποια σύνδεση εάν υπάρχει θέμα ασφαλείας.

[10] http://www.sans.org/resources/policies/DMZ_Lab_Security_Policy.pdf

7. Τα DMZ εργαστήρια θα παρέχουν και θα διατηρούν μέσα στον χώρο τους δικτυακές συσκευές μέχρι τα όρια τους με το οργανισμό.
8. Ο οργανισμός πρέπει να καταγράψει όλα τα διαστήματα διευθύνσεων των εργαστηρίων DMZ καθώς και τις πληροφορίες των επαφών τους.
9. Οι διευθυντές των εργαστηρίων DMZ έχουν την πλήρη ευθύνη ώστε να συμμορφωθούν τα εργαστήρια αυτά με αυτήν την πολιτική.
10. Άμεση πρόσβαση σε αρχεία καταχωρήσεων εξοπλισμού και συστήματος πρέπει να παρέχεται σε στελέχη της εταιρίας ασφαλείας και του οργανισμού εάν αυτό ζητηθεί(σύμφωνα με την πολιτική επιθεώρησης).
11. Ατομικοί εργαστηριακοί λογαριασμοί θα διαγράφονται με από 3 ημέρες όταν οι προσβάσεις αυτών δεν θα είναι πλέον εξουσιοδοτημένες. Κωδικοί ομαδικών λογαριασμών πρέπει να είναι σύμφωνοι με την πολιτική ασφαλείας για κωδικούς και πρέπει να αλλάζουν με τα από 3 ημέρες από την αλλαγή κάποιου μέλους της ομάδας.
12. Η Εταιρία θα εξετάζει αιτήσεις περιπτώσεων εξαίρεσης για κάθε περίπτωση χωριστά.

<u>Κύριες ρυθμίσεις παραμέτρων</u>

1. Παραγωγικοί πόροι δεν πρέπει να εξαρτώνται πάνω σε πόρους των DMZ εργαστηρίων.
2. Τα DMZ εργαστήρια δεν πρέπει να συνδέονται με το δίκτυο του οργανισμού απευθείας ή μέσω ασύρματης σύνδεσης.
3. Η φυσική τοποθεσία των DMZ πρέπει να είναι σε χωριστό χώρο με το εσωτερικό δίκτυο. Εάν αυτό δεν είναι δυνατό τότε πρέπει ο εξοπλισμός να είναι κλειδωμένος σε ένα rack με περιορισμένη πρόσβαση. Ο υπεύθυνος του εργαστηριού πρέπει έχει λίστα με τα άτομα που θα έχουν πρόσβαση στον εξοπλισμό.
4. Οι υπεύθυνοι των εργαστηρίων DMZ έχουν ευθύνη για την εφαρμογή των παρακάτω πολιτικών:
    a. Πολιτική Κωδικών.
    b. Πολιτική Ασύρματων Επικοινωνιών.
    c. Πολιτική Anti-Virus για Εργαστήρια.

5. Οι συσκευές firewall πρέπει να είναι διαμορφωμένες από το οργανισμό με τα ελάχιστα δικαιώματα πρόσβασης και με βάση τις λειτουργικές ανάγκες των DMZ. Όλα τα firewall φίλτρα θα συντηρούνται από την Εταιρία.
6. Οι συσκευές firewall πρέπει να είναι τα μοναδικά σημεία πρόσβασης μεταξύ των DMZ και του υπόλοιπου δικτύου του οργανισμού ή και του Internet. Οποιαδήποτε μορφή σύνδεσης μεταξύ DMZ και οργανισμού ή και Internet απαγορεύεται ρητώς.
7. Αρχικές ρυθμίσεις των firewall και οποίες αλλαγές σε αυτές θα επανεξετάζονται και θα επικυρώνονται από την εταιρία ασφαλείας. Η οποία μπορεί να ζητήσει επιπλέον μέτρα προστασίας.
8. Κίνηση δεδομένων από τα DMZ στο εσωτερικό δίκτυο του οργανισμού όπως και V.P.N πρόσβαση υπάγεται στην πολιτική για απομακρυσμένη πρόσβαση.
9. Όλα τα switchers και τα routers που χρησιμοποιούνται για εκπαίδευση ή δοκιμές πρέπει να συμβαδίζουν σύμφωνα με το έγγραφα τυποποίησης των DMZ για switchers και routers.

10. Τα λειτουργικά συστήματα των υπολογιστών υπηρεσίας εσωτερικά των DMZ που χρησιμοποιούν υπηρεσίες Internet, πρέπει να είναι ρυθμισμένα σύμφωνα με τα πρότυπα ασφαλείας για εγκατάσταση και ρυθμίσεων σε υπολογιστές υπηρεσίας.
11. Τωρινά εφαρμόσιμα patch ή hot fixes ασφαλείας για οποιαδήποτε εφαρμογή Internet πρέπει να εφαρμοστούν. Ομάδες διαχειριστών πρέπει να έχουν κάποιες διαδικασίες σε αναμονή ώστε να έχουν τα απαραίτητα patch/hot-fixes.
12. Όλα τα εφαρμόσιμα patch ή hot fixes ασφαλείας για οποιαδήποτε εφαρμογή Internet πρέπει να εφαρμοστούν. Ομάδες διαχειριστών πρέπει να έχουν κάποιες διαδικασίες σε αναμονή ώστε να έχουν τα απαραίτητα patch/hot-fixes.
13. Οι υπηρεσίες και οι εφαρμογές που δεν εξυπηρετούν τις επιχειρησιακές απαιτήσεις πρέπει να τεθούν εκτός λειτουργίας.
14. Οι εμπιστευτικές πληροφορίες του οργανισμού είναι απαγορευμένες στον εξοπλισμό σε εργαστήρια όπου το προσωπικό εκτός οργανισμού έχει φυσική πρόσβαση (π.χ., εργαστήρια κατάρτισης), σύμφωνα με την πολιτική ταξινόμησης ευαισθησίας πληροφοριών.
15. Απομακρυσμένη διαχείριση θα τελούνται μόνο μέσα από ασφαλή κανάλια(π.χ. κρυπτογραφημένα δίκτυα με IPSEC ή SSH) ή κονσόλα πρόσβασης ανεξάρτητη από τα DMZ δίκτυα.

Επιβολή

Οποιοσδήποτε υπάλληλος έχει βρεθεί να παραβιάσει την πολιτική αυτή είναι υπαγόμενος σε πειθαρχική ενέργεια συμπεριλαμβανόμενης και της λήξης της απασχόλησης.

5.10 E-mail Policy[11]*

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.

Εμβέλεια

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

<u>Απαγορευμένη χρήση</u>

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.

<u>Προσωπική χρήση</u>

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.

[11] http://www.sans.org/resources/policies/Email_Policy.pdf

<u>Παρακολούθηση</u>

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.

5.11 Identification and Authentication Policy[12]

Σκοπός

Ο σκοπός αυτής της πολιτικής είναι να καθιερωθεί μια πολιτική για τη χρήση και την επέκταση ποικίλων λύσεων ελέγχου πρόσβασης για να εξασφαλίσει την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα των πληροφοριακών στοιχείων. Αυτή η πολιτική είναι να διατηρηθεί ένα επαρκές επίπεδο ασφάλειας για να προστατεύσει τα στοιχεία, τα οικονομικά στοιχεία, και τα συστήματα πληροφοριών από την αναρμόδια πρόσβαση. Αυτή η πολιτική καθορίζει τους απαραίτητους κανόνες να επιτύχουν αυτήν την προστασία, και να εξασφαλίσουν μια ασφαλή και αξιόπιστη λειτουργία των συστημάτων πληροφοριών Αυτή η πολιτική ισχύει για όλους τους υπολογιστές και τα συστήματα επικοινωνιών, που ανήκουν ή που χρησιμοποιούνται, από έναν και οργανισμό ή τμήματα του. Ομοίως, αυτή η πολιτική ισχύει για όλες τις πλατφόρμες, τα λειτουργικά συστήματα, και τις εφαρμογές.

Εμβέλεια

Αυτή η πολιτική επεξηγεί την ανάγκη για το λογισμικό ελέγχου πρόσβασης να είναι ένα αναπόσπαστο τμήμα του διοικητικού προγράμματος συστημάτων πληροφοριών ενός οργανισμού. Η πολιτική είναι να μπορούν οι έλεγχοι μετριασμού να επιτρέπουν την εξουσιοδοτημένη πρόσβαση, διατηρώντας ένα επαρκές επίπεδο ασφάλειας στην προστασία των ενημερωτικών δεδομένων. Για τον σκοπό αυτής της πολιτική, αυτοί οι τύποι ελέγχων θα αναφερθούν ως "λύσεις ελέγχου πρόσβασης συστημάτων."

Λύσεις ελέγχου πρόσβασης συστημάτων

<u>Πολιτική</u>

Πρόσβαση στα στοιχεία πληροφοριών θα χορηγηθούν σε διαφορετικά επίπεδα, βασισμένα στους επιχειρησιακούς κανόνες που θεσπίζονται από τον κάτοχο εκείνων των πληροφοριών, για έναν εξουσιοδοτημένη χρήστη ή μια οντότητα για να δημιουργεί, διαβάζει, αναπροσαρμόσει, να διαγράψει ή να διαβιβάσει εκείνες τις πληροφορίες. Οι χρήστες θα έχουν παρεχόμενη πρόσβαση βασισμένη στην έννοια "least privilege". Η πρόσβαση θα ρυθμιστεί και θα ελεγχθεί μέσω των διακριτικών ελέγχων πρόσβασης, προσδιορισμού και πιστοποίησης ταυτότητας, και των ιχνών ελέγχου.

Χρήση των στοιχείων πληροφοριών θα περιοριστούν και θα επιτραπούν μόνο ανάλογα με τις ανάγκες για να υποστηρίξουν τις εξουσιοδοτημένες επιχειρησιακές δραστηριότητες. Οι επιχειρησιακοί κανόνες που ισχύουν ουσιαστικά από κοινού με έλεγχους πρόσβασης βασισμένους στους χρήστες θα αναθεωρηθούν για την επαρκή πρόσβαση και την προστασία επιπέδων ασφάλειας, και μπορούν να χρησιμεύσουν ως το θεμέλιο για την καθιέρωση της συμμόρφωσης με αυτήν την πολιτική.

[12] http://www.tess-llc.com/Identification%20&%20Authentication%20PolicyV4.pdf

Οποιαδήποτε προσπάθεια να παρακαμφθούν οι μηχανισμοί ασφάλειας πληροφοριών για να αποκτήσουν πρόσβαση ή για να εκμεταλλευτούν οποιεσδήποτε γνωστές ή άγνωστες ευπάθειες θα θεωρηθούν ως γεγονός ασφάλειας, και θα αντιμετωπιστούν σύμφωνα με το καθιερωμένο γεγονός εκθέτοντας τις οδηγίες ή/ και τις κατάλληλες με το ανθρώπινο δυναμικό πολιτικές και διαδικασίες. Όλες οι πληροφορίες θεωρούνται περιουσιακά στοιχεία και προστατεύονται, με όλες τις μορφές, από εκούσια ή σκόπιμη αλλά αναρμόδιος, κοινοποίηση (εμπιστευτικότητα), τροποποίηση ή καταστροφή (ακεραιότητα), ή ανικανότητα να υποβληθούν σε επεξεργασία εκείνες οι πληροφορίες (διαθεσιμότητα).

* Περισσότερα στο:
http://www.tess-llc.com/Identification%20&%20Authentication%20PolicyV4.pdf

5.12 Network Security Policy[13]*

Σκοπός

Για να εξασφαλίσει την προστασία των πληροφοριών στα δίκτυα και την προστασία των υποδομών υποστήριξης. Η ασφαλής διαχείριση των δικτύων, που μπορεί να εκταθεί τα οργανωτικά όρια του οργανισμού, απαιτεί την προσεκτική εκτίμηση στη ροή πληροφοριών, τις νομικές επιπτώσεις, τον έλεγχο, και την προστασία. Πρόσθετοι έλεγχοι μπορούν επίσης να απαιτηθούν για να προστατεύσουν τις ευαίσθητες πληροφορίες που περνούν μέσα από τα δημόσια δίκτυα.

