Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών

(«ENISA»)

Παραδοτέο ENISA:

Πακέτο Πληροφοριών για Μικρομεσαίες Επιχειρήσεις (ΜΜΕ)

Με παραδείγματα

εκτίμησης κινδύνων / διαχείρισης κινδύνων

για δύο ΜΜΕ

(διατίθεται επίσης στην ιστοσελίδα www.enisa.europa.eu/rmra)

Υλοποιήθηκε από το

Τεχνικό Τμήμα του ENISA

Τμήμα Διαχείρισης Κινδύνων

σε συνεργασία με:

τον κ. Γεώργιο Πάτση

Obrela Security Industries (OSI)

www.obrela.com

Φεβρουάριος 2007

Σύνοψη

Το παρόν έγγραφο αποτελεί το δεύτερο παραδοτέο του ENISA όπως αναφέρεται στο Πρόγραμμα Εργασίας του 2006 του ENISA. Μέρη του παρόντος υλικού βασίζονται στην ανάγκη για μια απλουστευμένη προσέγγιση για την εκτίμηση κινδύνων που διαβιβάστηκε στον ENISA.

Ο στόχος αυτού του εγγράφου είναι να παράσχει μια απλουστευμένη και συνολική θεώρηση της διαχείρισης κινδύνων/εκτίμησης κινδύνων για χρήση στις μικρομεσαίες επιχειρήσεις (ΜΜΕ). Για την επίτευξη του στόχου αυτού, το παρόν έγγραφο διαρθρώνεται κατά τμηματικό τρόπο. Συγκροτείται, δηλαδή, από διάφορα μέρη, καθένα από τα οποία αφιερώνεται σε συγκεκριμένες ανάγκες των ενδιαφερόμενων μερών που συμμετέχουν στην διαδικασία εκτίμησης και διαχείρισης κινδύνων.

Η φιλοσοφία που διέπει την παραγωγή αυτού του υλικού έγκειται στο να προστατεύσει τους (μη ειδικούς) χρήστες από την πολυπλοκότητα των δραστηριοτήτων που σχετίζονται με την διαχείριση και την εκτίμηση κινδύνων. Κατά συνέπεια, ορισμένα πολύπλοκα ζητήματα ασφάλειας έχουν απλουστευθεί στο ελάχιστο που απαιτείται προκειμένου να επιτευχθεί ένα αποδεκτό επίπεδο ασφάλειας.

Δεν υπάρχει αμφιβολία ότι εφόσον απαιτείται υψηλό επίπεδο ασφάλειας πρέπει να ληφθεί υπόψη ο μέγιστος βαθμός πολυπλοκότητας της διαχείρισης ασφάλειας, συμπεριλαμβανομένης της εμβάθυνσης στη λεπτομερή μορφή των ανάλογων μέτρων και της ανάλογης τεχνολογίας. Υπ' αυτή την έννοια, θεωρείται ότι οι ιδέες και η προσέγγιση, που εκτίθενται στο παρόν, καλύπτουν ένα αποδεκτό επίπεδο ασφάλειας για μικρές επιχειρήσεις με περιορισμένες επενδύσεις στην ασφάλεια. Περισσότερο προηγμένοι τύποι ασφάλειας (π.χ. στοιχεία υποδομής ζωτικής σημασίας) θα απαιτούσαν ενδελεχέστερη θεώρηση η οποία υπερβαίνει το πεδίο εφαρμογής του παρόντος εγγράφου.

Το εν λόγω υλικό έχει παραχθεί προβλέποντας το συνολικό εύρος δεξιοτήτων των διαφορετικών ενδιαφερόμενων μερών που συμμετέχουν στην διαδικασία εκτίμησης κινδύνων. Η προτεινόμενη διαδικασία εκτίμησης κινδύνων διαρθρώνεται μέσω μιας απλουστευμένης προσέγγισης εκτίμησης τεσσάρων φάσεων. Δεν υποθέτουμε ότι υφίσταται οποιαδήποτε προηγμένη γνώση ζητημάτων ασφάλειας από μέρους των χρηστών του υλικού αυτού. Όπου απαιτείται αυτή η γνώση, η παρούσα προσέγγιση αντιπροσωπεύει ένα «μαύρο κουτί» που προσφέρει περιορισμένο αριθμό περιεκτικών επιλογών.

Ένα άλλο κριτήριο που πρέπει να ληφθεί υπόψη είναι η σχέση κόστους - αποτελεσματικότητας σε όλα τα στάδια της εκτίμησης και της διαχείρισης κινδύνων. Το παρόν υλικό μπορεί να βοηθήσει τους υπεύθυνους για την λήψη αποφάσεων να καθορίσουν ποια προσέγγιση ταιριάζει περισσότερο στην επιχείρηση τους για την εκτίμηση των κινδύνων, βάσει δεικτών κόστους και απόδοσης. Επιπλέον, στην περίπτωση που έχει επιλεγεί η διαδικασία αυτοαξιολόγησης, αυτό το έγγραφο παρέχει τα απαραίτητα εργαλεία για τη διεξαγωγή της ίδιας διαδικασίας, χωρίς να απαιτείται προηγούμενη εμπειρία σ' αυτό το πεδίο.

Η απλουστευμένη προσέγγιση εκτίμησης κινδύνων, που παρουσιάζεται σ' αυτό το έγγραφο, αποτελεί ένα παράδειγμα ορθής πρακτικής για την αξιολόγηση των πληροφοριακών κινδύνων. Θεωρείται, ωστόσο, ότι υπάρχουν και άλλες παρόμοιες προσεγγίσεις/ορθές πρακτικές, οι οποίες θα μπορούσαν να χρησιμοποιηθούν αντ' αυτής. Σε αυτό το πλαίσιο, η παρούσα προσέγγιση δεν αποτελεί ούτε προσπάθεια αντικατάστασης υφιστάμενων προτύπων ούτε επαναπροσδιορισμού ορθών πρακτικών. Αντιθέτως, έχει σχεδιαστεί για να παράσχει στις ενδιαφερόμενες ΜΜΕ ένα εργαλείο που δεν θα μπορούσαν να βρουν εύκολα αλλού.

Η εφαρμογή των ιδεών, οι οποίες εκτίθενται στο παρόν, καταδεικνύεται με την χρήση παραδειγμάτων. Έχουν επιλεγεί δυο αντιπροσωπευτικοί τύποι ΜΜΕ, των οποίων οι κίνδυνοι εκτιμώνται αξιοποιώντας την παρούσα προσέγγιση εκτίμησης. Τα παραδείγματα αυτά παρουσιάζονται στο πλαίσιο της προτεινόμενης απλουστευμένης προσέγγισης εκτίμησης κινδύνων.

