Πλαίσιο ανάπτυξης πολιτικής ασφάλειας παρόχου διαδικτυακών υποδομών και υπηρεσιών

Διπλωματική εργασία

Κατατίθεται για την απόκτηση
του διπλώματος στο τμήμα Μηχανικών Η/Υ,
τηλ/ων και δικτύων του Πανεπιστημίου Θεσσαλίας

Αθηνά Μπασιούκα

Επιβλέποντες καθηγητές: Τασιούλας Λέανδρος
Ηλιούδης Χρήστος

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Πώς έχει επηρεάσει η τεχνολογία των υπολογιστικών δικτύων την ζωή μας; Πώς έχει επιδράσει στην οικονομία, την επιχειρηματικότητα, την επικοινωνία μας και την καθημερινότητά μας;

«Πολύ θετικά», θα πει κάποιος με μια πρώτη σκέψη. Και πράγματι, η θετική επιρροή του Διαδικτύου, εξαιρετικά δύσκολα μπορεί να αμφισβητηθεί. Οι αρχαίοι έλληνες από την άλλη, έλεγαν «ουδέν καλόν αμιγές κακού» για να επιβεβαιωθούν ακόμη και στην περίπτωση των νέων τεχνολογιών. Το Internet έφερε πολλά καλά, και κάπου μέσα σε αυτόν τον σωρό των καλών, έφερε και τα άσχημα.

Πώς οριοθετούμε την ασφάλεια στο διαδίκτυο λοιπόν; Αφενός, όπως και στην πραγματική ζωή, με την επιβολή μέτρων και κανόνων. Αφετέρου, χρησιμοποιώντας υπέρ μας το όπλο της τεχνολογίας: αναπτύσσοντας τα κατάλληλα λογισμικά και θέτοντάς τα σε λειτουργία.

Το πρώτο βήμα, ο καθορισμός δηλαδή της λειτουργίας ενός δικτύου που χαρακτηρίζεται ως επιτρεπτή, είναι η βάση στην οποία στηρίζεται όλο το υπόλοιπο σύστημα. Η βάση αυτή στα δίκτυα ονομάζεται «πολιτική ασφάλειας» και πρόκειται για ένα κείμενο το οποίο σε ανθρώπινη γλώσσα εξηγεί τι επιτρέπεται και τι δεν επιτρέπεται να κάνει ένας χρήστης. Την χαρακτηρίζουμε στην πορεία της παρούσας εργασίας ως *πρωταρχικό δομικό στοιχείο* της ασφάλειας.

Στην παρούσα διπλωματική λοιπόν, μελετάμε – ανά κεφάλαιο – τα εξής:

Δεύτερο κεφάλαιο διπλωματικής εργασίας

Εξηγούμε λεπτομερειακά τι είναι μια πολιτική ασφάλειας περιγράφοντας τα χαρακτηριστικά της, τα περιεχόμενα που πρέπει να έχει και παρουσιάζοντας τα εμπλεκόμενα σε αυτή μέρη.

Στην πορεία του κεφαλαίου αυτού, γίνεται σαφές ότι η πολιτική ασφάλειας είναι ταυτισμένη με την έννοια της συμμόρφωσης.

Η πολιτική ασφάλειας είναι ένα σημαντικό κείμενο, όχι μόνο επειδή θέτει τα όρια, αλλά και επειδή είναι ενδεικτική της γενικότερης φιλοσοφίας και κουλτούρας ενός οργανισμού που διαθέτει τηλεπικοινωνιακό δίκτυο. Και μπορεί η πολιτική ασφάλειας να χρειάζεται σε όλους όσους έχουν πληροφοριακό δίκτυο, το περιεχόμενό της όμως διαφοροποιείται και προσαρμόζεται στην κάθε περίπτωση.

Στο δεύτερο κεφάλαιο γίνεται επίσης παρουσίαση των τρόπων διαφύλαξης επικοινωνιών και πληροφοριών: κρυπτογραφικοί αλγόριθμοι, passwords, antivirus προγράμματα.

Η ασφάλεια είναι μια πολυπαραγοντική διαδικασία που αφορά τους πάντες στο Internet: τον πάροχο δικτύου, τον οργανισμό, τους μόνιμους χρήστες, τους επισκέπτες.

Τρίτο κεφάλαιο διπλωματικής εργασίας

Συνεχίζοντας την θεωρητική προσέγγιση των πολιτικών ασφάλειας, σε αυτό το κεφάλαιο ορίζουμε το πλαίσιο σύμφωνα με το οποίο πρέπει να υλοποιείται μία πολιτική ασφάλειας ανεξαρτήτως περιβάλλοντος, εξωτερικών παραγόντων, χρονικής περιόδου και συγκεκριμένων οργανισμών.

Εδώ είναι το σημείο που αναλύουμε την έννοια του risk analysis κάνοντας μια εκτενή αναφορά σε αυτό, η οποία κινείται στον άξονα: Πιθανότητα (αναφορά στην

στατιστική Bayes) εμφάνισης ενός επεισοδίου ασφάλειας – επιπτώσεις στην εύρυθμη λειτουργία του δικτύου ενός οργανισμού. Η παρουσίαση του τρόπου λειτουργίας της δημοφιλούς μεθόδου ανάλυσης και διαχείρισης επικινδυνότητας CRAMM (CCTA Risk Analysis and Management Method) υποδεικνύει μέσα από αριθμημένα βήματα πώς λαμβάνει χώρα μια τέτοια διαδικασία. *Η ανάλυση της επικινδυνότητας (risk analysis) υποδεικνύει τα μέτρα που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν το σύστημα*. Η προαναφερθείσα μεθοδολογία υιοθετεί την έννοια της επικινδυνότητας (προέρχεται από το χώρο της χρηματοοικονομικής διοίκησης), η οποία εξαρτάται από την πιθανότητα πραγματοποίησης ενός επεισοδίου ασφάλειας και από το κόστος που αυτό θα επιφέρει.

Πέρα από τα ζητήματα διαχείρισης software, hardware και ανθρώπινου δυναμικού, στο κεφάλαιο αυτό φαίνεται επίσης ο συσχετισμός της πολιτικής ασφάλειας και με την διαχείριση φυσικών καταστροφών που μπορεί να προκύψουν.

Από το κεφάλαιο 3 δεν θα μπορούσε να απουσιάζει η παρουσίαση του νομικού πλαισίου, που δείχνει τον συσχετισμό της τεχνολογίας με την κοινωνία.

Τέταρτο κεφάλαιο διπλωματικής εργασίας

Έπειτα από την θεωρητική και εκτενή αναφορά στις διαδικασίες της ανάλυσης ρίσκου και αποτίμησης κινδύνου, εδώ κάνουμε μία παρουσίαση κάποιων γνωστών λογισμικών, που χρησιμοποιούνται για τον σκοπό αυτό. Καίριος είναι ο ρόλος της ανάλυσης ρίσκου: ποιοι κίνδυνοι υφίστανται; Ποιοι είναι οι πόροι που χρήζουν προστασίας; Αυτά είναι τα ερωτήματα που πρέπει να απαντηθούν πρωτίστως και στην συνέχεια να προταθούν μέτρα. Αυτή η δουλειά γίνεται πλέον από μία σειρά λογισμικών, τα λεγόμενα risk analysis tools. Στο τέταρτο κεφάλαιο της εργασίας παρουσιάζονται κάποια από τα πιο γνωστά εργαλεία που χρησιμοποιούνται για τον σκοπό αυτό. Μεταξύ των διαφόρων εργαλείων παρατηρούνται σημαντικές διαφορές που έχουν να κάνουν με παράγοντες κόστους, εξάρτησης ή όχι από άλλα λογισμικά, δημιουργίας report στο τελευταίο στάδιο και πολλά άλλα.

Πέμπτο κεφάλαιο διπλωματικής εργασίας

Στο πέμπτο κεφάλαιο παρουσιάζουμε το εργαλείο ανάλυσης ρίσκου και αποτίμησης κινδύνων (Security Assesment Tool-SAT) το οποίο κατασκευάσαμε εμείς. Στο εργαλείο αυτό επιχειρήσαμε να συλλέξουμε μία σειρά ερωτήσεων που να καλύπτει τα πλέον συνηθισμένα και συχνά ζητήματα ασφάλειας που προκύπτουν σε ένα δίκτυο.

Μια συνοπτική περιγραφή της λειτουργίας του εργαλείου είναι η εξής: Ο χρήστης δημιουργεί ένα προφίλ, συμπληρώνει ένα ερωτηματολόγιο και στο τελευταίο βήμα λαμβάνει μία γραπτή αναφορά που του υποδεικνύει τα κενά ασφάλειας ή κάνει ορισμένες συμπληρώσεις στα ήδη υπάρχοντα μέτρα.

Εργαλεία όπως αυτό, είναι ουσιαστικοί σύμμαχοι στην εφαρμογή μιας ορθής, εύχρηστης και κατά το δυνατόν πληρέστερης πολιτικής ασφαλείας.

Έκτο κεφάλαιο διπλωματικής εργασίας

Το κεφάλαιο αυτό φέρει τον τίτλο «Συμπεράσματα και μελλοντικές επεκτάσεις». Όπως εύκολα αντιλαμβάνεται κανείς, βγαίνει ένα γενικό συμπέρασμα από την παρούσα διπλωματική εργασία και γίνονται κάποιες προτάσεις σε κάποιον που θα θελήσει να επεκτείνει το λογισμικό που φτιάξαμε.

Στο τέλος της εργασίας, υπάρχει ένα παράρτημα κώδικα, στο οποίο γίνονται αναφορές μέσω του πέμπτου κεφαλαίου, ενώ ο συνολικός κώδικας του λογισμικού, βρίσκεται σε ξεχωριστό αρχείο pdf.

Κεφάλαιο 2

Πλαίσιο ανάπτυξης

Εισαγωγή – Ορισμός

Θεωρώντας το σύνολο των προβλημάτων ασφάλειας που καλείται να αντιμετωπίσει σήμερα ένα πληροφοριακό σύστημα και λαμβάνοντας υπόψη τους τρόπους αντιμετώπισης των κινδύνων αυτών, εύκολα αντιλαμβανόμαστε ότι η δημιουργία μιας πολιτικής ασφάλειας που να ανταποκρίνεται στις απαιτήσεις λειτουργίας ενός συστήματος είναι πρωταρχικής σημασίας.

Η ουσία της πολιτικής ασφάλειας εμπεριέχεται στον ορισμό της ο οποίος συμπυκνώνει το νόημά της. Πρόκειται στην ουσία για ένα σύνολο από αρχές και οδηγίες **υψηλού επιπέδου** που αφορούν τη σχεδίαση και διαχείριση συστημάτων ασφαλείας, υποδεικνύοντας με τον τρόπο αυτό πώς πρέπει να λειτουργεί ένας οργανισμός.

Παρακάτω, θα εξετάσουμε τη σημασία της ύπαρξης πολιτικής ασφάλειας σε ένα δίκτυο και θα κατανοήσουμε γιατί αυτή κρίνεται απαραίτητη. Θα δούμε τα χαρακτηριστικά της και τα εμπλεκόμενα μέρη σε αυτή. Το μεγαλύτερο μέρος του κεφαλαίου αυτού, αφιερώνεται στον καθορισμό του πλαισίου, σύμφωνα με το οποίο πρέπει να αναπτύσσεται και να εφαρμόζεται η πολιτική ασφάλειας. Θα εξετάσουμε ζητήματα όπως είναι η πολιτική πρόσβασης σε ένα δίκτυο και τα δεδομένα του και θα σταθούμε στο ζήτημα της προστασίας προσωπικών δεδομένων μελετώντας πώς η πολιτική ασφάλειας μπορεί να συμβάλει στο καίριο αυτό θέμα. Στη συνέχεια, θα μιλήσουμε για συγκεκριμένα θέματα πάνω στην ασφάλεια δικτύων όπως είναι η τήρηση αντιγράφων ασφαλείας και η ασφάλεια περιμέτρου, πάντα όμως μέσα από το πρίσμα του καθορισμού τους από μία πολιτική ασφάλειας. Θα δούμε το ζήτημα της εγκατάστασης και διαχείρισης τηλεπικοινωνιακού εξοπλισμού και πώς αυτά μπορούν να γίνουν σε ένα δίκτυο χωρίς να επιφέρουν προβλήματα ή κάποιου είδους δυσλειτουργίες. Θα δούμε πώς συμβάλει η πολιτική ασφάλειας στη χρήση κρυπτογραφικών αλγορίθμων και κωδικών ασφάλειας και γενικότερα θα οριστεί το πλαίσιο αποδεκτής χρήσης ενός δικτύου μέσα από τα δικαιώματα και τις υποχρεώσεις χρηστών και παρόχων δικτύου.

Ποιους αφορά η πολιτική ασφάλειας

Η πολιτική ασφάλειας *είναι το πρωταρχικό δομικό στοιχείο για κάθε προσπάθεια εφαρμογής ασφάλειας πληροφοριών σε δίκτυα.* Ορίζει την γενική προσέγγιση που ένας οργανισμός θα πρέπει να έχει προς την κατεύθυνση της υλοποίησης ασφάλειας, χωρίς όμως να παρέχει τεχνικές λεπτομέρειες. Οτιδήποτε προκύπτει από αυτή είναι υποχρεωτικό για όλα τα μέλη του προσωπικού ενός οργανισμού. Πιο συγκεκριμένα, αναφέρεται σε δύο βασικούς συντελεστές: 1) Δρώντα υποκείμενα και 2) Αντικείμενα (και/ή) δεδομένα που πρέπει να προστατευθούν.

Πηγαίνοντας ένα βήμα πιο πέρα, επισημαίνουμε ότι η ασφάλεια και η μυστικότητα των πληροφοριακών συστημάτων εννοιολογικά κατοπτρίζεται στα ακόλουθα επίπεδα [1]:

- Γενικές αρχές (generic principles): Πρόκειται για κοινωνικά και πολιτικά εξαρτημένες αρχές που κυβερνούν την ασφάλεια δεδομένων και πληροφοριακών συστημάτων.
- Αρχές (principles): Προκύπτουν από τις γενικές αρχές όταν αυτές εξετάζονται στα πλαίσια του συγκεκριμένου διαχειριστικού περιβάλλοντος που εξετάζουμε.
- Οδηγίες (quidelines): Πρόκειται για συγκεκριμένα λειτουργικά βήματα που θα πρέπει να ακολουθούνται από τα μέλη του προσωπικού με σκοπό την ικανοποίηση μια συγκεκριμένης αρχής και προκύπτουν όταν οι αρχές εξετάζονται στα πλαίσια ενός συγκεκριμένου τεχνολογικού περιβάλλοντος.
- Κανόνες (measures): Προκύπτουν από τις οδηγίες, όταν αυτές εξετάζονται μέσα σε ένα συγκεκριμένο περιβάλλον εγκατάστασης.

Η πολιτική ασφάλειας ενός οργανισμού αφορά τα δύο μεσαία επίπεδα. Αποτελείται δηλαδή από ένα σύνολο αρχών, καθεμία από τις οποίες αναλύεται σε ένα σύνολο οδηγιών. Στην τελική της μορφή εκφράζεται ως ένα σύνολο από κανόνες που προσδιορίζουν επακριβώς το ρόλο κάθε εμπλεκόμενου μέσα σε μία εταιρία ή έναν οργανισμό, ορίζει τα δικαιώματα ελέγχου προσπέλασης και διασαφηνίζει οτιδήποτε μπορεί να προκύψει σε έναν οργανισμό σχετικά με ζητήματα ασφάλειας.

Γενικά χαρακτηριστικά πολιτικής ασφάλειας

Τα στοιχεία που πρέπει να περιλαμβάνει μια πολιτική ασφάλειας είναι τα ακόλουθα [2]:

- Αγαθά: είναι οι οντότητες, δηλαδή το υλικό, λογισμικό και οι πληροφορίες του πληροφοριακού συστήματος που **έχουν αξία και πρέπει να προστατευθούν.**
- Ρόλοι και αρμοδιότητες: πρόκειται για τα **καθήκοντα και τις αρμοδιότητες του κάθε ρόλου** για θέματα που αφορούν το πληροφοριακό σύστημα και την ασφάλειά του.
- Στόχοι: όπως υποδηλώνεται, πρόκειται για τον **στόχο** ασφάλειας που θα **καθορίσει** την γενικότερη πολιτική.
- Πεδίο εφαρμογής της πολιτικής ασφάλειας: είναι η **εμβέλεια**, η έκταση και ο χώρος που αφορά η πολιτική ασφάλειας.
- Οδηγίες, κατευθυντήριες γραμμές.
- Κουλτούρα, άλλες πολιτικές, νομοθεσία: αφορά το σύνολο των πεποιθήσεων, αξιών και νόμων που **συνθέτουν την κουλτούρα του οργανισμού** και του περιβάλλοντός του και ανατροφοδοτούν τους μηχανισμούς του μέσω μιας διαδικασίας συνεχούς εκμάθησης.
- Υλοποίηση και εφαρμογή της πολιτικής ασφάλειας – Ενημέρωση και συμμόρφωση: Πρόκειται γα το **οργανωτικό πλαίσιο** ρόλων, αρμοδιοτήτων, κανονισμών για την υλοποίηση και εφαρμογή της πολιτικής ασφάλειας, για την **ενημέρωση του προσωπικού** σχετικά με τη **συμμόρφωση** και τις ενέργειες που λαμβάνονται στην **περίπτωση παραβίασης** της πολιτικής ασφάλειας.
- Επισκόπηση και αναθεώρηση της πολιτικής: είναι η αναθεώρηση της πολιτικής όταν αυτό χρειάζεται και καθορίζεται από τις εκάστοτε συνθήκες έτσι ώστε να είναι επίκαιρη και να καλύπτει τις απαιτήσεις του πληροφοριακού συστήματος σε κάθε αλλαγή που μπορεί να παρουσιαστεί και σε κάθε νέα ανάγκη που μπορεί να προκύψει.

Τα βασικά χαρακτηριστικά της πολιτικής ασφάλειας εκφράζονται στις παρακάτω απαιτήσεις [2]:

1. Η πολιτική ασφάλειας απαιτεί συμμόρφωση από το προσωπικό του οργανισμού. Οι κανονισμοί που δηλώνονται μέσω αυτής καθορίζουν οτιδήποτε αφορά την ασφάλεια του πληροφοριακού συστήματος και γι' αυτό η πολιτική ασφάλειας πρέπει να είναι διαθέσιμη πάντα στους εργαζόμενους.
2. Εκφράζει γενικότερες απόψεις ή αρχές του οργανισμού. Όπως άλλωστε είδαμε, η υλοποίηση της πολιτικής ασφάλειας επηρεάζεται από την υπάρχουσα κουλτούρα και το γενικότερο σύνολο αρχών και πεποιθήσεων.
3. Οφείλει να είναι σαφής ώστε να μην παρουσιάζονται δυσκολίες στην κατανόησή της και να είναι απαλλαγμένη από μη απαραίτητους τεχνικούς όρους.
4. Πρέπει να είναι εφαρμόσιμη από άποψη κόστους.
5. Μια μελλοντική επέκταση στο πληροφοριακό σύστημα του οργανισμού πρέπει να μπορεί εύκολα να αποτυπωθεί στην ήδη

υπάρχουσα πολιτική ασφάλειας. Πρέπει δηλαδή να είναι επεκτάσιμη.

6. Η τροποποίηση της πολιτικής ασφάλειας πρέπει να γίνεται μόνο όταν συμβαίνουν σημαντικές αλλαγές στην οργανωτική δομή του οργανισμού, στις απαιτήσεις ασφάλειας ή στις τεχνολογικές εξελίξεις.

Στάδια ανάπτυξης

Μια πολιτική ασφάλειας, για να θεωρηθεί επιτυχής, πρέπει να περάσει από τα τρία ακόλουθα στάδια [3]:

1. Ανάπτυξη πολιτικής ασφάλειας
2. Εφαρμογή πολιτικής ασφάλειας
3. Μετέπειτα χειρισμός πολιτικής ασφάλειας

Η πολιτική ασφάλειας αποτελεί δυναμικό στοιχείο της ασφάλειας ενός υπολογιστικού στοιχείου. Δεν είναι κάτι στάσιμο και εξελίσσεται συνεχώς. Ερωτήματα όπως: Είναι πλήρης; Αντικατοπτρίζει τις ανάγκες του οργανισμού και του δικτύου; Και πολλά άλλα, πρέπει να απαντώνται συνεχώς.

Φυσικά, η ύπαρξη και μόνο της πολιτικής ασφάλειας δεν είναι αρκετή. Τα περιεχόμενα της για να είναι αποτελεσματικά πρέπει να εφαρμόζονται στην πράξη. Αυτό συνεπάγεται ότι η πολιτική ασφάλειας πρέπει να είναι διαθέσιμη στους χρήστες με τρόπο εύκολο.

Όπως θα δούμε και στη συνέχεια, η πολιτική ασφάλειας απορρέει μεταξύ άλλων και μέσα από την ανάλυση ρίσκου. Επιπλέον, βάση της αποτελεί η νομοθεσία και οι αρχές μια χώρας, αφού σύμφωνα με αυτές καθορίζονται πολλές παράμετροι της πολιτικής ασφάλειας (π.χ. ζητήματα που έχουν να κάνουν με την ασφάλεια προσωπικών δεδομένων).

Απαιτήσεις ασφάλειας

Για να προκύψει η πολιτική ασφάλειας, **είναι απαραίτητο να έχει προηγηθεί προσδιορισμός των απαιτήσεων ασφάλειας του πληροφοριακού συστήματος**. Ο προσδιορισμός των απαιτήσεων μπορεί να βασίζεται στην ανάλυση επικινδυνότητας. Το τελευταίο στάδιο της ανάλυσης επικινδυνότητας καλείται ανάλυση μέγιστου κέρδους – ελάχιστου κόστους και ως στόχο έχει την επίτευξη μιας ισορροπίας ανάμεσα στην αξία του πληροφοριακού συστήματος και της σοβαρότητας των κινδύνων που καλείται να αντιμετωπίσει και στην παρεχόμενη ασφάλεια.

Για την παροχή της ασφάλειας αυτής λαμβάνονται τα κατάλληλα μέτρα που αντανακλούν την διασφάλιση των βασικών απαιτήσεων ασφάλειας και περιλαμβάνουν αναλυτικούς κανόνες και οδηγίες για την επίτευξη των στόχων ασφαλείας που έχουν τεθεί. **Τα μέτρα ασφάλειας λοιπόν, προάγουν στο σύνολό τους την πολιτική ασφάλειας** και αν θελήσουμε να τα κατατάξουμε σε θεματικές κατηγορίες, έχουμε τις εξής [2]:

1. *Μέτρα ασφάλειας για την οργάνωση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος.*

Εδώ τα μέτρα ασφάλειας αφορούν τον γενικό σχεδιασμό της ασφάλειας του πληροφοριακού συστήματος καθώς και τον έλεγχο και εποπτεία της. Καθορίζονται οι ρόλοι και αρμοδιότητες των εμπλεκομένων στο πληροφοριακό σύστημα και ο άμεσος στόχος είναι η εκπαίδευση και ενημέρωση των χρηστών ώστε να κάνουν χρήση του συστήματος με τον τρόπο που ορίζεται ως επιτρεπτός.

2. *Ασφάλεια ανάπτυξης και συντήρησης του πληροφοριακού συστήματος.*

Τα μέτρα ασφάλειας εδώ, αφορούν την ανάπτυξη και συντήρηση εφαρμογών, τη διαχείριση υποστήριξης και απόκτησης λογισμικού και υλικού από προμηθευτές, την απογραφή τους και τη διαχείριση αλλαγών.

3. *Φυσική ασφάλεια.*

Πρόκειται για μέτρα που αφορούν την ασφάλεια κτιριακών εγκαταστάσεων και φυσικά την ασφάλεια του εξοπλισμού πληροφορικής και τηλεπικοινωνιών. Εδώ κατατάσσονται και τα μέτρα για την προστασία από φυσικές καταστροφές.

4. *Ασφάλεια δεδομένων.*

Στην ασφάλεια των δεδομένων υπάγονται μηχανισμοί που αφορούν την εξασφάλιση ακεραιότητας και εμπιστευτικότητας των δεδομένων καθώς επίσης και την κατηγοριοποίηση και ταξινόμησή τους.

5. *Ασφάλεια της υπολογιστικής και τηλεπικοινωνιακής υποδομής.*

Εδώ τα μέτρα ασφάλειας αφορούν εφεδρικά αντίγραφα ασφαλείας, αντιμετώπιση ιών, διαχείριση των passwords και έλεγχος προσπέλασης, ασφάλεια βάσεων δεδομένων, ασφάλεια κατά τη σύνδεση στο Internet, κλπ. Εδώ κατατάσσονται επίσης μηχανισμοί καταγραφής συμβάντων και περιστατικών ή προσπαθειών παραβίασης της ασφάλειας του πληροφοριακού συστήματος.

6. *Ανάκαμψη από καταστροφές.*

Η περίπτωση αυτή καλύπτεται από το **σχέδιο έκτακτης ανάγκης**. Πρόκειται για ένα γραπτό κείμενο το οποίο συμπληρώνει την πολιτική ασφάλειας. Τα μέτρα που προβλέπονται εκεί στοχεύουν στον προσδιορισμό των πιθανών κινδύνων που καθορίζουν μια κατάσταση ως έκτακτη και επιτρέπουν την ανάκληση του σχεδίου. Ειδικότερα στοχεύουν στο να ελαχιστοποιηθούν οι διακοπές κανονικής λειτουργίας, στον προσδιορισμό της έκτασης μιας ζημιάς και στην αποφυγή της κλιμάκωσής της. Προβλέπουν για το σύστημα ομαλή υποβάθμισή του και την εκ των προτέρων εγκατάσταση εναλλακτικών μέσων λειτουργίας. Χαρακτηριστικό παράδειγμα

κατάστασης που πραγματεύεται το σχέδιο έκτακτης ανάγκης είναι η ανάκαμψη του πληροφοριακού συστήματος μετά από κάποια φυσική καταστροφή, για παράδειγμα μετά από σεισμό.

Πολιτική ασφάλειας παρόχου

Ο πάροχος δικτύου διαδικτυακών επικοινωνιών είναι οποιοσδήποτε οργανισμός ή επιχείρηση παρέχει δίκτυο διαδικτυακών επικοινωνιών ή παρέχει στο προσωπικό του δικτυακή υποδομή για χρήση στα πλαίσια της εργασίας του. Οι πάροχοι λοιπόν είναι αυτοί που οφείλουν να διαθέτουν πολιτική ασφάλειας, εφόσον διαθέτουν δίκτυο.

Παρότι ο λόγος ύπαρξης της πολιτικής ασφάλειας είναι ίδιος για όλους, είναι σαφές ότι το περιεχόμενό της είναι διαφοροποιημένο έτσι ώστε να ανταποκρίνεται στις ειδικές απαιτήσεις ασφάλειας του κάθε παρόχου. Σε κάθε περίπτωση, ορίζονται με ξεχωριστό τρόπο η πρόσβαση σε πληροφορίες, οι ενέργειες που ακολουθούνται και επιτρέπονται για τη διατήρηση της ασφάλειας και τα μέτρα που εφαρμόζονται σε περιπτώσεις παραβίασης της ασφάλειας. Η πολιτική ασφάλειας, μεταξύ των παραπάνω, οφείλει να προβλέπει μέτρα για την διασφάλιση των δεδομένων των χρηστών, των προσωπικών τους στοιχείων και το απόρρητο των επικοινωνιών, έτσι όπως αυτό ορίζεται από την εκάστοτε νομοθεσία.

Αναφέραμε ήδη κάποια γενικά χαρακτηριστικά που πρέπει να έχει μια πολιτική ασφάλειας. Η λίστα των χαρακτηριστικών όμως για να θεωρείται επαρκής είναι μεγάλη [4]. Η πολιτική ασφάλειας πρέπει να είναι **πλήρης**. Αυτό σημαίνει ότι πρέπει να καλύπτει κάθε συμμετέχων μέρος και να λαμβάνει υπόψη κάθε πιθανή περίπτωση παραβίασης της ασφάλειας. Μεγάλη βαρύτητα δίνεται στο ζήτημα της **ανεξαρτησίας από το χρησιμοποιούμενο υλικό και λογισμικό** του παρόχου από τεχνικής άποψης. Γενικά πρέπει να είναι ευέλικτη και να είναι μακροπρόθεσμα βιώσιμη. Δεν πρέπει η παραμικρή αλλαγή στο σύστημα να έχει αντίκτυπο στην πολιτική ασφάλειας. Επισημαίνουμε επιπλέον ότι αν ο πάροχος διαθέτει γενικότερη πολιτική ασφάλειας πληροφοριών και πληροφοριακών συστημάτων, όπως για παράδειγμα πολιτική ασφάλειας που αφορά πρόσβαση σε φυσικούς χώρους, τότε η πολιτική ασφάλειας δικτύου για την οποία κάνουμε εδώ λόγο, αποτελεί μέρος της γενικότερης πολιτικής.

Μία ενδεικτική ακολουθία βημάτων που ο πάροχος πρέπει να ακολουθήσει προκειμένου να καλύψει τις απαιτήσεις της πολιτικής ασφάλειας είναι και η εξής [4]: αρχικά πρέπει να εντοπίζονται τα στοιχεία του δικτύου και οι πληροφορίες που χρήζουν προστασίας. Αυτό το βήμα είναι πολύ σημαντικό και η βάση για οποιαδήποτε περαιτέρω απόφαση, όπως επίσης και το να προσδιοριστούν οι κίνδυνοι και οι ευπάθειες στους οποίους είναι εκτεθειμένα. Λαμβάνοντας υπόψη τους κινδύνους αλλά και το πόσο πιθανό είναι να εισέλθει το σύστημα σε κάποια κρίσιμη κατάσταση, υλοποιούνται τα κατάλληλα μέτρα προστασίας. Τα μέτρα αυτά ο πάροχος καλείται να τα ελέγχει και να τα αναθεωρεί όταν αυτό επιβάλλεται από τις συνθήκες και τους νέους κινδύνους που πιθανόν προκύπτουν. Και φυσικά, οποιαδήποτε επένδυση γίνεται στον τομέα της ασφάλειας του δικτύου και οποιοδήποτε μέτρο λαμβάνεται, οφείλει να ακολουθεί την **αρχή της αναλογικότητας**. Τα μέτρα προστασίας είναι αντίστοιχα του μεγέθους του δικτύου και του αριθμού των χρηστών που το χρησιμοποιούν.

Πολιτική πρόσβασης

Μεταξύ άλλων, έγινε λόγος για τα μέτρα που ορίζονται στην πολιτική ασφάλειας και καθορίζουν το ζήτημα της πρόσβασης των χρηστών στο σύστημα και τις πληροφορίες του. Αναπόσπαστο κομμάτι δηλαδή της πολιτικής ασφάλειας, αποτελεί η πολιτική πρόσβασης που η σωστή εφαρμογή της θεωρείται κρίσιμη για την ομαλή λειτουργία ενός δικτύου. Προβλέπονται λοιπόν σε μία πολιτική ασφάλειας διαδικασίες που αφορούν στον τομέα αυτό.

Ένα πρώτο θέμα που ανακύπτει είναι ο τρόπος ένταξης νέων χρηστών στο σύστημα και τα δικαιώματα που τους παρέχονται [4]. Αναφορικά με τις διαδικασίες εξουσιοδότησης για τα διάφορα δικαιώματα πρόσβασης, όπως είναι η ανάγνωση ενός αρχείου, η τροποποίηση ή η διαγραφή του, αυτές ελέγχονται και παραχωρούνται μόνο στους χρήστες που πρέπει και στο βαθμό που ο καθένας από αυτούς δικαιούται. Στην περίπτωση που στο δίκτυο γίνεται χρήση κρυπτογράφησης, ο πάροχος μέσω της πολιτικής ασφάλειας ορίζει τις διαδικασίες πρόσβασης των χρηστών στα συστήματα κρυπτογράφησης / αποκρυπτογράφησης και στα ζητήματα της διαχείρισης, διανομής και αρχειοθέτησης των κλειδιών κρυπτογράφησης.