Έλεγχοι δικτύων

Τα δίκτυα πρέπει να διαχειρίζονται και να ελέγχονται επαρκώς, προκειμένου να προστατευθούν από τις απειλές, και για να διατηρήσουν την ασφάλεια των συστημάτων και των εφαρμογών που χρησιμοποιούν το δίκτυο, συμπεριλαμβανομένων των πληροφοριών κατά τη μεταφορά.

Οδηγός Υλοποίησης

Οι διαχειριστές των δικτύων πρέπει να εφαρμόσουν ελέγχους για να εξασφαλίσουν την ασφάλεια των πληροφοριών στα δίκτυα, και την προστασία των συνδεδεμένων υπηρεσιών από μη εξουσιοδοτημένη πρόσβαση. Ειδικότερα, τα ακόλουθα στοιχεία πρέπει να ληφθούν υπόψη:

Η λειτουργική ευθύνη για τα δίκτυα πρέπει να χωριστεί από τις λειτουργίες των υπολογιστών όπου απαιτείται.

Οι ευθύνες και οι διαδικασίες για τη διαχείριση του απομακρυσμένου εξοπλισμού, συμπεριλαμβανομένου του εξοπλισμού στις περιοχές χρηστών, πρέπει να καθιερωθούν.

Οι ειδικοί έλεγχοι πρέπει να καθιερωθούν για να προστατεύσουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων που περνούν μέσα από τα δημόσια δίκτυα ή από τα ασύρματα δίκτυα, και για να προστατεύσουν τα συνδεδεμένες συστήματα και τις εφαρμογές. Ειδικοί έλεγχοι μπορούν επίσης να χρειαστούν για να διατηρήσουν τη διαθεσιμότητα των υπηρεσιών και των υπολογιστών δικτύων που συνδέονται.

Η κατάλληλη καταχώρηση στοιχείων και έλεγχος πρέπει να εφαρμοστούν για να επιτρέψουν την καταγραφή των σχετικών ενεργειών ασφάλειας.

Οι δραστηριότητες διαχείρισης πρέπει να συντονιστούν πολύ και για να βελτιστοποιήσουν την υπηρεσία στον οργανισμό και για να εξασφαλίσουν ότι οι έλεγχοι εφαρμόζονται με συνέπεια πάνω σε όλη την υποδομή επεξεργασίας πληροφοριών.

[13] Από το έγγραφο του ISO 27002

Άλλες πληροφορίες

Πρόσθετες πληροφορίες για την ασφάλεια δικτύων μπορούν να βρεθούν στο ISO/IEC 18028, Information technology – Security techniques – IT network security.

Ασφάλεια Υπηρεσιών Δικτύου

<u>Έλεγχος</u>

Τα χαρακτηριστικά γνωρίσματα ασφάλειας, τα επίπεδα υπηρεσιών, και οι διοικητικές απαιτήσεις όλων των υπηρεσιών δικτύων πρέπει να προσδιοριστούν και να περιληφθούν σε οποιαδήποτε συμφωνία υπηρεσιών δικτύων, εάν αυτές οι υπηρεσίες παρέχονται στο εσωτερικό ή εξωτερικό περιβάλλον.

<u>Οδηγός Υλοποίησης</u>

Η δυνατότητα του φορέα παροχής υπηρεσιών δικτύων να διαχειριστεί τις συμφωνηθείσες υπηρεσίες με έναν ασφαλή τρόπο πρέπει να καθοριστεί και να ελεγχθεί τακτικά, και το δικαίωμα να ελέγχει πρέπει να αναγνωριστεί.

Οι ρυθμίσεις ασφάλειας πού απαραίτητες για τις ιδιαίτερες υπηρεσίες, όπως τα χαρακτηριστικά γνωρίσματα ασφάλειας, τα επίπεδα υπηρεσιών, και οι διοικητικές απαιτήσεις, πρέπει να προσδιοριστούν. Η οργάνωση πρέπει να εξασφαλίσει ότι οι φορείς παροχής υπηρεσιών δικτύων εφαρμόζουν αυτά τα μέτρα.

<u>Άλλες Πληροφορίες</u>

Οι υπηρεσίες δικτύων περιλαμβάνουν τη παροχή συνδέσεων, V.P.N, και των δικτύων μεγάλης αξίας και λύσεων διαχείρισης ασφάλειας δικτύων όπως firewall και τα συστήματα ανίχνευσης εισβολής. Αυτές οι υπηρεσίες μπορούν να κυμανθούν από απλό εύρος ζώνης στις σύνθετες προστιθεμένης αξίας προσφορές.

Τα χαρακτηριστικά γνωρίσματα ασφάλειας των υπηρεσιών δικτύων θα μπορούσαν να είναι:

a) Τεχνολογία πού εφαρμόζεται για την ασφάλεια των υπηρεσιών δικτύων, όπως η πιστοποίηση ταυτότητας, κρυπτογράφηση, και τους ελέγχους σύνδεσης δικτύου.
b) Τεχνικοί παράμετροι που απαιτούνται για την ασφαλή σύνδεση με τις υπηρεσίες δικτύων σύμφωνα με τους κανόνες σύνδεσης ασφάλειας και δικτύων.
c) Διαδικασίες για τη χρήση υπηρεσιών δικτύων για να περιορίσει την πρόσβαση στις υπηρεσίες ή τις εφαρμογές δικτύων, όπου είναι απαραίτητο.

5.13 Password Protection Policy[14]*

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.

[14] http://www.sans.org/resources/policies/Password_Policy.pdf

- 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.

5.14 Personnel Security Policy[15]*

- 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

[15] Από το έγγραφο ISO 27002

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 μάνατζερ 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.

5.15 Physical Security Policy[16]*

• 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.

[16] Από το έγγραφο ISO 27002

- 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.

5.16 Privacy Policy[17]

Έλεγχος

Η προστασία και το απόρρητο των δεδομένων πρέπει να εξασφαλιστούν όπως απαιτείται στη σχετική νομοθεσία, κανονισμούς, και εάν υπάρχουν εφαρμόσιμες, γραπτές προτάσεις.

Οδηγός Υλοποίησης

Μία πολιτική για το απόρρητο και την προστασία στον οργανισμό πρέπει να σχεδιαστεί και να υλοποιηθεί. Αυτή η πολιτική πρέπει να κοινοποιηθεί σε όλα τα πρόσωπα που συμμετέχουν στην επεξεργασία των προσωπικών πληροφοριών.

Η συμμόρφωση με αυτήν την πολιτική και με όλη την σχετική νομοθεσία και κανονισμούς προστασίας των δεδομένων απαιτεί την κατάλληλους διοικητική δομή και τον έλεγχο. Συχνά αυτό επιτυγχάνεται καλύτερα από το διορισμό αρμόδιου, όπως ένας ανώτερος υπάλληλος προστασίας των δεδομένων, ο οποίος θα πρέπει να παρέχει οδηγίες στους διευθυντές, τους χρήστες, και τους φορείς παροχής υπηρεσιών για τις μεμονωμένες ευθύνες τους και τις συγκεκριμένες διαδικασίες που πρέπει να ακολουθούν. Ευθύνη για το χειρισμό προσωπικών πληροφοριών και η διασφάλιση της επίγνωσης των αρχών προστασίας των δεδομένων πρέπει να εξεταστεί σύμφωνα με τη σχετικούς νομοθεσία και τους κανονισμούς. Τα κατάλληλα τεχνικά και οργανωτικά μέτρα πρέπει να εφαρμοστούν για να προστατευθούν οι προσωπικές πληροφορίες.

Άλλες πληροφορίες

Διάφορες χώρες έχουν εισαγάγει νομοθεσία που τοποθετεί ελέγχους στη συλλογή, την επεξεργασία, και τη διαβίβαση προσωπικών στοιχείων(γενικά πληροφορίες για τα ζωντανά άτομα που μπορούν να προσδιοριστούν από εκείνες τις πληροφορίες). Ανάλογα με την αντίστοιχη εθνική νομοθεσία, τέτοιοι έλεγχοι μπορούν να επιβάλουν ευθύνες σε εκείνους που συλλέγουν, που επεξεργάζονται, και που διαδίδουν τις προσωπικές πληροφορίες, και μπορούν να περιορίσουν τη δυνατότητα να μεταφέρουν ότι στοιχεία σε άλλες χώρες.

[17] Από το έγγραφο ISO 27002

5.17 Remote Access Policy[18]

Σκοπός

Ο σκοπός αυτής της πολιτικής είναι να καθοριστούν τα πρότυπα για τη σύνδεση του δικτύου του οργανισμού με οποιοδήποτε άλλο δίκτυο ή απομακρυσμένο υπολογιστή. Αυτά τα πρότυπα έχουν ως σκοπό να ελαχιστοποιήσουν την πιθανή έκθεση από τις ζημίες που μπορούν να προκύψουν από την αναρμόδια χρήση των πόρων του. Οι ζημίες περιλαμβάνουν την απώλεια ευαίσθητων ή εμπιστευτικών δεδομένων, πνευματική ιδιοκτησία, ζημία στη δημόσια εικόνα, ζημία σε κρίσιμα εσωτερικά συστήματα, κ.λ.π. .

Εμβέλεια

Αυτή η πολιτική ισχύει για όλους τους υπάλληλους, προμηθευτές και συνεργάτες του οργανισμού που χρησιμοποιούν ή διαθέτουν Η/Υ ή σταθμό εργασίας που συνδέεται στο δίκτυο του οργανισμού. Αυτή η πολιτική ισχύει για τις συνδέσεις απομακρυσμένης πρόσβασης που χρησιμοποιούνται για να κάνουν την εργασία εξ ονόματος του οργανισμού, συμπεριλαμβανομένης της χρήσης e-mail και της παρακολούθησης των web πόρων του intranet.

Οι εφαρμογές απομακρυσμένης πρόσβασης που καλύπτονται από αυτήν την πολιτική περιλαμβάνουν, αλλά δεν περιορίζονται, σε εισερχόμενων κλήσεων modem, frame relay, ISDN, το DSL, VPN, SSH, και τους cable modems, κ.λ.π..

Πολιτική

<u>Γενικά</u>

Είναι ευθύνη των υπάλληλων, προμηθευτών και συνεργατών του οργανισμού με προνόμια απομακρυσμένης πρόσβασης στο δίκτυο του οργανισμού ώστε να εξασφαλιστεί ότι στη απομακρυσμένη σύνδεση τους δίνεται η ίδια εκτίμηση με την επιτόπια σύνδεση χρηστών.

Η γενική πρόσβαση στο Internet για ψυχαγωγική χρήση από άμεσα οικιακά μέλη μέσω δικτύου του οργανισμού σε προσωπικούς υπολογιστές επιτρέπεται για τους υπαλλήλους που χρησιμοποιούν σταθερές υπηρεσίες. Ο υπάλληλος του οργανισμού είναι αρμόδιος για να εξασφαλίσει ότι οικογενειακό μέλος δεν παραβιάζει οποιουσδήποτε πολιτική του οργανισμού, δεν εκτελεί τις παράνομες δραστηριότητες, και δεν χρησιμοποιεί την πρόσβαση για τα εξωτερικές επιχειρησιακές δραστηριότητες. Ο υπάλληλος φέρει την ευθύνη για τις συνέπειες εάν χρησιμοποιηθεί κατ' άσχημο τρόπο η πρόσβαση.