Αξίζει να αναφερθεί ότι αυτό το έγγραφο είναι το πρώτο από μια σειρά ανάλογων εγγράφων που θα δοθούν στην δημοσιότητα από τον ENISA για την παροχή πληροφόρησης σχετικά με την διαχείριση και την εκτίμηση κινδύνων για τις ΜΜΕ. Παράλληλα, θα υπόκειται σε περαιτέρω βελτιώσεις, προσαρμογές και επεκτάσεις. Στις δραστηριότητες του ENISA, που έπονται στο μέλλον, περιλαμβάνονται η επαλήθευση αυτού του υλικού μέσω πιλοτικών προγραμμάτων σε ΜΜΕ, η αξιολόγηση/επιθεώρηση μέσω ομάδων εμπειρογνωμόνων, η διάχυση μέσω επαγγελματικών ενώσεων και/ή ενώσεων επαγγελματικής κατάρτισης κτλ. Ο τελικός στόχος έγκειται στην διαμόρφωση μιας έκδοσης αυτού του εγγράφου που να μπορεί να χρησιμοποιηθεί από τις ΜΜΕ «ως έχει», χωρίς να χρειάζεται δηλαδή περαιτέρω βελτιώσεις/επεξηγήσεις/προσαρμογές. Γι' αυτό τον λόγο, αναφερόμαστε στο παρόν έγγραφο

ως «δοκιμαστική έκδοση», που σημαίνει ότι θα ακολουθήσουν πρόσθετες βελτιώσεις και προσαρμογές μετά από διάφορες πιλοτικές εφαρμογές, φάσεις ανάπτυξης και διάδοσης του παρόντος, οδηγώντας, συνεπώς, μεσοπρόθεσμα, στην ωρίμανση του παρουσιαζόμενου στο παρόν υλικού.

Στοιχεία επικοινωνίας: Τεχνικό Τμήμα του ENISA, Τμήμα Διαχείρισης Κινδύνων, Δρ. Λ. Μαρίνος, Ανώτερος Ειδικός Διαχείρισης Κινδύνων, ηλεκτρονικό ταχυδρομείο (e-mail): RiskMngt@enisa.europa.eu

Περιεχόμενα

Πίνακας Σχημάτων

Πίνακας Πινάκων

1. Αντικείμενο και πεδίο εφαρμογής

Οι μικρομεσαίες επιχειρήσεις (ΜΜΕ) αποτελούν τομέα προτεραιότητας ενδιαφέροντος στον οποίο επικεντρώνεται η κυβερνητική οικονομική πολιτική και θεωρούνται μείζονος σημασίας για την κοινωνικοοικονομική ανάπτυξη στην Ευρωπαϊκή Ένωση. Οι ΜΜΕ συνήθως δημιουργούνται από επιχειρηματικό πάθος και ελλιπή χρηματοδότηση, με επιχειρησιακά συστήματα, τα οποία συχνά είναι ετερογενή και ανεξάρτητα. Επιπρόσθετα, οι υλικοί και άυλοι επιχειρηματικοί πόροι των ΜΜΕ ορίζονται στοιχειωδώς και η αξία αυτών των πόρων, συχνά, είναι γνωστή μόνο εν μέρει. Συνήθως, αυτό συμβαίνει με έναν από τα πιο σημαντικούς πόρους, δηλαδή, τις πληροφορίες.

Όπως συμβαίνει με κάθε άλλο επιχειρηματικό πόρο, οι πληροφορίες απαιτείται να διαχειρίζονται και να προστατεύονται με στρατηγική. Ασφάλεια των πληροφοριών θεωρείται η προστασία των πληροφοριών μέσα σε μια επιχείρηση, συμπεριλαμβανομένων των συστημάτων και του υλικού εξοπλισμού που χρησιμοποιούνται για την αποθήκευση, την επεξεργασία και την μετάδοση αυτών των πληροφοριών. Είναι επιβεβλημένο η επιχειρηματική ηγεσία των ΜΜΕ να κατανοήσει την αξία των πληροφοριών, που εμπεριέχονται στα επιχειρησιακά συστήματά τους και να διαθέτει πλαίσιο αξιολόγησης και υλοποίησης της ασφάλειας των πληροφοριών. Πολυάριθμα διεθνώς εγκεκριμένα πλαίσια και προγράμματα ασφάλειας μπορούν να εφαρμοστούν για να προστατεύσουν έναν οργανισμό από την απώλεια πληροφοριών και την ενδεχόμενη ευθύνη. Δεδομένου ότι αυτά τα πλαίσια είναι περίπλοκα, καθολικά και, σε τελευταία ανάλυση, ακριβά στην εφαρμογή τους, υιοθετούνται κυρίως από μεγάλους οργανισμούς.

Συνήθως, λόγω της δυναμικής και της ad hoc ανάπτυξης πολλών ΜΜΕ, δεν αντιμετωπίζονται συστηματικά ούτε τα ζητήματα ενσωμάτωσης ούτε τα θέματα ασφάλειας κατά το στάδιο της δημιουργίας μιας επιχείρησης. Για τον λόγο αυτό, πολιτικές και πλαίσια για τον σχεδιασμό της ασφάλειας πληροφοριών και της ανάκτησης από καταστροφή είναι συνήθως πολύ στοιχειώδεις(-η) ή ακόμα και απούσες/απόντα. Συχνά, είναι πιθανό η βασική κατανόηση των κινδύνων που αφορούν στην ασφάλεια των πληροφοριών να μην εκτείνεται πολύ πιο πέρα από τους ιούς και το αντιικό λογισμικό. Οι ακούσιες απειλές θέτουν ορισμένους από τους υψηλότερους κινδύνους για την ασφάλεια των πληροφοριών στις ΜΜΕ και, επιπλέον, συχνά παραμελούνται η κατάρτιση του προσωπικού και τα προγράμματα ενημέρωσης.

Τα αποτελέσματα των ερευνών αποκαλύπτουν ότι το επίπεδο της ευαισθητοποίησης σε θέματα της ασφάλειας των πληροφοριών μεταξύ ηγετών των ΜΜΕ είναι τόσο μεταβλητό όσο και η κατάσταση των πληροφοριακών συστημάτων, της πληροφορικής τεχνολογίας και της ασφάλειας των πληροφοριών τους. Αν και μια μειονότητα των ΜΜΕ δέχεται ένθερμα πλαίσια ασφάλειας όπως το ISO / IEC 27001 ή το διεθνές ισοδύναμο ISO 17799, τα περισσότερα διοικητικά στελέχη των ΜΜΕ δεν έχουν ακουστά για τα πρότυπα ασφάλειας και θεωρούν την ασφάλεια των πληροφοριών μόνο σαν μια τεχνική παρέμβαση σχεδιασμένη να αντιμετωπίζει τις απειλές από τους ιούς και να επιλαμβάνεται της δημιουργίας εφεδρικών αντιγράφων ασφάλειας δεδομένων.

Τα διοικητικά στελέχη όχι μόνον κατηγορούνται για το ότι δεν κατανοούν το καθοριστικό ζήτημα που περιβάλλει την ασφάλεια των πληροφοριών, αλλά οι έρευνες καταλήγουν στο ότι η ηγεσία των ΜΜΕ είναι ανάγκη να καταπιαστεί με, να κατανοήσει και να υλοποιήσει επίσημες διαδικασίες ασφάλειας των πληροφοριών, συμπεριλαμβανομένων των τεχνικών και των οργανωτικών μέτρων. Χωρίς τέτοια μέτρα, οι οργανισμοί τους μπορεί να επηρεαστούν σε υπερβολικό βαθμό από ακούσιες απειλές/ εσκεμμένες επιθέσεις στα συστήματα πληροφοριών τους, που, εν τέλει, θα μπορούσαν να οδηγήσουν σε αποτυχία της επιχείρησης.