Σε πολλές περιπτώσεις, είναι απαραίτητη η **απομακρυσμένη πρόσβαση** κάποιου χρήστη στο εταιρικό δίκτυο. Μερικές φορές είναι αναγκαίο η δυνατότητα αυτή να δίνεται ακόμη και σε εξωτερικούς συνεργάτες, προμηθευτές ή πελάτες. Οι κανόνες που ορίζουν το γενικό πλαίσιο χρήσης της απομακρυσμένης πρόσβασης συνοψίζονται στα παρακάτω [5]:

- Οι χρήστες είναι υποχρεωμένοι να μην παρακάμπτουν τα δικαιώματα πρόσβασης που έχουν με τη σύνδεση αυτή.
- Δεν θα πρέπει να κάνουν χρήση της σύνδεσης αυτής για προσωπικούς λόγους, π.χ. Internet, παρά μόνο για σκοπούς που έχουν άμεση σχέση με την εργασία τους.
- Όταν μεταφέρουν αρχεία μέσω αυτής της σύνδεσης, οφείλουν να τηρούν την πολιτική ασφάλειας που ισχύει για τις διαβαθμισμένες πληροφορίες (κρυπτογράφηση, ταυτοποίηση). Επίσης, θα πρέπει να τηρούν τις αντίστοιχες πολιτικές χρήσης Διαδικτύου και ηλεκτρονικού ταχυδρομείου.
- Είναι απαραίτητο να υπάρχουν οι κατάλληλοι μηχανισμοί που να ελέγχουν την απομακρυσμένη σύνδεση και να διαχειρίζονται από το Τμήμα Ασφάλειας της εταιρίας.
- Ο έλεγχος πρόσβασης θα πρέπει να γίνεται με προηγμένους μηχανισμούς ταυτοποίησης, π.χ. κωδικοί μιας χρήσης, PKI/δημόσια και ιδιωτικά κλειδιά.
- Οι υπολογιστές που είναι συνδεδεμένοι με το εταιρικό δίκτυο δεν θα είναι συνδεδεμένοι και με άλλο δίκτυο ταυτόχρονα.
- Ο εξοπλισμός που χρησιμοποιείται για τις απομακρυσμένες συνδέσεις θα πρέπει να εγκρίνεται από το Τμήμα Ασφάλειας και να προβλέπει μηχανισμούς ταυτοποίησης/ αναγνώρισης.
- Όλοι οι υπολογιστές που χρησιμοποιούνται θα πρέπει να διαθέτουν ενημερωμένο λογισμικό καταπολέμησης ιών (anti-virus).

Οι παραπάνω κανόνες είναι ενδεικτικοί αλλά υποδεικνύουν ένα ζήτημα μείζονος σημασίας: όλο το ανθρώπινο δυναμικό των επιχειρήσεων οφείλει να είναι σωστά εκπαιδευμένο και πάντοτε ενημερωμένο για τους υφιστάμενους κινδύνους σε ένα δικτυωμένο περιβάλλον, προκειμένου να τηρούνται όλες οι πολιτικές ασφάλειας και να ελαχιστοποιείται το ρίσκο απώλειας ή διαρροής διαβαθμισμένου υλικού.

Αποδεκτή χρήση

Ένα ζήτημα στο οποίο στέκεται η πολιτική ασφάλειας είναι οι επιτρεπόμενες και μη επιτρεπόμενες δραστηριότητες των χρηστών σε ένα δίκτυο. Το δίκτυο πρέπει να χρησιμοποιείται με έναν προκαθορισμένο τρόπο και έτσι ώστε να προάγει τη λειτουργία και τους σκοπούς του οργανισμού. Η χρήση του πρέπει να είναι αποδεκτή και σύμφωνη με την ισχύουσα νομοθεσία. Είναι συνήθης πολιτική ενός οργανισμού να ζητά από τους νέους χρήστες να υπογράψουν ένα έγγραφο στο οποίο δηλώνουν ότι θα κάνουν αποκλειστικά νόμιμη χρήση του δικτύου. Χαρακτηριστικό παράδειγμα αποτελεί ένα πανεπιστήμιο στο οποίο οι νεοεισαχθέντες φοιτητές υπογράφουν το εν λόγω έγγραφο. Η ίδια διαδικασία είναι δυνατό να γίνεται και ηλεκτρονικά με τη συμπλήρωση από το χρήστη μιας σχετικής φόρμας.

Φυσικά, δεν ισχύουν για όλους τους χρήστες οι ίδιοι περιορισμοί. Λαμβάνονται υπόψη διαφορετικές κατηγορίες χρηστών και για την κάθε κατηγορία ισχύουν διαφορετικά πράγματα. Για την κάθε κατηγορία λοιπόν, ορίζονται τόσο δικαιώματα όσο και υποχρεώσεις. Και στις δύο αυτές κατηγορίες δίνονται παραδείγματα αποδεκτής και μη αποδεκτής χρήσης του πληροφοριακού συστήματος αντίστοιχα αλλά αναφέρονται και οι συνέπειες που έχει κάποιος αν δεν συμμορφώνεται με τις υποχρεώσεις που ορίζονται για αυτόν. Για παράδειγμα [4], μια υποχρέωση που έχουν οι χρήστες είναι να λαμβάνουν κάποια μέτρα που σχετίζονται με το απόρρητο των επικοινωνιών τους, όπως το να διαφυλάσσουν τον μυστικό κωδικό τους ή να κλειδώνουν τον υπολογιστή τους όταν απομακρύνονται από αυτόν. Επίσης, αν οποιοδήποτε κενό ασφάλειας υποπέσει στην αντίληψή τους, οφείλουν να το αναφέρουν στους υπεύθυνους ασφάλειας και σε καμία περίπτωση να επιχειρήσουν να το εκμεταλλευτούν έτσι ώστε να αποκτήσουν πρόσβαση που δεν δικαιούνται σε πληροφορίες άλλων χρηστών ή να προκαλέσουν οποιαδήποτε άλλου είδους καταστροφή.

Ασφαλώς, με αντίστοιχο τρόπο, ορίζονται δικαιώματα και υποχρεώσεις για τον πάροχο. Και κάτι που πρέπει να τονιστεί είναι ότι στην περίπτωση που προκύψει κάποιο ζήτημα παραβίασης της ασφάλειας και *ο πάροχος δεν μπορεί να το αντιμετωπίσει με τα μέσα που διαθέτει*, πρέπει να ενημερώνει άμεσα τους χρήστες σχετικά με τους ενδεχόμενους κινδύνους που αντιμετωπίζουν παρέχοντάς τους ταυτόχρονα και αν είναι εφικτό στοιχεία και συμβουλές για την προφύλαξή τους.

Πολιτική ασφάλειας και εμπλεκόμενα μέρη

Η ανάπτυξη της επικοινωνίας μέσω του Internet και γενικότερα μέσω δικτύων, είναι τόσο προς όφελος των παρόχων, αφού θα τους οδηγήσει στην επιχειρηματική ανάπτυξη όσο και προς όφελος των χρηστών, αφού οι παρεχόμενες υπηρεσίες τους αφορούν και τους εξυπηρετούν. Αυτό συνεπάγεται πως οι κανόνες που ορίζονται σε

μία πολιτική ασφάλειας πρέπει να γίνουν αποδεκτοί από όλους ανεξαιρέτως τους εμπλεκόμενους.

Πάροχοι: Οι πάροχοι είναι αυτοί που πρωτίστως πρέπει να δίνουν το καλό παράδειγμα σε κάθε επιχειρηματικό τους βήμα και οι πράξεις τους να είναι νόμιμες, ειλικρινείς και να διέπονται από διαφάνεια [6]. Θα πρέπει να έχουν ως στόχο να αυξήσουν την εμπιστοσύνη των χρηστών στις παρεχόμενες εφαρμογές.

Χρήστες: Οι χρήστες είναι υποχρεωμένοι να χρησιμοποιούν τις εφαρμογές όπως αυτές παρέχονται από τον εκάστοτε πάροχο. Σε περίπτωση που υποπίπτει στην αντίληψή τους μη ορθή συμπεριφορά, είναι υποχρεωμένοι να ειδοποιούν άμεσα τον πάροχο. Πρέπει να κατανοήσουν ότι είναι υπεύθυνοι για κάθε τους πράξη [6].

Στην περίπτωση που οι πάροχοι και οι χρήστες δεν είναι συνεπείς στις υποχρεώσεις τους, διώκονται βάσει της υπάρχουσας νομοθεσίας. Κάθε περίπτωση εκβιασμού, λιβελογραφίας, συκοφαντικής δυσφήμισης, ρατσιστικής μεταχείρισης, παιδοφιλίας, παρακολούθησης απόρρητων πληροφοριών ή διαρροής τους, καλύπτεται νομικά και επιφέρει τις ανάλογες κυρώσεις.

Προστασία απορρήτου επικοινωνιών και δεδομένων

Ένα ζήτημα που προκύπτει και έχει μεγάλη σημασία είναι αυτό της προστασίας των δεδομένων σε ένα δίκτυο επικοινωνιών. Η προστασία δεδομένων αφορά τόσο τα προσωπικά στοιχεία ενός χρήστη, όπως είναι η ταυτότητά του, αλλά και γενικότερες πληροφορίες και στοιχεία αποθηκευμένα σε κάποιον υπολογιστή. Η πολιτική ασφάλειας καλείται να προβλέπει το ζήτημα αυτό και να προστατεύει τους χρήστες και τις πληροφορίες τους.

Σε κάθε περίπτωση, η χρήση των πληροφοριών μπορεί να γίνεται μόνο με τη σύμφωνη γνώμη του χρήστη και αφού αυτός ενημερωθεί για το λόγο που χρειάζεται να γίνει συλλογή των πληροφοριών. Μία γενική αρχή που θα πρέπει βέβαια να διέπει το στήσιμο ενός δικτύου και των υπηρεσιών του είναι ο περιορισμός των απαιτούμενων στοιχείων στο ελάχιστο δυνατό για την παροχή κάποιας υπηρεσίας. Προκύπτει από αυτό ότι υπάρχουν υπηρεσίες στις οποίες είναι απαραίτητη η συλλογή κάποιων στοιχείων του χρήστη, όπως είναι η παροχή απόδειξης για την αγορά ενός προϊόντος. Και στην περίπτωση αυτή όμως, τα προσωπικά στοιχεία που συλλέγονται πρέπει να είναι τα ελάχιστα απαιτούμενα.

Οι περιπτώσεις λοιπόν όπου διακριτά επιτρέπεται να καταγράφονται προσωπικά δεδομένα είναι οι εξής [7]:

1. Όταν **με τη συγκατάθεσή του** ο χρήστης δίνει τα προσωπικά του στοιχεία (όποτε για παράδειγμα επιθυμεί να αγοράσει κάποιο προϊόν /υπηρεσία ή να κατεβάσει κάποιο πρόγραμμα στον προσωπικό του υπολογιστή ή και να εγγραφεί σε κάποια υπηρεσία του διαδικτύου). Τα στοιχεία αυτά μπορεί να είναι στοιχεία ταυτότητας, στοιχεία επαγγελματικά, στοιχεία εκπαίδευσης ή και ακόμα οικονομικά στοιχεία όπως είναι ο αριθμός της πιστωτικής κάρτας.
2. Όταν **χωρίς την συγκατάθεση του χρήστη**, συλλέγονται προσωπικά στοιχεία μέσω cookies τα οποία καταγράφουν και επεξεργάζονται τη συμπεριφορά του χρήστη κατά την πλοήγησή του στο διαδίκτυο (π.χ. προτιμήσεις).

3. Όταν στα πλαίσια του παρόχου υπηρεσιών πρόσβασης στο Internet τηρείται αρχείο με τα προσωπικά στοιχεία του χρήστη και κατ' επέκταση στοιχεία των ηλεκτρονικών διευθύνσεων τις οποίες επισκέπτεται, τον ακριβή χρόνο και τη διάρκεια της επίσκεψης.

Είναι γεγονός ότι σε όλες τις παραπάνω περιπτώσεις, η συλλογή και επεξεργασία προσωπικών δεδομένων μπορεί να οδηγήσει σε παραβίαση της ιδιωτικής και προσωπικής ζωής του χρήστη όταν αυτή δεν εφαρμόζεται σύμφωνα με την ισχύουσα νομοθεσία. Προκύπτει ως συμπέρασμα λοιπόν, ότι οι χρήστες χρειάζονται τεχνολογίες που θα προστατεύουν την ασφάλεια των επικοινωνιών τους ενώ παράλληλα θα εξασφαλίζουν τα δικαιώματά τους σε σχέση με την ελευθερία έκφρασης και την ιδιωτικότητα των πληροφοριών που σχετίζονται με την προσωπική τους ζωή και γίνονται αντικείμενο επεξεργασίας από διάφορους φορείς (τρίτοι).

Μέτρα προφύλαξης του χρήστη

Η πολιτική ασφάλειας είναι ένα μέσο από το οποίο οι χρήστες μπορούν να ενημερώνονται για τα μέτρα προστασίας που μπορούν να λαμβάνουν έτσι ώστε να διασφαλίζεται η επικοινωνία και τα δεδομένα τους. Οι πάροχοι οφείλουν να ενημερώνουν τους χρήστες για τα μέτρα αυτά και να τους στρέφουν προς τη χρήση κατάλληλων λογισμικών και τεχνολογιών κρυπτογράφησης.

Στην πράξη τώρα, οι χρήστες οφείλουν να [7]:

- Χρησιμοποιούν όλα τα διαθέσιμα μέσα για να προστατεύουν τα δεδομένα που τους αφορούν και τις επικοινωνίες, όπως τα νόμιμα διαθέσιμα τεχνολογικά εργαλεία κρυπτογράφησης δεδομένων, ηλεκτρονικού ταχυδρομείου, κωδικών πρόσβασης κλπ.
- Είναι προσεκτικοί σε σχέση με τις πληροφορίες που μεταβιβάζουν σε κάθε επίσκεψή τους στις ιστοσελίδες ενός δικτυακού τόπου. Οι προσωπικές πληροφορίες που μεταβιβάζονται ποικίλλουν και αφορούν σε:
    - **Πληροφορίες που μεταβιβάζονται εις γνώσιν του χρήστη,** π.χ. ονοματεπώνυμο, ταχυδρομική διεύθυνση, κλπ.
    - **Πληροφορίες που μεταβιβάζονται εν αγνοία του χρήστη**, π.χ. IP διεύθυνση. Τις περισσότερες φορές η μεταβίβαση αυτών των πληροφοριών είναι αναγκαία για λόγους επίτευξης της επικοινωνίας και επιβάλλεται από την φύση της σχεδίασης των επικοινωνιακών πρωτοκόλλων.
- Αναζητούν και να τους παρέχονται, στο βέλτιστο βαθμό, τεχνολογίες που εξασφαλίζουν την ανωνυμία στο βαθμό εκείνο που δεν θίγονται άλλοι νόμοι και αρχές που θεωρούνται ανώτερες από την προσωπική ζωή, π.χ. δημόσιο συμφέρον κλπ.
- Επιδιώκουν τη χρήση ψευδωνύμων, σε περιπτώσεις που είναι νομικά αδύνατη η παροχή παντελούς ανωνυμίας.
- Αποκαλύπτουν **μόνο** τα δεδομένα εκείνα που είναι **απαραίτητα** για την επίτευξη των **σκοπών** που επιδιώκονται μέσω της **συγκεκριμένης** επικοινωνίας ή συναλλαγής. Ιδιαίτερη προσοχή πρέπει να δοθεί στην περίπτωση αποκάλυψης ευαίσθητων πληροφοριών, όπως είναι ο αριθμός πιστωτικής κάρτας. Σε αυτές τις περιπτώσεις συστήνεται η χρήση τεχνολογιών διασφάλισης εμπιστευτικότητας πληροφοριών,

όπως είναι το πρωτόκολλο επικοινωνίας Secure Socket Layer, SSL. Το πρωτόκολλο αυτό χρησιμοποιείται συχνά σε συνδυασμό με το πρωτόκολλο HTTP για την παροχή ασφαλών διμερών επικοινωνιών με χρήση υπηρεσιών WWW. Τυπικά, ο χρήστης μπορεί να αναγνωρίσει την ενεργοποίηση αυτού του πρωτοκόλλου αναζητώντας τα αρχικά https:// στην τοποθεσία της ηλεκτρονικής σελίδας με την οποία έχει συνδεθεί.

- Η ηλεκτρονική διεύθυνση αλληλογραφίας αποτελεί προσωπικό στοιχείο και προστατεύεται όπως τα υπόλοιπα προσωπικά στοιχεία. Για το λόγο αυτό, θα πρέπει να αποφεύγεται η συμμετοχή σε λίστες με ηλεκτρονικές ταχυδρομικές διευθύνσεις που δεν κάνουν γνωστό τον σκοπό για τον οποίο συλλέγονται, την διάρκεια της επεξεργασίας, τους πιθανούς αποδέκτες των στοιχείων και επίσης δεν παρέχουν έναν ρητό τρόπο διαγραφής τους από αυτές.
- Οι χρήστες πρέπει να αποφεύγουν τη χρήση cookies στον υπολογιστή τους μέσω απενεργοποίησης των κατάλληλων ρυθμίσεων στον web browser, γιατί είναι γνωστό πως με τη χρήση τους είναι δυνατή η δημιουργία καταναλωτικού προφίλ.

Μέτρα προφύλαξης για τον πάροχο

Ως γνωστό, υπάρχει κατάλληλή νομοθεσία για την προστασία των προσωπικών δεδομένων. Η πολιτική ασφάλειας ενός παρόχου οφείλει να είναι σύμφωνη με τη νομοθεσία και να την εφαρμόζει στην πράξη. Η παραβίαση των κανόνων που τίθενται από τη νομοθεσία και από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα θα πρέπει σε κάθε περίπτωση να επιφέρει τις ανάλογες κυρώσεις.

Στην πράξη, οι πάροχοι οφείλουν να [7]:

- Παρέχουν εξασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων όταν αυτά υποβάλλονται ηλεκτρονικά.
- Χρησιμοποιούν λογισμικό ή /και υλικό το οποίο έχει πιστοποιηθεί σχετικά με την ποιότητά του και εξασφαλίζει την ασφάλεια των μεταδιδόμενων πληροφοριών.
- Συντάσσουν ένα κώδικα δεοντολογίας για την προστασία των προσωπικών δεδομένων και ο οποίος θα είναι σύμφωνος με την ισχύουσα νομοθεσία.
- Ενημερώνουν τους χρήστες και διευκολύνουν την πρόσβασή τους σε πόρους σχετικά με την ασφάλεια πληροφοριών και την προστασία της ιδιωτικής τους ζωής. Για παράδειγμα, θα πρέπει σε όλα τα έντυπα που μοιράζουν στους συνδρομητές τους να τους ενημερώνουν σχετικά με το δικαίωμα αντίρρησής τους στην συλλογή προσωπικών ή /και ευαίσθητων δεδομένων που τους αφορούν και με οποιοδήποτε άλλο ζήτημα είναι δυνατό να προκύψει πάνω στη διασφάλιση του απορρήτου.
- Συλλέγουν τα στοιχεία των συνδρομητών με διαφανή τρόπο. Αυτό πρακτικά σημαίνει ότι θα πρέπει να αποφεύγεται η χρήση των cookies. Η μέθοδος που συνίσταται είναι η χρήση ηλεκτρονικών φορμών. Τα στοιχεία που θα συλλέγονται θα πρέπει να είναι ακριβώς εκείνα που

απαιτούνται. Ο πάροχος μπορεί να επιθυμεί να συλλέξει επιπρόσθετα στοιχεία. Τα στοιχεία αυτά θα πρέπει με κάποιο τρόπο (π.χ. της ύπαρξη ενός αστερίσκου) να σημειώνονται ως μη υποχρεωτικά προς συμπλήρωση και να υπάρχει ρητή ένδειξη για τον σκοπό της συλλογής τους.

- Μην υποβιβάζουν τη λειτουργικότητα που προσφέρεται σε ένα χρήστη σε περίπτωση που ο τελευταίος απέφυγε την παροχή προσωπικών δεδομένων που δεν αναγράφονταν ως απαραίτητα. Για παράδειγμα δεν θα πρέπει να περιορίζεται το υλικό που εμφανίζεται στον brower ενός χρήστη επειδή αρνήθηκε την εγκατάσταση cookies στον δίσκο του υπολογιστή του. Επιπλέον, δεν θα πρέπει να μειώνονται οι επιλογές πρόσβασης σε περίπτωση που ο χρήστης απέφυγε να συμπληρώσει τα πεδία με προσωπικά δεδομένα τα οποία έχουν μαρκαριστεί ως προαιρετικά (στην περίπτωση συλλογής στοιχείων με ηλεκτρονικές φόρμες) και φυσικά δε θα πρέπει σε καμία περίπτωση να πριμοδοτείται με οποιοδήποτε τρόπο η συγκατάθεση του χρήστη στη συλλογή μη απαραίτητων στοιχείων.
- Αποφεύγουν τη μεταβίβαση των προσωπικών /ευαίσθητων δεδομένων σε χώρες εκτός ΕΕ ή τρίτες χώρες που δεν παρέχουν επίπεδο ασφάλειας ανάλογο με αυτό που παρέχεται από Ευρωπαϊκές χώρες. Για το λόγο αυτό, θα πρέπει να αποφεύγεται η απόκτηση ψηφιακών πιστοποιητικών από χώρα που δεν παρέχει ικανοποιητικό επίπεδο ασφάλειας εκτός αν πληρούνται ορισμένες προϋποθέσεις.
- Αποφεύγεται η παρακολούθηση και καταγραφή των επικοινωνιών των χρηστών παρά μόνο σε περιπτώσεις όπου αυτό είναι απαραίτητο για την τιμολόγησή τους.
- Σε περιπτώσεις όπου η καταγραφή των επικοινωνιών είναι απαραίτητη για την εξυπηρέτηση του χρήστη π.χ. χρήση τεχνολογίας proxy για την μείωση του κόστους σύνδεσης με δικτυακούς τόπους όπου ο χρήστης επισκέπτεται συχνά, θα πρέπει να γίνονται γνωστοί στον χρήστη οι κίνδυνοι που απορρέουν από μια τέτοια υπηρεσία και να ζητείται η ρητή συγκατάθεσή του για την συμμετοχή του σε τέτοιου είδους υπηρεσίες.
- Είναι υπεύθυνοι για τα διαφημιστικά λογότυπα (banners) που φιλοξενούνται από τις σελίδες τους και για τις προσωπικές πληροφορίες που μπορούν να υποκλαπούν σε περίπτωση ενεργοποίησης ενός τέτοιου λογότυπου όταν ο χρήστης πιέσει το ποντίκι του υπολογιστή του πάνω σε αυτό.

Αντίγραφα ασφαλείας

Το ζήτημα των αντιγράφων ασφαλείας είναι μείζονος σημασίας σε ένα δίκτυο, ειδικότερα μετά από περιπτώσεις επιθέσεων ή ευπαθειών στο τηλεπικοινωνιακό σύστημα. Στην πολιτική ασφάλειας του δικτύου θα πρέπει να περιλαμβάνονται οι διαδικασίες και οι έλεγχοι που θα εξασφαλίσουν ότι το δίκτυο ή κάποια μεμονωμένα τμήματα του εξοπλισμού που έχουν υποστεί ζημιά, μπορούν να ανακτήσουν τη

λειτουργία εντός μιας λογικής χρονικής περιόδου μετά από οποιοδήποτε πρόβλημα έχει προκύψει.

Να διασαφηνίσουμε αρχικά ότι με τον όρο «αντίγραφα ασφαλείας» αναφερόμαστε στα δεδομένα διάρθρωσης των δικτυακών στοιχείων [8]. Για τα δεδομένα αυτά λοιπόν, ο πάροχος οφείλει να αναπτύξει ένα σχέδιο για να μπορεί να ανταποκρίνεται σε περιπτώσεις έκτακτης ανάγκης. Το σχέδιο αυτό πρέπει να περιλαμβάνει: α) την εκτέλεση αντιγράφων ασφαλείας, και β) διαδικασίες που μπορούν να χρησιμοποιηθούν για να διευκολύνουν τη συνέχιση της λειτουργίας σε περίπτωση ανάγκης για την ανάκτηση από μία επίθεση. Το σχέδιο πρέπει επίσης να τεκμηριώνεται και να ενημερώνεται σε τακτά χρονικά διαστήματα αλλά και να δοκιμάζεται ώστε να εξασφαλίζεται ότι τα εφεδρικά αντίγραφα ασφαλείας είναι δυνατό να ανακτηθούν.

Καταρχάς πρέπει να προσδιορίζονται τα στοιχεία που είναι απαραίτητο να αποθηκευτούν σε αντίγραφα ασφαλείας. Αυτό προκύπτει μετά από ανάλυση της ευαισθησίας των προγραμμάτων και των πληροφοριών που χειρίζονται, λαμβάνουν, αποθηκεύουν και μεταδίδουν τα δικτυακά στοιχεία. Στα αντίγραφα ασφαλείας πρέπει να διατίθεται το ίδιο επίπεδο προστασίας με τα αρχικά στοιχεία αλλά η γενική αρχή είναι ότι η συχνότητα και η έκταση των αντιγράφων πρέπει να είναι σύμφωνες με τη σημασία και τη σπουδαιότητα των πληροφοριών.

Τα αρχεία που προσδιορίζουν την κατάσταση και τη διάρθρωση των συσκευών σε ένα δίκτυο πρέπει να αντιγράφονται. Αυτό γίνεται γιατί σε περίπτωση βλάβης ή κακόβουλης αλλαγής κάποιας συσκευής, είναι απαραίτητος ο επαναπρογραμματισμός της στην αρχική κατάσταση. Πιο συγκεκριμένα, αυτά που συνίστανται είναι [8]:

1. Τα δεδομένα διάρθρωσης του δικτύου να αντιγράφονται τακτικά ώστε σε περίπτωση αποτυχίας του συστήματος, τα δεδομένα και τα configuration files να μπορούν να ανακτηθούν.
2. Τα εφεδρικά αντίγραφα πρέπει να αποθηκεύονται με ασφαλή τρόπο σε αρχεία μόνο αναγνώσιμα έτσι ώστε να μην είναι δυνατό το overwrite πάνω σε αυτά. Πρέπει επίσης να κλειδώνονται ώστε τα δεδομένα να είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό.
3. Η χρήση ενός εφεδρικού firewall μπορεί να αποδειχθεί ιδιαίτερα χρήσιμη. Μπορεί να τεθεί σε λειτουργία σε περίπτωση βλάβης του αρχικού firewall και να χρησιμοποιείται ενώ το τελευταίο είναι υπό επισκευή.

Πολιτική ασφάλειας περιμέτρου

Το κομμάτι της πολιτικής ασφάλειας που πραγματεύεται το ζήτημα της προστασίας των δικτυακών πόρων από μη εξουσιοδοτημένους χρήστες, καλείται πολιτική ασφάλειας περιμέτρου. Εδώ, ο πάροχος πρέπει να ορίζει τους μηχανισμούς που χρησιμοποιούνται για το σκοπό αυτό, όπως είναι τα συστήματα firewall και να πραγματοποιεί στους μηχανισμούς αυτούς ρυθμίσεις που εξασφαλίζουν το επιθυμητό επίπεδο ασφάλειας σύμφωνα με τις διεθνώς και ευρέως αποδεκτές πρακτικές που αφορούν την πολιτική ασφάλειας περιμέτρου.

Πιο συγκεκριμένα, για τα συστήματα firewall, ο πάροχος οφείλει να τα χρησιμοποιεί για να προστατεύει το δίκτυό του κατά τη σύνδεση με το Internet ή με άλλα δίκτυα. Το firewall παίζει το ρόλο ενός φράγματος ανάμεσα στο δίκτυο του παρόχου και τον εξωτερικό κόσμο, *συμβάλλοντας καθοριστικά στη δημιουργία μιας*

πολιτικής ασφάλειας περιμέτρου. Το σύστημα αυτό, το οποίο μπορεί να είναι είτε υλικό είτε λογισμικό, **οριοθετεί μια περίμετρο προστασίας** [5] προκαλώντας ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο – εσωτερικό δίκτυο του οργανισμού (το οποίο θεωρείται ασφαλές και έμπιστο) και στο εξωτερικό Διαδίκτυο (που θεωρείται μη ασφαλές και μη έμπιστο). Επιτρέπεται λοιπόν, η προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά. Το ποιοι εξωτερικοί χρήστες επιτρέπεται να έχουν τελικά πρόσβαση και ποια δεδομένα μπορούν να εισέρχονται ή να απορρίπτονται είναι ζήτημα της προαναφερθείσας πολιτικής. Το firewall διαμορφώνεται σύμφωνα με την πολιτική αυτή (firewall configuration) και διαπιστώνεται εν τέλει πως **μπορεί να θεωρηθεί ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας** που καθορίζει τις παρεχόμενες υπηρεσίες και τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη-έμπιστες δικτυακές περιοχές.

Άρρηκτα συνδεδεμένη με τα συστήματα firewall είναι η έννοια της **αποστρατικοποιημένης ζώνης** (demilitarized zone - DMZ). Το firewall, πέραν του σαφούς διαχωρισμού μεταξύ εσωτερικού δικτύου και Διαδικτύου, *διακρίνει και το εσωτερικό δίκτυο του παρόχου σε δύο περιοχές*:

α. Εσωτερικό έμπιστο (trusted) δίκτυο

β. Δίκτυο αποστρατικοποιημένης ζώνης

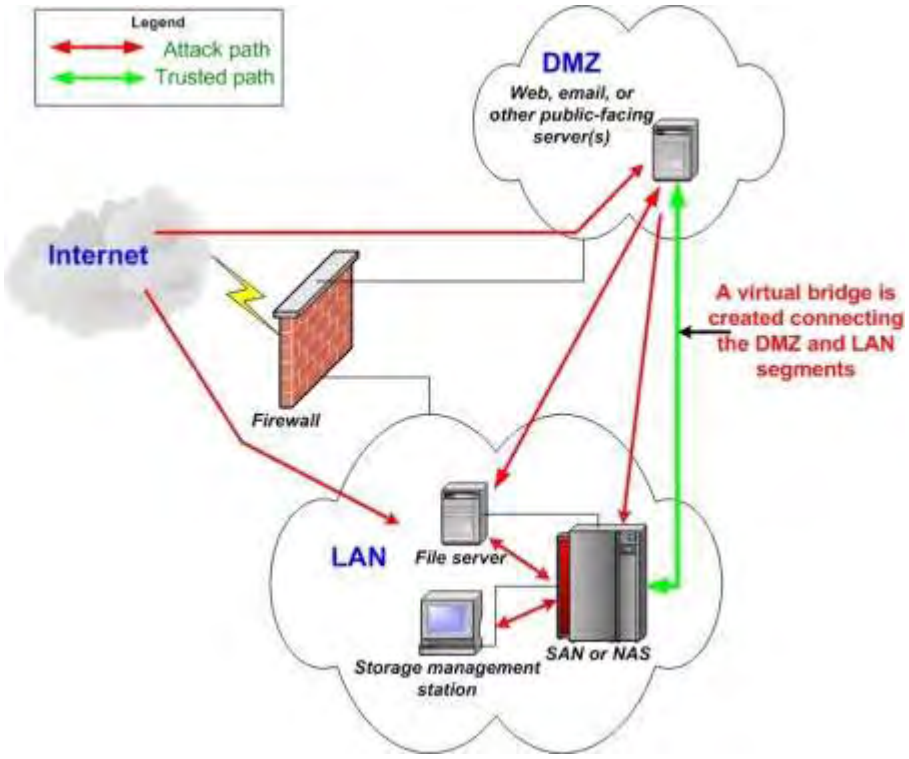


Figure 1: Σχηματική αναπαράσταση συστήματος firewall [5]

Το firewall επιβάλλεται να μην επιτρέπει την απευθείας πρόσβαση σε δεδομένα που υπάρχουν στο πληροφοριακό σύστημα, αλλά η πρόσβαση σε αυτά να γίνεται μετά τον έλεγχο στην αποστρατικοποιημένη ζώνη. Στην **DMZ** αναλύονται οι επιχειρηματικές ανάγκες και η στρατηγική της επιχείρησης όσον αφορά στο Internet και τοποθετούνται συστήματα που παρέχουν υπηρεσίες προσβάσιμες από χρήστες μέσω του Διαδικτύου.