Παρακαλώ αναθεωρήστε τις ακόλουθες πολιτικές για τις λεπτομέρειες της προστασίας των πληροφοριών κατά πρόσβαση του δικτύου του οργανισμού μέσω απομακρυσμένης πρόσβασης, και την αποδεκτή χρήση του δικτύου:

[18] http://www.sans.org/resources/policies/Remote_Access_Policy.pdf

- Πολιτική Αποδεκτής Κρυπτογράφησης
- Πολιτική Virtual Private Network
- Πολιτική Ασύρματων Επικοινωνιών
- Πολιτική Αποδεκτής Χρήσης

Για πρόσθετες πληροφορίες σχετικά με τις δυνατότητες των συνδέσεων απομακρυσμένης πρόσβασης, που περιλαμβάνουν πώς να ξεκινήσει ή να αποσυνδέσει την υπηρεσία, τις συγκρίσεις δαπανών, την ανίχνευση λαθών, κ.λπ., να απευθύνεται στην ιστοσελίδα του οργανισμού.

Απαιτήσεις

1. Πρέπει να διασφαλιστεί ότι η απομακρυσμένη πρόσβαση θα ελέγχεται αυστηρά. Ο έλεγχος θα διασφαλίζεται μέσω της μία φοράς πιστοποίησης ταυτότητας κωδικού ή των δημόσιων/ ιδιωτικών κλειδιών με ισχυρούς κωδικούς-φράσεις. Πληροφορίες για τη δημιουργία ενός ισχυρού κωδικού-φράσης δείτε την πολιτική κωδικού πρόσβασης.
2. Ποτέ οποιοιδήποτε υπάλληλος του οργανισμού δεν πρέπει να παρέχει την άδεια εισόδου του ή τον κωδικό πρόσβασης ηλεκτρονικού ταχυδρομείου σε κανένα, ακόμη και σε οικογενειακά μέλη.
3. Υπάλληλοι και εργολάβοι με προνόμια απομακρυσμένης πρόσβασης πρέπει να εξασφαλίσουν ότι προσωπικοί υπολογιστές ή τερματικοί σταθμοί του οργανισμού που χρησιμοποιούνται από τους ίδιους, που συνδέονται απομακρυσμένα με το δίκτυο, δεν συνδέονται με οποιοδήποτε άλλο δίκτυο συγχρόνως, με εξαίρεση τα προσωπικά δίκτυα που είναι υπό τον πλήρη έλεγχο του χρήστη.
4. Υπάλληλοι και εργολάβοι με προνόμια απομακρυσμένης πρόσβασης στο δίκτυο του οργανισμού δεν πρέπει να χρησιμοποιούν ηλεκτρονικό ταχυδρομείο εκτός οργανισμού (δηλ., Hotmail, Yahoo), ή άλλές εξωτερικές πήγες για εργασία και δεν είναι ποτέ συγκεχυμένη με την προσωπική εργασία.
5. Οι δρομολογητές που είναι αφιερωμένοι για γραμμές ISDN και είναι διαμορφωμένοι για την πρόσβαση στο δίκτυο πρέπει να καλύπτουν τις ελάχιστες απαιτήσεις πιστοποίησης ταυτότητας CHAP(Challenge-Handshake Authentication Protocol).
6. Η επαναδιαμόρφωση οικιακού εξοπλισμού για split-tunneling ή για dual homing δεν επιτρέπεται σε καμία περίπτωση.
7. Το Frame Relay πρέπει να καλύπτει τις ελάχιστες απαιτήσεις πιστοποίησης σύμφωνα με τα πρότυπα DLCI(data link connection identifier).
8. Διαμόρφωση υλικού που δεν είναι σύμφωνη με τα πρότυπα πρέπει να εγκριθεί από τις υπηρεσίες απομακρυσμένης πρόσβασης, και εταιρία ασφαλείας να εγκρίνει παραμέτρους ασφαλείας για πρόσβαση στο υλικό αυτό.
9. Όλοι οι υπολογιστές υπηρεσίας που είναι συνδεμένοι με το εσωτερικό δίκτυο του οργανισμού μέσω απομακρυσμένης σύνδεσης πρέπει να χρησιμοποιούν antivirus με τελευταίες ενημερώσεις, αυτό περιλαμβάνει και προσωπικούς υπολογιστές. Οι συνδέσεις με ομάδες τρίτων πρέπει να συμμορφωθούν με τις απαιτήσεις όπως δηλώνονται στη συμφωνία με ομάδες τρίτων χρηστών.
10. Ο προσωπικός εξοπλισμός που χρησιμοποιείται για να σύνδεση με δίκτυα του οργανισμού πρέπει να καλύπτει τις απαιτήσεις εξοπλισμού που ανήκουν στο οργανισμό για απομακρυσμένη πρόσβαση.

11. Οι οργανώσεις ή τα άτομα που επιθυμούν να εφαρμόσουν μη συνηθισμένες λύσεις για απομακρυσμένη πρόσβαση σε δίκτυο του οργανισμού πρέπει να λάβουν την προγενέστερη έγκριση από τις υπηρεσίες απομακρυσμένης πρόσβασης και την εταιρία ασφαλείας.

Επιβολή

Οποιοσδήποτε υπάλληλος έχει βρεθεί να παραβιάσει την πολιτική αυτή είναι υπαγόμενος σε πειθαρχική ενέργεια συμπεριλαμβανόμενης και της λήξης της απασχόλησης.

5.18 Mobile Computing and Storage Devices[19]

Σκοπός

Σκοπός αυτής της πολιτικής είναι να καθιερώσει έναν εξουσιοδοτημένη μέθοδο για τον έλεγχο κινητών υπολογιστών και συσκευών αποθήκευσης που περιέχουν ή έχουν πρόσβαση σε πηγές πληροφοριών του οργανισμού.

Εμβέλεια

Υπάλληλοι, συνεργάτες, σύμβουλοι, εργολάβοι, και άλλοι που χρησιμοποιούν κινητούς Η/Υ και συσκευές αποθήκευσης στο δίκτυο του οργανισμού.

Πολιτική

Οι κινητοί Η/Υ και μέσα αποθήκευσης που περιέχουν ή που έχουν πρόσβαση στις πηγές πληροφοριών, πρέπει να εγκριθούν πριν από τη σύνδεση με τα συστήματα πληροφοριών. Αυτό αναφέρεται σε όλες τις συσκευές που συνδέουν με το δίκτυο του οργανισμού, ανεξάρτητα από την ιδιοκτησία τους.

Οι κινητοί Η/Υ και μέσα αποθήκευσης περιλαμβάνουν αλλά δεν περιορίζονται σε : laptop, PDA, USB συσκευές, CD, DVD, flash μνήμες, modems, ασύρματες συσκευές χειρός, ασύρματες κάρτες δικτύου, ή άλλη υπάρχουσα ή μελλοντική συσκευή κινητού υπολογιστή ή συσκευή αποθήκευσης, που ανήκουν σε κάποιο άτομο ή στο οργανισμό, που μπορεί να συνδεθεί ή να έχει πρόσβαση στα συστήματα πληροφοριών του οργανισμού. Μια ανάλυση κινδύνου για κάθε νέο τύπο μέσου θα διεξάγεται και θα τεκμηριώνεται πριν από τη χρήση ή τη σύνδεσή του στο δίκτυο του οργανισμού, εκτός και εάν έχει ήδη εγκριθεί. Θα διατηρείται ένας κατάλογος εγκεκριμένων κινητών υπολογιστών και αποθήκευσης

Οι κινητοί υπολογιστές και μέσα αποθήκευσης χάνονται εύκολα ή μπορεί να κλαπούν εύκολα, παρουσιάζοντας υψηλό κίνδυνο για την άνευ αδείας πρόσβαση και την εισαγωγή του κακόβουλου λογισμικού στο δίκτυο του οργανισμού. Αυτοί οι κίνδυνοι να εξαλείφουν ή να μετριαστούν σε αποδεκτά επίπεδα.

Οι φορητοί υπολογιστές και τα φορητά μέσα αποθήκευσης που περιέχουν εμπιστευτικές, προσωπικές, ή ευαίσθητες πληροφορίες του οργανισμού πρέπει να χρησιμοποιούν κρυπτογράφηση ή εξίσου ισχυρά μέτρα για να προστατεύσουν τα δεδομένα ενώ είναι αποθηκευμένα.

Εκτός αν η γραπτή έγκριση έχει ληφθεί από το επιστημονικό υπεύθυνο του οργανισμού και ανώτερο υπάλληλο του, βάσεις δεδομένων ή τμήμα αυτής, που υπάρχουν στο δίκτυο του οργανισμού, δεν θα μεταφέρονται στις κινητούς υπολογιστές ή κινητά μέσα αποθήκευσης.

[19] http://www.sans.org/resources/policies/Remote_Access.pdf

Το τεχνικό προσωπικό και οι χρήστες, που περιλαμβάνουν τους υπαλλήλους, τους συμβούλους, τους προμηθευτές, τους αναδόχους, και τους σπουδαστές, θα έχουν τη γνώση, να υπογράψουν, και να εμμείνουν στην χρήσης υπολογιστών και πολιτική ασφάλειας του οργανισμού. Η συμμόρφωση, με τα πρότυπα απομακρυσμένης πρόσβασης, κινητά μέσα, και άλλές εφαρμόσιμες πολιτικές, διαδικασίες, και πρότυπα είναι υποχρεωτικές.

5.19 Resource Utilization Security Policy[20]

Σκοπός

Ο σκοπός αυτής της πολιτικής χρήσης των πόρων είναι να μεγιστοποιηθεί η διαθεσιμότητα τους μέσα σε ένα οργανισμό. Οι αποτυχίες μεταξύ του τελικού χρήστη και των επιθυμητών στοιχείων πρέπει να αποβληθούν. Αυτή η πολιτική ανακουφίζει τις αποτυχίες μεταξύ των τελικών χρηστών με την εφαρμογή και τη διατήρηση ενός υψηλού επιπέδου ανοχής βλαβών, χωρίς παραγωγή των τεράστιων κύριων επενδύσεων στον οργανισμό.

Εμβέλεια

Αυτή η πολιτική διευκρινίζει ότι η διατήρηση ενός υψηλού επιπέδου πρόσβασης στοιχείων και η μεγιστοποίηση της αποδοτικότητας ενός χρήστη είναι δύο σημαντικοί στόχοι. Αυτή η πολιτική υπαγορεύει ότι οι διοικητές συστημάτων θα εφαρμόσουν τις λύσεις χρησιμοποίησης των στοιχείων για να αυξήσουν πολύ τη γενική διαθεσιμότητα των στοιχείων με την ανάπτυξη των ισχυρών ανεκτικών συστημάτων βλαβών από το κέντρο στοιχείων στον υπολογιστή γραφείου, το χαρακτηρισμό του ενσωματωμένου πλεονασμού και τον έλεγχο βλαβών των κρίσιμων συστατικών που χρησιμοποιούνται για να καταχωρήσουν, να διαχειριστούν και να μεταφέρουν τα δεδομένα. Αυτή η πολιτική βεβαιώνει ότι οι ευαίσθητες πληροφορίες προστατεύονται κατάλληλα, και έχει την ικανότητα να εξετάσει την αυξανόμενη απειλή των βασισμένων σε υπολογιστή επιθέσεων προκειμένου να μετριαστεί ο κίνδυνος των σοβαρών διασπάσεων και ζημιών στην κρίσιμη υποδομή ενός οργανισμού.

Πολιτική

<u>Ανοχή βλαβών</u>

Για να εξασφαλίσουν αξιοποίηση των πόρων, οι υπεύθυνοι των συστημάτων επικαλούνται τις ικανότητες πλεονασμού συστημάτων στα κρίσιμα συστήματα. Αυτό θα μετριάσει τον κίνδυνο υποβιβασμένων και περιορισμένων ανοχών βλαβών επιτρέποντας τη σωστή λειτουργία των προσδιορισμένων ικανοτήτων σε περίπτωση προσδιορισμένων αποτυχιών. Οι διαχειριστές θα εξασφαλίσουν ότι οποιαδήποτε αποτυχία που ανιχνεύεται είναι ελέγξιμη.