Βάσει των περιεχομένων αυτού του πακέτου πληροφοριών, οι ΜΜΕ θα είναι σε θέση να διενεργούν εκτιμήσεις κινδύνων στα περιβάλλοντά τους, να επιλέγουν και να εφαρμόζουν κατάλληλα μέτρα για την διαχείριση κινδύνων που σχετίζονται με τη ασφάλεια πληροφοριών. Σ' αυτό το έγγραφο, υποβοηθούμε τις ΜΜΕ ως προς τον καθορισμό του έργου αυτού, την απόφαση του τρόπου εφαρμογής και διεξαγωγής του και, αν διαθέτουν επαρκείς πόρους, παρέχουμε τις κατευθυντήριες γραμμές για την διενέργεια μιας αυτοαξιολόγησης των πληροφοριακών κινδύνων. Γι' αυτόν τον

σκοπό, προσφέρουμε μια απλή μέθοδο εκτίμησης κινδύνων που οδηγεί σε γρήγορη, σφαιρική αναγνώριση και μετριασμό των πληροφοριακών κινδύνων.

Η μέθοδος αξιολόγησης, που παρουσιάζεται σ' αυτό το έγγραφο, βασίζεται σ' ένα απλουστευμένο μοντέλο που έχει παραχθεί για μικρές επιχειρήσεις, οι οποίες παρουσιάζουν ορισμένα κοινά χαρακτηριστικά. Πρώτον, η οργανωτική διάρθρωσή τους είναι σχετικά επίπεδη και άτομα από διαφορετικά επίπεδα οργάνωσης είναι συνηθισμένα να εργάζονται από κοινού. Δεύτερον, συχνά απαιτούνται άτομα για πολλαπλές εργασίες, εκθέτοντας τα μέλη του προσωπικού σ' ολόκληρο το εύρος των διεργασιών και των διαδικασιών που χρησιμοποιούνται στον οργανισμό.

2. Δομή του εγγράφου

Προκειμένου να καλύψουμε τις ανάγκες διαφόρων τύπων ΜΜΕ έχουμε επιλέξει μια αρθρωτή δομή γι' αυτό το έγγραφο. Ανάλογα με τις ανάγκες μιας συγκεκριμένης ΜΜΕ και τον βαθμό στον οποίο προσπαθεί να αντεπεξέλθει στην εκτίμηση κινδύνων, μπορεί να αποβούν χρήσιμα διαφορετικά μέρη αυτού του εγγράφου. Για τις ΜΜΕ, για τις οποίες απαιτείται μια επισκόπηση της διαχείρισης κινδύνων προκειμένου να καθορίσουν την μελλοντική τους στρατηγική θα είναι χρήσιμο το γενικό μέρος αυτού του εγγράφου (βλ. Κεφάλαιο 3. Καθοδήγηση για τον υπεύθυνο λήψης αποφάσεων και Κεφάλαιο 4. Μια απλουστευμένη προσέγγιση: επισκόπηση).

Στην περίπτωση που μια ΜΜΕ αποφασίσει να εφαρμόσει την διαδικασία διαχείρισης κινδύνων με δική της προαίρεση, τότε χρειάζονται τα μέρη αυτού του εγγράφου που περιλαμβάνουν την λεπτομερή περιγραφή της μεθόδου εκτίμησης κινδύνων και τα παραδείγματα (βλ. Κεφάλαιο 5. Κατευθυντήριες γραμμές αυτοαξιολόγησης με δύο παραδείγματα). Στην περίπτωση της αυτοαξιολόγησης το αναλυτικό υλικό, που βρίσκεται στα παραρτήματα, είναι απαραίτητο προκειμένου να καθοριστούν τα μέτρα που πρέπει να εφαρμοστούν στον οργανισμό (βλέπε Παράρτημα Α. Κάρτες οργανωτικού ελέγχου, Παράρτημα Β. Κάρτες ελέγχου πόρων). Για να καταστεί σαφής ο τρόπος με τον οποίο μπορεί να χρησιμοποιηθεί το έγγραφο αυτό, παρέχουμε ορισμένες περιπτώσεις χρήσης βάσει των ποικίλων πιθανών ρόλων των αναγνωστών:

- **Άτομα με διευθυντικά προσόντα:** μελετήστε το κεφάλαιο 3 για τους υπεύθυνους λήψης αποφάσεων. Επεξηγεί το υπόβαθρο της ασφάλειας των πληροφοριών και την αναγκαιότητα της διαχείρισης κινδύνων. Σκιαγραφεί πιθανές επιλογές για την υλοποίηση της διαδικασίας διαχείρισης κινδύνων και καθορίζει τα κριτήρια με τα οποία λαμβάνονται αποφάσεις. Τα ενδιαφερόμενα διοικητικά στελέχη θα ήθελαν ίσως να κατανοήσουν την δομή της προτεινόμενης διαδικασίας εκτίμησης κινδύνων σ' αυτό το έγγραφο, όπως αυτή παρουσιάζεται στο κεφάλαιο 4.
- **Μη πεπειραμένα μέλη μιας ομάδας εκτίμησης κινδύνων:** τα μέλη μιας ομάδας εκτίμησης κινδύνων θα χρειαστεί να κατανοήσουν την προτεινόμενη απλουστευμένη προσέγγιση εκτίμησης κινδύνων και να διαβάσουν τα επιμέρους στοιχεία της, καθώς και τα εκτιθέμενα παραδείγματα (βλέπε Κεφάλαιο 4. Μια απλουστευμένη προσέγγιση: επισκόπηση).
- **Έμπειρα μέλη μιας ομάδας εκτίμησης κινδύνων:** τα έμπειρα μέλη μιας ομάδας εκτίμησης κινδύνων θα χρειαστεί να διαβάσουν την μέθοδο και να κατανοήσουν τα επιμέρους στοιχεία. Θα είναι, επίσης, σε θέση να αντεπεξέλθουν με το υλικό που εκτίθεται στα παραρτήματα και, συγκεκριμένα, με την επιλογή των μέτρων (στο παρόν έγγραφο αναφέρονται επίσης ως αντίμετρα, έλεγχοι ή έλεγχοι ασφάλειας). Εναλλακτικά, νέα μέτρα μπορούν να εφαρμοστούν για τους υφιστάμενους πόρους ή μπορεί να προστεθούν νέοι πόροι (βλέπε Παράρτημα Α. Κάρτες οργανωτικού ελέγχου, Παράρτημα Β. Κάρτες ελέγχου πόρων και Παράρτημα Γ. Οργανωτικοί έλεγχοι).