Αν θέλουμε να δώσουμε να δώσουμε μία λίστα με τις απαιτήσεις από την πολιτική ασφάλειας δικτύου και από την εφαρμογή συστήματος firewall, έχουμε τα παρακάτω [5]:

- Όλες οι συνδέσεις από το δίκτυο του οργανισμού προς το Internet θα πρέπει να γίνονται μέσω firewall.
- Θα πρέπει να είναι ξεκάθαρο ποιοι είναι υπεύθυνοι για τα firewalls, οι οποίοι και τα διαχειρίζονται.
- Τα firewalls θα πρέπει να παρακολουθούνται και να ελέγχονται σε τακτά χρονικά διαστήματα (audits).
- Εισερχόμενες συνδέσεις από το Internet θα πρέπει να χρησιμοποιούν προηγμένους μηχανισμούς ταυτοποίησης /αναγνώρισης, π.χ. με κωδικούς μιας χρήσης. Το ίδιο ισχύει και για τους λογαριασμούς των διαχειριστών.
- Όλες οι υπηρεσίες /εφαρμογές που δεν χρειάζονται θα πρέπει να είναι απενεργοποιημένες. Όλα τα λειτουργικά θα πρέπει να είναι ενημερωμένα με τα τελευταία patches /hot fixes των κατασκευαστών τους, ακόμη και για τις υπηρεσίες που δεν είναι ενεργοποιημένες.
- Οι υπεύθυνοι των συστημάτων θα πρέπει να είναι εκπαιδευμένοι και ενημερωμένοι για αυτά.
- Το firewall θα πρέπει να είναι διαθέσιμο όλο το εικοσιτετράωρο.
- Όλες οι αλλαγές και οι αναβαθμίσεις θα πρέπει να καταγράφονται και να ακολουθούν την αντίστοιχη πολιτική.
- Θα πρέπει να υπάρχει γρήγορη και αποτελεσματική ενημέρωση σε περίπτωση που κάποιο service δεν λειτουργεί.

Αποτελεί αυτονόητο γεγονός ο τακτικός έλεγχος και παρακολούθηση του firewall για να εντοπίζονται τυχόν κακές ρυθμίσεις και για να γίνεται αναδιαμόρφωση με βάση την αποτίμηση των υπαρχόντων κινδύνων.

Πολιτική διαχείρισης και εγκατάστασης τηλεπικοινωνιακού εξοπλισμού

Η *πολιτική ασφάλειας του δικτύου πρέπει να εμπεριέχει την Πολιτική Διαχείρισης και Εγκατάστασης του τηλεπικοινωνιακού εξοπλισμού*, η οποία μάλιστα θα εξασφαλίζει ότι αλλαγές στον υπάρχοντα εξοπλισμό και η εισαγωγή καινούργιου εξοπλισμού γίνεται με τρόπο σύμφωνο με τη διασφάλιση του απορρήτου των επικοινωνιών. Οι ελάχιστες διαδικασίες που πρέπει να περιλαμβάνει το τμήμα αυτό της πολιτικής ασφάλειας είναι [8]:

- Διαδικασίες για την δοκιμή και εγκατάσταση νέου τηλεπικοινωνιακού εξοπλισμού.

- Διαδικασίες για την καταγραφή των αλλαγών που πραγματοποιούνται σε υπάρχοντα τηλεπικοινωνιακό εξοπλισμό.

- Διαδικασίες για την ενημέρωση του παρόχου αναφορικά με την πραγματοποίηση αλλαγών σε υπάρχοντα τηλεπικοινωνιακό εξοπλισμό.

- Διαδικασίες για τον καθορισμό των αρμοδιοτήτων αναφορικά με τη διαχείριση και τη διαμόρφωση του εξοπλισμού.

- Διαδικασίες για την εξουσιοδότηση μελών του προσωπικού του παρόχου, τα οποία θα εφαρμόζουν την πολιτική αυτή για τις οργανικές μονάδες του δικτύου.

Διαχείριση τηλεπικοινωνιακού εξοπλισμού

Η έννοια της διαχείρισης σε ένα δίκτυο είναι πολύ μεγάλης σημασίας. Αφορά μία σειρά κανόνων και μηχανισμών που μας επιτρέπουν την παρακολούθηση της σωστής λειτουργίας του συστήματος, την πρόληψη προβλημάτων (που οφείλονται σε βλάβες, ασφάλεια, επέκταση), τη διόρθωσή τους όταν προκύπτουν και τον μελλοντικό σχεδιασμό [9].

Επίπεδα διαχείρισης				
Λειτουργίες Διαχείρισης		**Διαχείριση Στοιχείου**	**Διαχείριση Δικτύου**	**Διαχείριση Υπηρεσίας**
	Βλάβες	Διατήρηση και επίδειξη συναγερμών	Φιλτράρισμα και επίδειξη συναγερμών	Συσχέτιση, εντοπισμός αιτίας προβλήματος
	Configuration	Configuration συσκευής	Συνόλου συσκευών	Πρόβλεψη αναγκών
	Accounting	Συλλογή λογιστικών στοιχείων συσκευής	Συγκέντρωση λογιστικών στοιχείων	Χρέωση, έλεγχος απογραφής
	Απόδοση	Στατιστικά συσκευής	Στατιστικά δικτύου	Συμβόλαιο υπηρεσιών
	Ασφάλεια	Πρόσβαση/ χρήση συσκευής	Πρόσβαση/ διαχείριση δικτύου	VPN' s

Πίνακας 1: Διαχείριση δικτύων [9]

Στην παραπάνω εικόνα φαίνονται τα τρία επίπεδα της διαχείρισης σε ένα δίκτυο και οι λειτουργίες που σχετίζονται με κάθε ένα από αυτά. Ο τρόπος που γίνεται η διαχείριση του δικτύου πρέπει να ορίζεται με σαφήνεια στην γενικότερη πολιτική ασφάλειας.

Κύριο μέλημα του προσωπικού που διαχειρίζεται το δίκτυο είναι να ενημερώνεται για τα προβλήματα ασφάλειας του τηλεπικοινωνιακού εξοπλισμού τα

οποία διαπιστώνονται από τον κατασκευαστή ή από έγκυρους οργανισμούς σχετιζόμενους με την ασφάλεια, να αξιολογεί άμεσα κάθε σχετική πληροφορία πάνω στο θέμα αυτό και να προβαίνει, όταν χρειάζεται, στις κατάλληλες αναβαθμίσεις.

Δύο συσκευές που συναντώνται σε ένα δίκτυο είναι οι διακομιστές και οι δρομολογητές [8]. Αυτό που συνίσταται για τους διακομιστές είναι να χρησιμοποιούνται για την παροχή μίας μόνο υπηρεσίας, έτσι ώστε **να ελαχιστοποιείται η πιθανότητα διαχειριστικών λαθών** και να μειώνονται τα περιθώρια για παραβίαση της ασφάλειας του εν λόγω στοιχείου. Στην περίπτωση ωστόσο που ο διακομιστής χρησιμοποιείται για την παροχή περισσότερων της μίας υπηρεσιών, θα πρέπει να απενεργοποιούνται υπηρεσίες που δεν χρησιμοποιούνται, ιδιαίτερα όταν οι υπηρεσίες αυτές σχετίζονται με τη δικτυακή πρόσβαση. Αναφορικά με τους δρομολογητές ενός δικτύου, θα πρέπει όταν είναι εφικτό να απενεργοποιούνται από αυτούς υπηρεσίες που δεν χρησιμοποιούνται. Οι δικτυακές διευθύνσεις, οι θύρες και τα πρωτόκολλα σύμφωνα με τα οποία δρομολογούνται τα δεδομένα οφείλουν να ελέγχονται και να αποτιμώνται από τον υπεύθυνο διαχειριστή και να απενεργοποιούνται οι υπηρεσίες δρομολόγησης για τα παραπάνω στοιχεία που δεν πληρούν για οποιοδήποτε λόγο τις απαιτήσεις που τίθενται από την πολιτική ασφάλειας.

Σε περίπτωση που ο τηλεπικοινωνιακός εξοπλισμός παρέχει τη δυνατότητα υλοποίησης πολλαπλών επιπέδων δικαιωμάτων πρόσβασης σε πόρους και δεδομένα του, πέραν της χρήσης των κωδικών ασφάλειας, το configuration του εξοπλισμού θα πρέπει να αξιοποιεί αυτή τη δυνατότητα. Με τον τρόπο αυτό, μειώνεται η πιθανότητα παραβίασης της ασφάλειας είτε από τυχαία ενέργεια μη εξουσιοδοτημένου χρήστη ή από προσχεδιασμένη απειλή.

Αναφορικά με την εγκατάσταση λογισμικού στον εξοπλισμό του δικτύου, θα πρέπει να γίνεται μόνο από το εξουσιοδοτημένο προσωπικό και μόνο για τους σκοπούς υποστήριξης του εξοπλισμού και των υπηρεσιών που προσφέρει. Στην πολιτική ασφάλειας θα πρέπει να προβλέπεται η διατήρηση των παλιών εκδόσεων του λογισμικού για ορισμένο χρονικό διάστημα με σκοπό την επαναφορά τους στα συστήματα του δικτύου αν διαπιστωθεί πρόβλημα λειτουργίας το οποίο οφείλεται σε εγκατάσταση νέας έκδοσης λογισμικού ή αναβάθμισης λογισμικού. Επίσης, αρμοδιότητα του εξουσιοδοτημένου προσωπικού είναι να καταγράφει σε μόνιμη βάση όλες τις πράξεις που σχετίζονται με εγκατάσταση, απεγκατάσταση, αναβάθμιση και αλλαγή διαμόρφωσης του τηλεπικοινωνιακού εξοπλισμού του παρόχου. Στην καταγραφή αυτή, που μπορεί να γίνεται είτε έντυπα είτε ηλεκτρονικά, πρόσβαση έχει μόνο το αρμόδιο προσωπικό.

Εγκατάσταση τηλεπικοινωνιακού εξοπλισμού

Ο τηλεπικοινωνιακός εξοπλισμός ενός δικτύου εγκαθίσταται εντός των ορίων της περιμέτρου του και σύμφωνα με όσα ορίζονται στην πολιτική ασφάλειας περιμέτρου. Εξαιρούνται φυσικά οι περιπτώσεις για τις οποίες χρειάζεται εγκατάσταση εκτός της περιμέτρου, προκειμένου να επιτευχθεί ορθή λειτουργία του εξοπλισμού και των υπηρεσιών που παρέχονται.

Η εγκατάσταση του τηλεπικοινωνιακού εξοπλισμού περιλαμβάνει δύο στάδια [8]:

(a) Στάδιο προετοιμασίας

(b) Στάδιο εγκατάστασης και ελέγχου ορθής λειτουργίας

Για τα δύο αυτά στάδια έχουμε τα εξής:

Στάδιο προετοιμασίας

Επειδή πάντα υφίσταται ο κίνδυνος κάποιας δυσλειτουργίας του υπό εγκατάσταση εξοπλισμού, ο κίνδυνος αυτός πρέπει να αποτιμάται. Η αποτίμηση κινδύνου περιλαμβάνει, μεταξύ άλλων και την καταγραφή των αλληλεξαρτήσεων του υπό εγκατάσταση τηλεπικοινωνιακού εξοπλισμού με τα υπάρχοντα τμήματα τηλεπικοινωνιακού εξοπλισμού που βρίσκονται σε λειτουργία στο δίκτυο του παρόχου. Η διαδικασία αποτίμησης κινδύνου καθορίζει επίσης κατά πόσον οι δοκιμές αποδοχής του εξοπλισμού θα πρέπει να διεξαχθούν σε ξεχωριστό περιβάλλον δοκιμών ή όχι. Η αποτίμηση κινδύνου γίνεται τόσο σε επίπεδο υλικού και λογισμικού όσο και σε επίπεδο δικτυακής επικοινωνίας.

Αν πρόκειται για εγκατάσταση λογισμικού, τότε πρέπει να ελέγχεται η συμμόρφωσή του με τα καθιερωμένα διεθνή πρότυπα και τις διεθνώς καθιερωμένες πρακτικές. Κατά την αναβάθμιση λογισμικού, πρέπει να αποτιμάται η εξάρτησή του από το λειτουργικό σύστημα που υπάρχει στο αντίστοιχο υλικό καθώς και η εξάρτησή του από βιβλιοθήκες λογισμικού που τυχόν χρησιμοποιούνται.

Στάδιο εγκατάστασης και ελέγχου σωστής λειτουργίας

Είναι πολύ σημαντική η διαδικασία ελέγχου της ορθής λειτουργίας του τηλεπικοινωνιακού εξοπλισμού. Ανάλογα με τα αποτελέσματα της διαδικασίας αποτίμησης κινδύνου, ο εξοπλισμός εγκαθίσταται είτε στο ξεχωριστό περιβάλλον δοκιμής είτε στο περιβάλλον παραγωγής του παρόχου. Γίνεται με αυτό τον τρόπο ο έλεγχος και μπορούν να διαπιστωθούν τυχόν προβλήματα. Αν, λοιπόν, προκύψουν προβλήματα, αυτά πρέπει να συζητούνται με τον προμηθευτή του εξοπλισμού και να γίνεται προσπάθεια να επιλυθούν. Στην περίπτωση που οι δοκιμές λαμβάνουν χώρα σε περιβάλλον παραγωγής και όχι σε ξεχωριστό δοκιμαστικό περιβάλλον, είναι προτιμότερο να γίνεται σε ώρες μη αιχμής για να μην επηρεάζεται το υπόλοιπο δίκτυο και περιβάλλον εργασίας.

Αφού λοιπόν γίνει συνολική αποτίμηση του εξοπλισμού, το υπεύθυνο προσωπικό για την όλη διαδικασία πρέπει να προτείνει αιτιολογημένα την αποδοχή ή την απόρριψή του. Αν ο εξοπλισμός γίνεται αποδεκτός, τότε μπορεί να τεθεί σε λειτουργία.

Διαδικασία χειρισμού περιστατικών ασφαλείας

Η Διαδικασία Χειρισμού Περιστατικών Ασφαλείας (ή Δ.Χ.Π.Α.) χειρίζεται καταστάσεις που απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και τη διασφάλιση του απορρήτου των επικοινωνιών. Ενεργοποιείται σε περιπτώσεις [8] που διαπιστώνεται κίνδυνος για τη διασφάλιση του απορρήτου, που έχει καταγγελθεί παραβίαση απορρήτου και που υπάρχουν σοβαρές υπόνοιες ότι δε διασφαλίζεται το απόρρητο των επικοινωνιών.

Σκοπός της ενεργοποίησης της Δ.Χ.Π.Α. είναι να καταγραφούν όλες οι λεπτομέρειες ενός περιστατικού, να ενημερωθούν οι υπεύθυνοι ασφάλειας και οι

χρήστες, να επαναδιασφαλιστεί το απόρρητο κατά το συντομότερο δυνατό και να διερευνηθούν τα αίτια.

Για τους παραπάνω λόγους, είναι απαραίτητο να ορίζεται ομάδα που θα αποτελείται από εξειδικευμένους τεχνικούς και από διοικητικά στελέχη για να χειριστεί το συμβάν. Οι τεχνικοί έχουν την ευθύνη να επιβεβαιώσουν το συμβάν και να προβούν άμεσα στην αποκατάσταση του προβλήματος ενώ τα διοικητικά στελέχη πρέπει να αξιολογήσουν και να διαχειριστούν σε συνεργασία με την τεχνική ομάδα. Με βάση την αξιολόγηση του συμβάντος, κρίνεται και ο τρόπος με τον οποίο θα αντιμετωπιστεί. Επίσης, πρέπει να ορίζεται και επικοινωνιακή πολιτική για κάθε περίπτωση ανάλογου περιστατικού. Ανάλογα με την κρισιμότητα του συμβάντος, ειδοποιούνται τα κατάλληλα στελέχη του οργανισμού.

Στον παρακάτω πίνακα, φαίνεται ο τρόπος με τον οποίο αντιμετωπίζονται τα συμβάντα με βάση την κρισιμότητά τους, αν δηλαδή αυτή κρίνεται ως «κρίσιμη», «σοβαρή», «πιθανή» ή «ελάχιστη».

Κρισιμότητα	**Ομάδα άμεσης επέμβασης:** περιλαμβάνει στοιχεία επικοινωνίας και ρόλο του κάθε προσώπου	**Ενέργειες:** περιλαμβάνουν τεχνικές επιταγές, σχέδιο αποκατάστασης και διοικητικές ενέργειες	**Επικοινωνιακή πολιτική:** περιλαμβάνει λίστα των φορέων και των ατόμων που πρέπει να λάβουν γνώση του συμβάντος και τη συχνότητα ενημέρωσης τους
Κρίσιμη	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος • Φορείς
Σοβαρή	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος • Φορείς
Πιθανή	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος • Φορείς
Ελάχιστη	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος • Φορείς

Πίνακας 2: Αντιμετώπιση συμβάντων σύμφωνα με την κρισιμότητά τους [8]

Ο πάροχος οφείλει να διατηρεί την Δ.Χ.Π.Α. ενημερωμένη με τα σωστά στοιχεία επικοινωνίας για οποιονδήποτε εμπλέκεται. Τα στοιχεία των προσώπων και φορέων που πρέπει να ειδοποιηθούν άμεσα στην περίπτωση που διαπιστώνεται κάποιο συμβάν πρέπει επαρκούν για την άμεση ειδοποίησή τους. Φυσικά, οι ενέργειες που εκτελούνται από την τεχνική ομάδα και τα τεχνικά ευρήματα που προέκυψαν πρέπει να καταγράφονται με τρόπο σαφή.

Έλεγχος ασφάλειας δικτύου

Ο έλεγχος του δικτύου ενός οργανισμού πρέπει να γίνεται από ειδική ομάδα που συγκροτείται για το σκοπό αυτό και η οποία μπορεί να είναι είτε εσωτερική (απαρτίζεται από εργαζόμενους στον οργανισμό που ανήκει το δίκτυο) είτε εξωτερική (απαρτίζεται από εξειδικευμένο προσωπικό άλλου οργανισμού, με τον οποίο συνάπτεται η κατάλληλη συμφωνία). Ο λόγος για τον οποίο πραγματοποιείται ο

έλεγχος ασφάλειας δικτύου είναι αρχικά για να εξακριβωθεί πώς διασφαλίζονται οι βασικές απαιτήσεις της ασφάλειας των πληροφοριών: ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα. Γίνεται επίσης για να παρακολουθούνται οι ενέργειες των χρηστών, όπου κάτι τέτοιο κρίνεται απαραίτητο και αφού πρώτα οι χρήστες ενημερώνονται.

Στη διαδικασία του ελέγχου ασφάλειας δικτύου, ο πάροχος έχει ορισμένες υποχρεώσεις. Οφείλει να παρέχει τα αναγκαία πρωτόκολλα, τις δικτυακές συνδέσεις και ό,τι άλλο είναι απαραίτητο για να εκτελεστεί ο έλεγχος. Σε κάθε περίπτωση, ο έλεγχος ασφάλειας πρέπει να γίνεται με τρόπο τέτοιο ώστε να μην εμποδίζεται η παροχή υπηρεσιών προς τους χρήστες και κατά τις ημερομηνίες και ώρες που έχουν προσυμφωνηθεί. Πρέπει τέλος, να λαμβάνονται όλα τα δυνατά μέτρα ώστε να ελαχιστοποιούνται οι επιρροές στην διαθεσιμότητα του δικτύου.

Αποτίμηση κινδύνων

Η Διαδικασία Αποτίμησης Κινδύνων είναι η διαδικασία εντοπισμού, ελέγχου και αξιολόγησης των τρωτών σημείων και απειλών ασφαλείας των πληροφοριακών συστημάτων του παρόχου σε ό,τι αφορά στην εμπιστευτικότητα και ακεραιότητα των δεδομένων και τη διαθεσιμότητα των παρεχόμενων υπηρεσιών. Ο σκοπός της παραπάνω διαδικασίας είναι να βοηθήσει τον πάροχο να επιλέξει τις διαδικασίες και πρακτικές που θα ελαχιστοποιήσουν την πιθανότητα παραβίασης του απορρήτου επικοινωνιών των χρηστών καθώς και το κόστος εφαρμογής τους.

Η αποτίμηση των κινδύνων πρέπει να γίνεται από ειδική ομάδα προσωπικού που περιλαμβάνει τεχνικό προσωπικό αλλά και ανώτερα στελέχη για να επιτυγχάνεται ένα κατά το δυνατό ολοκληρωμένο αποτέλεσμα που λαμβάνει υπόψη όλες τις αναγκαίες πτυχές. Η ομάδα αυτή καλείται να συνέρχεται ανά τακτά χρονικά διαστήματα αλλά και εκτάκτως, όταν προκύπτει ζήτημα ασφάλειας. Στην περίπτωση που η ομάδα ανήκει σε τρίτο (με σύμβαση υπεργολαβίας), την τελική ευθύνη για τη Διαδικασία Αποτίμησης Κινδύνων έχει ο πάροχος.

Αν θέλουμε να περιγράψουμε βηματικά τη διαδικασία, τότε μπορούμε να πούμε τα εξής [8]:

- Αρχικά, καταγράφονται οι πόροι που χρησιμοποιούνται για την παρακολούθηση, αποθήκευση και γενικότερα για κάθε είδους επεξεργασία και δημοσιοποίηση δεδομένων επικοινωνίας. Πρέπει να καταγράφονται επίσης τα ήδη ισχύοντα μέτρα ασφαλείας.
- Οι πόροι αυτοί που έχουν καταγραφεί στο προηγούμενο βήμα πρέπει να κατηγοριοποιηθούν. Σύμφωνα λοιπόν με τη σημασία τους ως προς το απόρρητο των δεδομένων που χειρίζεται ο κάθε πόρος, χαρακτηρίζεται ως «κρίσιμος», «βασικός» ή «κανονικός».
- Για τον κάθε καταγεγραμμένο πόρο, καταγράφονται όλες οι ευπάθειες που είναι δυνατό να θέσουν σε κίνδυνο το απόρρητο των επικοινωνιών των χρηστών.
- Οι ευπάθειες που καταγράφονται σε προηγούμενο βήμα χαρακτηρίζονται ως «κρίσιμες», «σημαντικές» ή «δευτερεύουσες» ανάλογα με το πόσο επικίνδυνες είναι για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών.

- Στη συνέχεια, καταγράφονται οι απειλές που είναι δυνατό να εκμεταλλευτούν μια ευπάθεια.
- Οι απειλές αυτές καταγράφονται και κατά παρόμοιο τρόπο χαρακτηρίζονται (κρίσιμη, σημαντική, δευτερεύουσα).
- Από τα παραπάνω προκύπτουν κάποια αποτελέσματα που υποδεικνύουν ποιοι συνδυασμοί «πόρου – ευπάθειας – απειλής» παρουσιάζουν τον μεγαλύτερο κίνδυνο για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών και ποιοι μικρότερο.
- Από τα δεδομένα που προκύπτουν, προτείνονται λύσεις. Η λύση που προτείνεται μπορεί να αφορά είτε τεχνικά βήματα είτε πολιτικές – διαδικασίες αντιμετώπισης του κινδύνου.
- Τέλος, επιλέγεται η λύση που αιτιολογημένα θεωρείται καταλληλότερη.

Έλεγχος και εποπτεία

Όλα τα παραπάνω αποτελούν επιμέρους τμήματα μίας ολοκληρωμένης πολιτικής ασφάλειας. Το θέμα που προκύπτει είναι αυτό του ελέγχου και της εποπτείας σχετικά με την τήρηση ή μη των παραπάνω μέτρων που διασφαλίζουν κατά την εφαρμογή τους την ασφάλεια και το απόρρητο σε ένα δίκτυο και στα δεδομένα του. Είναι λοιπόν αναγκαία η ύπαρξη μιας ανώτερης Αρχής και η επιτροπή η οποία θα την συνιστά, θα διενεργεί αυτόν τον έλεγχο.

Οι πάροχοι οφείλουν να συμμορφώνονται με τους κανονισμούς που τίθενται από την Αρχή και να θέτουν στη διάθεσή της οτιδήποτε ζητηθεί και μπορεί να διευκολύνει το έργο της. Οι αλλαγές που θέτει η Αρχή πρέπει να γίνονται αποδεκτές και να εφαρμόζονται εντός καθορισμένης προθεσμίας. Οι έλεγχοι αφορούν το σύνολο των περιπτώσεων που μελετήσαμε παραπάνω: πολιτική ασφάλειας περιμέτρου, πολιτική διαχείρισης και εγκατάσταση τηλεπικοινωνιακού εξοπλισμού, πολιτική αντιγράφων ασφαλείας, διαδικασία χειρισμού περιστατικών ασφάλειας, διαδικασία ελέγχου ασφάλειας δικτύου, διαδικασία αποτίμησης κινδύνου.

Πολιτική ασφάλειας και χρήση κρυπτογραφικών αλγορίθμων

Η κρυπτογράφηση έχει ως βασικό σκοπό να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και τη μη-αποποίηση ευθύνης στις συναλλαγές και τις επικοινωνίες μέσω του Διαδικτύου. Οι πάροχοι οφείλουν να εφαρμόζουν αλγορίθμους και τεχνικές κρυπτογράφησης τόσο στα συστήματα μετάδοσης δεδομένων που χρησιμοποιούν, όσο και στις εφαρμογές και διαδικασίες του Διαδικτύου (π.χ. ηλεκτρονικό εμπόριο, τραπεζικές συναλλαγές) που παρέχουν.

Σχετικά με τα συστήματα μετάδοσης, οι πάροχοι είναι υποχρεωμένοι να ακολουθούν τα διεθνή πρότυπα, ανάλογα με την τεχνολογία μετάδοσης που ακολουθείται. Το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο ώστε να

εξασφαλίζεται η μη παραβίασή του (εννοείται σε λογικό χρόνο και με λογικούς υπολογιστικούς πόρους). Άμεση συνέπεια αυτού, είναι ότι το κλειδί της κρυπτογράφησης πρέπει να είναι μεγάλο, αφού στη γενική περίπτωση, όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο δυσκολότερη γίνεται η παραβίαση της κρυπτογράφησης. Είναι αυτονόητο ότι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται θα πρέπει να είναι ευρέως αποδεκτοί. Πολύ γνωστοί αλγόριθμοι είναι οι RSA, Diffie-Hellman, DES, AES και IDEA.

Επιπλέον οι πάροχοι είναι υποχρεωμένοι να κάνουν χρήση των εκάστοτε ευρέως χρησιμοποιούμενων πρωτοκόλλων για την παροχή των υπηρεσιών τους. Ενδεικτικά, αναφέρονται παρακάτω, ορισμένα πρωτόκολλα ανά τύπο εφαρμογής [6]:

a. Για εφαρμογές παγκόσμιου ιστού, π.χ. ηλεκτρονικό εμπόριο, χρησιμοποιούνται τα πρωτόκολλα SSL (Secure Sockets Layer) και S-HTTP (Secure HTTP). Εξασφαλίζουν αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα στην ανταλλαγή δεδομένων μεταξύ στοιχείων του παγκόσμιου ιστού (browsers και servers).
b. Για εφαρμογές ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται τα πρωτόκολλα S/MIME και PEM (Privacy Enhanced Mail), τα οποία κάνουν χρήση ψηφιακών υπογραφών και κρυπτογράφησης στα μεταδιδόμενα μηνύματα. Χρησιμοποιείται επίσης και το PGP (Pretty Good Privacy).
c. Το SET (Secure Electronic Tsansaction) χρησιμοποιείται επίσης για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών.

Πολιτική ασφάλειας και χρήση κωδικών ασφάλειας (passwords)

Γενικά μιλώντας, έχουμε να επισημάνουμε ότι οι κωδικοί ασφάλειας είναι ένα πολύ σημαντικό πεδίο της ασφάλειας των υπολογιστών και αποτελούν την τελευταία γραμμή άμυνας ενάντια σε αυτούς που θα προσπαθήσουν να επιβουλευτούν έναν υπολογιστή ή ένα δίκτυο.

Η πολιτική ασφάλειας του παρόχου στο θέμα που αφορά τους κωδικούς ασφάλειας θα πρέπει να επιβάλει κανόνες έτσι ώστε να: (α) Δημιουργούνται συμπαγείς κωδικοί, (β) Προστατεύονται οι κωδικοί αυτοί, (γ) Μεταβάλλονται συχνά.

Αρχικά πρέπει να προσδιορίζεται ποια είναι τα συστήματα του δικτύου που χρειάζονται προστασία μέσω κωδικών πρόσβασης και σε ποια η πρόσβαση μπορεί να είναι ελεύθερη. Για να αποκτήσουν οι χρήστες πρόσβαση στα στοιχεία που προστατεύονται πρέπει να διαθέτουν login name και password. Το τμήμα της πολιτικής ασφάλειας που πραγματεύεται το ζήτημα των κωδικών ασφάλειας πρέπει επομένως να περιλαμβάνει τους κανόνες σύμφωνα με τους οποίους γίνεται η δημιουργία των ονομάτων χρηστών (user names) και τους κανόνες σύμφωνα με τους οποίους γίνεται η δημιουργία των passwords. Πρέπει επίσης να προβλέπεται η διαδικασία διανομής login name και password στον κάθε χρήστη. Για λόγους ασφάλειας, πρέπει επίσης οι κωδικοί να αλλάζουν τακτικά, γεγονός το οποίο επίσης πρέπει να προβλέπεται.

Η πολιτική ασφάλειας για τα passwords οφείλει επίσης να πληροί τα ακόλουθα χαρακτηριστικά [6]:

- Οι χρησιμοποιούμενοι κωδικοί ασφάλειας πρέπει να είναι συμπαγείς έτσι ώστε να μη μπορεί να τους μαντέψει όποιος επιβουλεύεται στο σύστημα. Το ιδανικό λοιπόν είναι το password να έχει ένα ελάχιστο μήκος και να αποτελεί συνδυασμό γραμμάτων, αριθμών και μη αλφαριθμητικών χαρακτήρων. Οι υπεύθυνοι ασφάλειας του συστήματος οφείλουν να πραγματοποιούν περιοδικούς ελέγχους προκειμένου να διαπιστώνουν κατά πόσο οι κωδικοί ασφάλειας είναι συμπαγείς. Οι έλεγχοι πρέπει να περιλαμβάνουν δοκιμές της αντοχής στις μεθόδους αποκρυπτογράφησης των υφιστάμενων κωδικών με αυτοματοποιημένο τρόπο μέσω κατάλληλων εργαλείων λογισμικού. Αν από τους ελέγχους προκύπτει η ύπαρξη ακατάλληλων κωδικών ασφάλειας, οι χρήστες που τους κατέχουν θα πρέπει άμεσα να προβαίνουν στην αντικατάστασή τους.
- Η πρόσβαση στο αρχείο που φυλάσσονται οι κωδικοί πρόσβασης επιβάλλεται να είναι περιορισμένη.
- Δεν πρέπει να χρησιμοποιείται συνεχώς ο ίδιος κωδικός ασφάλειας. Οι χρήστες πρέπει να αλλάζουν το password με συγκεκριμένη συχνότητα. Ειδικότερα σε περιπτώσεις που, για παράδειγμα, αποχωρεί κάποιος χρήστης ή παραβιάζεται κάποιος λογαριασμός η αλλαγή του κωδικού θα πρέπει να γίνεται άμεσα.
- Ως επιπλέον μέτρο μπορεί να ισχύει η αδρανοποίηση του κωδικού ασφαλείας στην περίπτωση επαναλαμβανόμενης εισαγωγής λανθασμένων passwords (π.χ. μετά από τρεις συνεχόμενες αποτυχημένες απόπειρες).

Αν ο οργανισμός που διαθέτει το δίκτυο παρέχει στους χρήστες πρόσβαση από απόσταση μέσω Internet θα πρέπει να λαμβάνει επιπλέον μέτρα για τη δημιουργία και διαχείριση των κωδικών ασφάλειας. Στα βαθμό που είναι τεχνικά δυνατό, θα πρέπει να υφίσταται μια κοινή αρχιτεκτονική ταυτοποίησης για όλες τις εφαρμογές που παρέχεται πρόσβαση μέσω Internet, η οποία να βασίζεται σε διεθνώς αποδεκτά πρότυπα.