<u>Προτεραιότητα Υπηρεσιών</u>

Οι διαχειριστές συστημάτων θα εφαρμόσουν αποτελεσματικούς μηχανισμούς για να ελέγξουν τη χρήση των πόρων του οργανισμού από τους χρήστες έτσι ώστε οι υπηρεσίες υψηλής προτεραιότητας να ολοκληρώνονται πάντα χωρίς την αδικαιολόγητη παρέμβαση ή καθυστέρηση που προκαλείται από τις χαμηλές δραστηριότητες προτεραιότητας.

[20] http://www.tess-llc.com/Resource%20Utilization%20PolicyV4.pdf

1. Ο διαχειριστής συστημάτων θα αναθέσει μια προτεραιότητα σε κάθε αντικείμενο και εκείνη την πρόσβαση θα μεσολαβήσει βάσει της ανατεθειμένης προτεραιότητας του αντικείμενο.
2. Ο διαχειριστής συστημάτων θα αναθέσει μια προτεραιότητα σε κάθε αντικείμενο και ότι κάθε πρόσβαση σε όλα τα διαμοιρασμένους πόρους θα μεσολαβήσουν βάσει της ανατεθειμένης προτεραιότητας του θέματος.

* Περισσότερα στο:
http://www.tess-llc.com/Resource%20Utilization%20PolicyV4.pdf

5.20 Router Security Policy[21]

Σκοπός

Η παρούσα πολιτική περιγράφει μια απαραίτητη ελάχιστη διαμόρφωση ασφάλειας για όλους τους δρομολογητές και τους κατανεμητές που συνδέουν το δίκτυο του οργανισμού ή άλλα δίκτυα που συνδέονται σε αυτό.

Εμβέλεια

Επηρεάζονται όλοι οι routers και τα switches που συνδέονται με το δίκτυο του οργανισμού. Οι routers και τα switches μέσα στα εσωτερικά, εξασφαλισμένα εργαστήρια δεν επηρεάζονται. Οι δρομολογητές και οι διακόπτες μέσα στις περιοχές DMZ εμπίπτουν στην πολιτική ασφαλείας DMZ.

Πολιτική

Κάθε δρομολογητής πρέπει να ανταποκριθεί στα ακόλουθα πρότυπα διαμόρφωσης:

1. Κανένας τοπικός λογαριασμός χρήστη δεν θα διαμορφώνεται στο δρομολογητή. Οι δρομολογητές πρέπει να χρησιμοποιούν TACACS + για όλες τις πιστοποιήσεις ταυτότητας χρηστών.
2. Ο κωδικός ενεργοποίησης στο δρομολογητή πρέπει να κρατηθεί σε μια ασφαλή κρυπτογραφημένη μορφή. Ο δρομολογητής πρέπει να έχει τον κωδικό ενεργοποίησης σαν παρόντα κωδικό πρόσβασης λειτουργίας δρομολογητή από την οργάνωση υποστήριξης των δρομολογητών.
3. Απαγορεύονται τα ακόλουθα:
    - Μεταδόσεις κατευθείαν σε IP.
    - Εισερχόμενα πακέτα προερχόμενα από μη έγκυρη διεύθυνση όπως RFC1918 διεύθυνση.
    - Μικρές υπηρεσίες TCP.
    - Μικρές υπηρεσίες UDP.
    - Όλες οι δρομολογήσεις από πηγή.
    - Όλες η υπηρεσίες που τρέχουν από router.
4. Χρησιμοποίηση συλλογικών standard SNMP συμβολοσειρών.
5. Πρέπει να προστεθούν κανόνες πρόσβασης σύμφωνα με τις ανάγκες του οργανισμού.
6. Ο δρομολογητής πρέπει να περιληφθεί στο σύστημα διαχείρισης του οργανισμού με ένα οριζόμενο σημείο της επαφής.
7. Κάθε δρομολογητής πρέπει να φέρει την ακόλουθη δήλωση σε σαφή όψη: "Η ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΗ ΠΡΟΣΒΑΣΗ ΣΕ ΑΥΤΗΝ ΤΗΝ ΣΥΣΚΕΥΗ ΔΙΚΤΥΟΥ ΕΙΝΑΙ ΑΠΑΓΟΡΕΥΜΕΝΗ. Πρέπει να έχετε τη ρητή άδεια για να έχετε πρόσβαση ή να διαμορφώσετε αυτήν την συσκευή. Όλες οι δραστηριότητες που εκτελούνται σε αυτήν την συσκευή μπορούν να καταγραφούν, και οι παραβιάσεις αυτής της πολιτικής μπορούν να οδηγήσουν στην πειθαρχικό παράπτωμα, και μπορούν να οδηγήσουν στην επιβολή νόμου. Δεν υπάρχει κανένα δικαίωμα στη μυστικότητα σε αυτήν την συσκευή."

[21] http://www.sans.org/resources/policies/Router_Security_Policy.pdf

8. Δεν μπορεί ποτέ να χρησιμοποιηθεί Telnet μέσω οποιοδήποτε δικτύου για να διαχείριση ενός δρομολογητή, εκτός αν υπάρχει μια ασφαλής σύνδεση που προστατεύει το ολόκληρο μονοπάτι επικοινωνίας. SSH είναι το προτιμημένο πρωτόκολλο.

Επιβολή

Οποιοσδήποτε υπάλληλος έχει βρεθεί να παραβιάσει την πολιτική αυτή είναι υπαγόμενος σε πειθαρχική ενέργεια συμπεριλαμβανόμενης και της λήξης της απασχόλησης.

5.21 Server Security Policy[22]*

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.

Εμβέλεια

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

<u>Ιδιοκτησία Και Ευθύνες</u>

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.

<u>Γενικές Οδηγίες Ρυθμίσεων</u>

- 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.

[22] http://www.sans.org/resources/policies/Server_Security_Policy.pdf

- 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.

5.22 Server Malware Protection Policy[23]*

Σκοπός

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

Εμβέλεια

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 Διαδίκτυο
- 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

[23] http://www.sans.org/resources/policies/Server_Malware_Protection_Policy.pdf

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.

5.23 User Data Protection Policy[24]

Σκοπός

Μια οργάνωση στηρίζεται στις πηγές τεχνολογιών πληροφοριών για να χειριστεί σήμερα τα τεράστια ποσά πληροφοριών. Επειδή οι πληροφορίες μπορούν να ποικίλουν ευρέως στον τύπο και στο βαθμό ευαισθησίας, οι υπάλληλοι πρέπει να είναι σε θέση να ασκήσουν ευελιξία στο χειρισμό και την προστασία των δεδομένων. Δεν θα ήταν πρακτικό ή οικονομικώς αποδοτικό να απαιτηθεί ότι όλες οι πληροφορίες αντιμετωπίζονται με τον ίδιο τρόπο ή υπόκεινται στις ίδιες απαιτήσεις προστασίας. Χωρίς κάποιο βαθμό τυποποίησης, εντούτοις, οι ασυνέπειες μπορούν να αναπτυχθούν και θα μπορούσαν να εισαγάγουν κινδύνους.

Εμβέλεια

Η πολιτική προστασίας δεδομένων χρηστών είναι χτισμένη επάνω στην πολιτική προσδιορισμού και πιστοποίησης ταυτότητας. Το μεγαλύτερο πλαίσιο για την πολιτική ενός οργανισμού είναι βασισμένη στις ακόλουθες τρεις βασικές αρχές:

1. Μυστικότητα. Καλύπτει τα δικαιώματα και τις επιθυμίες ενός ατόμου να περιορίσει την κοινοποίηση των μεμονωμένων και εταιρικών πληροφοριών.
2. Εμπιστευτικότητα. Αναγνωρίζει ότι οι ευαίσθητες πληροφορίες μπορούν να δημοσιευθούν και να μοιραστούν για νόμιμους λόγους, εφ' όσον λαμβάνονται οι επαρκείς παροχές για να προστατεύσουν τα στοιχεία. Η εμπιστευτικότητα αναφέρεται στις ελεγχόμενες συνθήκες στις οποίες οι πληροφορίες μοιράζονται ή δημοσιεύονται. Αυτές οι ελεγχόμενες συνθήκες θα διευκρινιστούν σε πρόσθετες πολιτικές και διαδικασίες.
3. Ασφάλεια. Αποτελείται από τον έλεγχο και τις διαδικασίες (π.χ. πολιτικές και διαδικασίες, σχέδιο και εφαρμογή των τεχνικών μέτρων) που καθιερώνονται για να προστατεύσουν ευαίσθητές πληροφορίες και συστήματα ενός οργανισμού. Τέτοια μέτρα ασφάλειας όχι μόνο στοχεύουν στην προστασία της μυστικότητας, αλλά και την εξασφάλιση της πιστοποίησης ταυτότητας, της ακεραιότητας, της ασφάλειας, της αξιοπιστίας, και της διαθεσιμότητας των συστημάτων πληροφοριών.

Πολιτική

<u>User Data Protection</u>

Αυτή η πολιτική ισχύει για πληροφορίες με τις ακόλουθες μορφές με ιδιαίτερο ενδιαφέρον για την προστασία των μεμονωμένων και εταιρικών ευαίσθητων πληροφοριών:

1. Ασφάλεια. Προστατεύστε τις μεμονωμένες και εταιρικές ευαίσθητες πληροφορίες από την απώλεια, τη ζημία, την ακατάλληλη πρόσβαση, και την αναρμόδια κοινοποίηση ή τη χρήση.
2. Ακεραιότητα. Παρέχετε τη λογική διαβεβαίωση ότι τα δεδομένα, μόλις εισαχθούν, δεν θα υπόκεινται στην αναρμόδια τροποποίηση, και ότι τα

[24] http://www.tess-llc.com/User%20Data%20Protection%20PolicyV4.pdf

δεδομένα θα παραμείνουν αμετάβλητα κατά τη διάρκεια της μετάδοσης, αποθήκευση, αντιγραφής, και επαναχρησιμοποίησης.

3. Υπευθυνότητα. Ελέγξτε και καταγράψτε τα σχετικά με την ασφάλεια γεγονότα και συνδέστε τα με το δημιουργό.
4. Τεχνικές οδηγίες. Παρέχετε τις τεχνικές οδηγίες και τις συνεργάσιμες λύσεις για να ανταποκριθείτε σε αυτές τις απαιτήσεις.

Τα προνόμια ενός υπολογιστή και συστήματος επικοινωνιών όλων των χρηστών, των συστημάτων, και των προγραμμάτων θα περιοριστούν βασισμένα στην ακόλουθη αρχή "ελάχιστων προνομίων":

1. Στους χρήστες θα χορηγηθούν τα "ελάχιστα προνόμια" που απαιτούνται για να ολοκληρώσουν τις στοιχειώδεις εργασίες τους.
2. Σε εφαρμογές θα χορηγηθούν τα "ελάχιστα προνόμια" για να εκτελέσουν τις λειτουργίες τους.
3. Σε γενικά συστήματα υποστήριξης θα χορηγηθούν τα "ελάχιστα προνόμια" για να εκπληρώσουν το ρόλο τους σε ένα μεγαλύτερο δίκτυο.

* Περισσότερα στο:
http://www.tess-llc.com/User%20Data%20Protection%20PolicyV4.pdf

5.24 VPN Security Policy[25]*

Σκοπός

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

Εμβέλεια

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 ξανά συνδεθεί 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.

[25] http://www.sans.org/resources/policies/Virtual_Private_Network.pdf

Επιβολή

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

5.25 Wireless Communication Policy[26]*

Σκοπός

Αυτή η πολιτική καθορίζει τις συνθήκες τις οποίες πρέπει να πληροί 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.

Εμβέλεια

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.

[26] http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf

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.