3. Καθοδήγηση για τον υπεύθυνο λήψης αποφάσεων

3.1 Τι πρέπει να λάβει υπόψη του ο υπεύθυνος λήψης αποφάσεων

Σήμερα, ένα από τα πολυτιμότερα κεφάλαια μιας επιχείρησης είναι η δημιουργία, η επεξεργασία και η χρήση των πληροφοριών. Η δημοσιοποίηση, η διακύβευση ή η μη διαθεσιμότητα αυτού του πόρου μπορεί να **έχει σοβαρές συνέπειες** για την επιχείρηση, να στοιχειοθετήσει **παράβαση νομοθετικών κανόνων και κανονισμών** και να **επηρεάσει αρνητικά το εμπορικό της σήμα.**

Η επαρκής ασφάλεια των πληροφοριών και των συστημάτων επεξεργασίας πληροφοριών αποτελεί θεμελιώδη ευθύνη της διεύθυνσης της επιχείρησης. Οι ιδιοκτήτες και οι υπεύθυνοι λήψης αποφάσεων πρέπει να συνειδητοποιήσουν την τρέχουσα κατάσταση του προγράμματος ασφάλειας των πληροφοριών τους προκειμένου να προβούν σε σωστές κρίσεις και επενδύσεις περιορίζοντας ανάλογα τους κινδύνους σ' ένα αποδεκτό επίπεδο. Οι κίνδυνοι που συνδέονται με τις πληροφορίες μπορούν να οδηγήσουν σε κρίσιμες καταστάσεις όταν παρεκταθούν σε ζωτικής σημασίας εμπορικά και νομικά ζητήματα της επιχείρησης. Συνεπώς, οι κίνδυνοι που συνδέονται με τις πληροφορίες μπορούν να οδηγήσουν σε γενικότερες και κρισιμότερες κατηγορίες κινδύνων όπως:

- **Ο νομικός κίνδυνος / κίνδυνος συμμόρφωσης,** που είναι ο κίνδυνος ο οποίος προκύπτει από παραβιάσεις της νομοθεσίας ή τη μη συμμόρφωση με λογιστικούς κανόνες, κανονισμούς, εναρμονισμένες πρακτικές ή ηθικά πρότυπα. Νομικοί κίνδυνοι ή κίνδυνοι συμμόρφωσης μπορούν να δημιουργήσουν αρνητική δημόσια εικόνα για μία επιχείρηση, να οδηγήσουν στην επιβολή ποινικών και αστικών χρηματικών προστίμων, την καταβολή αποζημίωσης και την ακύρωση συμβολαίων. Η υποκλοπή πληροφοριών που αφορούν πελάτες, όπως πληροφορίες πιστωτικών καρτών, πληροφορίες οικονομικής φύσεως, πληροφορίες για θέματα υγείας ή άλλα προσωπικά δεδομένα μπορούν, επίσης, να εγείρουν πιθανούς κινδύνους από απαιτήσεις τρίτων. **Αναγνωρίζοντας την ασφάλεια των πληροφοριών ως ένα πολύπλευρο ζήτημα που προκαλεί ιδιαίτερη ανησυχία και προκειμένου να προστατευθούν τα πολιτικά δικαιώματα και να διασφαλιστεί η εταιρική ευθύνη, οι κυβερνήσεις της ΕΕ και η Ευρωπαϊκή Ένωση έχουν θεσπίσει νόμους και κανονισμούς, οι οποίοι απαιτούν την συμμόρφωση των φορέων ανεξάρτητα από το μέγεθός τους ή τον κλάδο οικονομικής δραστηριότητας στον οποίο ανήκουν. Αυτοί οι κανονισμοί υποχρεώνουν τις εταιρείες να εφαρμόζουν εσωτερικούς ελέγχους ώστε να προστατευθούν έναντι των κινδύνων που συνδέονται με τις πληροφορίες. Στοχεύουν, επίσης, στην βελτίωση των πρακτικών και των διαδικασιών διαχείρισης κινδύνων.**
- **Οι κίνδυνοι οικονομικής σταθερότητας**. Η έλλειψη κατάλληλης παραγωγικής υποδομής, υποδομής διαχείρισης ή προσωπικού για την υλοποίηση της επιχειρηματικής στρατηγικής του φορέα μπορεί να οδηγήσει σε αδυναμία επίτευξης των διακηρυγμένων σκοπών και οικονομικών στόχων που έχουν τεθεί σ' ένα καλά διαχειριζόμενο και ελεγχόμενο περιβάλλον. Η **λανθασμένη διαχείριση της ασφάλειας των πληροφοριών μπορεί να επεκταθεί σε κινδύνους που σχετίζονται με την οικονομική σταθερότητα της επιχείρησης. Τέτοιοι κίνδυνοι, με την σειρά τους, μπορούν να οδηγήσουν σε απάτες, ξέπλυμα βρώμικου χρήματος, οικονομική αστάθεια κτλ**.
- **Ο κίνδυνος παραγωγικότητας,** που είναι ο κίνδυνος ζημιών εκμετάλλευσης και **χαμηλής ποιότητας παροχής υπηρεσιών προς τον πελάτη,** σαν συνέπεια της μη απαρέγκλιτης τήρησης βασικών διαδικασιών και ελέγχων επεξεργασίας. Ο κίνδυνος αυτός, συνήθως, αφορά όλες τις συνεργατικές δραστηριότητες παραγωγής, οι οποίες, κατά κάποιο τρόπο, συνεισφέρουν στην συνολική παράδοση ενός προϊόντος ή την συνολική παροχή μιας υπηρεσίας. Ο κίνδυνος παραγωγικότητας δεν περιορίζεται στην χρήση της τεχνολογίας - μπορεί εξίσου να είναι το αποτέλεσμα οργανωτικών δραστηριοτήτων. Ο κίνδυνος που

προκύπτει από ανεπαρκή ή ελλιπώς ελεγχόμενα συστήματα και εφαρμογές λογισμικού, τα οποία χρησιμοποιούνται για να υποστηρίξουν το γραφείο εξυπηρέτησης, τις διαδικασίες διαχείρισης κινδύνων, το τμήμα λογιστηρίου ή άλλες μονάδες, υπάγεται σ' αυτήν την οικογένεια κινδύνων. Η ανεπαρκής διαχείριση της ασφάλειας των πληροφοριών μπορεί να οδηγήσει σε υψηλούς κινδύνους για την παραγωγικότητα συμπεριλαμβανομένων των υψηλών λειτουργικών εξόδων, των φαινομένων δυσλειτουργίας, των αποφάσεων κακής διαχείρισης (τιμή, ρευστότητα και ανοίγματα σε πιστωτικό κίνδυνο) και σε απουσία **της ιδιωτικότητας, καθώς και στην διακοπή της παροχής υπηρεσιών προς τους πελάτες.**

- **Φήμη και Εμπιστοσύνη Πελατών.** Ενδεχομένως, ο πιο δύσκολος και, ωστόσο, ένας από τους πιο σημαντικούς κινδύνους που πρέπει να γίνει κατανοητός είναι ο κίνδυνος πρόκλησης βλάβης στην φήμη της επιχείρησης, ένας άυλος αλλά σημαντικός πόρος. Θα δώσουν οι πελάτες τους αριθμούς της πιστωτικών καρτών τους σε μια εταιρεία απ' τη στιγμή που θα διαβάσουν στον τύπο ότι κάποιος παρείσφρησε στην βάση δεδομένων της εταιρείας; Θα παραμείνουν οι υψηλά ιστάμενοι υπάλληλοι σε μια τόσο ζημιωμένη εταιρεία; Και, ποια θα είναι η αντίδραση των μετόχων της εταιρείας; Ποια είναι η αναμενόμενη απώλεια των μελλοντικών εσόδων της επιχείρησης; Ποια είναι η αναμενόμενη απώλεια της χρηματιστηριακής κεφαλαιοποίησης;