Θα πρέπει σε κάθε περίπτωση και για κάθε εφαρμογή να αποτιμάται κατά πόσο η χρήση login name / password είναι επαρκής ή αν πρέπει να χρησιμοποιούνται πρόσθετες τεχνικές ταυτοποίησης. Υπάρχουν για παράδειγμα περιπτώσεις στις οποίες είναι απαραίτητο να παράγεται εκ νέου κωδικός ασφάλειας κάθε φορά που κάποιος χρήστης χρειάζεται να αποκτήσει πρόσβαση από απόσταση. Στις εφαρμογές αυτού του είδους, πρέπει να προδιαγράφεται μια διαδικασία δημιουργίας βραχύβιων κωδικών.

Για την προστασία των κωδικών ασφαλείας, θα πρέπει να λαμβάνονται υπόψη τα εξής [6]:

- Οι χρήστες δε θα πρέπει να μοιράζονται τον κωδικό τους με άλλους χρήστες, εκτός αν ο λογαριασμός στον οποίο αντιστοιχεί ο κωδικός προβλέπεται ρητώς για πρόσβαση πολλαπλών χρηστών.
- Οι χρήστες δε θα πρέπει να αποκαλύπτουν σε οποιονδήποτε τους κωδικούς ασφάλειας που τους έχουν δοθεί. Η απαγόρευση αυτή περιλαμβάνει και άτομα που υπό άλλες συνθήκες θεωρούνται έμπιστα (προϊστάμενους, φίλους, συνεργάτες, μέλη οικογένειας).

- Οι κωδικοί ασφάλειας δεν θα πρέπει να συμπεριλαμβάνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου.
- Οι κωδικοί δε θα πρέπει να αναφέρονται κατά τη διάρκεια τηλεφωνικών συνδιαλέξεων.
- Οι κωδικοί δεν θα πρέπει να καταγράφονται από τους χρήστες σε ερωτηματολόγια ή άλλα έγγραφα, ακόμη και αν αυτά αποτελούν επίσημα έγγραφα του παρόχου.
- Το password δεν θα πρέπει να χρησιμοποιείται για να παρέχει πρόσβαση στο σύστημα σε μη εξουσιοδοτημένα άτομα.
- Ο κωδικός ασφάλειας πρέπει να απομνημονεύεται από τον χρήστη.
- Ο χρήστης οφείλει να αναφέρει στους υπεύθυνους ασφαλείας οποιοδήποτε γεγονός υποπέσει στην αντίληψή του σχετικά με την παραβίαση της ασφάλειας του λογαριασμού του.

Πολιτική ασφάλειας και προστασία από ιούς

Στην πολιτική ασφάλειας ενός οργανισμού πρέπει να περιγράφονται διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης ιών έτσι ώστε να εξασφαλίζεται στο μέγιστο δυνατό βαθμό η προστασία του δικτύου. Είναι γνωστό πως οι ιοί μπορούν να προκαλέσουν σημαντικές καταστροφές σε ένα σύστημα, συμπεριλαμβανομένων και των παρακάτω:

(α) Καταστροφή διαβαθμισμένων – απόρρητων πληροφοριών.
(β) Υποκλοπή διαβαθμισμένων – απόρρητων πληροφοριών.
(γ) Παρακολούθηση και καταγραφή των ενεργειών των χρηστών.
(δ) Υποκλοπή διαβαθμισμένων – απόρρητων επικοινωνιών.

Υποχρεώσεις παρόχου [6]

Ο πάροχος λοιπόν, για την αποτροπή ιών, οφείλει να:

- Διαθέτει δικτυακό εξοπλισμό που περιορίζει την μετάδοση ιών. Για παράδειγμα, η μετάδοση ορισμένων ιών είναι δυνατόν να περιοριστεί μέσω χρήσης firewall, αρκεί αυτά να παραμετροποιούνται εγκαίρως.
- Διαθέτει το απαραίτητο λογισμικό για την προστασία από ιούς όλων των υπηρεσιών και εφαρμογών που παρέχει στους χρήστες.
- Διαθέτει εγκατεστημένο στο σύστημα λογισμικό προστασίας από ιούς, το οποίο θα εξετάζει αυτομάτως όλα τα εισερχόμενα δεδομένα.
- Διατηρεί μια ομάδα ειδικών για την προστασία από τους ιούς, που θα φροντίζει να ενημερώνεται σχετικά με την πιθανότητα επίθεσης από νέους ιούς με σκοπό την έγκαιρη εγκατάσταση ή /και παραμετροποίηση των μέσων προστασίας.
- Ενημερώνει τους χρήστες σχετικά με το πώς μπορούν να προστατευθούν από τους ιούς.

Για την ανίχνευση των ιών, οφείλει να:

- Ανανεώνει τα συστήματα προστασίας από ιούς ανά τακτά χρονικά διαστήματα ώστε να αποτρέπεται η μετάδοση νέων ιών.
- Εξασφαλίζει ότι όλα τα αρχεία που είναι αποθηκευμένα στα συστήματα του δικτύου και τα οποία είναι πιθανό να περιέχουν ιούς, εξετάζονται καθημερινά από προγράμματα ανίχνευσης ιών.
- Ενημερώνει τους χρήστες το συντομότερο δυνατό σε περιπτώσεις που υπάρχει έξαρση μετάδοσης κάποιου επικίνδυνου ιού. Η ενημέρωση μπορεί να γίνεται με διάφορους τρόπους. Μπορεί να γίνεται μέσω ηλεκτρονικού ταχυδρομείου, με ταυτόχρονη παρουσίαση του προβλήματος στην κεντρική σελίδα του δικτυακού τόπου του οργανισμού. Ο πάροχος πρέπει να δίνει πληροφορίες για την αντιμετώπιση του ιού παρέχοντας links σε δικτυακούς τόπους μέσω των οποίων ο χρήστης μπορεί να βρει το απαραίτητο λογισμικό για την αντιμετώπιση του ιού.
- Ενημερώνει τους χρήστες σχετικά με περιπτώσεις φάρσας, όπου ο χρήστης γίνεται αποδέκτης ενός mail που τον προειδοποιεί για την ύπαρξη ενός υποτιθέμενου ιού στο υπολογιστικό του σύστημα και τον παροτρύνει να προβεί σε ενέργειες που τελικά προκαλούν βλάβη στη σωστή λειτουργία του συστήματος.

Για την αντιμετώπιση ιών, οφείλει να:

- Ορίσει ομάδα αντιμετώπισης ιών, που θα αναλαμβάνει την ανίχνευση και αφαίρεση όλων των ιών από τα υπολογιστικά συστήματα του δικτύου.
- Απομονώνει εκτός δικτύου υπολογιστικά συστήματα στα οποία έχει ανιχνευθεί κάποιος ιός. Μέχρι ο ιός να αφαιρεθεί ολοκληρωτικά, το σύστημα είναι απαραίτητο να παραμένει εκτός δικτύου.
- Αν ο χρήστης ζητήσει βοήθεια από τον πάροχο για την αντιμετώπιση ιών, ο πάροχος πρέπει να είναι σε θέση να παραπέμψει το χρήστη σε πληροφοριακές ιστοσελίδες για να πάρει τα στοιχεία που του χρειάζονται.

Υποχρεώσεις χρηστών [6]

Για την αποτροπή ιών, ο χρήστης καλείται να:

- Αναζητά βοήθεια από τον πάροχο ή οποιονδήποτε άλλο οργανισμό που μπορεί να βοηθήσει σχετικά με οποιαδήποτε μη φυσιολογική συμπεριφορά στο δίκτυο.
- Έχει εγκατεστημένο στον υπολογιστή του ειδικό λογισμικό προστασίας από ιούς.

Για την ανίχνευση ιών, ο χρήστης συνίσταται να:

- Χρησιμοποιεί την υπηρεσία αυτόματης ενημέρωσης του λογισμικού για νέους ιούς τακτικά.
- Εξετάζει συχνά τα αρχεία του προσωπικού του υπολογιστή.

Για την αντιμετώπιση ιών, ο χρήστης συνίσταται να:

- Αποσυνδέει το υπολογιστικό του σύστημα από το δίκτυο έως ότου ο ιός αφαιρεθεί ολοκληρωτικά.
- Επικοινωνήσει με τον πάροχο και να ζητήσει πληροφορίες σχετικά με την αντιμετώπιση του ιού.

Κεφάλαιο 3

Μεθοδολογικό πλαίσιο

Εισαγωγή

Στο προηγούμενο κεφάλαιο είδαμε αναλυτικά το ζήτημα της πολιτικής ασφάλειας σε έναν οργανισμό. Εξετάσαμε τη σημασία και τα περιεχόμενα της και είδαμε τους παράγοντες αυτούς που ορίζουν το πλαίσιο αποδεκτής χρήσης ενός δικτύου μέσα από τα δικαιώματα και τις υποχρεώσεις χρηστών και παρόχου.

Αυτό που θα πρέπει να έχει γίνει ήδη σαφές είναι πως στο έγγραφο της πολιτικής ασφάλειας, το οποίο κοινοποιείται σε όλα τα μέλη ενός οργανισμού, καθορίζονται οι στόχοι της ασφάλειας καθώς και ο τρόπος με τον οποίο οι στόχοι αυτοί θα υλοποιηθούν. Περιλαμβάνει πιο συγκεκριμένα, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των συστημάτων. Παρότι όμως τα στοιχεία αυτά είναι κοινά, οι Πολιτικές Ασφάλειας παρουσιάζουν σημαντικές διαφορές μεταξύ των οργανισμών. Οι διαφορές αυτές οφείλονται στις διαφορετικές απαιτήσεις αλλά και στις διαφορετικές συνθήκες (π.χ. ισχύουσα νομοθεσία).

Σε αυτό το κεφάλαιο λοιπόν, θα επιδιώξουμε να ορίσουμε το πλαίσιο σύμφωνα με το οποίο πρέπει να υλοποιείται μία πολιτική ασφάλειας ανεξαρτήτως περιβάλλοντος, εξωτερικών παραγόντων, χρονικής περιόδου και συγκεκριμένων οργανισμών.

Πριν προχωρήσουμε στην ανάλυσή μας, πρέπει να διασαφηνίσουμε πως *η πολιτική ασφάλειας δε σχετίζεται μόνο με το πληροφοριακό σύστημα αλλά και με τον οργανισμό μέσα στον οποίο αυτό λειτουργεί*.

Ασφάλεια

Ο λόγος για το οποίο παρέχουμε μέτρα προστασίας σε ένα δίκτυο είναι ένας και μοναδικός: η ασφάλεια. Τα πρόβλημα της ασφάλειας είναι πολύ σημαντικό στα σύγχρονα πληροφοριακά συστήματα. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως παράλληλα σημαντικά τα προβλήματα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών. **Η ασφάλεια αποτελεί αναγκαία συνθήκη** και είναι απαραίτητη σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας, όπως είναι η ποιότητα και η απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας ενός οργανισμού.

Αν θέλουμε να δώσουμε έναν ορισμό [10], τότε θα πούμε πως η ασφάλεια πληροφοριακού συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του πληροφοριακού συστήματος, αλλά και το σύστημα ολόκληρο από κάθε σκόπιμη ή τυχαία απειλή.

Η δημιουργία μίας πολιτικής ασφάλειας λοιπόν, εξυπηρετεί αυτό ακριβώς το σκοπό, την ασφάλεια δηλαδή των πληροφοριών και των υπολογιστικών πόρων καθώς επίσης και την προστασία των χρηστών. **Η πολιτική θα λέγαμε πως στον τομέα της ασφάλειας αφορά το υψηλότερο επίπεδο, αυτό των διοικητικών μέτρων.** Περιλαμβάνει γενικές συστάσεις, τις οδηγίες, οι οποίες καλύπτουν μεταξύ άλλων την προσδοκώμενη συμπεριφορά των ατόμων σε έναν οργανισμό και ενημερώνει με σαφήνεια για τα ζητήματα ασφάλειας και υποδομών.

Σήμερα είναι πάρα πολλοί οι οργανισμοί των οποίων η λειτουργία και οι δραστηριότητες εξαρτώνται από την πληροφοριακή τους υποδομή. Η προστασία ενός πληροφοριακού συστήματος είναι επομένως εξαιρετικά σοβαρή υπόθεση και απαιτεί την υλοποίηση μιας μελέτης που θα απαντά με σαφήνεια σε συγκεκριμένα ερωτήματα με στόχο να αποκτήσουμε μία άποψη για την τρέχουσα κατάσταση. Ορισμένα ερωτήματα είναι:

- Ποια στοιχεία θέλουμε να προστατέψουμε; Ποια από αυτά είναι περισσότερο σημαντικά;
- Ποιες απειλές αντιμετωπίζει το σύστημά μας;
- Ποια είναι τα αδύνατα σημεία του συστήματός μας;
- Ποια μέτρα προστασίας πρέπει εν τέλει να λάβουμε;

Πληροφοριακά συστήματα

Για να κατανοήσουμε τη σημασία της δημιουργίας μίας πολιτικής ασφάλειας προσαρμοσμένης κάθε φορά σε συγκεκριμένο και διαφορετικό περιβάλλον, θα ήταν χρήσιμο να πούμε δυο λόγια για τα πληροφοριακά συστήματα και τη φύση τους.

Ένα πληροφοριακό σύστημα σχετίζεται διπλά με τον ανθρώπινο παράγοντα. Δημιουργείται από αυτόν για να τον υπηρετήσει στη συνέχεια [10]. Ο άνθρωπος όμως έχει συμπεριφορά που δύσκολα μπορεί να εκτιμηθεί ή να προβλεφθεί. Συνεπώς κανείς δεν εγγυάται ότι οι ίδιοι άνθρωποι κάτω από τις ίδιες συνθήκες θα έχουν την ίδια συμπεριφορά. Στο ζήτημα αυτό, η πολιτική ασφάλειας υποδεικνύει τον ορθό τρόπο συμπεριφοράς για τους χρήστες καθώς και τις ενέργειες στις οποίες πρέπει να προβαίνουν σε περίπτωση που αντιληφθούν παραβίαση της ασφάλειας.

Επιπλέον, τα πληροφοριακά συστήματα σχετίζονται με την πληροφορία. Η πληροφορία είναι αγαθό με ιδιαίτερα μεγάλή ζήτηση. Φέρει όμως την ιδιαιτερότητα ότι μπορεί να αναπαραχθεί άπειρες φορές χωρίς να αλλοιωθεί το πρωτότυπό της. Κατά συνέπεια, οποιαδήποτε κλοπή της δε γίνεται εύκολα αντιληπτή. Η πολιτική ασφάλειας καλείται να οχυρώνει το σύστημα και να εμποδίζει την κλοπή πληροφοριών που μπορεί να αφορούν από επιστημονική γνώση του οργανισμού μέχρι προσωπικά δεδομένα των χρηστών.

Πρέπει επίσης να σημειωθεί ότι το πληροφοριακό σύστημα μιας επιχείρησης αποτελεί σημαντική οικονομική επένδυση και στηρίζεται στην πληροφορική, τομέας που χαρακτηρίζεται από μεγάλο ρυθμό ανάπτυξης. Οι εξελίξεις είναι εξαιρετικά γρήγορες και οι κίνδυνοι για τα συστήματα δεν είναι δυνατό ποτέ να εξαλειφθούν. **Η πολιτική ασφάλειας οφείλει όμως να ορίζει τις διαδικασίες αναβάθμισης του συστήματος καθώς επίσης και την κατάρτιση που πρέπει να έχει το προσωπικό για να παρακολουθεί επιτυχώς τις εξελίξεις που συνεχώς τρέχουν.**

Ανάλυση και Διαχείριση Επικινδυνότητας

Αν και η σημασία της ασφάλειας για όσους ασχολούνται με αυτή είναι γνωστή, η ένταξή της στο πλαίσιο λειτουργίας ενός οργανισμού δεν είναι ούτε εύκολη ούτε αυτονόητη.

Ορισμένες δυσκολίες που αντιμετωπίζουν οι άνθρωποι που αναλαμβάνουν την κατοχύρωση της ασφάλειας σε ένα σύστημα είναι μεταξύ άλλων [11]: 1) Δυσκολία να αιτιολογηθεί το κόστος των μέτρων ασφαλείας, 2) Δυσκολία επικοινωνίας μεταξύ επαγγελματιών της πληροφορικής και των διοικητικών στελεχών επιχειρήσεων και οργανισμών, 3) Δυσκολία εξασφάλισης της ενεργητικής συμμετοχής των χρηστών στην προστασία του πληροφοριακού συστήματος, 4) Λανθασμένη επικρατούσα αντίληψη ότι η ασφάλεια αποτελεί αποκλειστικά τεχνικό ζήτημα, 5) Ο προσδιορισμός και η αποτίμηση των οργανωσιακών επιπτώσεων από την εφαρμογή ενός σχεδίου ασφάλειας.

Ορισμένες από τις παραπάνω δυσκολίες είναι εύλογο να προκύπτουν αν αναλογιστεί κανείς την ίδια τη φύση της ασφάλειας. Η ανάγκη για ένα μέτρο προστασίας μπορεί να αποδειχθεί ακόμα και αφού έχει συμβεί κάποια ευπάθεια και είμαστε αναγκασμένοι να υποστούμε τις συνέπειες. Αναφορικά με την επικοινωνία των ειδικών της πληροφορικής με τα διοικητικά στελέχη, η δυσκολία έγκειται στο ότι είναι δύσκολο να αιτιολογηθούν τα μέτρα ασφαλείας με χρηματοοικονομικούς όρους. Αυτό φέρει ως αποτέλεσμα τη μη εξασφάλιση της διαρκούς υποστήριξης της ανώτερης διοίκησης. Η επιβολή ασφάλειας γίνεται περισσότερο δύσκολη όταν προτείνονται μέτρα με διοικητικό και οργανωτικό χαρακτήρα. Η διοίκηση και οι χρήστες ανησυχούν για τις επιπτώσεις αυτών των μέτρων, ειδικότερα όταν αμφισβητείται η παγιωμένη αντίληψη ότι το ζήτημα της ασφάλειας είναι ένα τεχνικό ζήτημα.

Επιπλέον, αναφέραμε ήδη πως για την επιβολή μέτρων προστασίας είναι απαραίτητη η μελέτη του συστήματος για να εντοπίζονται οι πόροι που χρήζουν προστασίας, τα αδύνατα σημεία και οι ενδεχόμενες απειλές. Αν εντοπιστούν τα παραπάνω, τότε θα έχει δοθεί σε ικανοποιητικό βαθμό μία άποψη για την τρέχουσα κατάσταση που θα μας βοηθήσει να λάβουμε τα αναγκαία μέτρα Πρέπει ωστόσο να επισημάνουμε ότι οι απειλές έχουν δυναμικό χαρακτήρα και χρειάζεται η συνεχής παρακολούθηση της ασφάλειας στο σύστημα. Η **ανάλυση και διαχείριση**

επικινδυνότητας σε ένα πληροφοριακό σύστημα δίνει τις απαντήσεις στα παραπάνω ερωτήματα.

Επικινδυνότητα

Η ανάλυση της επικινδυνότητας (risk analysis) υποδεικνύει τα μέτρα που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν το σύστημα. Η προαναφερθείσα μεθοδολογία υιοθετεί την έννοια της επικινδυνότητας (προέρχεται από το χώρο της χρηματοοικονομικής διοίκησης), η οποία εξαρτάται από την πιθανότητα πραγματοποίησης ενός επεισοδίου ασφάλειας και από το κόστος που αυτό θα επιφέρει.

Αναφέραμε τις έννοιες «πιθανότητα» και «κόστος». Για την κάθε μία από αυτές, έχουμε να αναφέρουμε τα εξής:

- Η **πιθανότητα** πραγματοποίησης ενός επεισοδίου εκτιμάται ως συνάρτηση της πιθανότητας εμφάνισης μιας απειλής και της ευπάθειας του συστήματος που, αν δε ληφθεί υπόψη, θα επιτρέψει στην απειλή να πραγματοποιηθεί.
- Το **κόστος** από την πραγματοποίηση ενός επεισοδίου εκτιμάται με βάση την επίπτωση που θα έχει η ζημιά πάνω στα περιουσιακά στοιχεία του οργανισμού. Η ζημιά εννοείται πως είναι αντίστοιχη της αξίας των στοιχείων αυτών.

Μέσω λοιπόν της ανάλυση επικινδυνότητας δίνεται η δυνατότητα αποτίμησης της επικινδυνότητας σε χρηματικούς όρους, έτσι ώστε να συγκριθεί με το κόστος των σχετικών αντιμέτρων που χρειάζεται να ληφθούν.

Το ακόλουθο βήμα της ανάλυσης επικινδυνότητας είναι η διαχείρισή της. Η διαχείριση επικινδυνότητας είναι ο αντικειμενικός στόχος και αφορά τον έλεγχο της επικινδυνότητας ώστε να παραμένει σε αποδεκτά επίπεδα. Η επικινδυνότητα μπορεί να μειωθεί (με εφαρμογή των κατάλληλων μέτρων), να μεταβιβαστεί (με ασφάλιση) ή να αναληφθεί (αποδοχή των συνεπειών αν συμβεί επεισόδιο) [11].

Μεθοδολογία της ανάλυσης και διαχείρισης επικινδυνότητας

Η μεθοδολογία της ανάλυσης και διαχείρισης επικινδυνότητας υιοθετεί τις βασικές αρχές και το υπόβαθρο της στατιστικής επιστήμης και των πιθανοτήτων. Πιο συγκεκριμένα, γίνεται κατά κύριο λόγο χρήση του κλάδου της στατιστικής Bayes.

Η στατιστική κατά Bayes θεμελιώνει την άποψη ότι η πιθανότητα να συμβεί ένα γεγονός στο μέλλον αποτελεί μετρήσιμο μέγεθος. Η πιθανότητα αυτή μπορεί να προσδιοριστεί, αν αναλυθούν οι παράγοντες από τους οποίους εξαρτάται. Για να γίνουμε περισσότερο σαφείς, ας πάρουμε ένα παράδειγμα από τον τομέα της ασφάλειας, που άλλωστε είναι και αυτός που μας ενδιαφέρει. Για να υπολογίσουμε την πιθανότητα να κλαπούν τα απόρρητα δεδομένα που διατηρούμε στον υπολογιστή μας, θα λάβουμε υπόψη τη πιθανότητα ένας επίδοξος εισβολέας να προσπαθήσει να εισβάλει στον υπολογιστή μας και την πιθανότητα η εισβολή αυτή να είναι πετυχημένη. Στη γλώσσα της ανάλυσης επικινδυνότητας, η πρώτη πιθανότητα μας δίνει το μέγεθος της απειλής και η δεύτερη μας δίνει το μέγεθος της ευπάθειας του συστήματός μας [11].

Ορισμένα στάδια που θα πρέπει να ακολουθηθούν κατά την ανάλυση επικινδυνότητας είναι τα παρακάτω:

- Προσδιορισμός και αποτίμηση των αγαθών.
- Εκτίμηση της απειλής.
- Εκτίμηση της ευπάθειας.
- Εκτίμηση των υφιστάμενων μέτρων προστασίας.
- Υπολογισμός της επικινδυνότητας.

Με τα παραπάνω ολοκληρώνεται η ανάλυση της επικινδυνότητας και ακολουθεί η διαχείριση της επικινδυνότητας. Ο στόχος είναι ο περιορισμός της επικινδυνότητας εντός αποδεκτών ορίων και σε γενικές γραμμές, τα στάδια της διαχείρισης είναι:

- Επιλογή αντιμέτρων.
- Καθορισμός πολιτικής ασφάλειας.
- Σύνταξη σχεδίου ασφάλειας. Το Σχέδιο Ασφάλειας αποτελεί το βασικό εργαλείο για τη διαχείριση της επικινδυνότητας και περιλαμβάνει την πολιτική ασφάλειας, τα αντίμετρα και τη στρατηγική εφαρμογής του σχεδίου.
- Εφαρμογή και παρακολούθηση του σχεδίου ασφάλειας.

Το εύλογο ερώτημα βέβαια που τίθεται είναι σε ποιο βαθμό μπορούμε να περιορίσουμε την επικινδυνότητα και αν μπορούμε εν τέλει να την μηδενίσουμε.

Μηδενική επικινδυνότητα

Μηδενική επικινδυνότητα έχουμε όταν, είτε η αξία των στοιχείων του συστήματος είτε η πιθανότητα πραγματοποίησης ενός επεισοδίου ασφάλειας είναι ίσες με το μηδέν. Αν λοιπόν, κατά την ανάλυση επικινδυνότητας εντοπίσουμε ότι κάποια στοιχεία του συστήματος έχουν ελάχιστη/μηδενική αξία τότε δε θα τα συμπεριλάβουμε στη διαχείριση επικινδυνότητας [11]. Ο λόγος είναι αυτονόητος: δεν έχει νόημα να ξοδεύουμε χρήματα και πόρους για να προστατεύουμε στοιχεία χαμηλής αξίας.

Αντίστροφα, μπορεί να έχουμε στοιχεία σημαντικής αξίας και να την μειώσουμε ή να την μηδενίσουμε. Ένα χαρακτηριστικό παράδειγμα είναι αυτό της τήρησης προσωπικών δεδομένων στο σύστημά μας. Για να προστατέψουμε τα προσωπικά δεδομένα απαιτείται υψηλό κόστος. Είναι λοιπόν πιθανό να αποφασίσουμε ότι δε συμφέρει να διατηρούμε τέτοιου είδους δεδομένα και να διακόψουμε τη συλλογή τους. Μπορούμε όμως να επιλέξουμε τη διέξοδο του outsourcing, αναθέτοντας την προστασία των ευαίσθητων δεδομένων σε τρίτους.

Σχετικά με το αν μπορούμε να μηδενίσουμε την πιθανότητα να συμβεί ένα περιστατικό ασφάλειας, η απάντηση είναι «όχι». Οι απειλές που αντιμετωπίζει ένα ανοιχτό σύστημα που λειτουργεί σε δυναμικό περιβάλλον χαρακτηρίζονται από συνεχή μεταβλητότητα, γεγονός που τις καθιστά εξαιρετικά σύνθετες. Δε πρέπει επίσης να ξεχνάμε ότι οι επιθέσεις και οι απειλές εναντίον των πληροφοριακών συστημάτων είναι αποτέλεσμα κακόβουλης ανθρώπινης συμπεριφοράς, που ούτως ή άλλως είναι εξαιρετικά δύσκολο να προβλεφθεί και να μοντελοποιηθεί.

Αφού λοιπόν ο μηδενισμός της επικινδυνότητας δεν είναι εφικτός, η προσοχή εστιάζεται στον περιορισμό της σε αποδεκτά επίπεδα.

Πλεονεκτήματα και μειονεκτήματα

Η ανάλυση και διαχείριση επικινδυνότητας παρουσιάζει τόσο πλεονεκτήματα όσο και μειονεκτήματα. Αναφορικά με τα πλεονεκτήματα έχουμε να επισημάνουμε τα εξής [11]:

- Το κόστος των μέτρων που λαμβάνονται για την προστασία του συστήματος, πλέον αιτιολογείται.
- Αποτελεί ένα εργαλείο επικοινωνίας ανάμεσα στους ειδικούς της πληροφορικής και τη διοίκηση του οργανισμού, καθώς επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντάς την ασφάλεια ως επένδυση που αποτιμάται με όρους κόστους/ οφέλους.
- Διευκολύνει την καλύτερη κατανόηση της φύσης και της λειτουργίας του πληροφοριακού συστήματος αφού αποτελεί ένα μέσο ανάλυσης και τεκμηρίωσής του.
- Έχει εφαρμοστεί με επιτυχία σε πλήθος περιπτώσεων.

Η μεθοδολογία της ανάλυσης και διαχείρισης επικινδυνότητας παρουσιάζει όμως και σημαντικά μειονεκτήματα. Εντοπίζουμε τα παρακάτω [11]:

- Μπορεί να στηρίζεται σε ένα απλοϊκό μοντέλο του ΠΣ και αγνοεί τα ιδιαίτερα χαρακτηριστικά και τις απαιτήσεις του οργανισμού στον οποίο ανήκει το ΠΣ.
- Η αξία των αγαθών και το μέγεθος των απειλών εκτιμώνται υποκειμενικά. Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών – πιθανοτικών μοντέλων, στα οποία στηρίζεται και την «αντικειμενικότητα» των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.
- Βασίζεται σε απλές στατιστικές μεθόδους για τον υπολογισμό της πιθανότητας μιας απειλής, γεγονός που έχει αμφισβητηθεί από σχετικούς ερευνητές.

Η μέθοδος CRAMM

Μία δημοφιλής μέθοδος ανάλυσης και διαχείρισης επικινδυνότητας η οποία υποστηρίζεται μάλιστα και από software tools είναι η CRAMM [11]. Η πλήρης ονομασία της μεθόδου είναι CCTA Risk Analysis and Management Method και αναπτύχθηκε από την υπηρεσία Central Computer and Telecommunications Agency (CCTA) της Βρετανίας. Εκεί εφαρμόζεται από δημόσιους οργανισμούς ενώ γενικά είναι η πιο διαδεδομένη μέθοδος στον ευρωπαϊκό χώρο και έχει εφαρμοστεί επιτυχώς σε μεγάλο αριθμό μεσαίων και μεγάλων οργανισμών.

Αναφορικά με το λογισμικό της μεθόδου, αυτό έχει τον ακόλουθο ρόλο:

- παρακολουθεί την εφαρμογή της μεθοδολογίας για να διαπιστωθεί η σωστή ή όχι εφαρμογή της και αποθηκεύει τα στοιχεία που συλλέγονται,
- υποστηρίζει όλους τους σύνθετους υπολογισμούς που απαιτούνται για τον προσδιορισμό της επικινδυνότητας,
- ενσωματώνει μία βιβλιοθήκη αντιμέτρων και τους μηχανισμούς συμπερασματολογίας που αυτά επιλέγουν και

- παρέχει reports για όλα τα στάδια της μεθόδου.

Η ανάλυση και διαχείριση επικινδυνότητας με τη μέθοδο CRAMM ακολουθεί τα παρακάτω τρία κύρια στάδια:

1. Προσδιορισμός και αξιολόγηση των αγαθών.
2. Ανάλυση επικινδυνότητας.
3. Διαχείριση επικινδυνότητας.

Αναφέραμε ήδη ότι η σωστή και ομαλή συνεννόηση μεταξύ της τεχνικής ομάδας και της Διοίκησης του οργανισμού είναι πολύ σημαντική για τη λήψη μέτρων που αφορούν στην ασφάλεια. Πριν την εφαρμογή της CRAMM λοιπόν, απαιτείται συνάντηση της ομάδας εργασίας με τη Διοίκηση. Στη συνάντηση αυτή προσδιορίζονται τα ακόλουθα ζητήματα:

- Τα όρια της μελέτης
- Οι χρήστες των δεδομένων και τα άτομα που θα συνεργαστούν για τη μελέτη.
- Η εξασφάλιση εξουσιοδότησης για συλλογή των απαιτούμενων στοιχείων και για διεξαγωγή των συνεντεύξεων.
- Το χρονοδιάγραμμα και το πλάνο διεξαγωγής της μελέτης.

Προσδιορισμός και αξιολόγηση των αγαθών

Το πρώτο στάδιο της μεθόδου CRAMM αναφέρεται στον προσδιορισμό και την αξιολόγηση των στοιχείων του ΠΣ που χρήζουν προστασίας. Αποτελείται από τα παρακάτω βήματα:

Βήμα 1 : Δημιουργία του μοντέλου του ΠΣ

Εδώ είναι το στάδιο που προσδιορίζονται τα στοιχεία που απαιτούν προστασία. Στα στοιχεία κατατάσσονται το λογισμικό, το υλικό, τα δεδομένα και τα τηλεπικοινωνιακά μέσα. Δημιουργείται λοιπόν, στα πλαίσια της CRAMM, ένα μοντέλο του συστήματος που παρουσιάζει τις συσχετίσεις μεταξύ αυτών των στοιχείων. Η δημιουργία ακολουθεί τα παρακάτω βήματα:

- Προσδιορίζονται και ομαδοποιούνται τα δεδομένα που επεξεργάζεται το ΠΣ.
- Προσδιορίζεται το υλικό που υποστηρίζει την επεξεργασία των δεδομένων.
- Προσδιορίζονται οι χώροι που βρίσκονται τα υλικά στοιχεία.
- Προσδιορισμός λογισμικού που χρησιμοποιείται στην επεξεργασία των δεδομένων.
- Δημιουργία των μοντέλων που συσχετίζουν τα παραπάνω.
- Το μοντέλο που προκύπτει εισάγεται στο λογισμικό της CRAMM.