Παρακάτω παρατίθεται πίνακας με τις πολιτικές από την SANS που δείχνει ποίες έχουν μεταφραστεί στα πλαίσια αυτής της πτυχιακής εδώ της πτυχιακής και ποίες στη πτυχιακής της Αλεξάκη Ευφροσύνης με τίτλο "Καταγραφή Πολιτικών Ασφάλειας σύμφωνα με το πρότυπο ISO27002".

Α/Α	Πολιτικη/Περιγραφη Πολιτικης	Αλεξάκη (12/49)	Χαβιαράς (27/49)
1	**Acceptable Encryption Policy**		☺
2	**Acceptable Use Policy**	☺	☺
3	**Acquisition Assessment Policy**		
4	**Analog/ISDN Line Policy**		☺
5	**Anti-Virus Process**	☺	☺
6	**Application Service Provider Policy**		
7	**Audit Vulnerability Scanning Policy**		
8	**Automatically Forwarded Email Policy**		
9	**Backup Policy**		☺
10	**Bluetooth Device Security Policy**		
11	**Certification and Accreditation Policy**		☺
12	**Cryptography Policy**		
13	**Communications Policy**		
14	**Data Classification Policy**		
15	**Database Credentials Coding Policy**		
16	**Dial-in Access Policy**		☺

17	**Disaster Recovery Policy**		☺
18	**DMZ Security Policy**		☺
19	**DMZ Lab Security Policy**		
20	**E-mail Policy**	☺	☺
21	**E-mail Retention**		
22	**Ethics Policy**		
23	**Extranet Policy**		
24	**Identification and Authentication Policy**		☺
25	**Information Data Ownership Policy**		
26	**Information Sensitivity Policy**.	☺	
27	**Information System Audit Logging Requirements**		
28	**Internal Lab Security Policy**.		
29	**Internet DMZ Equipment Policy**		
30	**Lab Anti-Virus Policy**	☺	☺
31	**Network Security Policy**		☺
32	**Password Protection Policy**	☺	☺
33	**Personal Communication Device**		
34	**Personnel Security Policy**	☺	☺

35	**Physical Security Policy**	☺	☺
36	**Privacy Policy**		☺
37	**Remote Access Policy**		☺
38	**Removable Media Policy**		
39	**Remote Access - Mobile Computing and Storage Devices**		☺
40	**Resource Utilization Security Policy**		☺
41	**Risk Assessment Policy**	☺	
42	**Router Security Policy**		☺
43	**Security Awareness Policy**		☺
44	**Security Training Policy**		☺
45	**Server Security Policy**	☺	☺
46	**Server Malware Protection Policy**	☺	☺
47	**Telecommuting/Teleworking Securiti Policy**		
48	**The Third Party Network Connection Agreement**		
49	**User Data Protection Policy**		☺

50	**VPN Security Policy**	☺	☺
51	**Wireless Communication Policy**	☺	☺

Πίνακας 3:Πίνακας πολιτικών που έχουν μεταφραστεί

Κεφάλαιο 6

Κατάρτιση και Συνειδητοποίηση Πάνω Σε Θέματα Ασφαλείας

Η συνειδητοποίηση και η κατάρτιση σε θέματα ασφάλειας είναι ίσως ένα από τα πιο αγνοημένα μέρη ενός προγράμματος διαχείρισης ασφάλειάς. Στο αυτο κεφάλαιο εξετάζουμε τρόπους, πολιτικές για την εκπαίδευση και ευαισθητοποίηση των ατόμων που δραστηριοποιούνται σε έναν οργανισμό πάνω σε θέματα ασφαλείας.

6.1 Τρόποι και καθοδήγηση για τον σχεδιασμό προγράμματος κατάρτισης και συνειδητοποίησης[27]

Οι καλύτεροι υπεύθυνοι είναι οι εργαζόμενοι

Η συνειδητοποίηση και η κατάρτιση ασφάλειας πρέπει να είναι ένα αναπόσπαστο τμήμα του προγράμματος ασφάλειάς ενός οργανισμού. Αν και πολλές επιχειρήσεις αγνοούν την ευκαιρία να πουν στους υπάλληλους τους πώς να βοηθήσουν με την προστασία της εταιρικής υποδομής, η συνειδητοποίηση και η κατάρτιση ασφάλειας είναι πραγματικά η πρώτη γραμμή υπεράσπισης για το πώς ο οργανισμός πρέπει να προστατεύει τα σημαντικά περιουσιακά του στοιχειά. Οι εργαζόμενοι είναι οι διαχειριστές των κρίσιμων στοιχείων και πληροφοριών περιουσιακών στοιχείων, και με την κατάλληλη κατάρτιση οι εταιρίες μπορούν να στρατολογήσουν τη βοήθεια των υπαλλήλων τους για να μετριάσουν τους κινδύνους.

Ενώ οι περισσότεροι υπάλληλοι είναι πιθανώς ευσυνείδητοι, και κάνουν το καλύτερό για να εκτελέσουν τα καθήκοντά τους όπως αναμένεται, ο χαρακτηριστικός υπάλληλος τεχνολογίας πληροφοριών είναι απασχολημένο πρόσωπο. Υπάρχουν συχνά πολύ περισσότερες στοιχειώδεις εργασίες να εκτελέσουν από όσο χρόνο υπάρχει σε μια τυπική εργάσιμη μέρα. Εάν η διοίκηση δεν το κάνει προτεραιότητα να υπογραμμίσει τη συνειδητοποίηση και την κατάρτιση ασφάλειας, είναι πιθανόν οι υπάλληλοι να μην δώσουν πολλή προσοχή. Εντούτοις, εάν η οργάνωσή καθιερώσει ακόμη και ένα απλό πρόγραμμα σε σταθερή, για παράδειγμα τριμηνιαία βάση, η ενημέρωση ασφάλειας μπορεί να σώσει τα πολύτιμα περιουσιακά στοιχεία από μια ακριβή και μεγάλου αντίκτυπου καταστροφή.

Φάσεις για το πρόγραμμα συνειδητοποίησης και κατάρτισης ασφαλείας

To N.I.S.T (National Institute of Standards and Technology, US Department of Commerce) ορίζει[28] τέσσερα κρίσιμα βήματα που ένα επιμορφωτικό πρόγραμμα συνειδητοποίηση ασφάλειας και πρέπει να περιλαμβάνει:

1. Σχέδιο και ορισμός του προγράμματος συνειδητοποίησης και επιμόρφωσης.
2. Ανάπτυξη του υλικών για συνειδητοποίησης και επιμόρφωσης.
3. Εφαρμογή του προγράμματος συνειδητοποίησης και επιμόρφωσης.

[27] http://www.intranetjournal.com/articles/200410/ij_10_11_04a.html

[28] *NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program*, by Mark Wilson and Joan Hash, National Institute of Standards and Technology, Oct. 2003.

4. Μέτρηση της αποτελεσματικότητας και ενημέρωση του προγράμματος.

Κάποιος στην εταιρία, πιθανότατα ο C.I.O(Chief Information Officer), πρέπει να οριστεί υπεύθυνος για να εξασφαλίσει ότι και οι τέσσερις από αυτές τις φάσεις θα συντελούνται σύμφωνα με ένα καλοσχεδιασμένο χρονοδιάγραμμα. Η συνειδητοποίηση και η κατάρτιση ασφάλειας περιλαμβάνουν την απόδοση των ευθυνών ασφάλειας στους διαχειριστές πληροφοριών του οργανισμού, και ο C.I.O, ή ένας ισάξιος προϊστάμενος, πρέπει να οριστεί υπεύθυνος για να σιγουρευτεί ότι αυτή η απόδοση θα συμβεί.

Οι στόχοι της συνειδητοποίησης και κατάρτισης ασφαλείας

Ο στόχος του προγράμματος συνειδητοποίησης και επιμόρφωσης ασφάλειάς πρέπει να είναι η προστασία της εμπιστευτικότητας, η ακεραιότητας, και η διαθεσιμότητας των περιουσιακών στοιχείων και δεδομένων των τεχνολογιών πληροφοριών. Όταν κάποιος οργανισμός σχεδιάζει ένα τέτοιο πρόγραμμα , πρέπει να περάσει στους υπαλλήλους του πώς αναμένεται από εκείνους να συμπεριφερθούν στα θέματα ασφάλειας με το δέοντα σεβασμό.

Υπάρχουν πιθανώς πάρα πολλοί μηχανισμοί που μπορούν να ληφθούν για την προστασία πληροφοριών, και για το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφάλειάς σας πρέπει να ληφθεί υπόψη ότι υπάρχει, και πρέπει να είναι, πρακτικοί περιορισμοί ως προς ποια μέτρα προστασίας εφαρμόζονται, και το ποσό του χρόνου των υπαλλήλων λαμβάνεται για την εκπαίδευση τους στις διαδικασίες ασφάλειας. Επομένως, το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφάλειάς πρέπει να προωθείται έξυπνα.

Ο στόχος είναι υπάρχει μεγαλύτερο κέρδος στην ασφάλεια από τον χρόνο που λαμβάνεται για την καθοδήγηση των υπαλλήλων στους ρόλους και τις ευθύνες ασφάλειάς τους. Προκειμένου να γίνει αυτό, πρέπει να σχεδιαστεί το πρόγραμμά για να εστιάσει σε σημαντικά ζητήματα ασφαλείας- οι τομείς που θα μπορούσαν ενδεχομένως να μετριάσουν ένα υψηλό αντίκτυπο, και πιθανών κίνδυνων.

Παράδοση του μηνύματος ασφαλείας

Το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφάλειάς μπορεί να παραδοθεί σαν εκτύπωση υπομνημάτων, αφίσες, μαθημάτων ή μέσω πρωτοβουλιών από το Internet. Οι περισσότερες οργανώσεις σήμερα επιλέγουν να παρουσιάσουν το πρόγραμμά τους μέσα από το Web-based intranet τους. Μερικές επιχειρήσεις βάζουν σύντομες σειρές μαθημάτων on-line και καθοδηγούν τους υπαλλήλους τους για να συνδεθούν και να τις πάρουν. Αυτός είναι ένας καλός τρόπος να αναπτυχθεί η συνειδητοποίηση και η κατάρτιση ασφάλειας εργαζομένων επειδή δημιουργεί εγγραφές και ίχνη για έλεγχο που επιβεβαιώνει ότι ο υπάλληλος διάβασε τουλάχιστον ποίες είναι οι ευθύνες του. Μερικά μαθήματα περιλαμβάνουν σύντομες σειρές ερωτήσεων που εξετάζουν τη βασική γνώση ασφάλειας, προκειμένου να γίνει αντιληπτό εάν ο υπάλληλος καταλαβαίνει την εκπαίδευση.

Το μήνυμα της συνειδητοποίησης και εκπαίδευσης

Υπάρχουν βασικά σημεία που μπορούν να περιληφθούν στο πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφάλειάς. Οι υπαλλήλους θα συμβουλευθούν τις 10 σημαντικότερες πολιτικές ασφάλειας και θα μπορούν να βρουν online αντίγραφο του πλήρους αυτού συνόλου πολιτικών ασφάλειας.

Να σιγουρευτεί ότι φέρει η συνειδητοποίηση ασφαλείας θα έχει κοινωνική εφαρμογή και να εξηγηθεί στους υπαλλήλους να μην δίνουν τους κωδικούς πρόσβασής στον οποιοδήποτε τους καλεί στο τηλέφωνο, δεδομένου ότι ο καλών μπορεί να είναι ένας hacker που παριστάνει έναν συνάδελφο , το εταιρικό helpdesk, ή κάποιο άλλο νόμιμο πρόσωπο.