Πολλοί ιδιοκτήτες ΜΜΕ νομίζουν πως δεν βρίσκονται σε κίνδυνο λόγω του μεγέθους της επιχείρησής τους και των πληροφοριακών τους πόρων. Οι περισσότεροι θεωρούν ότι οι μεγάλες επιχειρήσεις, οι οποίες διαθέτουν περισσότερους πόρους, είναι οι μόνες που κινδυνεύουν. Όμως αυτό δεν είναι αληθές. Πρώτον, η ευαισθησία των πληροφοριών απευθύνεται στην ποιότητα και όχι στην ποσότητα των πληροφοριών. Δεύτερον, οι ΜΜΕ δεν διαθέτουν τους πόρους ή το προσωπικό για να αντιμετωπίσουν το ζήτημα της ασφάλειας με εξίσου εντατικές μεθόδους όπως αυτές που χρησιμοποιούνται στις μεγάλες επιχειρήσεις και, επομένως, είναι περισσότερο εκτεθειμένες. Πράγματι, η νέα τεχνολογία επιτρέπει στις μικρές επιχειρήσεις να χρησιμοποιούν πολλά από τα ίδια πληροφοριακά συστήματα που διαθέτουν οι μεγάλες επιχειρήσεις. Όμως, με τον τρόπο αυτό, οι μικρές επιχειρήσεις εκτίθενται οικειοθελώς σε πολλές απειλές που σχετίζονταν παραδοσιακά με τις μεγάλες επιχειρήσεις. **Στην πραγματικότητα, 56% των μικρών επιχειρήσεων αντιμετώπισαν τουλάχιστον ένα συμβάν ασφάλειας κατά τον τελευταίο χρόνο.** Δυστυχώς, ένα σημαντικό μέρος των επιχειρήσεων, οι οποίες αντιμετωπίζουν μείζονα βλάβη των υπολογιστικών τους συστημάτων, ποτέ δεν καταφέρνουν να επανακάμψουν και, έτσι, η επιχείρηση καταρρέει από μόνη της. Επομένως, προκειμένου να συνεχίσουν την επιτυχημένη πορεία τους, επιβάλλεται οι ιδιοκτήτες των ΜΜΕ και οι υπεύθυνοι λήψης αποφάσεων να αναγνωρίσουν αυτούς τους σκοπέλους και να λάβουν μέτρα ώστε να αντιμετωπίσουν τα ζητήματα της ασφάλειας των πληροφοριών.

Τα μέτρα (έλεγχοι) περιορισμού των κινδύνων της ασφάλειας των πληροφοριών πρέπει να είναι ανάλογα με τους κινδύνους που αντιμετωπίζουν οι εν λόγω πληροφορίες. Ωστόσο, η διαδικασία καθορισμού σχετικά με το ποιοι έλεγχοι ασφάλειας είναι ενδεδειγμένοι και αποτελεσματικοί από οικονομική άποψη, αρκετά συχνά είναι ένα πολυσύνθετο και, ορισμένες φορές, υποκειμενικό ζήτημα. **Μια απ' τις πρωταρχικές λειτουργίες για να τεθεί αυτή η διαδικασία σε μια πιο αντικειμενική βάση είναι η διαρκής εκτίμηση των κινδύνων που συνδέονται με την ασφάλεια.**

3.2 Τι απαιτείται να γνωρίζει ο υπεύθυνος λήψης αποφάσεων

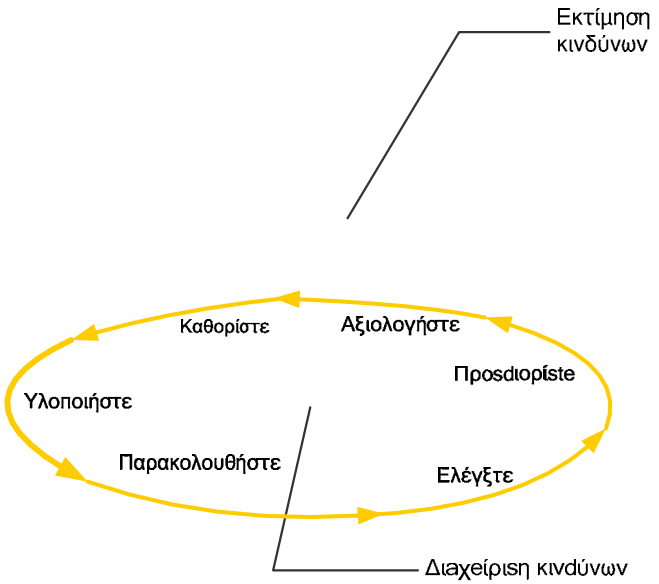
Η ασφάλεια των πληροφοριών έχει να κάνει με την αναγνώριση, τον μετριασμό και την διαχείριση κινδύνων που σχετίζονται με τις πληροφορίες. Η εκτίμηση κινδύνων είναι το πρώτο αναγκαίο μέτρο για την κατανόηση των κινδύνων, διεξάγοντας μια συνολική **αναγνώριση** και **αξιολόγηση** κινδύνων αναφορικά με τους κινδύνους ασφάλειας των πληροφοριών μιας επιχείρησης. Το αποτέλεσμα αυτής της δραστηριότητας είναι ουσιώδες για την διαχείριση της επιχείρησης καθώς οι ενεχόμενοι κίνδυνοι μπορούν να επηρεάσουν σε σημαντικό βαθμό την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών. **Μπορεί, επίσης, να είναι ζωτικής σημασίας για την διατήρηση του ανταγωνιστικού προβαδίσματος, της οικονομικής σταθερότητας, της νομικής συμμόρφωσης και της δυνατής εμπορικής εικόνας της επιχείρησης.**

Συνεπώς, η εκτίμηση κινδύνων μπορεί να βοηθήσει τους υπεύθυνους λήψης αποφάσεων να:

- **Αποτιμήσουν τις οργανωτικές πρακτικές και την τεχνολογική βάση που έχει εγκατασταθεί.**
- **Ενισχύσουν την προστασία των πληροφοριών βάσει των δυνητικών επιπτώσεων στον οργανισμό.**
- **Επικεντρώσουν τις ενέργειες για την ασφάλεια σε σημαντικά ζητήματα. Μπορούν να εγκαταλειφθούν μέτρα που σχετίζονται με αποδεκτούς κινδύνους.**
- **Διασφαλίσουν ότι τα εφαρμοζόμενα μέτρα και οι υλοποιούμενες δαπάνες είναι πλήρως ανάλογα με τους κινδύνους στους οποίους εκτίθεται ο οργανισμός. Κατ' αυτόν τον τρόπο, μπορεί να διατηρηθεί ισορροπία μεταξύ των εξόδων αντιμετώπισης ενός κινδύνου και των οφελών που προέρχονται από την αποφυγή της αρνητικής επίπτωσης.**

Κατά την διάρκεια μιας εκτίμησης κινδύνων, μία επιχείρηση πραγματοποιεί ενέργειες για να: (α) αναγνωρίσει τους κινδύνους ασφάλειας πληροφοριών, (β) αξιολογήσει τους κινδύνους ώστε να καθορίσει προτεραιότητες και (γ) ορίσει τον τρόπο με τον οποίο θα μετριάσει τους κινδύνους (βλ. επίσης Σχήμα 1).