Βήμα 2 : Αποτίμηση των στοιχείων του ΠΣ

Ο στόχος στο στάδιο αυτό είναι να προσδιοριστεί η σπουδαιότητα που έχουν τα δεδομένα για τον οργανισμό. **Εντοπίζονται με αυτό τον τρόπο τα δεδομένα που χρήζουν ιδιαίτερης προστασίας και πιο συγκεκριμένα, το είδος της προστασίας που απαιτείται. Η αξία των δεδομένων εκτιμάται με βάση την επίπτωση που θα έχει η απώλειά τους.** Συγκεκριμένα, εξετάζεται το μέγεθος της επίπτωσης στις περιπτώσεις της καταστροφής, της μη-εξουσιοδοτημένης μεταβολής, της αποκάλυψης και της μη-διαθεσιμότητας. Ειδικότερα, εξετάζονται οι εξής περιπτώσεις:

- *Μη-διαθεσιμότητα* [Λιγότερο από 15 λεπτά, 1 ώρα, 3 ώρες, 12 ώρες, 1 μέρα, 2 μέρες, 1 εβδομάδα, 2 εβδομάδες, 1 μήνα, 2 μήνες και περισσότερο].
- *Καταστροφή* [Απώλεια των δεδομένων μετά την τελευταία λήψη εφεδρικού αντιγράφου. Απώλεια όλων των δεδομένων και του αντιγράφου].
- *Αποκάλυψη* [Αποκάλυψη των δεδομένων σε άτομα εντός του οργανισμού. Αποκάλυψη των δεδομένων σε άτομα εκτός του οργανισμού. Αποκάλυψη των δεδομένων σε παρόχους υπηρεσιών].
- *Μη-εξουσιοδοτημένη μεταβολή* [Μικρής έκτασης λάθη. Μεγάλης έκτασης λάθη].
- *Ηθελημένη μεταβολή των δεδομένων*.
- *Λάθη μετάδοσης δεδομένων*.

Για κάθε περίπτωση εκτιμάται το χειρότερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίησή του. Το μέγεθος της επίπτωσης εκτιμάται ποσοτικά με βάση την κλίμακα 1-10. Η μεθοδολογία παρέχει οδηγίες για την αποτίμηση των επιπτώσεων που ανήκουν στις παρακάτω κατηγορίες:

- Επιπτώσεις που αφορούν τη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων.
- Επιπτώσεις από την αποκάλυψη προσωπικών πληροφοριών.
- Νομικές επιπτώσεις.
- Παρεμπόδιση της εφαρμογής της δικαιοσύνης και της εξιχνίασης αξιόποινων πράξεων.
- Οικονομικές απώλειες.
- Διατάραξη της δημόσιας τάξης.
- Εφαρμογή της πολιτικής του οργανισμού.
- Απώλεια της εμπιστοσύνης του κοινού στον οργανισμού.

Επίσης αποτιμώνται το λογισμικό και το υλικό του ΠΣ. Η αποτίμησή τους γίνεται βάση του κόστους αντικατάστασής τους.

Το λογισμικό της CRAMM, βάση του μοντέλου του ΠΣ, υπολογίζει την έμμεση αξία των στοιχείων του ΠΣ. Π.χ., η απώλεια ενός υπολογιστή συνεπάγεται και απώλεια των δεδομένων που επεξεργάζεται και η αξία των τελευταίων θα πρέπει να προστεθεί στην αξία του υπολογιστή. Η αποτίμηση των στοιχείων του ΠΣ βασίζεται σε συνεντεύξεις που γίνονται με χρήση δομημένων ερωτηματολογίων. Συνεντεύξεις λαμβάνονται από το τεχνικό και το διοικητικό προσωπικό, καθώς και από τους χρήστες των υπηρεσιών του συστήματος.

Βήμα 3 : Επιβεβαίωση και επικύρωση της αποτίμησης

Η αποτίμηση που προηγήθηκε στο προηγούμενο βήμα θα πρέπει να επιβεβαιωθεί από τη διοίκηση του οργανισμού. Η ομάδα εργασίας παρουσιάζει λοιπόν, τα αποτελέσματα του πρώτου σταδίου στη διοίκηση, σε μορφή έκθεσης. Τα αποτελέσματα εξετάζονται και επικυρώνονται. Η αποτίμηση λοιπόν, περιλαμβάνει:

- Τον ορισμό του προς ανάλυση συστήματος και των ορίων του.
- Τη μέθοδο εργασίας που ακολουθήθηκε.
- Την αποτίμηση των δεδομένων, του υλικού και του λογισμικού του ΠΣ.
- Γενικά συμπεράσματα του πρώτου σταδίου.

Ανάλυση επικινδυνότητας

Στη φάση αυτή και αφού αποτιμήθηκε η **αξία** των στοιχείων του ΠΣ, υπολογίζονται: 1) το επίπεδο των **Απειλών** και 2) το επίπεδο των **Αδυναμιών** του συστήματος.

Από τον συνδυασμό των τριών παραπάνω παραγόντων θα προκύψει ο ***Βαθμός Επικινδυνότητας*** *του συστήματος έτσι ώστε να επιλεγούν τα κατάλληλα αντίμετρα.*

Βήμα 1 : Προσδιορισμός των Απειλών που αφορούν το κάθε αγαθό

Το βήμα αυτό αφορά τον προσδιορισμό συγκεκριμένων απειλών για κάθε αγαθό του συστήματος.

Η CRAMM παρέχει έναν ενδεικτικό κατάλογο απειλών καθώς και συστάσεις για το ποιες κατηγορίες αγαθών ενός ΠΣ απειλούνται από τη συγκεκριμένη απειλή. Το λογισμικό έχοντας ένα πλήρες μοντέλο του ΠΣ έχει τη δυνατότητα να συνυπολογίσει πως όταν ένα από τα αγαθά του ΠΣ αντιμετωπίσει μια απειλή, τότε τόσο τα δεδομένα όσο και οι υπηρεσίες που αυτό υποστηρίζει αντιμετωπίζουν την ίδια απειλή. Για παράδειγμα, αν κλαπεί ένας Η/Υ τότε και τα δεδομένα που βρίσκονται αποθηκευμένα σε αυτόν θα κλαπούν μαζί του. Έτσι, ο αναλυτής δε χρειάζεται να υπολογίζει ο ίδιος όλες τις συσχετίσεις και αλληλεπιδράσεις.

Βήμα 2 : Εκτίμηση των Απειλών και Αδυναμιών

Για κάθε συνδυασμό Απειλής –Αγαθού εκτιμώνται το μέγεθος της απειλής και η σοβαρότητα των Αδυναμιών που μπορεί να οδηγήσουν στην πραγματοποίηση της απειλής. **Η εκτίμηση γίνεται βάση δομημένων ερωτηματολογίων στην κλίμακα 1-5 (very low, low, medium, high, very high).** Βάση των απαντήσεων, η εκτίμηση της απειλής γίνεται αυτόματα. Αντίστοιχα, για τις αδυναμίες συμπληρώνονται τα ερωτηματολόγια των αδυναμιών και υπολογίζεται η σοβαρότητα της αδυναμίας σε κλίμακα 1-3 (low, medium, high).

Το εργαλείο παρέχει ερωτηματολόγια για κάθε συνδυασμό Απειλής-Αγαθού. Οι απαντήσεις των ερωτηματολογίων εισάγονται στο εργαλείο και εκείνο υπολογίζει το επίπεδο των Απειλών και των Αδυναμιών παρέχοντας μία αναφορά ώστε να αξιολογηθούν τα αποτελέσματα της διαδικασίας αυτής.

Βήμα 3 : Υπολογισμός της επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής

Η CRAMM υπολογίζει τον Βαθμό Επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής, προκύπτει δηλαδή συγκεκριμένη αποτίμηση της επικινδυνότητας για κάθε επιμέρους συνδυασμό. Ουσιαστικά, ο Βαθμός Επικινδυνότητας απεικονίζει τις απαιτήσεις ασφάλειας για κάθε αγαθό του ΠΣ, καθώς μεγαλύτερη επικινδυνότητα συνεπάγεται υψηλότερες απαιτήσεις ασφάλειας. Ο υπολογισμός του Βαθμού επικινδυνότητας ακολουθεί την κλίμακα 1-7.

Στο σημείο αυτό θα τονίσουμε τη σημασία της υποστήριξης των υπολογισμών από το λογισμικό του CRAMM. Το πλήθος των συνδυασμών Αγαθού-Απειλής και κυρίως η πολυπλοκότητα της αλληλοσυσχέτισης των Αγαθών κάνουν πρακτικά αδύνατο τον εμπειρικό και χειρόγραφο υπολογισμό της επικινδυνότητας.

Βήμα 4 : Επιβεβαίωση και επικύρωση του Βαθμού Επικινδυνότητας

Τα αποτελέσματα που προκύπτουν από την εκτίμηση του Βαθμού Επικινδυνότητας θα πρέπει να εγκριθούν από την διοίκηση του οργανισμού. Προκύπτει λοιπόν η Αποτίμηση της Επικινδυνότητας που περιλαμβάνει:

- Περιγραφή των απειλών και των αδυναμιών που συνδέονται με αυτές.
- Εκτίμηση της σοβαρότητας κάθε απειλής και αδυναμίας.
- Εκτίμηση του Βαθμού επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής.
- Γενικά συμπεράσματα σχετικά με την επικινδυνότητα του ΠΣ.

Διαχείριση επικινδυνότητας

Με βάση τα αποτελέσματα της Ανάλυσης επικινδυνότητας που προηγήθηκε, η CRAMM παράγει ένα προτεινόμενο σχέδιο ασφάλειας. Το σχέδιο ασφάλειας αποτελείται από μία σειρά αντιμέτρων τα οποία θεωρούνται απαραίτητα για τη διαχείριση της επικινδυνότητας και τα οποία θα πρέπει φυσικά να εφαρμοστούν. **Περιλαμβάνει επίσης και μία σειρά εναλλακτικών επιλογών, ώστε να παρέχεται ευελιξία στην εφαρμογή του.** Πρέπει επίσης να αναφερθεί ότι λαμβάνεται υπόψη και το κόστος που έχουν τα αντίμετρα για τον οργανισμό.

Βήμα 1 : Προσδιορισμός της λίστας των προτεινόμενων αντιμέτρων

Το λογισμικό της μεθόδου CRAMM **διαθέτει μία βάση τεχνικών, διοικητικών και οργανωτικών αντιμέτρων** (περίπου 2000 αντίμετρα). Επιλέγεται λοιπόν αυτόματα ένας κατάλογος προτεινόμενων αντιμέτρων με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας. Από αυτόν τον κατάλογο θα πρέπει να γίνουν συγκεκριμένες επιλογές. Τα κριτήρια που λαμβάνονται υπόψη στην τελική επιλογή περιλαμβάνουν μεταξύ άλλων τα εξής:

- Την επίδραση που θα έχουν τα αντίμετρα στη λειτουργία του οργανισμού.
- Το διαθέσιμο budget για την ασφάλεια του ΠΣ.
- Το κόστος (χρηματικό + ανθρώπινοι πόροι) εγκατάστασης και λειτουργίας των αντιμέτρων.
- Τα μελλοντικά σχέδια του οργανισμού για ανάπτυξη ή επέκταση του συστήματος.
- Την άποψη της διοίκησης και τους στόχους της.
- Τις ενδείξεις ότι οι απειλές θα αυξηθούν στο μέλλον.
- Την αποτελεσματικότητα των αντιμέτρων. Συγκεκριμένα για τον παράγοντα αυτό, τα αντίμετρα χωρίζονται στις παρακάτω κατηγορίες ανάλογα με το στόχο τους και δίνονται με φθίνουσα σειρά αποτελεσματικότητας:
    - Μείωση των απειλών
    - Μείωση των αδυναμιών
    - Μείωση της επίπτωσης
    - Ανίχνευση της παραβίασης της ασφάλειας
    - Ανάκαμψη

Το λογισμικό δίνει τη δυνατότητα να παρακολουθηθεί η εφαρμογή τους μέσω της λειτουργίας «Κατάσταση Υλοποίησης Αντιμέτρων». Ένα αντίμετρο μπορεί να βρίσκεται σε μία από τις ακόλουθες καταστάσεις:

- Εγκατεστημένο
- Επιλεγμένο για εγκατάσταση

- Υπό υλοποίηση
- Έχει υλοποιηθεί
- Έχει ήδη καλυφθεί από άλλο αντίμετρο
- Αναλαμβάνεται η επικινδυνότητα (!) και δεν υλοποιείται
- Υπό συζήτηση
- Μη εφαρμόσιμο

Βήμα 2 : Κατάρτιση Σχεδίου – Πλάνου Ασφάλειας

Στο βήμα αυτό που είναι και το τελευταίο καταρτίζεται το Σχέδιο Ασφάλειας. Αυτό περιλαμβάνει την πολιτική Ασφάλειας και το Σχέδιο Εφαρμογής των Αντιμέτρων.

Η CRAMM παρέχει μία δομή για Security Policy. Το Σχέδιο Εφαρμογής Αντιμέτρων περιέχει τις επιπλέον ενέργειες που πρέπει να γίνουν για την ασφάλεια του πληροφοριακού συστήματος. Κεντρικό στοιχείο του είναι το σύνολο των αντιμέτρων, τα οποία ιεραρχούνται με βάση τις προτεραιότητες εφαρμογής τους. **Το σχέδιο ασφάλειας αποτελεί το κύριο προϊόν όλου του έργου.**

Μέθοδος CRAMM: Προϋποθέσεις επιτυχίας και προβλήματα

Αρκετές είναι οι φορές που κάναμε αναφορά στη συμμετοχή και τον ενεργό ρόλο της Διοίκησης ενός οργανισμού. Θα πρέπει να έχει γίνει σαφές ότι για την επιτυχία της μεθόδου CRAMM η συνεργασία των στελεχών είναι αναγκαία συνθήκη, κυρίως κατά τις διαδικασίες αξιολόγησης των αγαθών και εκτίμησης απειλών και αδυναμιών. Επιπλέον, απαιτείται προσεκτική επιλογή του δείγματος για τη διενέργεια συνεντεύξεων, με αρμόδια στελέχη σε διάφορα επίπεδα ιεραρχίας και ειδικότητας. Τέλος, σημαντική παράμετρο και βασική προϋπόθεση διασφάλισης ενός ελάχιστου πλαισίου επιτυχίας αποτελεί η ακριβής οριοθέτηση της μελέτης που θα συμβάλει στο να μη τεθεί σε κίνδυνο η διεκπεραίωση της.

Πλεονεκτήματα και μειονεκτήματα

Πλεονεκτήματα μεθόδου CRAMM

- Καλύπτει το σύνολο των σταδίων ανάλυσης και διαχείρισης επικινδυνότητας.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας (π.χ. θέματα προσωπικού, διαδικασιών, τεχνικά θέματα, φυσική ασφάλεια κλπ).
- Έχει δοκιμαστεί επιτυχώς και υπάρχει μεγάλη διεθνής εμπειρία από την εφαρμογή της.
- Συνοδεύεται από αυτοματοποιημένο εργαλείο που διευκολύνει την εφαρμογή της και επιλέγει αντίμετρα από μία μεγάλη βιβλιοθήκη αντιμέτρων.

Μειονεκτήματα μεθόδου CRAMM

- Στηρίζεται σε μεγάλο βαθμό στη συνεργασία των αναλυτών με τους χρήστες και τη διοίκηση του οργανισμού ενώ στηρίζεται σημαντικά στις απόψεις των χρηστών.
- Έχει υψηλό κόστος εφαρμογής από άποψης χρόνου και ανθρώπινης προσπάθειας.

- Εστιάζει ουσιαστικά μόνο στα δεδομένα και λαμβάνει υπόψη τον ανθρώπινο παράγοντα μόνο ως απειλή.
- Απαιτεί μερικές φορές την επέμβαση του αναλυτή για την προσαρμογή των αποτελεσμάτων των αυτόματων υπολογισμών.
- Το τελικό αποτέλεσμα στηρίζεται σε μεγάλο βαθμό σε υποκειμενικές εκτιμήσεις, οι οποίες όμως συχνά δε γίνονται αντιληπτές ως τέτοιες.
- Απαιτεί επεξεργασία των προτεινόμενων αντιμέτρων (π.χ. ομαδοποίηση, εξειδίκευση) για την προσαρμογή τους στο υπό μελέτη ΠΣ. Πολλά από τα αντίμετρα είναι πολύ γενικά.

Άξονες της πολιτικής ασφάλειας

Πρέπει να γίνει απολύτως σαφές ότι η καθεμία πολιτική ασφάλειας διαφέρει από την άλλη αφού οι απαιτήσεις και οι ιδιαιτερότητες που παρουσιάζει κάθε οργανισμός δεν είναι ίδιες. Υπάρχουν ωστόσο κάποιοι γενικοί άξονες που διαμορφώνουν μία πολιτική ασφάλειας και ο κάθε άξονας αντιπροσωπεύει ένα σύνολο από οδηγίες που αφορούν συγκεκριμένους τομείς στην ασφάλεια [12].

Ζητήματα προσωπικού

Τα μέτρα που λαμβάνονται σε αυτή τη κατηγορία αφορούν στη μείωση της επικινδυνότητας που οφείλεται σε ανθρώπινα λάθη ή απάτη/κλοπή/κατάχρηση των πόρων του πληροφοριακού συστήματος. Στοχεύουν επίσης στην ενημέρωση και κατάρτιση των χρηστών πάνω σε ζητήματα και απειλές ασφάλειας. Τα μέτρα που υπάγονται στον άξονα αυτό, μπορεί να αφορούν τα παρακάτω:

- Τον καθορισμό ρόλων και υπευθυνοτήτων για την προστασία των αγαθών του πληροφοριακού συστήματος.
- Τις διαδικασίες επιλογής νέου προσωπικού, ειδικά στις περιπτώσεις εκείνες που πρέπει να πληρωθεί μια θέση που χειρίζεται ευαίσθητα ή κρίσιμα για τον οργανισμό δεδομένα ή εφαρμογές (π.χ. οικονομικά στοιχεία).
- Τη συμμόρφωση με το νομικό πλαίσιο για την προστασία των ευαίσθητων προσωπικών δεδομένων και την προστασία της πνευματικής ιδιοκτησίας.
- Την κατάρτιση και ενημέρωση των χρηστών στην εφαρμογή των μέτρων ασφάλειας που προδιαγράφονται στην πολιτική ασφάλειας (π.χ. σωστή διαχείριση passwords).
- Την αντιμετώπιση και αναφορά περιστατικών ασφάλειας. **Μέσω της πολιτικής ασφάλειας θα πρέπει να καθορίζεται η διαδικασία με την οποία οι χρήστες καλούνται να αντιμετωπίσουν την πραγματοποίηση μιας απειλής κατά του συστήματος.** Θα πρέπει επίσης να ορίζεται το κανάλι επικοινωνίας μέσω του οποίου η πληροφορία για την πραγματοποίηση ενός περιστατικού ασφάλειας που αντιλήφθηκε ένας χρήστης θα φτάσει στον υπεύθυνο κατά το συντομότερο δυνατό. Αυτό έχει μεγάλη σημασία αφού η δυνατότητα ενός οργανισμού να αντιμετωπίσει τις απειλές που σχετίζονται με το πληροφοριακό του σύστημα εξαρτάται από την άμεση επισήμανση των παραβιάσεων της ασφάλειας και την εκτέλεση των προβλεπόμενων, στην πολιτική ασφάλειας, δράσεων.

Φυσική ασφάλεια

Τα μέτρα προστασίας που υποστηρίζουν τη φυσική ασφάλεια έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στο χώρο του οργανισμού και της καταστροφής των αγαθών του πληροφοριακού συστήματος. Αυτό επιτυγχάνεται με τη δημιουργία *επάλληλων περιμέτρων φυσικής ασφάλειας*, στη λογική των ομόκεντρων κύκλων, όπου στο κύκλο που βρίσκεται πιο εσωτερικά

τοποθετούνται τα αγαθά που πρέπει να προστατευτούν. Οι οδηγίες για τη φυσική ασφάλεια μπορεί να αφορούν τον έλεγχο φυσικής πρόσβασης σε κρίσιμους για το πληροφοριακό σύστημα χώρους, όπως είναι για παράδειγμα ο περιορισμός της κίνησης των επισκεπτών σε συγκεκριμένους χώρους, η χρήση ειδικών καρτών για την είσοδο σε κάποιο κτίριο, κλπ.

Έλεγχος πρόσβασης στα πληροφοριακά συστήματα

Η πρόσβαση των χρηστών των πληροφοριακών συστημάτων στις πληροφορίες και τις εφαρμογές θα πρέπει να καθορίζεται με βάση τις επιχειρηματικές ανάγκες και τις απαιτήσεις ασφάλειας του εκάστοτε οργανισμού.

Μία πρακτική που συνήθως χρησιμοποιείται για τον καθορισμό των δικαιωμάτων πρόσβασης είναι η **εφαρμογή της «need to know» αρχής**, με βάση την οποία δικαίωμα πρόσβασης στις πληροφορίες, τις εφαρμογές και τα υπολογιστικά συστήματα αποδίδεται στους χρήστες που χρειάζονται την πρόσβαση για την εκτέλεση της εργασίας τους.

Διαχείριση υλικού και λογισμικού

Οι οδηγίες που ανήκουν σε αυτόν τον άξονα, καλύπτουν τις εξής περιπτώσεις:

- Προμήθεια και συντήρηση υλικού. **Για την αγορά και χρήση προϊόντων υλικού θα πρέπει να ακολουθούνται οι οδηγίες που περιλαμβάνονται στην πολιτική ασφάλειας με στόχο την διατήρηση του επιθυμητού επιπέδου ασφάλειας.** Για το σκοπό αυτό θα πρέπει να καθορίζονται οι απαιτήσεις ασφάλειας που διέπουν την αγορά καθώς και τη συντήρηση του υλικού, όπως είναι για παράδειγμα η ύπαρξη πιστοποίησης του επιπέδου ασφάλειας με κάποια από τα γνωστά πρότυπα.
- Ανάπτυξη και συντήρηση λογισμικού. Θα πρέπει επίσης να προσδιορίζονται οι διαδικασίες για την ανάπτυξη και συντήρηση των εφαρμογών των πληροφοριακών συστημάτων. Πιο συγκεκριμένα, θα πρέπει να καλύπτονται οι ακόλουθες περιπτώσεις:
    - Αγορά πακέτων λογισμικού από εξωτερικούς παράγοντες.
    - Ανάπτυξη και συντήρηση λογισμικού από εξωτερικούς συνεργάτες.
    - Εσωτερική ανάπτυξη και συντήρηση των εφαρμογών.

Συμμόρφωση με νομικές υποχρεώσεις

Η αναγκαιότητα για τη ύπαρξη της πολιτικής ασφάλειας μπορεί να πηγάζει και από την τυπική υποχρέωση του οργανισμού να ακολουθεί το σχετικό νομικό και κανονιστικό πλαίσιο για τη λειτουργία του.

Ας δούμε ένα παράδειγμα για να γίνουμε περισσότερο συγκεκριμένοι: στις περιπτώσεις πληροφοριακών συστημάτων που περιλαμβάνουν ευαίσθητα προσωπικά

δεδομένα, η πολιτική ασφάλειας θα πρέπει να λαμβάνει υπόψη και να ικανοποιεί τις απαιτήσεις της ισχύουσας νομοθεσίας.

Διαδικασίες διαχείρισης πολιτικής ασφάλειας

Ένα σημαντικό κομμάτι της πολιτικής ασφάλειας περιγράφει και προσδιορίζει τις λοιπές δραστηριότητες που πρέπει να συνοδεύουν την εφαρμογή της, ώστε να είναι αποτελεσματική η διαχείριση της ασφάλειας των πληροφοριακών συστημάτων. Οι δραστηριότητες αυτές αφορούν την **αξιολόγηση και αναθεώρηση της πολιτικής** καθώς επίσης και τον **έλεγχο και τη συμμόρφωση με την πολιτική ασφάλειας.**

Οργανωτική δομή

Η εφαρμογή της πολιτικής ασφάλειας προϋποθέτει την ύπαρξη κατάλληλης οργανωτικής δομής, όπως **η δημιουργία των κατάλληλων ρόλων**, η θέσπιση διαδικασιών για τον εντοπισμό και την αναφορά περιστατικών ασφάλειας κλπ. Με τη δημιουργία κατάλληλων ρόλων, όπως είναι ο ρόλος του υπεύθυνου ασφάλειας, δημιουργείται η απαραίτητη οργανωτική δομή για την υλοποίηση των διαδικασιών διαχείρισης της πολιτικής ασφάλειας.

Σχέδιο συνέχισης λειτουργίας

Μεταξύ άλλων είναι χρήσιμο στην πολιτική ασφάλειας να συμπεριλαμβάνουμε κάποιες **οδηγίες για το τι πρέπει να γίνεται μετά την πραγματοποίηση ενός σημαντικού περιστατικού ασφάλειας**. Με αυτό τον τρόπο, οι λειτουργίες του οργανισμού που στηρίζονταν στο κομμάτι του πληροφοριακού συστήματος που υπέστη ζημιά θα εξακολουθήσουν να πραγματοποιούνται με κάποιους **εναλλακτικούς τρόπους** μέχρι την επαναφορά της πλήρους λειτουργικότητας του πληροφοριακού συστήματος.

Σκοπιμότητα της Πολιτικής Ασφάλειας

Θα πρέπει να έχει γίνει ήδη σαφές και από το προηγούμενο κεφάλαιο ότι η διαδικασία της ανάπτυξης και της εφαρμογής της πολιτικής ασφάλειας των πληροφοριακών συστημάτων έχει κρίσιμη σημασία για τον οργανισμό. Παρακάτω, θα επιχειρήσουμε να δώσουμε απάντηση στο ερώτημα «γιατί χρειαζόμαστε μία πολιτική ασφάλειας;» [12].

Καθοδήγηση της επιλογής και υλοποίησης των μέτρων ασφάλειας

Για να αντιμετωπιστούν τα προβλήματα ασφάλειας σε ένα πληροφοριακό σύστημα, οι υπεύθυνοι προβαίνουν στην αγορά κατάλληλου υλικού και λογισμικού. Δυστυχώς όμως δεν είναι λίγες οι φορές που οι δυνατότητες αυτών των προϊόντων δε χρησιμοποιούνται στο μέγιστο βαθμό των δυνατοτήτων τους αφού δεν υφίσταται η απαραίτητη οργανωτική υποδομή.

Τα μέτρα που πρέπει να ληφθούν για την επίτευξη της ασφάλειας υπάγονται σε δύο κατηγορίες. Μπορεί να είναι είτε τεχνικής φύσεως (π.χ. smart cards για τον έλεγχο πρόσβασης) είτε διοικητικής φύσεως (π.χ. ο καθορισμός διαδικασιών ελέγχου και συστήματος κυρώσεων για τους παραβάτες της πολιτικής ασφάλειας). Πρέπει επομένως να εξασφαλιστεί η **συνεπής** υλοποίηση όλων των μέτρων ασφάλειας για δύο λόγους:

1. Να αποφευχθεί η περίπτωση επικαλύψεων, να μην εφαρμοστούν δηλαδή μέτρα προστασίας που αντιμετωπίζουν τις ίδιες απειλές.
2. Να μην υπάρχουν συγκρούσεις και ασυμβατότητες, να μην υλοποιηθούν δηλαδή μέτρα προστασίας με αντικρουόμενους στόχους.

Δημιουργία «καναλιού επικοινωνίας» μεταξύ των εμπλεκομένων

Η πολιτική ασφάλειας, το έγγραφο δηλαδή στο οποίο δηλώνονται τα μέτρα για την ασφάλεια των πληροφοριακών συστημάτων, μπορεί να αποτελέσει ένα σημαντικό σημείο αναφοράς για την επικοινωνία και διαπραγμάτευση μεταξύ των εμπλεκόμενων φορέων ώστε να δημιουργηθεί μία κοινή αντίληψη για την αναγκαιότητα της ασφάλειας. Δεν πρέπει άλλωστε να ξεχνάμε ότι η διαχείριση της ασφάλειας των πληροφοριακών συστημάτων είναι μία διαδικασία στην οποία εμπλέκονται πολλοί και διαφορετικοί φορείς που μπορεί να βρίσκονται τόσο εντός όσο και εκτός οργανισμού. Η καλή επικοινωνία και συνεργασία των εμπλεκόμενων είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριακών συστημάτων.

Εξασφάλιση και διαχείριση των απαραίτητων πόρων

Ένας οργανισμός που θέλει να οχυρώσει το σύστημά του πρέπει να δαπανήσει σημαντικά ποσά στην προμήθεια και εφαρμογή μέτρων ασφαλείας καθώς και στην υλοποίηση συναφών διαδικασιών όπως είναι ο έλεγχος και η πιστοποίηση των

πληροφοριακών συστημάτων, ενώ παράλληλα απαιτείται και η εμπλοκή έμπειρου και εξειδικευμένου προσωπικού.

Η ασφάλεια λοιπόν ενός πληροφοριακού συστήματος θα πρέπει να αντιμετωπίζεται ως ένα αυτοτελές project μέσα στον οργανισμό. Θα πρέπει να αναγνωρίζονται οι διαφορετικοί εμπλεκόμενοι, να χρονοπρογραμματίζονται όλες οι ενέργειες που απαιτούνται και να δεσμεύονται οι απαραίτητοι πόροι. Ειδικά στη διασφάλιση των πόρων, ο ενεργός ρόλος της διοίκησης είναι πολύ σημαντικός.

Η ανάπτυξη μιας πολιτική ασφάλειας βοηθά στην αποδοτική διαχείριση της ασφάλειας του πληροφοριακού συστήματος σε έναν οργανισμό.

Εδραίωση της σημασίας της ασφάλειας των Πληροφοριακών Συστημάτων για τον οργανισμό

Μέσω της υλοποίησης πολιτικής ασφάλειας για έναν οργανισμό κατοχυρώνεται και θεμελιώνεται η ασφάλεια και διασφαλίζεται η εφαρμογή των μέτρων προστασίας από τους χρήστες. Με την πολιτική ασφάλειας, η διοίκηση δεσμεύεται για την ασφάλεια του πληροφοριακού συστήματος και την καθιστά σημαντικό ζήτημα μεταξύ των δραστηριοτήτων του οργανισμού.

Καλλιέργεια «κουλτούρας ασφάλειας»

Με τον όρο «κουλτούρα ασφάλειας» εννοούμε ότι οι χρήστες των πληροφοριακών συστημάτων αποκτούν κοινή αντίληψη και γνώση για την ανάγκη προστασίας και τους στόχους ασφάλειας. Η πολιτική ασφάλειας συμβάλει σημαντικά στη δημιουργία «κουλτούρας ασφάλειας» αφού δημιουργεί κοινές πρακτικές και πεποιθήσεις που αφορούν στην ανάγκη και τους τρόπους προστασίας των πληροφοριακών συστημάτων.

Για να κάνουμε περισσότερο σαφή την έννοια της «κουλτούρας ασφάλειας», επισημαίνουμε τα ακόλουθα: Η πολιτική ασφάλειας οφείλει να καλύπτει σε μεγάλο βαθμό το σύνολο των απαιτήσεων για την ασφάλεια ενός πληροφοριακού συστήματος, είναι όμως εξαιρετικά δύσκολο να καλύψει το σύνολο των περιπτώσεων. Αυτό συμβαίνει διότι η τεχνολογία αναπτύσσεται με γοργούς ρυθμούς αλλά και επειδή οι λειτουργίες των περισσότερων οργανισμών δεν είναι στατικές και αλλάζουν σε συνάρτηση με το περιβάλλον, που συνεχώς μεταβάλλεται. Αυτό έχει ως αποτέλεσμα τα πληροφοριακά συστήματα και οι χρήστες τους να αντιμετωπίζουν νέες απειλές και καταστάσεις που δεν έχουν προβλεφθεί. Δεν υπάρχει επομένως σαφής καθοδήγηση για τα περιστατικά αυτά μέσα στην πολιτική ασφάλειας. Αν οι χρήστες έχουν διαμορφωμένη μία κουλτούρα ασφάλειας είναι σε θέση να δράσουν με τρόπο που θα συντελεί στην προστασία των πληροφοριακών συστημάτων, συμβάλλοντας έτσι στην αποτελεσματικότερη αντιμετώπιση των απειλών.