Ενημέρωση των υπαλλήλων να ενημερώνουν το λογισμικό antivirus τους, και πόσο συχνά τους να το κάνουν αυτό. Τήρηση των υπολογιστών γραφείου ενημερωμένων με τα πιο πρόσφατα antivirus signatures καθώς είναι ένας καλός τρόπος να προστατευθεί η εταιρική υποδομή. Οι υπάλληλοι πρέπει επίσης να εκπαιδευτούν για τους κινδύνους στο άνοιγμα συνημμένων στα email. Ενώ δεν διανέμονται όλοι οι ιοί από τα συνημμένα, σε πολλές περιπτώσεις, αυτά είναι ένας ιδιαίτερα αξιοσημείωτος μηχανισμός διανομής ιών που ο υπάλληλος πρέπει να εστιάσει.

Οι υπάλληλοι πρέπει να καταλάβουν τι αποτελεί έναν ασφαλή κωδικό πρόσβασης και τι έναν αδύναμο κωδικό πρόσβασης. Μερικοί λιγότερο τεχνικοί υπάλληλοι δεν μπορούν να συνειδητοποιήσουν πόσο εύκολο είναι για τους hacker να εκτελέσουν dictionary attacks στους κωδικούς πρόσβασης εκτός αν τους το πουν. Οι καλοί κωδικοί πρόσβασης είναι πάντα μεικτοί, χαρακτήρες και αριθμοί, και δεν αποτελούνται από πραγματικές λέξεις. Εάν συστηματικά γίνεται ανίχνευση στους directory servers για αδύναμους κωδικούς πρόσβασης, πρέπει να γίνει σύσταση στους υπαλλήλους ότι οι κωδικοί ανιχνεύονται συστηματικά για περίπτωση μη-συμμόρφωσης.

Σε περίπτωση που ένας υπάλληλος υποψιαστεί έναν ιό ή μια επίθεση από το Διαδίκτυο, εκείνος ξέρει που θα το αναφέρει αυτό; Ποιον θα πρέπει να καλέσει; Πρέπει να καταστεί γνωστό αυτό, και πρέπει επίσης να εξασφαλιστεί ότι το πρόσωπο που καλούν θα καταλάβει πώς να χειριστεί κατάλληλα την κάθε περίπτωση.

Οι απαιτήσεις για την ασφάλεια των laptop πρέπει επίσης να μεταβιβαστούν στο πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφάλειάς. Επιτρέπεται στους υπαλλήλους να χρησιμοποιούν το laptop τους για προσωπική χρήση; Είναι μια απαίτηση ότι αυτοί δεν πρέπει να αφήνουν το laptop τους αφύλακτο ενώ είναι σε επιχειρησιακό ταξίδι; Οι λεπτομέρειες για τα laptop πρέπει να μεταβιβαστούν σαφώς αλλιώς οι υπάλληλοι θα δημιουργήσουν τους δικούς τους κανόνες για την ασφάλεια ενός εταιρικού laptop.

Οι υπάλληλοι πρέπει να εγκαταστήσουν firewall στο υπολογιστή γραφείου ή το laptop τους; Εάν αυτό συμβαίνει, είναι επιχειρησιακή ανάγκη να γνωστοποιηθεί συγκεκριμένα αυτό στους υπαλλήλους. Οι υπάλληλοι πρέπει να ξέρουν ποιος είναι ο υποτιθέμενος για να εγκαταστήσει το firewall, και πώς μπορούν να λάβουν την υποστήριξη για αυτό. Εάν αναμένεται να εγκαταστήσουν το firewall οι ίδιοι, πού μπορούν να βρουν τις οδηγίες για το πώς να κάνουν αυτό;

Θα πρέπει οι υπάλληλοι να εγκαταστήσουν τα patch ασφάλειάς τους από μόνοι τους στους υπολογιστές γραφείου και τα laptop; Ή η ομάδα υποστήριξης υποδομής θα το κάνει αυτό, ή αυτό έχει αυτοματοποιηθεί; Ανεξάρτητα από το πώς συμβαίνει αυτό, ο οργανισμός πρέπει να το εξηγήσει αυτό στους υπαλλήλους του. Εάν αναμένεται να εγκαταστήσουν μόνοι τους τα patch στα συστήματά τους, πρόκειται να παρέχετε τα γνωστά καλά patch σε αυτούς; Έχουν περάσει από test τα patches αυτά; Από πού λαμβάνονται αυτά; Εάν η ομάδα υποστήριξης ασφάλειας εγκαταστήσει στα συστήματά τους αυτόματα τα patch, πρέπει να εξηγηθεί αυτό έτσι ώστε οι υπάλληλοι να μην πηγαίνουν και λαμβάνουν αυτά τα patch μέσω του Διαδικτύου και προσπαθούν τα εγκαταστήσουν από μόνοι τους.

Αναβάθμιση και συνέχιση του προγράμματος συνειδητοποίησης και κατάρτισης

Εάν μια οργάνωση είναι μεγάλη, οι πιθανότητες είναι να έχει πολλούς νέους υπαλλήλους που έρχονται όλη την ώρα. Επομένως, πρέπει να θεσπισθεί το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφαλείας σε μια συνεχή βάση. Η ασφάλεια είναι μια συνεχής διαδικασία. Δεν είναι κάτι που μπορείς να το αντιμετωπίσεις μία φορά μόνο. Η οργάνωση και τα περιουσιακά στοιχεία της είναι πραγματικά ασφαλή μέσω της συνεχούς συνειδητοποίησης. Να κρατηθεί το momentum ασφάλειας συνεχές, και σε λίγο, οι φιλόδοξοι και δημιουργικοί υπάλληλοι θα προσφέρουν τις προτάσεις σχετικά με τον τρόπο με τον οποίο μπορεί να βελτιωθεί και να ενημερωθεί το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφαλείας.

Εάν εκτελείται το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφαλείας σε συνεχή βάση και κάθε λίγο αυτό τροποποιείται για να καταστεί κάθε φορά αποτελεσματικότερο και πιο τωρινό, θα μειωθεί πολύ η δυνατότητα έκθεσης σε κίνδυνο. Άσχετα εάν η επιχείρηση είναι ενός ατόμου ή πολλών, κάποιος είναι κύριος των περιουσιακών στοιχείων. Οι υπάλληλοί πληρώνονται για να φροντίσουν και να διαχειριστούν αυτά τα περιουσιακά στοιχεία, και να κάνοντας αυτό χωρίς προστασία συγχρόνως είναι ανεύθυνο. Οι περισσότεροι υπάλληλοι θα σεβαστούν το γεγονός ότι χρειάζονται να παίξουν το ρόλο τους στην ασφάλεια της ιδιοκτησίας αυτής.

Μια καλή συμβουλή

Το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφαλείας αξίζει πολύ το χρόνο και τα χρήματα που παίρνει για να σχεδιαστεί και να υλοποιηθεί. Η υποδομή τεχνολογιών πληροφοριών είναι πολύτιμη, και εάν πληγεί μπορεί να ασκήσει σοβαρή επίδραση στο προϋπολογισμό, πίστη πελατών, και μπορεί ακόμη και να δημιουργήσει νομικά προβλήματα. Ενώ το πρόγραμμα συνειδητοποίησης και επιμόρφωσης ασφαλείας δεν έχει καμία εγγύηση ότι η οργάνωσή δεν θα δεχθεί επίθεση από τον κυβερνοχώρο, θα μειώσει σίγουρα τον αντίκτυπο που μια τέτοια επίθεση έχει, και η διοίκηση θα είναι σε θέση ξέρει ότι έκανε τουλάχιστον μια προσπάθεια να καθιερωθεί

η συνειδητοποίηση και η κατάρτιση πάνω σε πολιτικές, διαδικασιών, και διεργασίες ασφαλείας.

6.2 Πολιτικές για συνειδητοποίηση και εκπαίδευση πάνω σε θέματα ασφαλείας

Παρακάτω περιγράφονται δυο πολιτικές που αφορούν μια για την εκπαίδευση πάνω σε θέματα ασφαλείας και μια πάνω στην συνειδητοποίηση τέτοιων θεμάτων.

6.2.1 Security Training Policy[29]

Καταλαβαίνοντας τη σημασία της ασφάλειας των υπολογιστών και τις μεμονωμένες ευθύνες και την υπευθυνότητα για την ασφάλεια υπολογιστών είναι συνυφασμένα με την επίτευξη των στόχων ασφάλειας μιας οργάνωσης. Αυτό μπορεί να επιτευχθεί με έναν συνδυασμό, με μια γενική εκπαίδευση συνειδητοποίησης σε θέματα ασφάλειας υπολογιστών και να στοχεύσει, στην παραγωγή συγκεκριμένης κατάρτισης. Η φιλοσοφία της προστασίας και συγκεκριμένες οδηγίες ασφάλειας πρέπει να διδαχθούν, και να ξανά επιβληθούν στους, τους χρήστες υπολογιστών. Οι πληροφορίες συνειδητοποίησης και κατάρτισης ασφάλειας πρέπει να αναβαθμίζονται συνεχώς και να ενισχύονται.

Σκοπός

Ο σκοπός της πολιτικής κατάρτισης ασφάλειας είναι να περιγραφούν οι απαιτήσεις που εξασφαλίζουν ότι κάθε χρήστης των πηγών πληροφοριών του Οργανισμού έχει επαρκή εκπαίδευση πάνω σε ζητήματα ασφάλειας υπολογιστών.

Εμβέλεια

Η πολιτική αυτή έχει εφαρμογή εξίσου για όλους τους χρήστες των πόρων πληροφοριών του Οργανισμού.

Πολιτική

Όλοι οι νέοι χρήστες πρέπει να ολοκληρώσουν την απαραίτητη ενότητα κατάρτισης και συνειδητοποίησης ασφάλειας πληροφοριών πριν από, ή τουλάχιστον μέσα σε 30 ημέρες από τη χορήγηση της πρόσβασης στα συστήματα του Οργανισμού. Η ενότητα κατάρτισης και συνειδητοποίησης ασφάλειας πρέπει να ξανά γίνεται ετησίως έκτοτε.
Όλοι οι χρήστες πρέπει να κάνουν μια δήλωση ότι έχουν διαβάσει και καταλαβαίνουν τις απαιτήσεις του Οργανισμού σύμφωνα με τις πολιτικές και τις διαδικασίες.
Όλοι οι χρήστες (υπάλληλοι, σύμβουλοι, ανάδοχοι, προσωρινοί, κ.λπ....) πρέπει να προμηθευτούν με ικανοποιητικό εκπαιδευτικό και ενισχυτικό υλικό για να τους επιτρέψει να προστατεύσουν κατάλληλα την υποδομή του οργανισμού.
Πρέπει να αναπτυχθεί και να διατηρηθεί μια διαδικασία επικοινωνίας μέσω του ηλεκτρονικού ταχυδρομείου και του Web για την μεταβίβαση νέου προγράμματος ασφάλειας πληροφοριών υπολογιστών, δελτία ασφάλειας πληροφοριών, και ενδιαφέροντα αντικείμενα ασφάλειας.
Παραβιάσεις της παραπάνω πολιτικής θα πρέπει αναφέρονται στο ISO.

[29] http://www.cis.tamuk.edu/help/policies/1_170_Security%20Training%20Policy.pdf

Πειθαρχικές πράξεις

Η παραβίαση αυτής της πολιτικής μπορεί να οδηγήσει σε πειθαρχική ενέργεια μέχρι και συμπεριλαμβανομένης της λήξης εργασίας για τους υπαλλήλους και τους προσωρινούς. Της λήξη των σχέσεων απασχόλησης στην περίπτωση της απόλυσης αναδόχων ή συμβούλων. Απόταξη για τους εθελοντές ή την αναστολή ή την αποβολή στην περίπτωση ενός σπουδαστή. Επιπλέον, τα άτομα αυτά υπόκεινται στην απώλεια προνομίων πρόσβασης, καθώς επίσης και ποινικές διώξεις.