Ωστόσο, η εκτίμηση κινδύνων για την ασφάλεια των πληροφοριών είναι μόνο το πρώτο βήμα για την διαχείριση κινδύνων ασφάλειας των πληροφοριών, η οποία αποτελεί τη συνεχή διαδικασία αναγνώρισης κινδύνων και εφαρμογής σχεδίων για την αντιμετώπισή τους. Το σχήμα 1 απεικονίζει μια διαδικασία διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών και το «μερίδιο» της διαχείρισης κινδύνων που συνιστά η εκτίμηση κινδύνων.



Σχήμα 1: Δραστηριότητες εκτίμησης κινδύνων σε σχέση με την διαχείριση κινδύνων για την ασφάλεια των πληροφοριών.

Σαφώς, η ίδια η **εκτίμηση κινδύνων** παρέχει μια κατεύθυνση για τις δραστηριότητες που αφορούν στην ασφάλεια των πληροφοριών ενός οργανισμού ενώ **δεν οδηγεί απαραίτητα σε σημαντικές βελτιώσεις εκτός κι αν έχει λάβει χώρα η εφαρμογή μέτρων.** Όπως συμβαίνει με κάθε άλλο τομέα διαχείρισης, η υλοποίηση μόνο ενός μέρους του κύκλου ζωής της διαχείρισης δεν φέρνει τα επιθυμητά αποτελέσματα. Καμία αξιολόγηση, ανεξάρτητα από το πόσο εμπεριστατωμένη ή εξειδικευμένη είναι, δε βελτιώνει την θεώρηση της ασφάλειας εκτός αν η επιχείρηση διεκπεραιώνει την εφαρμογή της. Πέρα από την εκτίμηση κινδύνων, η αποτελεσματική διαχείριση κινδύνων περιλαμβάνει τις **ακόλουθες ενέργειες**:

- **Προγραμματίστε** τον τρόπο με τον οποίο θα εφαρμοστεί η στρατηγική για την προστασία των πληροφοριών και τα σχέδια για τον μετριασμό των κινδύνων από την αξιολόγηση μέσα από την ανάπτυξη αναλυτικών σχεδίων δράσης. Η δραστηριότητα αυτή μπορεί να περιλαμβάνει μια λεπτομερή ανάλυση κόστους–οφέλους ποικίλων στρατηγικών και δράσεων.
- **Εφαρμόστε** τα επιλεγμένα αναλυτικά σχέδια δράσης.
- **Παρακολουθήστε** την πρόοδο και την αποτελεσματικότητα των σχεδίων. Η δραστηριότητα αυτή περιλαμβάνει την παρακολούθηση οποιωνδήποτε μεταβολών των επιπέδων κινδύνων.
- **Ελέγξτε** τις αποκλίσεις στην εκτέλεση των σχεδίων με την λήψη των κατάλληλων διορθωτικών μέτρων.

3.3 Με ποιον τρόπο θα ενεργήσετε όσον αφορά την ασφάλεια των πληροφοριών

Μέρος της ευθύνης των διευθυντών των μικρομεσαίων επιχειρήσεων είναι να προνοούν για την ασφάλεια του επιχειρηματικού τους περιβάλλοντος. Σύμφωνα με τις περισσότερες ισχύουσες νομικές απαιτήσεις, η ευθύνη για συμβάντα παραβίασης της ασφάλειας βαρύνει αυτούς. Όπως ακριβώς είναι υποχρεωμένοι να παρέχουν ένα ασφαλές και σταθερό φυσικό περιβάλλον, οφείλουν, παράλληλα, να διασφαλίζουν ότι οι πληροφορίες της επιχείρησής τους προστατεύονται. Δεδομένου του γεγονότος, ωστόσο, ότι οι υπολογιστές δεν είναι συσκευές «μιας επισκευής», η προστασία των πληροφοριών αποτελεί σταθερό μέλημα.

Οι υπεύθυνοι λήψης αποφάσεων μπορούν να θέσουν σε εφαρμογή την διαδικασία εκτίμησης κινδύνων για το περιβάλλον τους και να ενεργοποιήσουν την λήψη κατάλληλων μέτρων προκειμένου να αντιμετωπίσουν μη αποδεκτούς κινδύνους. Αυτό αποτελεί προϋπόθεση για την διαχείριση της ασφάλειας των πληροφοριών. Για την διεξαγωγή αυτής της διαδικασίας, μπορούν να εφαρμοστούν ποικίλες προσεγγίσεις σχετικά με την στελέχωση μιας τέτοιας προσπάθειας (επίσης γνωστή ως απόφαση κάποιου να «δημιουργήσει ή να αγοράσει»). Διαφοροποιούμε τρεις προσεγγίσεις:

- **Εσωτερική ανάθεση της εκτίμησης κινδύνων**: η εκτίμηση κινδύνων και ο προσδιορισμός των αναγκαίων μέτρων επιτελούνται από το εσωτερικό προσωπικό της επιχείρησης. Η εκτίμηση βασίζεται στην προσέγγιση εκτίμησης κινδύνων που έχει επιλέξει ο οργανισμός (π.χ. μία ορθή πρακτική, ένα γνωστό πρότυπο κτλ.). Η διαδικασία αυτή θα βοηθήσει την επιχείρηση να αποκτήσει άρτια γνώση της προσέγγισης εκτίμησης για επαναλαμβανόμενες περιπτώσεις εφαρμογής της συγκεκριμένης διαδικασίας.
- **Εξολοκλήρου εξωτερική ανάθεση της εκτίμησης κινδύνων**: σύμφωνα με αυτήν την προσέγγιση, η συνολική εκτίμηση κινδύνων διενεργείται από έναν εξωτερικό ανάδοχο. Η εκτίμηση βασίζεται στην προσέγγιση εκτίμησης κινδύνων που επιλέγει αυτός. Ο ανάδοχος μπορεί επίσης να αναλάβει την διενέργεια επαναλαμβανόμενων μελλοντικών εκτιμήσεων. Δεν προβλέπεται μεταφορά τεχνογνωσίας στο εσωτερικό προσωπικό της επιχείρησης για ολόκληρο τον κύκλο ζωής της εκτίμησης κινδύνων/διαχείρισης κινδύνων της ΜΜΕ.
- **Εν μέρει εξωτερική ανάθεση της εκτίμησης κινδύνων**: σύμφωνα με την προσέγγιση αυτή θεωρείται ότι η αρχική εκτίμηση κινδύνων διενεργείται από μια εξωτερική εταιρεία. Η εκτίμηση βασίζεται σε μια προσέγγιση εκτίμησης κινδύνων που είναι γνωστή στην ΜΜΕ. Κατά συνέπεια, περαιτέρω εκτιμήσεις κινδύνων μπορούν να διενεργηθούν από το προσωπικό της επιχείρησης. Η αρχική εκτίμηση, η οποία διενεργείται από εξωποριστή, χρησιμεύει ως μεταφορά τεχνογνωσίας στο προσωπικό της ΜΜΕ.