Ικανοποίηση νομικών υποχρεώσεων του οργανισμού

Οι στόχοι ασφάλειας των πληροφοριακών συστημάτων και τα μέτρα προστασίας που απαιτείται να λάβει ένας οργανισμός **εξαρτώνται επίσης από το νομικό και κανονιστικό πλαίσιο που διέπει τη λειτουργία του**. Η εφαρμογή

πολιτικής ασφάλειας αποτελεί σε πολλές περιπτώσεις νομική υποχρέωση για έναν οργανισμό. Για παράδειγμα, ένα νοσοκομείο θα πρέπει να ικανοποιεί τα απαιτήσεις για την προστασία των ευαίσθητων προσωπικών δεδομένων που αφορούν την υγεία των ασθενών όπως αυτές διατυπώνονται στην ισχύουσα νομοθεσία.

Υποστήριξη επιχειρηματικών αναγκών

Η εφαρμογή της πολιτικής ασφάλειας των πληροφοριακών συστημάτων συμβάλλει στην υποστήριξη των επιχειρηματικών δραστηριοτήτων καθώς αποτελεί βασικό στοιχείο για την ανάπτυξη σχέσεων εμπιστοσύνης με τους πελάτες και τους επιχειρηματικούς εταίρους του οργανισμού.

Νομικό και κανονιστικό πλαίσιο

Η υλοποίηση μιας πολιτική ασφάλειας, ανεξαρτήτως περιβάλλοντος και οργανισμού στο οποίο αναπτύσσεται, υπόκειται στους περιορισμούς που επιβάλλει το εκάστοτε νομικό πλαίσιο. Για παράδειγμα, μιλήσαμε αναλυτικά σε προηγούμενο κεφάλαιο για το μείζον ζήτημα της προστασίας των ευαίσθητων προσωπικών δεδομένων. Οι ενέργειες που γίνονται σε μία τέτοια περίπτωση οφείλουν να είναι σύμφωνες με τις υπάρχουσες διατάξεις που στην Ελλάδα, για το ζήτημα αυτό ορίζονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Θα δούμε λοιπόν παρακάτω ονομαστικά τους νόμους και τις διατάξεις που υπαγορεύουν την πολιτική ασφάλειας που θα αναπτύξει ένας οργανισμός για το πληροφοριακό του σύστημα και όχι μόνο.

Οι νέες μορφές διαφήμισης, ηλεκτρονικών συναλλαγών αλλά και η ανάγκη της ηλεκτρονικής οργάνωσης σε επιχειρήσεις έχουν σα συνέπεια την αυξημένη ζήτηση προσωπικών πληροφοριών. Η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να δημιουργήσει προβλήματα στην ιδιωτική ζωή του πολίτη για το λόγο αυτό η νομοθεσία που υφίσταται είναι αρκετά λεπτομερής και αυστηρή. Έχουμε λοιπόν τα εξής [13]:

- **Νόμος 2472/1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα [14].** Αντικείμενο του παρόντος νόμου είναι *η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα* για να προστατευθούν τα δικαιώματα και οι θεμελιώδεις ελευθερίες των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Διασαφηνίζονται επίσης θέματα όπως είναι τα δικαιώματα αυτού του οποίου τα στοιχεία υπόκεινται σε επεξεργασία, το είδος της επεξεργασία που επιτρέπεται και οι κυρώσεις που επιβάλλονται σε περίπτωση ανυπακοής. Τέλος, να πούμε ότι με το νόμο αυτό ιδρύθηκε και η Αρχή Προστασίας Προσωπικών Δεδομένων.
- **Νόμος 2474/1999, Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα [15].** Σκοπός του παρόντος νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η *θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα*.
- **Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα [16].** Αυτή η οδηγία *αποσκοπεί στην εναρμόνιση των διατάξεων των κρατών μελών* οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως δε το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, καθώς και στην ελεύθερη κυκλοφορία των δεδομένων αυτών και των τηλεπικοινωνιακών εξοπλισμών και υπηρεσιών στην Κοινότητα.
- Σύσταση Αρ. R (99) 5 της επιτροπής υπουργών των κρατών μελών για την προστασία της ιδιωτικότητας στο Διαδίκτυο [17]. Δίνονται κατευθυντήριες γραμμές για την προστασία των ατόμων, αναφορικά με τη συλλογή και επεξεργασία προσωπικών δεδομένων στις λεωφόρους πληροφοριών, οι οποίες μπορούν να ενσωματωθούν ή να προσαρτηθούν σε κώδικες συμπεριφοράς.

Ορίζονται υποχρεώσεις και δίνονται οδηγίες σε χρήστες και σε παρόχους τηλεπικοινωνιακών υπηρεσιών.

- **Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές** (digital signatures) **[18].** Στόχος της παρούσας οδηγίας είναι να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους. *Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης*, ώστε να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς.
- **Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου [19].** Έχει ως στόχο την ομαλή λειτουργία της εσωτερικής αγοράς, εξασφαλίζοντας την ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας μεταξύ των κρατών μελών.
- **Οδηγία 2001/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 22ας Μαΐου για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας [20].** Ορίζονται οι *περιπτώσεις κατά τις οποίες τα κράτη μέλη παρέχουν το αποκλειστικό δικαίωμα να επιτρέπουν ή να απαγορεύουν την άμεση ή έμμεση, προσωρινή ή μόνιμη αναπαραγωγή σε δημιουργούς*.
- **Σχέδιο ασφάλειας και σχέδιο έκτακτης ανάγκης [21].** Δε πρόκειται για νόμο αλλά για ένα άρθρο, συντεταγμένο από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που περιγράφει γενικές αρχές και οδηγίες που έχει υιοθετήσει η Αρχή για την λήψη μέτρων ασφάλειας και προστασίας των Πληροφοριακών Συστημάτων. Το παρόν κείμενο απευθύνεται σε κάθε υπεύθυνο επεξεργασίας που επεξεργάζεται προσωπικά δεδομένα με χρήση αυτοματοποιημένων συστημάτων.

Για τον οργανισμό που χρειάζεται για τη λειτουργία του την συλλογή ευαίσθητων προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να ακολουθεί μία σειρά συγκεκριμένων βημάτων. Η διαδικασία έχει ως εξής [22]:

- ✓ **Υποχρεωτική** συμπλήρωση ενός εντύπου με την επωνυμία Έντυπο 1.0 για την γνωστοποίηση τήρησης αρχείου/ επεξεργασίας προσωπικών δεδομένων.
- ✓ Για κάθε έναν από τους σκοπούς της επεξεργασίας θα πρέπει να συμπληρωθεί ένα αντίγραφο του Εντύπου 2.0.
- ✓ Σε περιπτώσεις όπου η επεξεργασία των προσωπικών δεδομένων λαμβάνει χώρα σε περισσότερους από έναν διαφορετικούς γεωγραφικούς χώρους, στα πλαίσια του ίδιου οργανισμού, θα πρέπει να συμπληρωθεί το Έντυπο 3.0. Το τμήμα αυτό της αίτησης συντελεί στη γνωστοποίηση των επιπλέον γεωγραφικών τόπων που αναφέρονται σε συγκεκριμένο σκοπό επεξεργασίας.
- ✓ Σε περιπτώσεις όπου λαμβάνει χώρα διασύνδεση αρχείων (έτσι όπως αυτή ορίζεται στο Άρθρο 8 του ν. 2472/97) θα πρέπει να συμπληρωθεί το Έντυπο 4.0.
- ✓ Σε περιπτώσεις όπου μέρος ή/ και το σύνολο των προσωπικών δεδομένων μεταβιβάζεται σε χώρες εκτός Ευρωπαϊκής Ένωσης θα πρέπει να συμπληρωθεί το Έντυπο 5.0 για την αίτηση άδειας διαβίβασης δεδομένων σε χώρες εκτός της Ε.Ε.

- ✓ Το βήμα που ακολουθεί είναι υποχρεωτικά να ενημερώνονται τα υποκείμενα των οποίων τα δεδομένα υπόκεινται σε συλλογή ή επεξεργασία.

Κεφάλαιο 4

Εργαλεία Risk Analysis και Security Assessment

Εισαγωγή – Βασικά χαρακτηριστικά εργαλείων

Η ανάγκη ύπαρξης συγκεκριμένου πλαισίου μέσα στο οποίο γίνεται η χρήση του δικτύου ενός οργανισμού έχει προβλεφθεί, όπως μαρτυρά η ύπαρξη μιας πληθώρας προϊόντων λογισμικού που διατίθενται στο εμπόριο. Τα εργαλεία αυτά εστιάζουν στους δύο βασικούς τομείς της **ανάλυσης ρίσκου** και της **αποτίμησης κινδύνων**, συμβάλλοντας αποτελεσματικά στην δημιουργία μιας πολιτικής ασφάλειας που θα είναι πλήρης, αλλά κυρίως «προσωποποιημένη» σε κάθε δίκτυο.

Στο παρόν κεφάλαιο θα παρουσιάσουμε μερικά από τα πιο γνωστά λογισμικά, τα οποία σε άλλες περιπτώσεις διατίθενται ως εμπορικά προϊόντα και σε άλλες διατίθενται δωρεάν.

Είναι πραγματικά πολύ δύσκολο να δώσουμε κάποιους κανόνες για την λειτουργία των risk analysis και security assessment tools, αφού η έρευνα μας έδειξε ότι διαφοροποιούνται σημαντικά μεταξύ τους. Ασφαλώς, εξυπηρετούν όλα τους έναν πολύ συγκεκριμένο σκοπό: Συμβάλλουν στην εκτίμηση των ευπαθειών και των κινδύνων που αντιμετωπίζει ένα πληροφοριακό σύστημα και ίσως – αλλά όχι σε όλες τις περιπτώσεις – προτείνουν λύσεις.

Από εκεί και πέρα, το κάθε εργαλείο έχει συνήθως μια δυνατότητα που το διαφοροποιεί από τα υπόλοιπα και του προσδίδει ένα πλεονέκτημα ή, σαφώς, και ένα μειονέκτημα. Μπορεί για παράδειγμα να παράγει στο τέλος κάποια reports, που αποδεικνύονται εξαιρετικά χρήσιμα όταν θέλουμε να παρουσιάσουμε τους πιθανούς κινδύνους σε κάποιους που δεν έχουν μεγάλη σχέση με την τεχνολογία. Άλλα εργαλεία υπολογίζουν εκτός από τις συνέπειες μιας ευπάθειας στο σύστημα και τα δεδομένα, και τις οικονομικές συνέπειες που θα προκύψουν για μια εταιρία. Ορισμένα, κρίνονται αρκετά δύσκολα για χρήση από «αρχάριους» και συνίστανται μόνο στους γνώστες του τεχνολογικού αντικειμένου. Κάποια είναι δωρεάν, ενώ άλλα είναι εξαιρετικά ακριβά. Και τέλος, ορισμένα εργαλεία απαιτούν πολύ συγκεκριμένες τεχνολογίες για να «τρέξουν» (servers, λειτουργικό, κλπ), ενώ άλλα είναι εντελώς ανεξάρτητα.

Παρακάτω έχει γίνει μια επιλογή από τα εργαλεία που υπάρχουν, τα οποία δίνονται μαζί με μια συνοπτική περιγραφή τους. Έτσι, θα γίνουν πολύ περισσότερο κατανοητά και σαφή τα όσα προαναφέρθηκαν.

Τα εργαλεία

Το Cramm

Έχουμε ήδη αναλύσει το Cramm [23] (CCTA Risk Analysis and Management Method) σε προηγούμενο κεφάλαιο αλλά επειδή στο σημείο αυτό κάνουμε μια συνολική παρουσίαση των βασικότερων εργαλείων ανάλυσης κινδύνου, κρίνεται απαραίτητη μια επιπλέον – συνοπτική έστω – αναφορά στο εργαλείο αυτό που έχει κερδίσει την προτίμηση μεγάλων ιδιωτικών και δημόσιων οργανισμών.

Το Cramm συνοψίζει την λειτουργία του στους τέσσερις ακόλουθους τομείς:

1. Προσδιορισμός και αξιολόγηση των αγαθών.
2. Ανάλυση επικινδυνότητας.
3. Διαχείριση επικινδυνότητας.
4. Παροχή reports για όλα τα προαναφερθέντα στάδια.

Για να εφαρμοστεί η μέθοδος, είναι αναγκαίο:

- Να προσδιορίζονται και να αξιολογούνται τα αγαθά που χρήζουν προστασίας (δεδομένα, υλικό, λογισμικό, χώροι και μεταξύ τους συσχετισμός).
- Να προσδιοριστεί η σπουδαιότητα των δεδομένων για τον οργανισμό με βάση την επίπτωση που θα έχει ενδεχόμενη απώλειά τους. Εξετάζονται οι περιπτώσεις μη διαθεσιμότητας, καταστροφής, αποκάλυψης, μη εξουσιοδοτημένης μεταβολής, ηθελημένης μεταβολής και λανθασμένης μετάδοσης. Για κάθε μία από τις προηγούμενες περιπτώσεις εκτιμάται το χειρότερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίησή του, με βάση μια κλίμακα από το 1 έως το 10.
- Να αποτιμηθεί το λογισμικό και το υλικό του πληροφοριακού συστήματος, βάση του κόστους αντικατάστασής τους.
- Να επιβεβαιωθεί από τη διοίκηση του οργανισμού η αποτίμηση των προηγούμενων βημάτων. Εδώ είναι εξαιρετικά χρήσιμα τα reports που εξάγει το Cramm και τα οποία παρουσιάζουν τα αποτελέσματα.

Μετά την αποτίμηση, σειρά έχουν ο υπολογισμός των απειλών και των αδυναμιών στο σύστημα που εξετάζεται, με στόχο να προκύψει ο βαθμός επικινδυνότητας και να επιλεγούν τα σωστά αντίμετρα. Ο τρόπος που γίνονται η ανάλυση και διαχείριση επικινδυνότητας, έχουν περιγραφεί λεπτομερώς στο κεφάλαιο 3.

Στα πλεονεκτήματα της μεθόδου Cramm συγκαταλέγεται το γεγονός ότι καλύπτει μεγάλο εύρος των συνιστωσών ασφάλειας αλλά και ότι συνοδεύεται από αυτοματοποιημένο εργαλείο που επιλέγει αντίμετρα από μία μεγάλη βιβλιοθήκη.

Ένα βασικό της μειονέκτημα είναι πως στηρίζεται σε μεγάλο βαθμό στην διοίκηση του οργανισμού (η οποία είναι πολύ πιθανό να μην έχει γνώσεις πάνω σε θέματα ασφάλειας) ενώ έχει υψηλό κόστος εφαρμογής αφού απαιτεί πολύ χρόνο και μεγάλη ανθρώπινη προσπάθεια.

Το εργαλείο εκτίμησης κινδύνου της Microsoft

Το λογισμικό που η Microsoft έχει αναπτύξει για την εκτίμηση κινδύνου και την ανάλυση ρίσκου σε ένα δίκτυο είναι το MSAT (Microsoft Security Assessment Tool). Παρέχεται δωρεάν στους χρήστες των Windows και πρόκειται για ένα εργαλείο που με μια λέξη μπορεί να χαρακτηριστεί πλήρες.

Πριν το τρέξει ο διαχειριστής του δικτύου, ζητείται η δημιουργία στοιχειώδους profile και ακολουθεί μια σειρά ερωτήσεων που εξαντλεί το πεδίο των ζητημάτων ασφάλειας.

Τα ερωτήματα είναι ομαδοποιημένα και ξεκινούν από γενικές πληροφορίες που έχουν να κάνουν με τον αριθμό των υπολογιστών ή των servers. Ακολουθεί ερωτηματολόγιο για τους κινδύνους που αντιμετωπίζει η εταιρία. Εδώ ο διαχειριστής απαντά σε ερωτήματα, όπως αν έχουν οι πελάτες πρόσβαση στο εσωτερικό δίκτυο, αν υφίστανται βάσεις δεδομένων ή αν στα γραφεία του οργανισμού δραστηριοποιείται και κάποιος άλλος φορέας. Το επόμενο κομμάτι του ερωτηματολογίου αφορά τις εφαρμογές, οπότε το αν η εταιρία παράγει software για πελάτες ή αν υπάρχει συνεργασία με τρίτους, είναι τα καίρια ζητήματα που πρέπει να διευκρινιστούν.

Κάθε ερώτημα που δίνει τις πληροφορίες που είναι αναγκαίες για να γίνουν οι σωστές εκτιμήσεις, γίνεται μέσω του εργαλείου αυτού: Αποθηκεύονται ευαίσθητα δεδομένα; Εφαρμόζεται το σύστημα της πρόσβασης βασισμένης σε ρόλους; Υπάρχει outsource; Ποιος είναι ο τομέας δραστηριοποίησης; Ποιος είναι ο αριθμός των εργαζομένων; Πόσο ισχυρό brandname έχει η εταιρία;

Στο τέλος, έπειτα από την συμπλήρωση όλων των ερωτημάτων (το πρόγραμμα επισημαίνει στον χρήστη αν έχει παραλείψει να δώσει κάποια απάντηση και τον υποχρεώνει να επιστρέψει στο σημείο εκείνο και να την συμπληρώσει) το MSAT παράγει ένα report που αποτελεί στην ουσία τον σκελετό της πολιτικής ασφάλειας που πρέπει να εφαρμοστεί σε αυτό – και μόνο – το δίκτυο.

Το Nmap

Ένα ακόμη δημοφιλές free open source εργαλείο είναι το Nmap (Network Map). Οι χρήστες του διαδικτύου επισημαίνουν ότι είναι κατάλληλο για scanning σε μεγάλα δίκτυα, μιας και είναι πολύ γρήγορο. Βρίσκει εφαρμογή στα περισσότερα λειτουργικά συστήματα, όπως Microsoft Windows, Linux, Solaris, IRIX, Mac OS, HP-UX, NetBSD και Sun OS.

Αξίζει να αναφέρουμε ότι συνοδεύεται από κατατοπιστικά tutorials ενώ έχει πάρει και το βραβείο «Information Security Product of the Year» του Linux Journal, Info World and Codetalker Digest.

Το αντιφατικό στοιχείο που παρουσιάζει ιδιαίτερο ενδιαφέρον είναι πως πρόκειται για ένα προϊόν εξαιρετικά διαδεδομένο μεταξύ των hackers.

Το Qualys Guard

Το Qualys Guard [24] είναι ένα εμπορικό προϊόν, το οποίο – όπως υπόσχεται η κατασκευάστρια εταιρία Qualys – βοηθά τους οργανισμούς να ασφαλίσουν το

δίκτυό τους πραγματοποιώντας ελέγχους σε αυτό με τρόπο αυτοματοποιημένο, ψάχνοντας για ευπάθειες.

Το γραφικό περιβάλλον χρήστη είναι βασισμένο στην πλατφόρμα AJAX, ενώ εφαρμόζει παράλληλες αρχιτεκτονικές σάρωσης που βοηθούν στην εξοικονόμηση του χρόνου έως και 4 φορές λιγότερο, σε σύγκριση με άλλα εργαλεία.

Το Nessus για απομακρυσμένο scanning

Ένα ακόμη εργαλείο, που διατίθεται δωρεάν, είναι και το Nessus [25]. Χρησιμοποιεί βάση δεδομένων στην οποία καταγράφει τα διάφορα χαρακτηριστικά των ευπαθειών και την οποία την ανανεώνει σε καθημερινή βάση. Χρησιμοποιεί την τεχνολογία RSS Feeds για να ενημερώνει ποια plugins προστίθενται στο Nessus και πότε.

Το διαφορετικό χαρακτηριστικό που έχει το εργαλείο αυτό είναι ότι έχει τη δυνατότητα να κάνει απομακρυσμένο scanning. Δεν είναι απαραίτητη δηλαδή η εγκατάστασή του σε έναν υπολογιστή, αλλά αν το nessus τρέχει σε ένα computer, τότε μπορεί να κάνει τον έλεγχο και σε άλλους υπολογιστές του δικτύου.

Κάτι που θα μπορούσε παρόλα αυτά να χαρακτηριστεί ως μειονέκτημα είναι το γεγονός ότι απαιτεί τεχνικές γνώσεις για να εφαρμοστεί και δεν προσφέρεται για χρήση από κάποιον αρχάριο.

Το Callio

Η εμπορική ονομασία του λογισμικού αυτού [26], είναι Callio Secura και η εταιρία Callio έχει αναπτύξει τρία υποπροϊόντα που εξυπηρετούν τον σκοπό του security management. Και τα τρία αυτά προϊόντα ακολουθούν το πρότυπο ISO 17799/BS 7799. Οι κατασκευαστές υπόσχονται εύκολο γραφικό περιβάλλον και πλήρη καθοδήγηση του χρήστη στην εφαρμογή του και να σημειώσουμε ότι στα θετικά συγκαταλέγεται το ότι διατίθεται σε τέσσερις διαφορετικές γλώσσες, μεταξύ των οποίων και τα κινέζικα.

Εκτός από το Callio Secura, διατίθενται τόσο το Callio Toolkit Pro 17799, όσο και το Callio Toolkit 17799. Το πρώτο περιέχει κάποια σημαντικά εργαλεία για να ακολουθεί η εφαρμογή τις απαιτήσεις των ISO 17799 και BS 7799-2. Το δεύτερο παρέχει οτιδήποτε χρειάζεται η εφαρμογή για να ακολουθεί το πρωτόκολλο ISO 17799. Διαπιστώνεται με αυτόν τον τρόπο το επίπεδο της συνεργασίας με το ISO 17799.

Το πρόγραμμα αυτό ομαδοποιεί τα στοιχεία του δικτύου, καταγράφοντας κάπου τα πλέον πολύτιμα και ευαίσθητα. Για κάθε ένα από αυτά τα ευαίσθητα αγαθά, το Callio υπολογίζει την πιθανότητα να αντιμετωπίσει πρόβλημα ασφάλειας. Επίσης, βοηθά στο να κατασκευαστούν ειδικά ερωτηματολόγια που θα συμπληρώνονται για να αξιολογηθεί το επίπεδο ασφάλειας στο δίκτυο, ενώ συμβάλλει και στην δημιουργία της πολιτικής ασφάλειας, ζήτημα μείζονος σημασίας.

Το Callio κάνει χρήση των ακόλουθων τεχνολογιών:

- Database : MySQL, SQL Server
- Web server : IIS, Apache
- Application server : BlueDragon JX Server

- Client : Internet Explorer

Έχει εύκολη διαδικασία εγκατάστασης αφού ένα web application εγκαθίσταται στον server του οργανισμού.

Ο Πρωτέας

Το εργαλείο Proteus [27] είναι ένα λογισμικό για εκτίμηση και ανάλυση κινδύνων το οποίο πωλείται στην τιμή των 6000 λιρών Αγγλίας, με άδεια χρήσης για ένα έτος.

Υποστηρίζει κάποιες τεχνικές που κάνουν ποσοτικές και ποιοτικές αναλύσεις για τους κινδύνους που υφίστανται. Χρησιμοποιεί κάποιες ειδικές κλίμακες προκειμένου να εκτιμήσει το ρίσκο και πιο συγκεκριμένα μελετά πέντε διαφορετικές περιπτώσεις: Φυσικός κίνδυνος, πληροφορίες, παροχή υπηρεσιών, εφαρμογές αλλά και οποιονδήποτε συνδυασμό των προαναφερθέντων.

Ένα επιπλέον σημαντικό χαρακτηριστικό είναι ότι ο Πρωτέας εφαρμόζει κάποια σχέδια δράσης (Action Plans) προκειμένου να αντιμετωπίσει τους κινδύνους που έχει εντοπίσει.

Οι τεχνολογίες που χρησιμοποιεί το πρόγραμμα είναι:

- Database : MS SQL
- Web server : IIS or Apache
- Application Server : PHP
- Client : I.E., Firefox

Η Cobra

Το κύριο και βασικό στοιχείο που πρέπει να επισημανθεί ευθύς εξαρχής όταν αναφερόμαστε στο εργαλείο Cobra [28] είναι ότι δε χρειάζεται συγκεκριμένες τεχνολογίες για να τρέξει αφού είναι αυτόνομο και ανεξάρτητο.

Προκειμένου να κάνει εκτίμηση των κινδύνων μετράει τον βαθμό του κινδύνου για κάθε περιοχή του συστήματος και αυτή την μέτρηση την συνδέει απευθείας με πιθανή επίδραση στην επιχείρηση. Είναι και αυτό εμπορικό προϊόν και ανάλογα με την έκδοση που αγοράζεται κοστίζει από 895 έως 1995 δολάρια.

Ebios

Πρόκειται για ένα open source προϊόν που ακολουθεί μια σειρά βημάτων για να περατώσει την διαδικασία της ανάλυσης ρίσκου. Μερικά από τα πιο σημαντικά βήματα είναι η μελέτη των πηγών κινδύνου, η αναγνώριση των υπό προστασία αντικειμένων ενώ έπειτα από κάθε βήμα παράγει το σχετικό report [29]. Επιτρέπει σε όλο το προσωπικό που χρησιμοποιεί το ΠΣ να εμπλακεί στα θέματα ασφάλειας και ενθαρρύνει τη διάδραση ανάμεσα στις διάφορες λειτουργίες του οργανισμού, εξετάζοντας το συνολικό κύκλο ζωής του συστήματος.

RiskWatch

Πρόκειται για ένα πολύ ακριβό λογισμικό μιας και κοστολογείται από την εταιρία παραγωγής για 15.000 δολάρια [29]. Διεξάγει αυτοματοποιημένα τόσο ανάλυση όσο και εκτίμηση κινδύνου. Το πρόγραμμα συνοδεύεται από βασικές γνώσεις που διαμορφώνονται από τον χρήστη, δίνοντάς του τη δυνατότητα να κατηγοριοποιήσει τα στοιχεία του δικτύου, τις ευπάθειες αλλά και να δημιουργήσει ερωτηματολόγια όπου αυτά χρειάζονται.

Το εργαλείο περιλαμβάνει ελέγχους που βασίζονται στα πρωτόκολλα ISO 17799 και US-NIST 800-26, ενώ υπολογίζει και το πιθανό οικονομικό κόστος που θα προκύψει για τον οργανισμό από κάποια ευπάθεια του συστήματος.

Συμπεράσματα

Αφού λοιπόν παρουσιάσαμε ένα μέρος από τα πιο δημοφιλή προϊόντα, πιστεύουμε ότι έγινε σαφής η διαφορετικότητα και η ξεχωριστή λειτουργικότητα του κάθε εργαλείου. Σε κάθε περίπτωση, ο διαχειριστής του δικτύου θα πρέπει να λαμβάνει υπόψη το γεγονός ότι το κάθε εργαλείο καλύπτει διαφορετικές πτυχές αυτού του τεράστιου κεφαλαίου που λέγεται «ανάλυση κινδύνων», έτσι ώστε σε κάθε περίπτωση να γίνεται η καλύτερη επιλογή.

Για την επιλογή λοιπόν του κατάλληλου εργαλείου, θα πρέπει να λαμβάνονται υπόψη οι ακόλουθοι παράγοντες [30]:

1. Πρέπει να απαντηθεί το ερώτημα «Τι ακριβώς θέλω να επιτύχω με την ανάλυση κινδύνου»; Είναι αυτονόητο ότι κανένα εργαλείο δεν είναι δυνατό να καλύπτει όλες τις ανάγκες και να κάνει κάθε πιθανό τεστ. Ακόμα και τα πιο δημοφιλή εργαλεία, ίσως να μην είναι κατάλληλα όταν ο διαχειριστής του δικτύου έχει κάποια πολύ εξειδικευμένη απαίτηση.
2. Τα open source προϊόντα κάνουν σε πολλές περιπτώσεις πολύ καλή δουλειά, οπότε η επιλογή τους συμβάλει στο να μειωθεί το κόστος για την κάλυψη των αναγκών ασφάλειας.
3. Σε καμία απολύτως περίπτωση δεν πρέπει να παραβλέπεται το γεγονός ότι τα εργαλεία βοηθούν και συμβάλλουν σε μια σωστή αποτίμηση και σε μια πλήρη πολιτική ασφάλειας αλλά ο ανθρώπινος παράγοντας είναι πολύ σημαντικός. Ας μη ξεχνάμε ότι μεγάλο ποσοστό ευπαθειών σε πληροφοριακά συστήματα οφείλεται σε ανθρώπινα λάθη, για το λόγο αυτό, είναι αναγκαίο, αυτός που αναλαμβάνει να φέρει εις πέρας την διαδικασία της αποτίμησης κινδύνου να είναι εξειδικευμένος επαγγελματίας.
4. Είναι πολύ σημαντικό, το εργαλείο, όχι απλώς να κάνει μια σωστή αποτίμηση, αλλά να παρουσιάζει τα αποτελέσματα με τρόπο κατανοητό, γεγονός που συντελεί και στη σύνταξη της πολιτικής ασφάλειας αλλά και στο να δοθούν αυτά στους άμεσα ενδιαφερόμενους (π.χ. στον διευθύνοντα σύμβουλο ενός οργανισμού που θα εγκρίνει το κονδύλι για την ασφάλεια).

Ίσως λοιπόν, το πλέον σίγουρο συμπέρασμα αυτού του κεφαλαίου να είναι ότι το κατάλληλο εργαλείο είναι αυτό που καθορίζεται κάθε φορά από την υφιστάμενη ανάγκη.

Κεφάλαιο 5

Το δικό μας Security Assesment Tool

Στο κεφάλαιο αυτό περιγράφουμε το εργαλείο Ανάλυσης Ρίσκου και Αποτίμησης Κινδύνων που κατασκευάσαμε εμείς. Το εργαλείο ονομάζεται SAT από τα αρχικά του Security Assesment Tool.

Η ιδέα για το εργαλείο αυτό προέκυψε έπειτα από την προσωπική εμπειρία που είχε η συγγραφέας της παρούσας διπλωματικής, κατά την εργασία της σε εκδοτικό οίκο. Στο ίδιο κτίριο λοιπόν, συστεγάζονται μία εφημερίδα, ένας ραδιοφωνικός σταθμός, ένα περιοδικό, το λογιστήριο και το διαφημιστικό τμήμα. Τα τμήματα συνδέονται μεταξύ τους μέσω ενός δικτύου και όλα, μα όλα τα αρχεία είναι διαθέσιμα σε έναν κοινό σκληρό δίσκο, ταξινομημένα απλώς σε διαφορετικούς φακέλους. Δεν έχει σημασία αν εργάζομαι στο περιοδικό, μπορώ ανά πάσα ώρα και στιγμή να ελέγξω αν έχουν πληρωθεί τα τιμολόγια του κάθε επιχειρηματία. Δεν έχει σημασία αν εργάζομαι στο τυπογραφείο, μπορώ να έχω πρόσβαση σε όλα τα αρχεία του ραδιοφώνου, ακόμη και στην αποκλειστική συνέντευξη που έδωσε ο δήμαρχος και που θα δημοσιευτεί μονάχα αν η δημοσκόπηση είναι υπέρ του δικού του συνδυασμού.

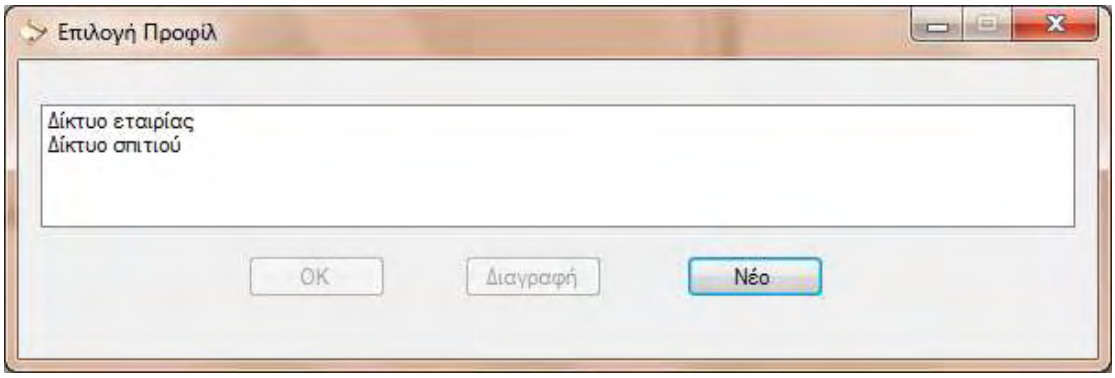
Η ασφάλεια λοιπόν είναι μια έννοια σχεδόν ανύπαρκτη σε πολλές επιχειρήσεις ακόμη. Κάποιοι επιχειρηματίες δείχνουν να έχουν καταλάβει πόσο σημαντικό είναι το να βρίσκεσαι εντός αγοράς με ανταγωνιστικά προϊόντα, δεν έχουν όμως αντιληφθεί σε καμία περίπτωση τον τρόπο που λειτουργούν τα δίκτυα και τις διαδικασίες που πρέπει να ακολουθούνται για τον καθορισμό των ρόλων μέσα στην εταιρία τους.