6.2.2 Information Security Awareness Policy[30]

Σκοπός

Η αποτελεσματική ασφάλεια πληροφοριών απαιτεί ένα υψηλό επίπεδο συμμετοχής από όλα τα μέλη ενός οργανισμού. Αυτή η πολιτική καθορίζει τις ευθύνες και τους ρόλους για την εμφύσηση της συνειδητοποίησης ασφάλειας πληροφοριών μεταξύ όλων των ιδιοκτητών, των διευθυντών, των φορέων παροχής υπηρεσιών και των χρηστών των πηγών πληροφοριών.

Πρότυπα και οδηγίες της πολιτικής

a. Όλοι πρέπει να είναι ενήμεροι καλά για τις ευθύνες τους ως ιδιοκτήτες πληροφοριών, διευθυντές, χρήστες, και φορείς παροχής υπηρεσιών.
b. Σε συνεργασία με το γραφείο εκπαίδευσης, ο ανώτερος υπάλληλος ασφάλειας πληροφοριών είναι αρμόδιος για τη διαχείριση ενός προγράμματος κατάρτισης και συνειδητοποίησης για όλα τα μέλη της κοινότητας του οργανισμού και για τη σύσκεψη με τα μέλη του οργανισμού για ζητήματα ασφάλειας πληροφοριών.
c. Τα μαθήματα και το υλικό εκπαίδευσης πρέπει να διαποτίζουν τη σημασία του κατάλληλου χειρισμού πληροφοριών και να εξηγούν τις επιπτώσεις αυτής της πολιτικής.
d. Η κατάρτιση πρέπει να περιλαμβάνει και συγκεκριμένες πληροφορίες για τη χρήση των προφυλάξεων ασφάλειας όπως η κρυπτογράφηση, antivirus εργαλεία, διαδικασίες για backup, η φυσική ασφάλεια και συνειδητοποίηση των τακτικών κοινωνικής μηχανικής.
e. Ο ανώτερος υπάλληλος ασφάλειας πληροφοριών είναι αρμόδιος για τη διατήρηση της ιστοσελίδας ασφάλειας πληροφοριών, από όπου οι πηγές ασφαλείας πληροφοριών θα είναι διαθέσιμες στο σύνολο της κοινότητας του οργανισμού.
f. Οι διευθυντές είναι αρμόδιοι να βλέπουν ότι οι υπάλληλοι έχουν την ικανότητά εκμεταλλεύονται τους διαθέσιμους πόρους για την συνειδητοποίησης της ασφάλειας.
g. Οι κάτοχοι πληροφοριών και οι φορείς παροχής υπηρεσιών πρέπει να εξοικειωθούν με τις αρχές για τα πρότυπα ασφαλείας πληροφοριών και τις διαδικασίες ασφάλειας πληροφοριών όπως αυτές εφαρμόζονται για τους πόρους πληροφοριών υπό την αιγίδα τους.

Ορισμοί

<u>Πηγή πληροφοριών</u>

Αυτός ο όρος περιλαμβάνει τις πληροφορίες με οποιαδήποτε μορφή και καταγραμμένες σε οποιαδήποτε μέσο που ανήκει ή παράγεται από οποιοδήποτε χρήστη του οργανισμού. Οι πηγές πληροφοριών περιλαμβάνουν επίσης όλο το υπολογιστικό, δικτυακό και εξοπλισμό που χρησιμοποιούνται για την επεξεργασία

[30] http://lits.ollusa.edu/LITSNavBar/Policies/SecurityAwarenessPolicy.shtml

και την αποθήκευση πληροφοριών που ανήκουν στον οργανισμό ή χρησιμοποιούνται από τον οργανισμό στο πλαίσιο άδειας ή σύμβασης.

Κάτοχοι πληροφοριών

Οι κάτοχοι πληροφοριών είναι εκείνα τα άτομα του οργανισμού που έχουν την αρχικά την ευθύνη για ιδιαίτερες πληροφορίες. Κάποιος γίνεται κάτοχος πληροφοριών είτε από διορισμό είτε λόγω έχει αποκτήσει, αναπτύξει, δημιουργήσει πληροφορίες για τις οποίες κανένα άλλο συμβαλλόμενο μέρος δεν έχει την ιδιοκτησία. Παραδείγματος χάριν, για λόγους αυτής της πολιτικής, ο υπεύθυνος βιβλιοθήκης ενός οργανισμού είναι ο κάτοχος των πληροφοριών των καταλόγων της βιβλιοθήκης και των σχετικών αρχείων και ο γραμματέας ενός οργανισμού είναι ο κάτοχος πληροφοριών των αρχείων συνεργατών. Τα μέλη του οργανισμού θεωρούνται κάτοχοι πληροφοριών της έρευνάς τους. Ο κάτοχος πληροφοριών του όρου όπως χρησιμοποιείται εδώ δεν υπονοεί την ιδιοκτησία υπό οποιαδήποτε νομική έννοια, όπως ένας κάτοχος πνευματικών δικαιωμάτων ή ενός διπλώματος ευρεσιτεχνίας. Σε αυτό το πλαίσιο, ο κάτοχος πληροφοριών σημαίνει μόνο το πρόσωπο με την αρχική ευθύνη για μια πηγή πληροφοριών.

Χρήστες

Όλα τα μέλη του οργανισμού είναι "χρήστες" των πηγών πληροφοριών, ακόμα κι αν δεν έχουν ευθύνη τους. Οι χρήστες περιλαμβάνουν:προσωπικό, ανάδοχοι, σύμβουλοι, εθελοντές, και προσωρινοί υπάλληλοι.

Φορείς παροχής υπηρεσιών

Οι φορείς παροχής υπηρεσιών είναι εκείνα τα γραφεία, μονάδες τμήματα και άτομα που διαχειρίζονται σημαντικές πηγές και συστήματα πληροφοριών με σκοπό να τα καταστήσουν διαθέσιμα σε άλλους. Περιλαμβάνει όλα τα τμήματα ενός οργανισμού.

Διευθυντές

Οι διευθυντές είναι εκείνοι που επιτηρούν τις καθημερινές διαδικασίες και τις δραστηριότητες άλλων υπαλλήλων ή χρηστών σε ένα γραφείο, μια μονάδα ή ένα τμήμα ενός οργανισμού.

Συμμόρφωση

Όλοι οι επικεφαλής τμημάτων του οργανισμού και διοικητές είναι αρμόδιοι για την συμμόρφωση των υπαλλήλων και συνολικά του οργανισμού με αυτήν την πολιτική. Οι παραβιάσεις αυτής της πολιτικής θα αντιμετωπιστούν σοβαρά και μπορούν να οδηγήσουν στην πειθαρχική ενέργεια σύμφωνα με τις διαδικασίες του οργανισμού.

Εικόνα 32:IT Security Training

Κεφάλαιο 7

Επίλογος-Συμπεράσματα

Στα πλαίσια αυτής εδώ της πτυχιακής εργασίας είδαμε το τι πρέπει να κάνει ένας οργανισμός, υπηρεσία, επιχείρηση για πιστοποιηθεί στα πλαίσια του ISO 27001. Δηλαδή είδαμε τα βήματα που πρέπει να ακολουθήσει για πιστοποιηθεί. Τον προσδιορισμό περιβάλλοντος του, καταγραφή της δραστηριότητας του και της πληροφοριακής δομής του. Εξέτασης της ήδη υπάρχουσας ασφαλείας και προσδιορισμός του νομικού και κανονιστικού πλαισίου ασφαλείας. Στην συνέχεια η αξιολόγηση και η διαχείριση των κινδύνων και των αδυναμιών του οργανισμού. Και τέλος η ανάπτυξη του συστήματος διαχείρισης ασφαλείας πληροφοριών σαν αποτέλεσμα των παραπάνω ενεργειών.

Παρουσιάσαμε πηγές για πολιτικές ασφαλείας και εργαλεία για την διαχείριση τους. Συγκεκριμένα ιστοσελίδες από το Internet για την εύρεση πολιτικών και εργαλείων. Συνοπτική παρουσίαση κάποιων πηγών πολιτικών ασφαλείας. Παρουσίαση και λειτουργία εργαλείων για την δημιουργία πολιτικών και λύσεων ασφαλείας.

Έγινε παρουσίαση πολιτικών ασφαλείας και εφαρμογή τους στα πλαίσια ενός εκπαιδευτικού οργανισμού για την ορθή χρήση των υποδομών του. Και τέλος εκπαίδευση και συνειδητοποίηση πάνω σε θέματα ασφαλείας, με πολιτικές και οδηγίες.

Παράρτημα

8.1 Πολιτικές ασφαλείας στα Αγγλικά

Εδώ παρουσιάζονται μερικές από τις πολιτικές ασφαλείας στα αγγλικά που έχουν μεταφραστεί στα πλαίσια αυτής εδώ της πτυχιακής. Παρακάτω ακολουθεί η λίστα με αυτές τις πολιτικές:

1. **Acceptable Use Policy**
2. **Analog/ISDN Line Security Policy**
3. **Backup policy**
4. **Dial-in Access Policy**
5. **DMZ Lab Security Policy**
6. **Network Security Policy**
7. **Privacy Policy**
8. **Remote Access**
9. **Router Security Policy**

8.1.1 Acceptable Use Policy[31]

Control

Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.

Implementation guidance

All employees, contractors and third party users should follow rules for the acceptable use of information and assets associated with information processing facilities, including:

a. rules for electronic mail and Internet usages;
b. guidelines for the use of mobile devices, especially for the use outside the premises of the organization;

Specific rules or guidance should be provided by the relevant management. Employees, contractors and third party users using or having access to the organization's assets should be aware of the limits existing for their use of organization's information and assets associated with information processing facilities, and resources. They should be responsible for their use of any information processing resources, and of any such use carried out under their responsibility.

[31] Από το ISO 27002

8.1.2 Analog/ISDN Line Security Policy[32]

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

This document explains <Company Name> analog and ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

2.0 Scope

This policy covers only those lines that are to be connected to a point inside <Company Name> building and testing sites. It does not pertain to ISDN/phone lines that are connected into employee homes, PBX desktop phones, and those lines used by Telecom for emergency and non-corporate information purposes.

3.0 Policy

3.1 Scenarios & Business Impact

There are two important scenarios that involve analog line misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of analog line numbers in the hope of connecting to a computer that has a modem attached to it. If the modem answers (and most computers today are configured out-of-the-box to auto-answer) from inside <Company Name> premises, then there is the possibility of breaching <Company Name>'s internal network through that computer, unmonitored. At the very least, information that is held on that computer alone can be compromised. This potentially results in the loss of millions of dollars worth of corporate information.

The second scenario is the threat of anyone with physical access into a <Company Name> facility being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted networking of <Company Name> through the computer's Ethernet connection, and then call out to an unmonitored site using the modem, with the ability to siphon <Company Name> information to an unknown location. This could also potentially result in the substantial loss of vital information. Specific procedures for addressing the security risks inherent in each of these scenarios follow.

3.2 Facsimile Machines

As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.
- No fax lines will be installed for personal use.

[32] http://www.sans.org/resources/policies/Analog_Line_Policy.pdf

- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a centralized administrative area designated for departmental use, and away from other computer equipment.
- A computer which is capable of making a fax connection is not to be allowed to use an analog line for this purpose.
- Waivers for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request.
- Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:
- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- When in use, the computer is to be physically disconnected from <Company Name>'s internal network.
- The line will be used solely for <Company Name> business, and not for personal reasons.
- All downloaded material, prior to being introduced into <Company Name> systems and networks, must have been scanned by an approved anti-virus utility (e.g., McAfee VirusScan) which has been kept current through regular updates.

3.3 Computer-to-Analog Line Connections

The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within <Company Name> will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to <Company Name>, and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case by case basis. Replacement lines, such as those requeested because of a move, fall under the category of "new" lines. They will also be considered on a case by case basis.