Το παρόν έγγραφο παρέχει στις ΜΜΕ όλο το σχετικό υλικό που απαιτείται για τη λήψη αποφάσεων του τύπου να "δημιουργήσει ή να αγοράσει" μια επιχείρηση. Επιπρόσθετα, παρέχουμε όλες τις απαραίτητες πληροφορίες ώστε να βοηθήσουμε τις ΜΜΕ να διενεργήσουν μια αυτοαξιολόγηση. Η προτεινόμενη προσέγγιση εκτίμησης κινδύνων μπορεί να χρησιμοποιηθεί σε αποφάσεις εσωτερικής ανάθεσης και εν μέρει εξωτερικής ανάθεσης ως κατευθυντήρια γραμμή για τις αρχικές και τις μελλοντικές εκτιμήσεις κινδύνων (βλ. Κεφάλαια 4. Μια απλουστευμένη προσέγγιση: επισκόπηση και 5. Κατευθυντήριες γραμμές αυτοαξιολόγησης με δύο παραδείγματα).

Κάθε προσέγγιση εκτίμησης κινδύνων, όταν συγκρίνεται με όλες τις άλλες προσεγγίσεις, συνδέεται με πλεονεκτήματα και μειονεκτήματα. Ο Πίνακας 1 δίνει μια πρώτη εντύπωση των πραγματικών περιστατικών που διέπουν την απόφαση του τύπου «να δημιουργήσει ή να αγοράσει» μία ΜΜΕ σε σχέση με το έργο της εκτίμησης κινδύνων. Οι ακόλουθες παράγραφοι περιέχουν μια λεπτομερή ανάλυση όσον αφορά στις παραμέτρους και τους παράγοντες που πρέπει να ληφθούν υπόψη όταν επιλέγουμε μια προσέγγιση εκτίμησης κινδύνων για μία ΜΜΕ.

Επιλογές μεθόδου υλοποίησης εκτίμησης κινδύνων	**Παράμετροι και παράγοντες μεθόδου υλοποίησης**				
	Απαιτούμενη εσωτερική εμπειρογνωμοσύνη	**Εξάρτηση από τρίτους**	**Απαιτούμενοι εσωτερικοί πόροι**	**Αντικειμενικότητα εκτίμησης**	**Έργο τρίτων[1]**
Εσωτερική	**Ναι**	**Μικρή**	**1-5 Άτομα**	**Χαμηλού**	**-**

ανάθεση				**επιπέδου**	
Εξολοκλήρου εξωτερική ανάθεση	**Όχι**	**Μεγάλη**	**1 Άτομο (για την διαχείριση σχεδίου)**	**Υψηλού επιπέδου**	**10-40 Ημέρες**
Εν μέρει εξωτερική ανάθεση	**Ναι**	**Μικρή**	**1-2 Άτομα**	**Μεσαίου επιπέδου**	**5-10 Ημέρες**

Πίνακας 1: Επιλογές μεθόδου υλοποίησης εκτίμησης κινδύνων

Στις ακόλουθες ενότητες, περιγράφουμε κάθε πιθανή επιλογή για την διενέργεια εκτίμησης κινδύνων/διαχείρισης κινδύνων. Ένα ερωτηματολόγιο θα βοηθήσει τους υπεύθυνους λήψης αποφάσεων να προσδιορίσουν εάν αυτή η επιλογή είναι η ενδεδειγμένη για έναν συγκεκριμένο τύπο ΜΜΕ.

3.3.1 Εσωτερική ανάθεση

Η εσωτερική ανάθεση μπορεί να προσφέρει πολλά **πλεονεκτήματα στον φορέα όπως την ανάπτυξη εσωτερικής τεχνογνωσίας και ικανοτήτων για την εκτίμηση και την διαχείριση κινδύνων. Σε αυτό το πλαίσιο, ανάλογα με τις τιμές παροχής συμβουλευτικών υπηρεσιών, που ισχύουν στην αγορά του τομέα της ασφάλειας, αυτή η προσέγγιση μπορεί να οδηγήσει σε μείωση των δαπανών.** Η επιλογή αυτή είναι ιδιαίτερα ελκυστική για οργανισμούς με απλή δομή, επιτυχημένο ιστορικό στην εσωτερική υλοποίηση παρόμοιων δραστηριοτήτων (δηλ. ISO9001), επαρκείς ικανότητες και δεξιότητες.

Το ακόλουθο σύνολο ερωτήσεων μπορεί να χρησιμοποιηθεί για να βοηθήσει να προσδιοριστεί εάν η εκτίμηση κινδύνων ως εσωτερική ανάθεση αποτελεί την σωστή απόφαση για έναν φορέα:

Ερωτήσεις για την λήψη απόφασης	**Απάντηση**	
	☺ **Ναι**	☹ **Όχι**
Είναι ο οργανισμός σας μικρός; Έχει επίπεδη ή απλή ιεραρχική δομή;		
Διαθέτετε **εσωτερική τεχνογνωσία σε συστήματα και δίκτυα ΤΠ;**		
Διαθέτει ο οργανισμός σας εξειδικευμένο και διαθέσιμο ανθρώπινο δυναμικό;		
Οι επιχειρηματικές σας δραστηριότητες εξαρτώνται σε μικρό βαθμό από συστήματα ΤΠ, περιλαμβάνονται σε αυτές η αποθήκευση ή η επεξεργασία ευαίσθητων δεδομένων πελατών, έχει, δε, ασχοληθεί ο οργανισμός σας με παρόμοιες δραστηριότητες, δηλαδή με διαδικασίες βελτίωσης ποιότητας;		
Μπορείτε να βρείτε μια ομάδα τριών έως πέντε ατόμων, τα οποία έχουν ευρεία και βαθιά κατανόηση του οργανισμού σας και διαθέτουν, επίσης, τα περισσότερα από τα ακόλουθα προσόντα; ▫ Ικανότητα επίλυσης προβλημάτων ▫ Ικανότητα αναλυτικής σκέψης ▫ Ικανότητα για συλλογική εργασία ▫ Ηγετικές ικανότητες ▫ **Ικανότητα κατανόησης των επιχειρηματικών**		

διεργασιών της εταιρίας και της υποκείμενης υποδομής του οργανισμού ▫ Δυνατότητα δαπάνης λίγων ημερών απασχόλησης σ' αυτή την μέθοδο		
Διαθέτετε μια σχετικά απλή υποδομή τεχνολογίας των πληροφοριών η οποία είναι καλά κατανοητή από τουλάχιστον ένα άτομο στον οργανισμό σας;		

Σε όσο περισσότερες ερωτήσεις δοθεί η απάντηση «ναι» τόσο μεγαλύτερη είναι η πιθανότητα να είναι η αυτοαξιολόγηση η κατάλληλη επιλογή για μία ΜΜΕ.