Είναι σαφές ότι σε τόσο μικρού δυναμικού επιχειρήσεις (το πολύ 15 εργαζόμενοι) είναι περιττό να επιχειρείται ανάλυση ρίσκου με πολύ ακριβά ή περίπλοκα εργαλεία. Τα δίκτυα αυτού του βεληνεκούς, πρέπει να πληρούν τις βασικές προϋποθέσεις ασφάλειας και για τον λόγο αυτό θελήσαμε να φτιάξουμε ένα εργαλείο κατανοητό και σαφές, που θα δίνει το στίγμα για την σημαντικότητα της ασφάλειας σε μικρές επιχειρήσεις που θα πρέπει να αποκτήσουν την πρώτη τους επαφή με τον τομέα αυτό.

Η δυνατότητα δημιουργίας προφίλ

Με την εκκίνηση του SAT εμφανίζεται το παράθυρο επιλογής προφίλ, στο οποίο ο χρήστης μπορεί να δημιουργήσει ένα νέο προφίλ ή να χρησιμοποιήσει ένα ήδη υπάρχον.

Η ύπαρξη των προφίλ (Σχ.1 Παρ.1) κρίθηκε απαραίτητη στην κατασκευή του προγράμματος διότι δίνει στον χρήστη την δυνατότητα να αποθηκεύει τις απαντήσεις του και να τις τροποποιεί, χωρίς να χρειάζεται να συμπληρώνει εκ νέου τις ερωτήσεις.

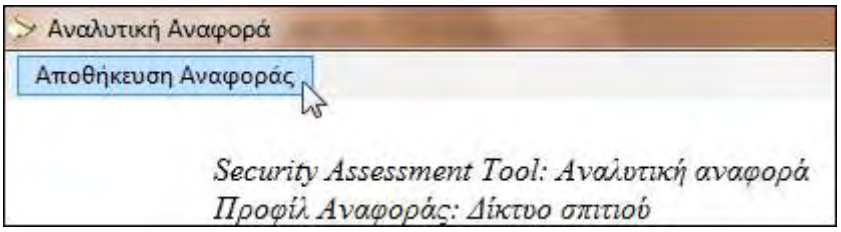


Σχ.1: Επιλογή Προφίλ

Αρκεί λοιπόν, να φορτώσει το υπάρχον και ήδη συμπληρωμένο ερωτηματολόγιο, να αλλάξει μόνο κάποιες απαντήσεις και να έχει αμέσως το νέο αποτέλεσμα.

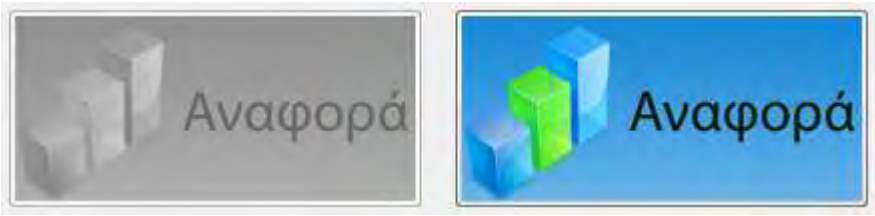
Στην αντίθετη περίπτωση, κάθε φορά, ο χρήστης θα πρέπει να συμπληρώνει τα ερωτήματα, προκειμένου να φτάσει στην τελική αναφορά, γεγονός που θα καθιστούσε το εργαλείο χρονοβόρο και δύσχρηστο.

Η αναφορά λοιπόν που δημιουργείται, αποθηκεύεται αυτομάτως στον φάκελο profiles. Εκτός αυτού όμως, δίνεται η δυνατότητα στον χρήστη να την αποθηκεύσει και σε μια τοποθεσία της επιλογής του, αφού στο τελικό παράθυρο, πάνω αριστερά υπάρχει η επιλογή «Αποθήκευση αναφοράς» (Σχ.2 Παρ.2), με το πάτημα της οποίας εμφανίζεται η λίστα αρχείων του υπολογιστή.



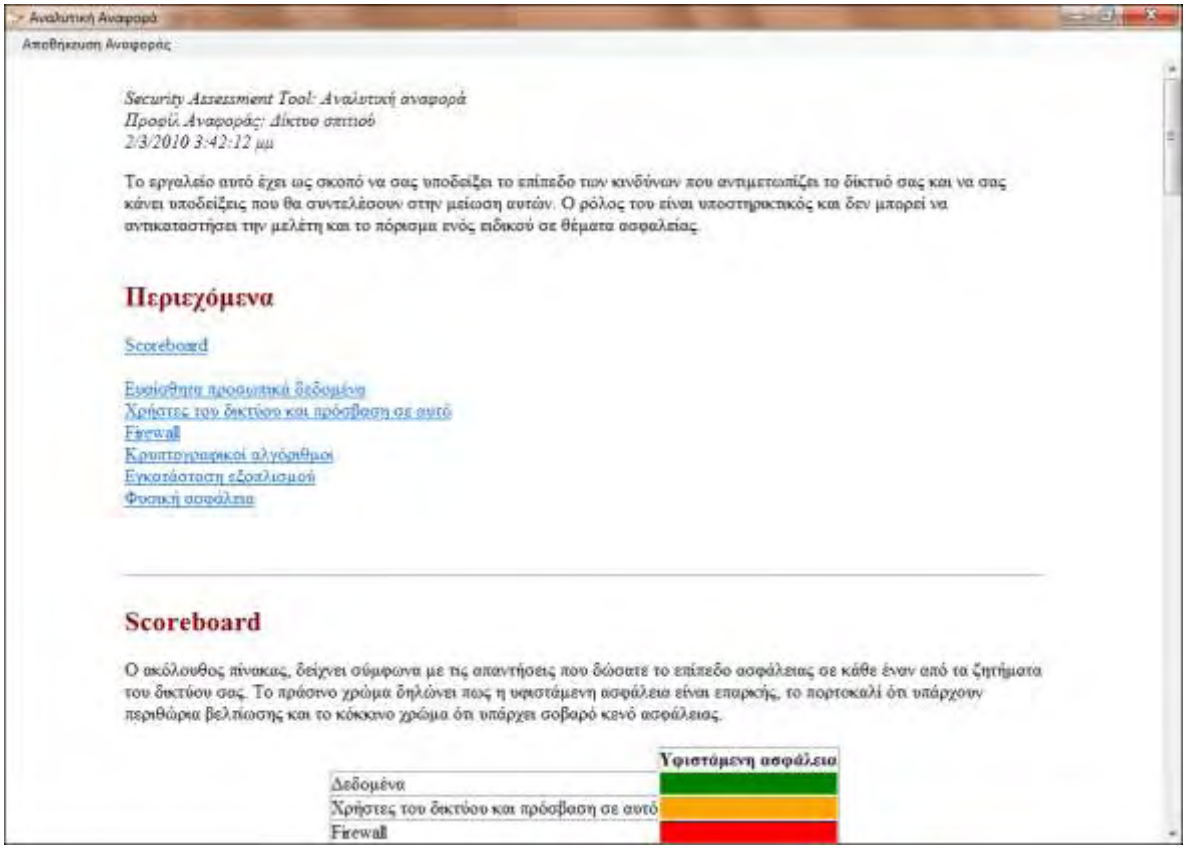
Σχ.2: Αποθήκευση Αναφοράς

Το πρόγραμμα λειτουργεί ως εξής: Μόλις ο χρήστης απαντήσει όλες τις ερωτήσεις, ενεργοποιείται (Σχ.3 Παρ.3) ένα κουμπί που φέρει το όνομα «Αναφορά», το οποίο, μετά την επιλογή του (κλικ από το ποντίκι) καλεί την διαδικασία για την παραγωγή των αποτελεσμάτων (τελική αναφορά) (Παρ.4).



Σχ.3: Ενεργοποίηση κουμπιού Αναφοράς

Στην διαδικασία αυτή, περιλαμβάνεται η παραγωγή κώδικα και η δημιουργία του αντίστοιχου αρχείου HTML, στο οποίο περιέχεται η σχετική αναφορά για την ασφάλεια του δικτύου. Στη συνέχεια, ακολουθεί η προβολή του αρχείου μέσω ενός Web Browser ο οποίος εμφανίζεται ως ξεχωριστό παράθυρο του προγράμματος (Σχ.4 Παρ.5).



Σχ.4: Προβολή Αναλυτικής Αναφοράς

Οι κατηγορίες ερωτήσεων

Τα ερωτήματα του εργαλείου κατηγοριοποιούνται σε 6 ενότητες, τις οποίες καλείται ο χρήστης να συμπληρώσει. Οι ενότητες αυτές, καθώς επίσης και τα ερωτήματα που συμπεριλαμβάνουν είναι οι ακόλουθες:

- Ενότητα ερωτήσεων *«Δεδομένα»*
    1. Φυλάσσονται ευαίσθητα προσωπικά δεδομένα στο δίκτυο;
    2. Διατηρούνται αντίγραφα ασφαλείας;

- Ενότητα ερωτήσεων *«Χρήστες του δικτύου και πρόσβαση σε αυτό»*
    1. Υπάρχει δυνατότητα απομακρυσμένης πρόσβασης στο δίκτυο; Ποιες κατηγορίες χρηστών έχουν πρόσβαση;
    2. Υπάρχει η δυνατότητα ασύρματης πρόσβασης στο δίκτυο;
    3. Πώς αποκτούν πρόσβαση οι εσωτερικοί χρήστες του δικτύου στα δεδομένα τους;
    4. Υπάρχει στην εταιρία λογισμικό του οποίου η κατασκευή έχει ζητηθεί από τρίτο μέρος;
    5. Υπάρχει υπεύθυνος ασφαλείας δικτύου που εργάζεται στην επιχείρηση;

6. Έχει υπάρξει σεμινάριο επιμόρφωσης προς τους υπαλλήλους για την ορθή χρήση του δικτύου; Πόσοι από τους υπαλλήλους το έχουν παρακολουθήσει;

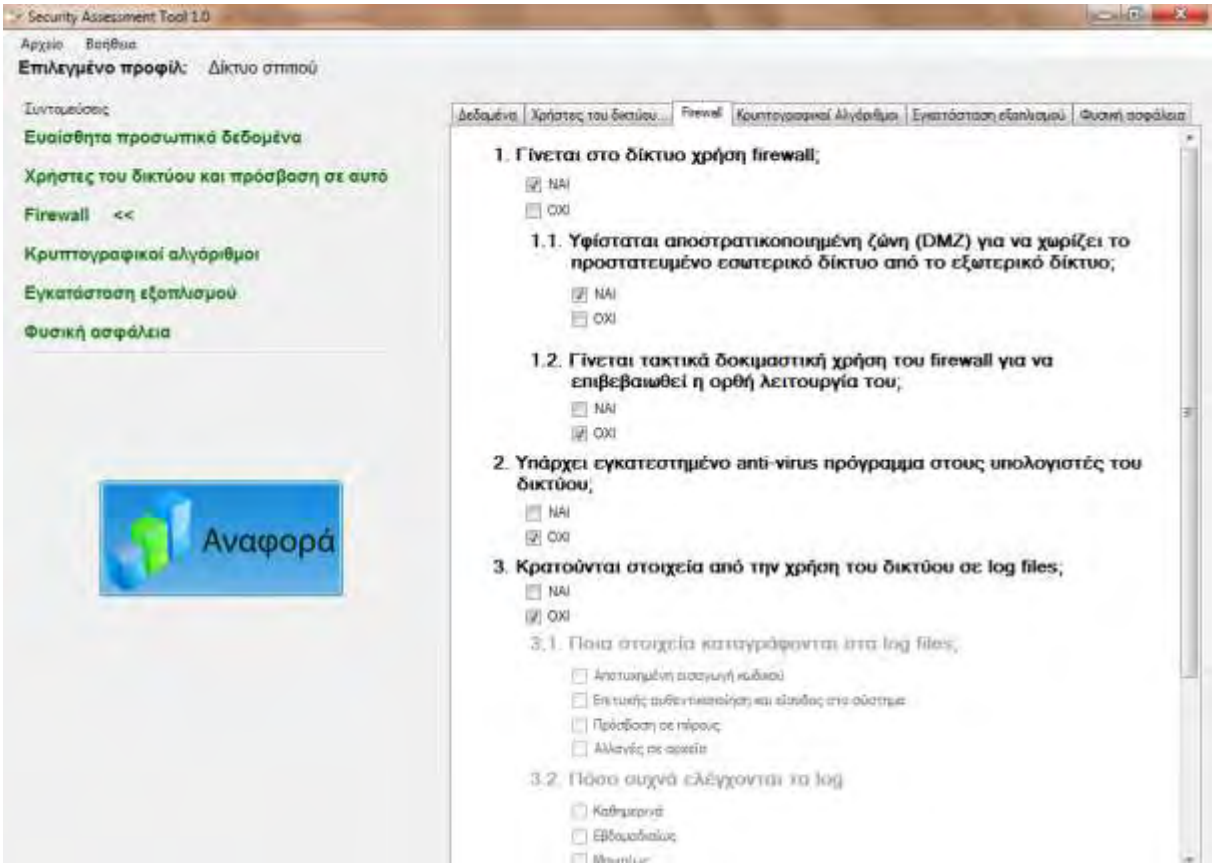
- Ενότητα ερωτήσεων *«Firewall»*
    1. Γίνεται στο δίκτυο χρήση firewall;
        a. Υφίσταται αποστρατικοποιημένη ζώνη (DMZ) για να χωρίζει το προστατευμένο εσωτερικό δίκτυο από το εξωτερικό δίκτυο;
        b. Γίνεται τακτικά δοκιμαστική χρήση του firewall για να επιβεβαιωθεί η ορθή λειτουργία του;
    2. Υπάρχει εγκατεστημένο anti-virus πρόγραμμα στους υπολογιστές του δικτύου;
    3. Κρατούνται στοιχεία από την χρήση του δικτύου σε log files;
        a. Ποια στοιχεία καταγράφονται στα log files;
        b. Πόσο συχνά ελέγχονται τα log files;
    4. Ποια πρωτόκολλα χρησιμοποιούνται για την επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου;

- Ενότητα ερωτήσεων *«Κρυπτογραφικοί αλγόριθμοι»*
    1. Γίνεται χρήση κρυπτογραφικών αλγορίθμων στα δεδομένα;
        a. Ποιοι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούνται;

- Ενότητα ερωτήσεων *«Εγκατάσταση εξοπλισμού»*
    1. Η εγκατάσταση και το configuration του δικτυακού εξοπλισμού γίνεται από εργαζόμενους / στελέχη της εταιρίας ή από εξωτερικούς συνεργάτες;
    2. Έπειτα από την εγκατάσταση νέου εξοπλισμού, γίνονται test ασφαλείας;

- Ενότητα ερωτήσεων *«Φυσική ασφάλεια»*
    1. Είναι ελεγχόμενη η πρόσβαση στο δίκτυο;
    2. Οι servers βρίσκονται σε προστατευμένο χώρο του κτιρίου;

Κατά την εκτέλεση του προγράμματος, οι ερωτήσεις παρουσιάζονται (Σχ.5) κατηγοριοποιημένες. Ορισμένες από αυτές εξαρτώνται από την απάντηση της προηγούμενης ερώτησης, έτσι δεν ενεργοποιούνται παρά μονάχα με την κατάλληλη απάντηση στην προηγούμενη ερώτηση.



Σχ.5: Κατηγοριοποίηση ερωτήσεων

Η τελική αναφορά ασφάλειας

Η τελική αναφορά απαρτίζεται από ένα κείμενο και ένα scoreboard. Ο πίνακας έχει σκοπό να δίνει μία πρώτη ενδεικτική εικόνα της ασφάλειας σε κάθε έναν από τους τομείς των ερωτήσεων. Έτσι, σύμφωνα με τις απαντήσεις που έδωσε κάποιος, το κάθε κουτί χρωματίζεται αναλόγως: το πράσινο χρώμα δηλώνει πως η υφιστάμενη ασφάλεια είναι επαρκής, το πορτοκαλί ότι υπάρχουν περιθώρια βελτίωσης και το κόκκινο χρώμα ότι υπάρχει σοβαρό κενό ασφάλειας.

Στο ακόλουθο μέρος της γραπτής αναφοράς, οι ερωτήσεις παρουσιάζονται μία-μία μαζί με τις απαντήσεις τους. Ανάλογα με την απάντηση που δόθηκε, το πρόγραμμα δίνει την καθοδήγηση που χρειάζεται ή υποδεικνύει κάποιο κενό ασφάλειας, προτείνοντας ταυτόχρονα κάποια λύση. Οι απαντήσεις που έχουν δοθεί σχολιάζονται, δίνοντας στον διαχειριστή κατευθύνσεις.

Ως παράδειγμα, αναφέρουμε το εξής: Αν ο χρήστης έχει τσεκάρει το κουτάκι που δείχνει πως οι χρήστες έχουν πρόσβαση στα δεδομένα χρησιμοποιώντας password, το SAT συμπληρώνει ότι «Το password καλείται να πληροί ορισμένες βασικές προϋποθέσεις προκειμένου να παρέχει επιθυμητό επίπεδο ασφάλειας. Προτείνετε στους χρήστες να επιλέγουν κωδικούς, μεγέθους τουλάχιστον 8 χαρακτήρων, που συνδυάζουν αλφαριθμητικά με σύμβολα. Ορίστε έναν μέγιστο αριθμό προσπαθειών που επιτρέπεται να δοκιμάσει κάποιος χρήστης να εισάγει

κωδικό πρόσβασης. Επιπλέον, ζητήστε από τους χρήστες να αλλάζουν τον κωδικό, όταν τους δίνεται ένα καινούργιο account».

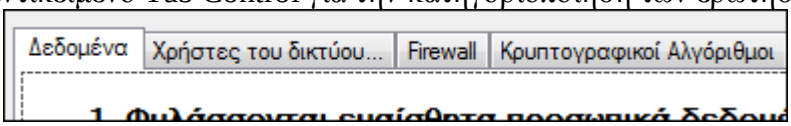
Ένα ακόμη παράδειγμα αφορά την επιλογή του χρήστη αναφορικά με το πόσοι από τους υπαλλήλους έχουν επιμορφωθεί πάνω στην σωστή χρήση του Internet. Αν η δοθείσα απάντηση είναι **26% - 50%,** τότε το SAT επισημαίνει: «Ο αριθμός των υπαλλήλων που έχουν παρακολουθήσει το επιμορφωτικό σεμινάριο είναι μικρός, γεγονός που μπορεί να προκαλέσει ζημιά ή και απώλειες στο υλικό και τους πόρους της εταιρίας. Φροντίστε για την επιμόρφωση όλων όσων χρειάζεται».

Για την κατασκευή του SAT

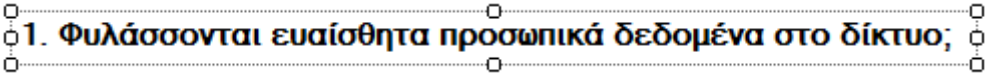
Το πρόγραμμα αναπτύχθηκε με την γλώσσα προγραμματισμού C# και χρησιμοποιήθηκαν βιβλιοθήκες του .NET Framework 2.0, το οποίο βασίζεται στην πλατφόρμα .NET, καθώς και εντολές HTML. Πιο συγκεκριμένα, χρησιμοποιήθηκαν:

Από τις βιβλιοθήκες .NET

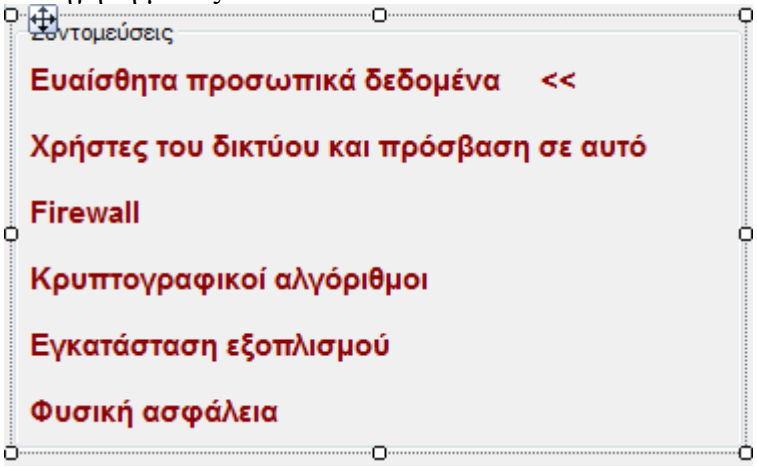
1. Ένα αντικείμενο Tab Control για την κατηγοριοποίηση των ερωτήσεων.



2. Αντικείμενα Label για την εμφάνιση των ερωτήσεων και την ευκολότερη πλοήγηση μεταξύ των Tabs.

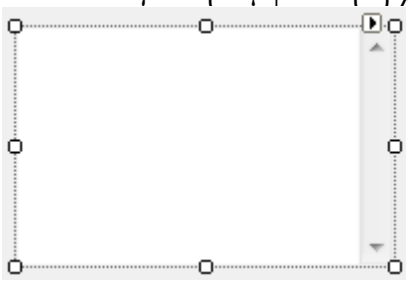


3. Ένα αντικείμενο Group Box για την ομαδοποίηση των Label τα οποία είναι υπεύθυνα για την πλοήγηση μεταξύ των Tabs.

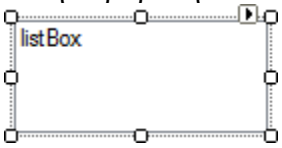


4. Αντικείμενα Button για την μετακίνηση σε επόμενο ή προηγούμενο Tab με ερωτήσεις και ένα ίδιο αντικείμενο για την εμφάνιση της αναφοράς.

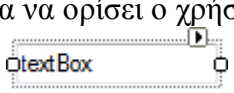
5. Ένα αντικείμενο Web Browser για την εμφάνιση αρχείου HTML.



6. Ένα αντικείμενο listBox για την προβολή των διαθέσιμων προφίλ.



7. Ένα αντικείμενο textBox για να ορίσει ο χρήστης ένα όνομα για νέο προφίλ.



8. Αντικείμενα checkBox για τις απαντήσεις του χρήστη

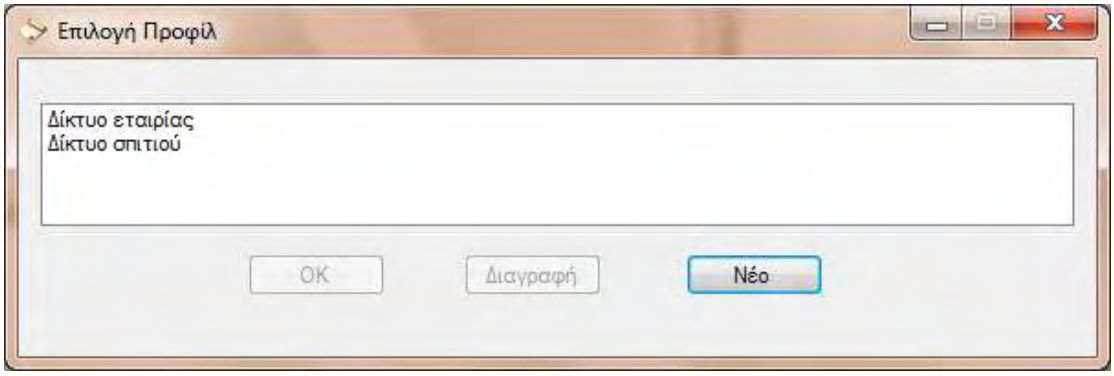
Εντολές HTML

Χρησιμοποιήθηκαν tags για την δημιουργία πινάκων, παραγράφων, επικεφαλίδων και την μορφοποίηση κειμένου.

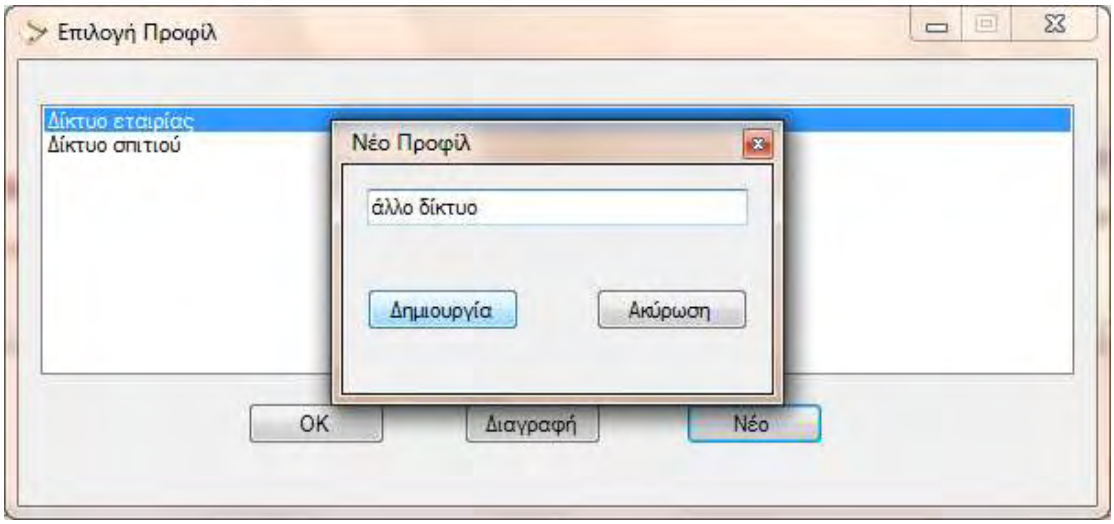
Λειτουργία του προγράμματος

Παρακάτω, δείχνουμε μία ενδεικτική λειτουργία του προγράμματος, μέσα από εικόνες.

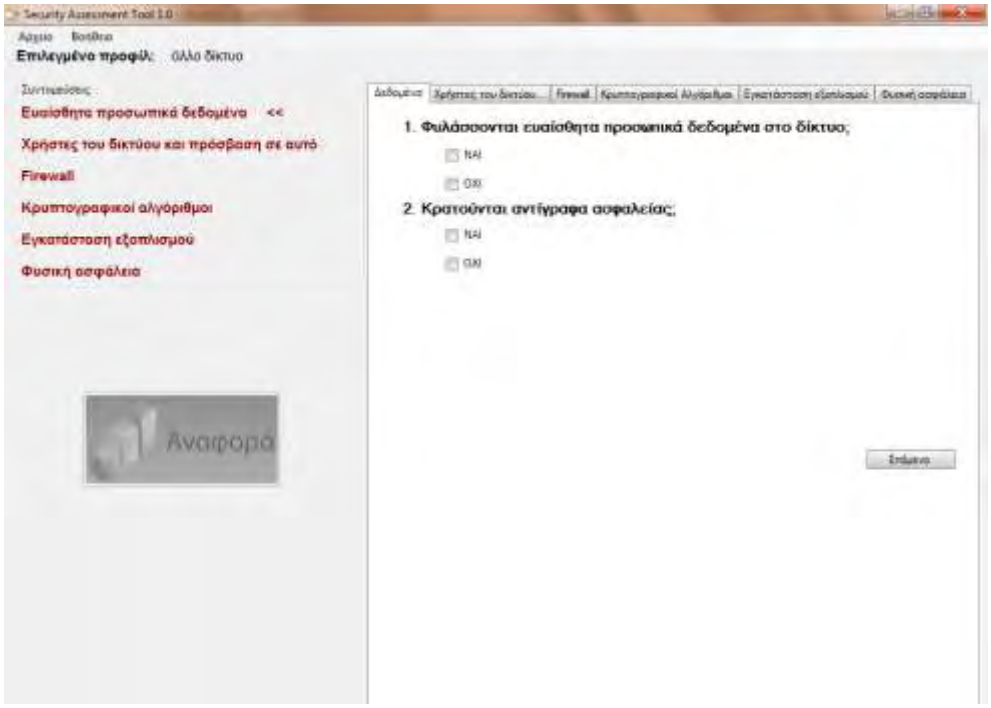
Πρώτο βήμα, όπως προαναφέραμε, η επιλογή προφίλ. Στον χρήστη εμφανίζεται αυτό το παράθυρο:

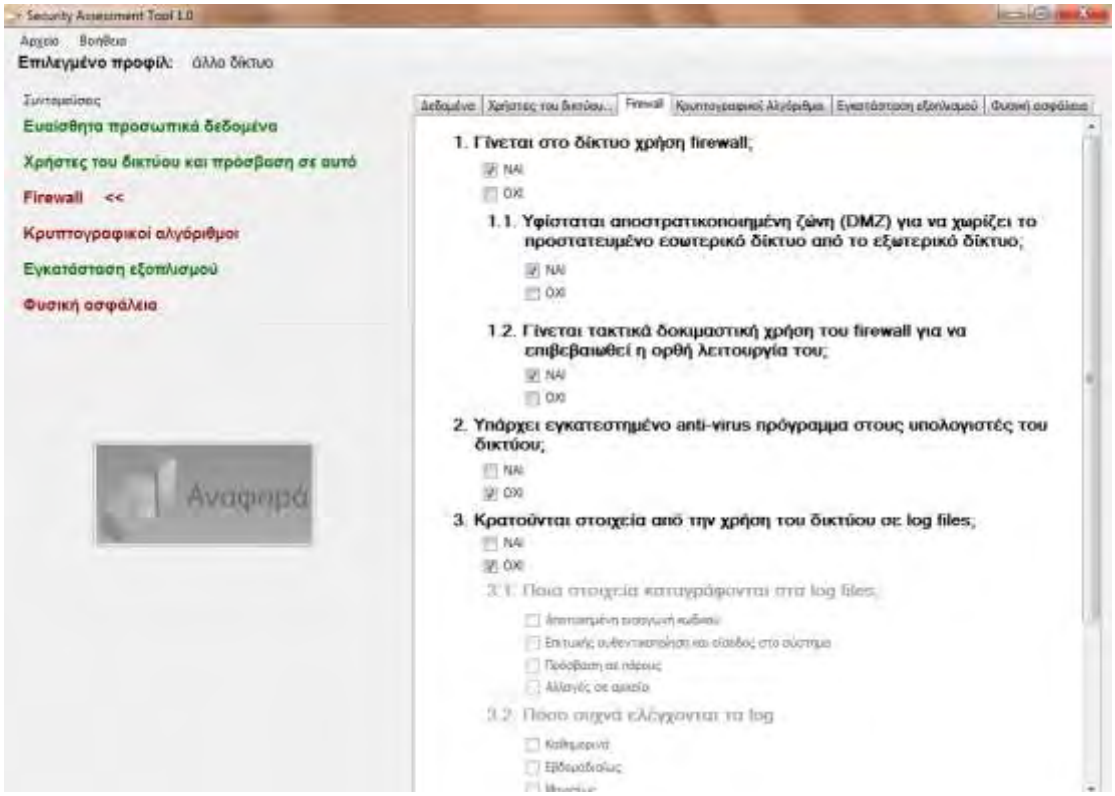


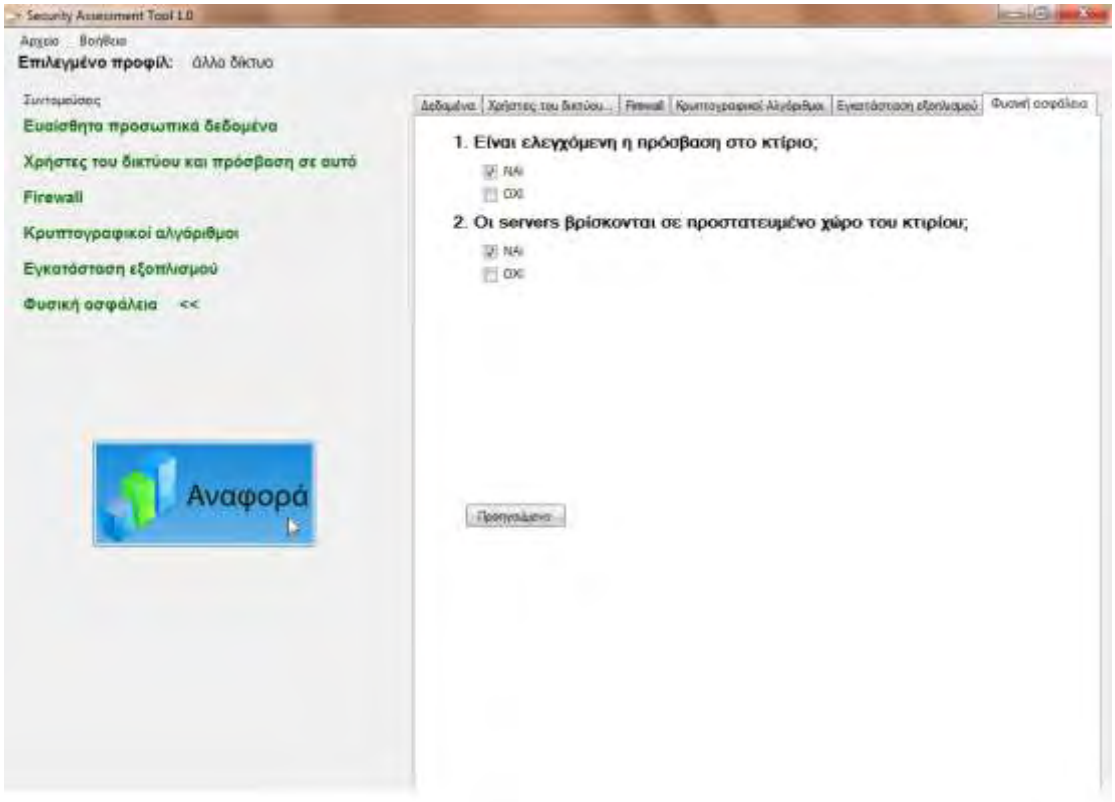
Αν δεν υπάρχει ήδη προφίλ, ο χρήστης δημιουργεί καινούργιο πατώντας στο κουμπί «Νέο»:



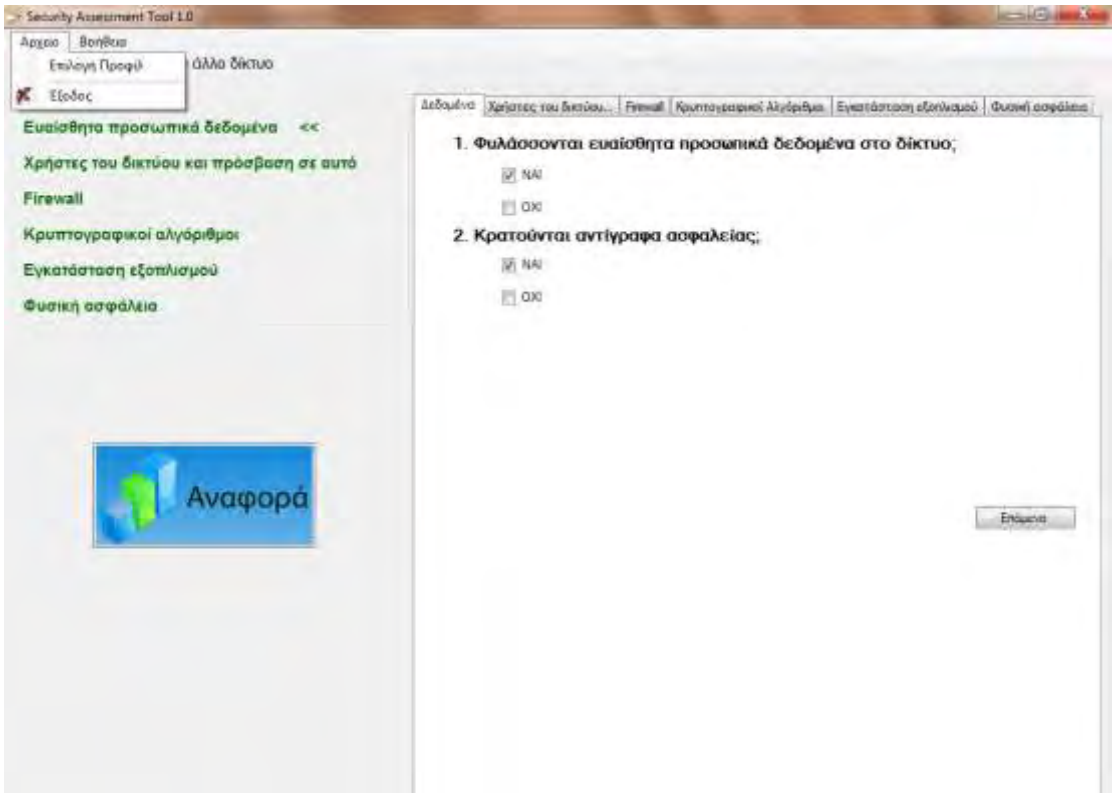
Ο χρήστης καλείται να συμπληρώσει τις απαντήσεις του. Παρακάτω δίνονται μερικές (τρεις) ενδεικτικές εικόνες του ερωτηματολογίου. Αριστερά, φαίνονται με κόκκινα γράμματα οι κατηγορίες των ερωτήσεων ενώ στο πάνω μέρος φαίνονται οι καρτέλες με τις ίδιες κατηγορίες:


Security Assessment Tool 1.0
Αρχείο Βοήθεια
Επιλεγμένο προφίλ: Άλλο δίκτυο
Συντομεύσεις
Ευαίσθητα προσωπικά δεδομένα <<
Χρήστες του δικτύου και πρόσβαση σε αυτό
Firewall
Κρυπτογραφικοί αλγόριθμοι
Εγκατάσταση εξοπλισμού
Φυσική ασφάλεια
Αναφορά
Δεδομένα
Χρήστες του δικτύου
Firewall
Κρυπτογραφικοί Αλγόριθμοι
Εγκατάσταση εξοπλισμού
Φυσική ασφάλεια
1. Φυλάσσονται ευαίσθητα προσωπικά δεδομένα στο δίκτυο;
ΝΑΙ
ΟΧΙ
2. Κρατούνται αντίγραφα ασφαλείας;
ΝΑΙ
ΟΧΙ
Επόμενο

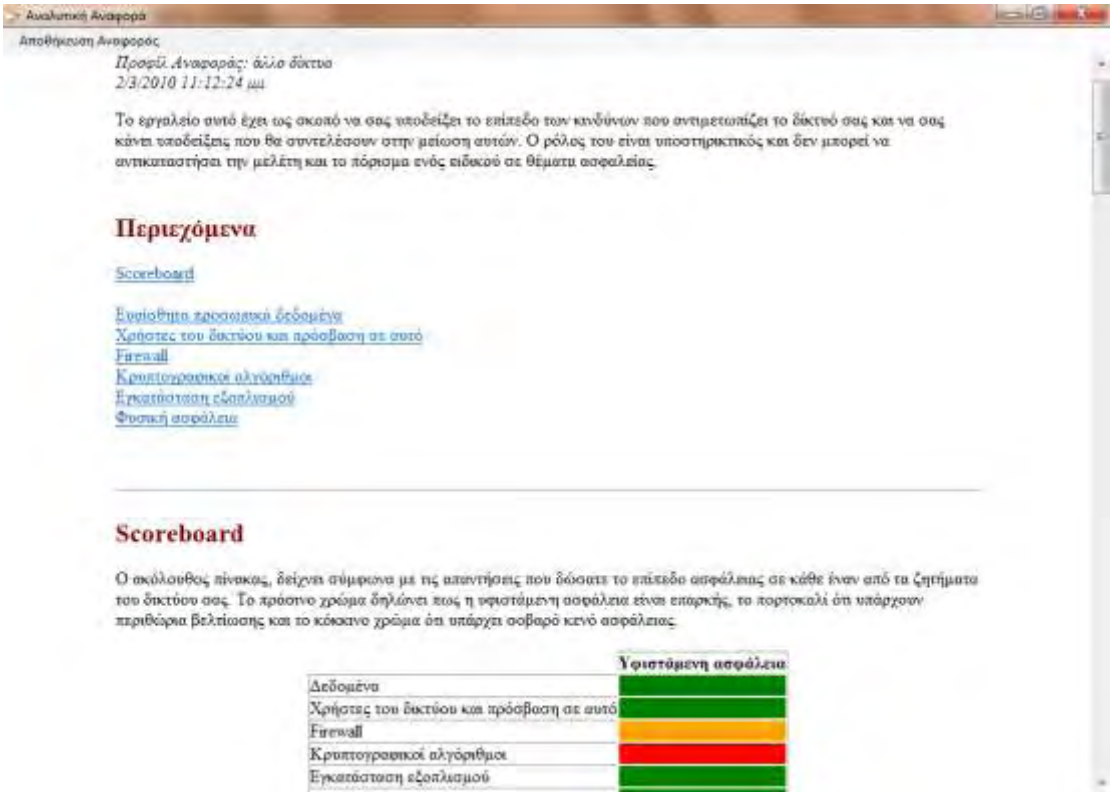

Security Assessment Tool 1.0
Αρχείο Βοήθεια
Επιλεγμένο προφίλ: Άλλο δίκτυο
Συντομεύσεις
Ευαίσθητα προσωπικά δεδομένα
Χρήστες του δικτύου και πρόσβαση σε αυτό
Firewall <<
Κρυπτογραφικοί αλγόριθμοι
Εγκατάσταση εξοπλισμού
Φυσική ασφάλεια
Αναφορά
Δεδομένα
Χρήστες του δικτύου
Firewall
Κρυπτογραφικοί Αλγόριθμοι
Εγκατάσταση εξοπλισμού
Φυσική ασφάλεια
1. Γίνεται στο δίκτυο χρήση firewall;
ΝΑΙ
ΟΧΙ
1.1. Υφίσταται αποστρατικοποιημένη ζώνη (DMZ) για να χωρίζει το προστατευμένο εσωτερικό δίκτυο από το εξωτερικό δίκτυο;
ΝΑΙ
ΟΧΙ
1.2. Γίνεται τακτικά δοκιμαστική χρήση του firewall για να επιβεβαιωθεί η ορθή λειτουργία του;
ΝΑΙ
ΟΧΙ
2. Υπάρχει εγκατεστημένο anti-virus πρόγραμμα στους υπολογιστές του δικτύου;
ΝΑΙ
ΟΧΙ
3. Κρατούνται στοιχεία από την χρήση του δικτύου σε log files;
ΝΑΙ
ΟΧΙ
3.1. Ποια στοιχεία καταγράφονται στα log files;
Αποτυχημένη εισαγωγή κωδικού
Επιτυχής αυθεντικοποίηση και είσοδος στο σύστημα
Πρόσβαση σε πόρους
Αλλαγές σε αρχεία
3.2. Ποιο συχνά ελέγχονται τα log
Καθημερινά
Εβδομαδιαίως


Security Assessment Tool 1.0
Αρχείο Βοήθεια
Επιλεγμένο προφίλ: Άλλο δίκτυο
Συντομεύσεις
Ευαίσθητα προσωπικά δεδομένα
Χρήστες του δικτύου και πρόσβαση σε αυτό
Firewall
Κρυπτογραφικοί αλγόριθμοι
Εγκατάσταση εξοπλισμού
Φυσική ασφάλεια <<
Αναφορά
Δεδομένα
Χρήστες του δικτύου...
Firewall
Κρυπτογραφικοί Αλγόριθμοι
Εγκατάσταση εξοπλισμού
Φυσική ασφάλεια
1. Είναι ελεγχόμενη η πρόσβαση στο κτίριο;
ΝΑι
ΟΧΙ
2. Οι servers βρίσκονται σε προστατευμένο χώρο του κτιρίου;
ΝΑι
ΟΧΙ
Προηγούμενο

Σημειώνουμε πως ενώ το πρόγραμμα έχει ξεκινήσει την λειτουργία του, το μενού πάνω αριστερά, δίνει στον χρήστη την δυνατότητα να αλλάξει το προφίλ ή σε όποια στιγμή να επιλέξει ένα ήδη υπάρχον:



Η προβολή αναφοράς είναι το τελευταίο βήμα που δίνει το αποτέλεσμα της συμπλήρωσης των ερωτήσεων:



Κεφάλαιο 6

Συμπεράσματα
Μελλοντικές επεκτάσεις

Τι πρόσφερε λοιπόν αυτή η διπλωματική εργασία; Καταρχήν πρέπει να διευκρινιστεί πως η συγγραφέας βρέθηκε μπροστά σε μία δυσάρεστη έκπληξη. Δεν βρήκε σε κάποιο ελληνικό ιστότοπο οργανισμού, πανεπιστημίου, νοσοκομείου κλπ, αυτό που εδώ ορίστηκε ως πολιτική ασφάλειας: Ένα κείμενο, γραμμένο σε απλή ελληνική γλώσσα που να ορίζει ποια είναι η επιτρεπτή χρήση ενός δικτύου και ποιος ο ενδεδειγμένος τρόπος συμπεριφοράς των χρηστών.

Πιθανόν λοιπόν η πολιτική ασφάλειας να θεωρείται κάτι πλεονάζον και κανείς δεν μπαίνει στον κόπο να την γράψει. Αφιερώθηκαν δύο ολόκληρα κεφάλαια αυτής την εργασίας ($2^{ο}$ και $3^{ο}$) για να εξηγήσουμε πόσο σημαντική είναι η πολιτική ασφάλειας και πόσες είναι οι παράμετροι που ρυθμίζει. Το σημαντικότερο όλων είναι να υπάρξει συνδετικός κρίκος μεταξύ διαχειριστή και προσωπικού: οι εργαζόμενοι ενός νοσοκομείου, γνωρίζουν τι είναι η χημειοθεραπεία αλλά πιθανόν να μην έχουν ιδέα από ασφαλείς ασύρματες συνδέσεις υπολογιστών. Είναι ζήτημα ουσίας, να έχουν πρόσβαση σε αυτές τις πληροφορίες. Και δεν υπάρχει καλύτερος τρόπος να γίνεται αυτό, πέρα από μια καλογραμμένη πολιτική ασφάλειας.

Το σκαλοπάτι που οδηγεί σε μια σωστή πολιτική ασφάλειας είναι η ανάλυση ρίσκου και η εκτίμηση κινδύνων στο δικτυακό περιβάλλον. Κανείς δεν αμφιβάλλει ότι αυτή η διαδικασία μπορεί να γίνει «χειροκίνητα». Ένα δυνατό ανθρώπινο μυαλό μπορεί να προβλέψει τα πάντα, ή σχεδόν τα πάντα. Σήμερα όμως το κατάλληλο λογισμικό είναι σύμμαχος και από αυτόν τον κανόνα δεν εξαιρείται ο τομέας που προαναφέραμε.

Πριν παρουσιάσουμε το δικό μας εργαλείο, κάναμε στο κεφάλαιο 4 μία αναφορά σε εργαλεία risk analysis, όπου είδαμε πλεονεκτήματα και μειονεκτήματα του καθένα. Εμείς, στο Security Assesment Tool δώσαμε βαρύτητα σε κάτι που διαπιστώσαμε ως έλλειψη σε ορισμένα λογισμικά: την αυτόματη δημιουργία γραπτής αναφοράς στο τέλος. Η ύπαρξη ενός γραπτού κειμένου δεν είναι χρήσιμη μόνο στον διαχειριστή. Είναι χρήσιμη κυρίως σε όλους όσους εμπλέκονται στην διοίκηση μιας εταιρίας και πιθανόν χρηματοδοτούν το δίκτυο. Η απλή γλώσσα είναι κατανοητή σε όλους.

Συμπερασματικά, η ασφάλεια και η διαχείριση ενός δικτύου είναι πάρα πολύ δύσκολες υποθέσεις. Είναι όμως απαραίτητες και λογισμικά όπως το SAT της παρούσης εργασίας, έχουν ως στόχο, να απλοποιήσουν εν μέρει κάποιες διαδικασίες.

Μελλοντικές επεκτάσεις

Η λειτουργία του δικού μας Security Assesment Tool έχει ως στόχο να καλύψει σε έναν σημαντικό βαθμό το μείζον ζήτημα της εκτίμησης κινδύνων σε ένα δίκτυο. Σε έναν σημαντικό βαθμό, εξυπηρετεί αυτή του την λειτουργικότητα, αφού οι ερωτήσεις καλύπτουν τα πλέον συνηθισμένα ζητήματα ασφάλειας που καλείται να αντιμετωπίσει ένας διαχειριστής.

Το ζήτημα της καλής λειτουργίας ενός δικτύου όμως, ενώ εξαρτάται σε μεγάλο βαθμό από την ασφάλεια, δεν εναπόκειται μόνο σε αυτή. Η **διαχείριση** είναι μία ακόμη λέξη κλειδί και δεν είναι υπερβολή να πούμε ότι από ένα γενικότερο πλαίσιο σωστής διαχείρισης ξεκινά ένα καλά δομημένο, χωρίς προβλήματα και απώλειες, δίκτυο.

Μία μελλοντική επέκταση του SAT λοιπόν θα μπορούσε να σταθεί πολύ περισσότερο σε αυτό το κομμάτι: το κομμάτι της διαχείρισης. Η καταγραφή επιπλέον

χαρακτηριστικών του δικτύου (π.χ. αριθμός ασύρματων και ενσύρματων συνδέσεων) αλλά και η καταγραφή περισσότερων λεπτομερειών γι' αυτό, όπως για παράδειγμα αριθμός των υπολογιστών που το αποτελούν, ταχύτητα μεταφοράς των δεδομένων, είδος του hardware που χρησιμοποιείται καθώς και άλλα σχόλια, θα ήταν χρήσιμα στον διαχειριστή, ο οποίος έχοντας μια πολύ καλή εικόνα για το πώς είναι δομημένο το δίκτυο, μπορεί να το βελτιώσει.

Η κατανομή των ρόλων είναι ένα κομμάτι στο οποίο μπορεί να υπάρξει πλούσιο πεδίο για μελλοντική επέκταση. Οργανισμοί και επιχειρήσεις έχουν υποστεί καταστροφικά λάθη εξαιτίας λανθασμένων επιλογών στο κρίσιμο αυτό ζήτημα: το Εθνικό Θησαυροφυλάκιο της Αγγλίας υπέστη διάρρηξη στις 22 Φεβρουαρίου 2006 από εισβολείς που πήραν φεύγοντας 53 εκατομμύρια στερλίνες. Ενώ στον οργανισμό εφαρμόζονταν προηγμένα συστήματα ασφαλείας, όλα εξουδετερώθηκαν από τον γενικό διευθυντή, ο οποίος εξαναγκάστηκε σε αυτή την πράξη αφού οι δράστες είχαν απαγάγει το παιδί και την σύζυγό του. Είναι προφανές ότι στον σχεδιασμό της ασφάλειας δεν είχε γίνει σωστή πρόβλεψη, αφού ο διευθυντής ήταν ο μόνος που είχε πρόσβαση παντού, γεγονός που αποδείχτηκε μοιραίο. Είναι λάθος να στηρίζεται όλο το σύστημα ασφαλείας σε έναν άνθρωπο και η κατανομή των ρόλων πρέπει να προβλέπεται απαραιτήτως στον σχεδιασμό.

Εκτός από τα παραπάνω, στο μέλλον, θα μπορούσε κάποιος να εργαστεί πάνω στην βελτίωση της παρουσίασης των γραπτών αναφορών. Είναι σημαντικό, ο διαχειριστής, να μελετάει μία αναφορά η οποία να είναι οπτικά ελκυστική και να τον βοηθάει στο να επικεντρωθεί στα καίρια σημεία της, να έχει όσο δυνατόν καλύτερες και κατατοπιστικές προτάσεις. Κάτι τέτοιο θα μπορούσε, ως ένα βαθμό, να επιτευχθεί πιθανώς με την προσθήκη στατιστικών γραφημάτων σε ορισμένα σημεία.

Είναι επίσης γεγονός ότι στις εταιρίες αυτό που έχει σημασία στο τέλος της ημέρας είναι το κόστος. Θα μπορούσαν λοιπόν στο πρόγραμμα να προστεθεί κάποια σειρά ερωτήσεων, μέσα από τις οποίες στην τελική αναφορά θα προκύπτει κάποιο συμπέρασμα για το οικονομικό κόστος που θα υπάρξει από μια ενδεχόμενη παραβίαση ασφάλειας. Αυτό είναι ένα επιχείρημα που πείθει τους περισσότερους διοικητικούς στην λήψη των αναγκαίων μέτρων.

Τέλος, η προσθήκη νέων κατηγοριών και ερωτήσεων ή τροποποίηση αυτών που υπάρχουν ήδη, προκειμένου να επιτευχθεί καλύτερη συλλογή δεδομένων για το διαχειριζόμενο δίκτυο, λόγω του ότι υπάρχει πάντα το ενδεχόμενο να εμφανιστούν νέες και καλύτερες τεχνολογίες, θα ήταν ένα καλό πεδίο για μελλοντική βελτίωση.

Επίλογος

Πόσο ασφαλείς μπορούμε να είμαστε τελικά; Αυτό είναι το μεγάλο ζητούμενο. Μπορούμε να είμαστε ασφαλείς σε ικανοποιητικό βαθμό, προφανώς. Η πολιτική ασφάλειας είναι το πρώτο σκαλοπάτι που πρέπει να ανέβει κάποιος αν θέλει να «χτίσει» ένα ασφαλές δίκτυο. Η ανάλυση ρίσκου και η αποτίμηση κινδύνων είναι διαδικασίες απαραίτητες, που πλέον διευκολύνονται σημαντικά από την ύπαρξη των σχετικών λογισμικών.

Ακόμη και στην περίπτωση ενός διαχειριστή ο οποίος δεν έχει εξαιρετικά υψηλό επίπεδο γνώσεων, το κατάλληλο εργαλείο μπορεί να κάνει σημαντικές υποδείξεις που θα δώσουν τις κατευθύνσεις για ένα σημαντικό επίπεδο ασφάλειας.

Η έννοια της ασφάλειας είναι μια έννοια συνδεδεμένη ούτως ή άλλως στενά με την ανθρώπινη φύση: θέλουμε να νιώθουμε ασφαλής, το επιζητούμε και το ίδιο επιθυμούμε για οτιδήποτε έχουμε δημιουργήσει. Το δίκτυο μιας εταιρίας ή ενός οργανισμού είναι σήμερα οι πνεύμονές της, αυτό που της δίνει την επικοινωνία με τον έξω κόσμο. Η οικονομία και η στρατηγική μιας εταιρίας είναι πλέον ταυτισμένη με το δίκτυό της: εφημερίδες, ξενοδοχεία, κατασκευαστικές εταιρίες, νοσοκομεία, υπουργεία, αλλά και μικρότερης κλίμακας επαγγελματικοί χώροι, όπως δικηγορικά γραφεία και κτηματομεσιτικά γραφεία, δεν μπορούν πια να φανταστούν την λειτουργία τους χωρίς Internet και γενικότερα χωρίς δικτύωση μεταξύ των εργαζομένων. Είναι ζήτημα ουσίας λοιπόν το δίκτυο αυτό να λειτουργεί σωστά, ελλοχεύοντας τους ελάχιστους δυνατούς κινδύνους για τα δεδομένα και του ανθρώπους του.

Είδαμε όμως στην παρούσα διπλωματική εργασία πως αυτοί οι ίδιοι οι άνθρωποι είναι που μπορούν να δημιουργήσουν προβλήματα. Τα εργαλεία αποτίμησης κινδύνων καλούνται να κάνουν μία εξαιρετικά δύσκολη δουλειά. Το να προβλεφθούν οι κίνδυνοι σε οποιαδήποτε ενέργεια της ζωής μας είναι σχεδόν αδύνατο, από την άποψη ότι οι πιθανοί συνδυασμοί ενεργειών που δύνανται να προκαλέσουν πρόβλημα είναι αμέτρητοι. Η κύρια δυσκολία όμως σε μια επιτυχημένη διαδικασία ανάλυσης ρίσκου δεν είναι αυτή. Η κύρια δυσκολία είναι αυτή που αναφέρθηκε και πιο πάνω: η ανθρώπινη φύση που κρύβει εκπλήξεις, ευχάριστες ή – στην προκειμένη περίπτωση – δυσάρεστες.

Από μια άποψη λοιπόν, η πολιτική ασφάλειας είναι ο «ψυχολόγος» του πληροφοριακού συστήματος. Λαμβάνοντας υπόψη την εξάρτηση του από τον παράγοντα «άνθρωπο», η πολιτική ασφάλειας καλείται να προβλέψει πιθανές ενέργειες και αντιδράσεις κάποιου, πράγμα εξαιρετικά πολύπλοκο εξαιτίας της ίδιας της πολυπλοκότητας των ανθρώπων.

Συμπερασματικά, οι μηχανισμοί και οι τεχνικές από μόνα τους δεν συνιστούν μέτρα ασφαλείας. Απόδειξη το παράδειγμα με το θησαυροφυλάκιο της Αγγλίας που προαναφέρθηκε. Αυτά πρέπει να λειτουργούν κάτω από ένα μοντέλο ασφάλειας.

Βιβλιογραφία

[1] Ασφάλεια πληροφοριακών συστημάτων και δικτύων, Γ. Πάγκαλος, Ι. Μαυρίδης, κεφάλαιο 2 «Πολιτικές και Μοντέλα Ασφάλειας ΠΣ»

[2] Σχέδιο ασφάλειας και σχέδιο έκτακτης ανάγκης, Βασίλειος Ζορκάδης, Ευφροσύνη Σιουγλέ, www.dpa.gr (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

[3] http://www.information-security-policies-and-standards.com/

[4] Απόφαση αριθ. 632 α «Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές»

[5] http://media.techtarget.com/digitalguide/images/Misc/firewall_dmz.jpg

[6] Απόφαση αριθ. 634 α «Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου»

[7] «e-Business και Προστασία Προσωπικών Δεδομένων: σεβασμός του πολίτη στην Ψηφιακή Εποχή», Κωνσταντίνος Μουλίνος, Κωνσταντίνα Καμπουράκη, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[8] Απόφαση αριθ. 633 α «Κανονισμός για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών

[9] Διάλεξη no5 από το μάθημα «Σχεδιασμός και υλοποίηση τηλεπικοινωνιακών δικτύων» του κ. Αρσένη Σπύρου που διδάχθηκε στο Τμήμα Μηχανικών Η/Υ, τηλεπικοινωνιών και δικτύων του Πανεπιστημίου Θεσσαλίας, κατά το εαρινό εξάμηνο 2003 (ppt αρχείο), διαφάνεια 18.

[10] Ασφάλεια πληροφοριακών συστημάτων, κεφάλαιο 10, Προσεγγίσεις Ασφάλειας Πληροφοριακών Συστημάτων, Ευάγγελος Κιουντούζης

[11] Ασφάλεια πληροφοριακών συστημάτων, κεφάλαιο 11, Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας ΠΣ, Σπύρος Κοκολάκης

[12] Ασφάλεια πληροφοριακών συστημάτων, κεφάλαιο 12, Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων, Μαρία Καρύδα

[13] Δικτυακός τόπος Αρχής Προστασίας Προσωπικών Δεδομένων, www.dpa.gr

[14] Νόμος 2472/1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

[15] Νόμος 2474/1999, Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

[16] Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.

[17] Σύσταση Αρ. R (99) 5 της επιτροπής υπουργών των κρατών μελών για την προστασία της ιδιωτικότητας στο Διαδίκτυο.

[18] Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

[19] Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου.

[20] Οδηγία 2001/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 22ας Μαΐου για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας.

[21] Σχέδιο ασφάλειας και σχέδιο έκτακτης ανάγκης, Βασίλειος Ζορκάδης, Ευφροσύνη Σιουγλέ, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

[22] Δικτυακός τόπος Αρχής Προστασίας Προσωπικών Δεδομένων, www.dpa.gr

[23] Ασφάλεια πληροφοριακών συστημάτων, κεφάλαιο 11, Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας ΠΣ, Σπύρος Κοκολάκης

[24] www.qualys.com/products/release/5-0/

[25] www.nessus.org

[26] www.callio.com

[27] www.riskworld.net

[28] http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html

[29] http://www.enisa.europa.eu/rmra/rm_ra_tools.html

[30] http://searchsecurity.techtarget.com/tip

Παραρτήματα κώδικα

Παράρτημα 1: *Επιλογή προφίλ*

```
/*
 * Profiles.cs
 */
using System;
using System.Drawing;
using System.Windows.Forms;

namespace SAT
{
	/// <summary>
	/// Description of Profiles.
	/// </summary>
	public partial class Profiles : Form
	{
		public Profiles()
		{
			InitializeComponent();
		}
		…
		…
}
```

Παράρτημα 2: *Αποθήκευση Αναφοράς*

```
/*
 * anaforaViewer.cs
 */
void Save_Dialog()
{
	saveFileDialog.Filter = "HTML Files (*.htm)|*.htm|" + "All Files|";
	saveFileDialog.AddExtension = true;
	saveFileDialog.RestoreDirectory = true;
	saveFileDialog.InitialDirectory =
Environment.GetFolderPath(Environment.SpecialFolder.Personal);

	// Εμφάνιση παραθύρου για αποθήκευση
	if( saveFileDialog.ShowDialog() == DialogResult.OK )
	{
		//Κλήση της Copy() για την αποθήκευση της αναφοράς
		Copy(saveFileDialog.FileName);
	}

}
void Copy(string targetPath)
{
	string sourcePath = @"profiles\" + profileName + @"\" + profileName + ".htm";
```

```
        //Αντιγραφή της αναφοράς που δημιούργησε το πρόγραμμα εκεί που θέλει ο χρήστης
        System.IO.File.Copy(sourcePath, targetPath);
}
```

Παράρτημα 3: *Ενεργοποίηση κουμπιού αναφοράς*

```
/*
 * MainForm.cs
 */

/* ενεργοποίηση όταν όλα τα labels έχουν χρώμα πράσινο */
void energopoihshReport(object sender, EventArgs e)
{
         if (dedomenaLabel.ForeColor == Color.DarkGreen && prosbasiLabel.ForeColor ==
Color.DarkGreen && asfaleiaLabel.ForeColor == Color.DarkGreen && fysAsfaleiaLabel.ForeColor
== Color.DarkGreen && algorithmoiLabel.ForeColor == Color.DarkGreen &&
exoplismosLabel.ForeColor == Color.DarkGreen)
                  reportButton.Enabled = true;
        else
                 reportButton.Enabled = false;
}
```

Παράρτημα 4: *Παραγωγή αποτελεσμάτων*

```
/*
 * MainForm.cs
 */
void dhmiourgia_Arxeiou_Html()
{
        int scoreboardSynolo = scoreboardTab_1 + scoreboardTab_2 + scoreboardTab_3 +
scoreboardTab_4 + scoreboardTab_5 + scoreboardTab_6;

        FileStream fs = new FileStream(@"profiles\" + profileName + @"\" + profileName + ".htm",
FileMode.Create);

        StreamWriter Report = new StreamWriter(fs, Encoding.UTF8);

        DateTime dt = DateTime.Now; //Trexousa hmeromhnia kai wra


        /* Άρχή του αρχείου αναφοράς */
        Report.WriteLine("<html>");
        …
        …
        if (scoreboardTab_3 >= 18)
                Report.WriteLine("        <td bgcolor=\"green\">");
        else if (scoreboardTab_3 < 18 && scoreboardTab_3 >= 10)
                Report.WriteLine("        <td bgcolor=\"orange\">");
        else
                Report.WriteLine("        <td bgcolor=\"red\">");
```

```
…
…
                Report.WriteLine("");
                Report.WriteLine("  ");
                Report.WriteLine("</body>");
                Report.WriteLine("");
                 Report.WriteLine("</hmtl>");
                 /* Τέλος αρχείου αναφοράς */

                 Report.Close();          //Κλείσιμο αρχείου
                 fs.Close();      //Κλείσιμο fileStream
}
```

Παράρτημα 5: *Εμφάνιση Web Browser*

```
/*
 * MainForm.cs
 */
void ReportButtonClick(object sender, EventArgs e)
{
        dhmiourgia_Arxeiou_Html();
        //Δημιουργία ανικειμένου για την προβολή της αναφοράς
        anaforaViewer a = new anaforaViewer(profileName);

        // Εμφάνιση παραθύρου με την αναφορά
        a.ShowDialog();
}
```