3.4 Requesting an Analog/ISDN Line

Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to Telecom:

- A clearly detailed business case of why other secure connections available at <Company Name> cannot be used,
- The business purpose for which the analog line is to be used,
- The software and hardware to be connected to the line and used across the line,
- And to what external connections the requester is seeking access.

The business case must answer, at a minimum, the following questions:

- What business needs to be conducted over the line?
- Why is a <Company Name>-equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?

- Why is <Company Name>'s current dial-out access pool unable to accomplish the same tasks as an analog line?
- In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:
- Will the machines that are using the analog lines be physically disconnected from <Company Name>'s internal network?
- Where will the analog line be placed? A cubicle or lab?
- Is dial-in from outside of <Company Name> needed?
- How many lines are being requested, and how many people will use the line?
- How often will the line be used? Once a week, 2 hours per day...?
- What is the earliest date the line can be terminated from service?
- The line must be terminated as soon as it is no longer in use.
- What other means will be used to secure the line from unauthorized use?
- Is this a replacement line from an old location? What was the purpose of the original line?
- What types of protocols will be run over the line?
- Will a <Company Name>-authorized anti-virus scanner be installed on the machine(s) using the analog lines?
- The requester should use the Analog/ISDN Line Request Form to address these issues and submit a request.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.1.3 Backup Policy[33]

Control

Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Implementation guidance

Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
The following items for information back up should be considered:

a. the necessary level of back-up information should be defined;
b. accurate and complete records of the back-up copies and documented restoration procedures should be produced;
c. the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization;
d. the back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
e. back-up information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;
f. back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;
g. restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;
h. in situations where confidentiality is of importance, back-ups should be protected by means of encryption. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. For critical systems, the backup arrangements should cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information, and also any requirement for archive copies to be permanently retained should be determined.

Other information

Back up arrangements can be automated to ease the back-up and restore process. Such automated solutions should be sufficiently tested prior to implementation and at regular intervals.

[33] Από το ISO 27002

8.1.4 Dial-In Access Policy[34]

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

The purpose of this policy is to protect <Company Name>'s electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

2.0 Scope

The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

3.0 Policy

<Company Name> employees and authorized third parties (customers, vendors, etc.) can use dial-in connections to gain access to the corporate network. Dial-in access should be strictly controlled, using onetime password authentication. [Add something in about how "Dial –in access should be requesting using the corporate account request process"] It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to <Company Name> is not used by non-employees to gain access to company information system resources.
An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and <Company Name> are literal extensions of <Company Name>'s corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect
<Company Name>'s assets. Analog and non-GSM digital cellular phones cannot be used to connect to <Company Name>'s corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to <Company Name>'s network. For additional information on wireless access to the <Company Name> network, consult the *Wireless Communications Policy*.
Note: Dial-in accounts are considered 'as needed' accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

[34] http://www.sans.org/resources/policies/Dial-in_Access_Policy.pdf

8.1.5 DMZ Lab Security Policy[35]

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in <Company Name> labs located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to <Company Name> from the damage to public image caused by unauthorized use of <Company Name> resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope

<Company Name> Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside <Company Name> corporate Internet firewalls are considered part of the DMZ Labs and are subject to this policy. This includes DMZ Labs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to labs residing inside <Company Name>'s corporate Internet firewalls. Standards for these labs are defined in the *Internal Lab Security Policy*

3.0 Policy

3.1. Ownership and Responsibilities

1. All new DMZ Labs must present a business justification with sign-off at the business unit Vice President level. InfoSec must keep the business justifications on file.
2. Lab owning organizations are responsible for assigning lab managers, point of contact (POC), and back up POC, for each lab. The lab owners must maintain up to date POC information with InfoSec [and the corporate enterprise management system, if one exists]. Lab managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ
4. Labs must be requested through a <Company Name> Network Support Organization and approved by InfoSec.
5. All ISP connections must be maintained by a <Company Name> Network Support Organization.
6. A Network Support Organization must maintain a firewall device between the DMZ Lab(s) and the Internet.

[35] http://www.sans.org/resources/policies/DMZ_Lab_Security_Policy.pdf

7. The Network Support Organization and InfoSec reserve the right to interrupt lab connections if a security concern exists.
8. The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the Network Support Organization point of demarcation.
9. The Network Support Organization must record all DMZ Lab address spaces and current contact information [in the corporate enterprise management system, if one exists].
10. The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.
11. Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*
12. Individual lab accounts must be deleted within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
13. InfoSec will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production resources must not depend upon resources on the DMZ Lab networks.
2. DMZ Labs must not be connected to <Company Name>'s corporate internal networks, either directly or via a wireless connection.
3. DMZ Labs should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.
4. Lab Managers are responsible for complying with the following related policies:
    a. *Password Policy*
    b. *Wireless Communications Policy*
    c. Lab Anti-Virus Policy
5. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs. All firewall filters will be maintained by InfoSec.
6. The firewall device must be the only access point between the DMZ Lab and the rest of <Company Name>'s networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec (including both general configurations and rule sets). InfoSec may require additional security measures as needed.
8. Traffic from DMZ Labs to the <Company Name> internal network, including VPN access, falls under the *Remote Access Policy*
9. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
10. Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards. [Add url link to site where your internal configuration standards are kept].

11. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/ hotfixes.
12. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/ hotfixes.
13. Services and applications not serving business requirements must be disabled.
14. <Company Name> Confidential information is prohibited on equipment in labs where non- <Company Name> personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy*
15. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Definitions

Access Control List (ACL):
Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

DMZ (de-militarized zone):
Networking that exists outside of <Company Name> primary corporate firewalls, but is still under <Company Name> administrative control.

Network Support Organization:
Any InfoSec-approved support organization that manages the networking of non-lab networks.

Least Access Principle:
Access to services, hosts, and networks is restricted unless otherwise permitted.

Internet Services:
Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.

Network Support Organization Point of Demarcation:
The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or firewall.

Lab Manager:
The individual responsible for all lab activities and personnel.

Lab:
A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.

Firewall:
A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by InfoSec.

Internally Connected Lab:
A lab within <Company Name>'s corporate firewall and connected to the corporate production network.

8.1.6 Network Security Policy[36]

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure. The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection. Additional controls may also be required to protect sensitive information passing over public networks.

Network controls

Control

Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Implementation guidance

Network managers should implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a. operational responsibility for networks should be separated from computer operations where appropriate;
b. responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established;
c. special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications (see 11.4 and 12.3); special controls may also be required to maintain the availability of the network services and computers connected;
d. appropriate logging and monitoring should be applied to enable recording of security relevant actions;
e. management activities should be closely co-ordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure.

Other information

Additional information on network security can be found in ISO/IEC 18028, *Information technology –Security techniques – IT network security.*

[36] Από το ISO 27002

Security of network services

Control

Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided inhouse or outsourced.

Implementation guidance

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels, and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Other information

Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and intrusion detection systems.

These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a. technology applied for security of network services, such as authentication, encryption, and network connection controls;
b. technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
c. procedures for the network service usage to restrict access to network services or applications, where necessary.

8.1.7 Privacy Policy[37]

Control

Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

Implementation guidance

An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information. Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who should provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personal information and ensuring awareness of the data protection principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personal information should be implemented.

Other information

A number of countries have introduced legislation placing controls on the collection, processing, and transmission of personal data (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing, and disseminating personal information, and may restrict the ability to transfer that data to other countries.

[37] Από το ISO 27002

8.1.8 Remote Access Policy[38]

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

The purpose of this policy is to define standards for connecting to <Company Name>'s network from any host. These standards are designed to minimize the potential exposure to <Company Name> from damages which may result from unauthorized use of <Company Name> resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical <Company Name> internal systems, etc.

2.0 Scope

This policy applies to all <Company Name> employees, contractors, vendors and agents with a <Company Name>-owned or personally-owned computer or workstation used to connect to the <Company Name> network. This policy applies to remote access connections used to do work on behalf of <Company Name>, including reading or sending email and viewing intranet web resources.
Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of <Company Name> employees, contractors, vendors and agents with remote access privileges to <Company Name>'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Company Name>.
2. General access to the Internet for recreational use by immediate household members through the <Company Name> Network on personal computers is permitted for employees that have flat-rate services. The <Company Name> employee is responsible to ensure the family member does not violate any <Company Name> policies, does not perform illegal activities, and does not use the access for outside business interests. The <Company Name> employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of <Company Name>'s network:

[38] http://www.sans.org/resources/policies/Remote_Access_Policy.pdf

a. *Acceptable Encryption Policy*
b. *Virtual Private Network (VPN) Policy*
c. *Wireless Communications Policy*
d. *Acceptable Use Policy*

4. For additional information regarding <Company Name>'s remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any <Company Name> employee provide their login or email password to anyone, not even family members.
3. <Company Name> employees and contractors with remote access privileges must ensure that their <Company Name>-owned or personal computer or workstation, which is remotely connected to <Company Name>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. <Company Name> employees and contractors with remote access privileges to <Company Name>'s corporate network must not use non-<Company Name> email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct <Company Name> business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the <Company Name> network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to <Company Name> internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to <Company Name>'s networks must meet the requirements of <Company Name>-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the <Company Name> production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Cable Modem:
Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP:
Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.

DLCI:
Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem:
A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing:
Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the corporate network via a local Ethernet connection, and dialling into AOL or other Internet service provider (ISP). Being on a <Company Name>- provided Remote Access home network, and connecting to another network, such as a spouse's remote.

8.1.9 Router Security Policy[39]

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of <Company Name>.

2.0 Scope

All routers and switches connected to <Company Name> production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

3.0 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
5. Use corporate standardized SNMP community strings.
6. Access rules are to be added as business needs arise.
7. The router must be included in the corporate enterprise management system with a designated point of contact.
8. Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."
9. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

[39] http://www.sans.org/resources/policies/Router_Security_Policy.pdf

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Production Network:
The "production network" is the network used in the daily business of <Company Name>. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to <Company Name> employees or impact their ability to do work.

Lab Network:
A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to <Company Name> nor affect the production network.

6.0 Revision History

2007-04-18
• Added 3.0.8 “Telnet”

Βιβλιογραφία

- Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών-Τεχνική Προσέγγιση INNOVA A.E.
- Cisco web tools :http://www.ciscowebtools.com/spb/ .
- Cisco Security Policy Designer http://www.ciscowebtools.com/spb/
- Cisco Security Solution Designer http://www.ciscowebtools.com/designer/
- CIS Tamuk http://www.cis.tamuk.edu/help/policies/1_170_Security%20Training%20Policy.pdf
- Disaster Recovery Toolkit :http://www.businesscontinuityworld.com/access.htm
- HIMSS Privacy Security: http://www.himss.org/ASP/privacySecurityTree.asp?faid=78&tid=4#PSToolkit#PSToolkit.
- International Standard ISO/IEC 27001 Information Technology, code of practice for information security management.
- Intranet Journal http://www.intranetjournal.com/articles/200410/ij_10_11_04a.html
- ISO 17999 Security Policies: http://www.17799-toolkit.com/17799policies.htm.
- L.L.U:http://lits.ollusa.edu/LITSNavBar/Policies/SecurityAwarenessPolicy.shtml
- OSCE Gender and Security Sector Reform Toolkit: :http://www.osce.org/item/29669.html
- SANS Institute, The SANS Security Policy Project, http://www.sans.org/resources/policies
- SOFOTEX Callio Toolkit:http://www.sofotex.com/Callio-Toolkit-17799-download_L20800.html
- SSi Security Management: http://www.securednetworking.com/network_security_management.htm
- The free Encyclopedia http://www.wikipedia.com
- Tivoli Security Policy Manager : http://www-01.ibm.com/software/tivoli/products/security-policy-mgr/
- UCISA Information Security Toolkit: http://www.ucisa.ac.uk/Home/members/activities/ist.aspx.
- Zone Labs Security Policy Management Toolkit: http://www.networkworld.com/news/2002/0205zlabs.html