Χρησιμοποιώντας την προτεινόμενη προσέγγιση εκτίμησης κινδύνων και ορθές πρακτικές (βλ. κεφάλαια 4. Μια απλουστευμένη προσέγγιση: επισκόπηση και 5. Κατευθυντήριες γραμμές αυτοαξιολόγησης με δύο παραδείγματα) οι υπεύθυνοι λήψης αποφάσεων θα μπορέσουν να θέσουν σε εφαρμογή μεθόδους εκτίμησης κινδύνων αποτελεσματικής προσέγγισης με σκοπό την αναγνώριση και την διαχείριση κινδύνων ασφάλειας των πληροφοριών τους, καθιστώντας εφικτή την συνεχή βελτίωση της θεώρησης της ασφάλειάς τους.

3.3.2 Εξολοκλήρου εξωτερική ανάθεση

Μέσω της εξολοκλήρου εξωτερικής ανάθεσης, μία ΜΜΕ μεταβιβάζει εξολοκλήρου την εκτίμηση και διαχείριση κινδύνων σ' έναν εξωτερικό ανάδοχο. Η εν λόγω ανάθεση μπορεί να περιλαμβάνει αρχικές καθώς και επαναλαμβανόμενες εκτιμήσεις και δραστηριότητες διαχείρισης που καλύπτουν τον συνολικό κύκλο ζωής της διαχείρισης κινδύνων (π.χ. εφαρμογή και διατήρηση μέτρων). Ο ανάδοχος εφαρμόζει την δική του προσέγγιση εκτίμησης κινδύνων/διαχείρισης κινδύνων. Με τον τρόπο αυτό, ο ανάδοχος δεν μεταφέρει τεχνογνωσία στον πελάτη. Σ' αυτό το σημείο πρέπει να σημειωθεί ότι η εξωτερική ανάθεση δραστηριοτήτων εκτίμησης και διαχείρισης δεν απαλλάσσει την διεύθυνση της ΜΜΕ από την ευθύνη της για την ασφάλεια (των πληροφοριών).

Ανάλογα με την δομή, την στρατηγική, τους διαθέσιμους πόρους και την κατάσταση της αγοράς, η εξωτερική ανάθεση **μπορεί να προσφέρει συγκεκριμένα πλεονεκτήματα.** Η απόφαση για την εξωτερική ανάθεση της εκτίμησης κινδύνων των πληροφοριών επιτρέπει στην ΜΜΕ να επικεντρωθεί σε βασικές επιχειρηματικές στρατηγικές ενόσω οι περιφερειακές δραστηριότητες ασκούνται από ένα εξωτερικό εμπειρογνώμονα με εξειδίκευση σε θέματα ασφάλειας των πληροφοριών.

Οι ακόλουθες ερωτήσεις μπορεί να χρησιμοποιηθούν για να βοηθήσουν να καθοριστεί αν η εξολοκλήρου εξωτερική ανάθεση της εκτίμησης κινδύνων αποτελεί την σωστή απόφαση για έναν οργανισμό:

Ερωτήσεις για την λήψη απόφασης	**Απάντηση**	
	☺ **ΝΑΙ**	☹ **Όχι**
Θεωρείτε ότι είναι απαραίτητο να **διατηρείται αυξημένη η προσοχή σας** σε κύριες ικανότητες και στρατηγικές επιχειρηματικές διεργασίες;		
Σας **φαίνεται δύσκολο να διαθέσετε από δύο έως πέντε άτομα,** τα οποία έχουν ευρεία και βαθιά κατανόηση του οργανισμού σας και διαθέτουν, επίσης, τα περισσότερα από τα ακόλουθα προσόντα; o **Ικανότητα κατανόησης των επιχειρηματικών διεργασιών και της υποκείμενης υποδομής του οργανισμού**		

o Ικανότητα επίλυσης προβλημάτων o Ικανότητα αναλυτικής σκέψης o Ικανότητα για συλλογική εργασία o Ηγετικές ικανότητες o Δυνατότητα δαπάνης λίγων ημερών απασχόλησης σ' αυτή την μέθοδο		
Έχετε **εξαιρετικά πολύπλοκη και σχετικά μεγάλη υποδομή ΤΠ;**		
Στις επιχειρηματικές δραστηριότητες και τις υπηρεσίες που παρέχετε περιλαμβάνονται και **οικονομικές συναλλαγές**;		
Εκμεταλλεύεστε επιχείρηση η οποία υπόκειται σε μεγάλο βαθμό σε αυστηρούς νομικούς και κανονιστικούς περιορισμούς και/ή εντολές της ΕΕ ή της χώρας δραστηριοποίησής σας;		
Διαθέτετε μια σχετικά απλή υποδομή τεχνολογίας των πληροφοριών που είναι καλά κατανοητή από τουλάχιστον ένα άτομο στον οργανισμό σας;		

Και σε αυτή τη περίπτωση, όσο περισσότερες απαντήσεις «ναι» ανακύψουν για έναν οργανισμό τόσο περισσότερο η εξωτερική ανάθεση εξυπηρετεί τις ανάγκες του.

Για την εξωτερική ανάθεση δραστηριοτήτων εκτίμησης κινδύνων σ' έναν τρίτο απαιτείται **μια διαδικασία επιλογής παρόχου, η οποία περιλαμβάνει αφενός την επιμελή και συνολική αξιολόγησή του και αφετέρου την αξιολόγηση των ικανοτήτων του στην ασφάλεια των πληροφοριών (βλέπε επίσης** Παράρτημα Ε. Απλές συμβουλές, Τρίτοι, Πάροχοι υπηρεσιών).

Εφόσον γίνει η επιλογή αυτή, μια συμφωνία επιπέδου υπηρεσίας πρέπει να αποτελεί την πρωταρχική βάση συνεργασίας. Σε αυτήν την συμφωνία πρέπει να οριοθετούνται βασικά στοιχεία όπως η επαγγελματική πιστοποίηση των μηχανικών ασφάλειας του παρόχου, η εμπιστευτικότητα και η μη δημοσιοποίηση, το χρονοδιάγραμμα, η κατανομή πόρων, το κόστος και η μεθοδολογία που θα εφαρμοστεί.

Όταν επίκειται η σύναψη μιας Συμφωνίας Επιπέδου Υπηρεσίας (ΣΕΥ), πρέπει να ληφθούν υπόψη οι ακόλουθες ερωτήσεις (δηλαδή σαν ένα είδος καταλόγου ελέγχου για το περιεχόμενο μιας ΣΕΥ):

- **Καλύπτονται θέματα αστικής ευθύνης;** Τι θα συμβεί, για παράδειγμα, αν κατά την διάρκεια της εκτίμησης, διακοπούν ή διαταραχθούν σημαντικές επιχειρηματικές δραστηριότητες εξαιτίας της ανικανότητας του παρόχου να διενεργήσει μια εκτίμηση της υποκείμενης υποδομής ΤΠ και δικτύων;
- **Προσδιορίζονται με σαφήνεια οι ευθύνες** από την ΣΕΥ; Ποιος θα είναι υπεύθυνος και για ποια ενέργεια/πράξη; Ποια θα είναι η συμμετοχή του οργανισμού όσον αφορά τους πόρους;
- **Τεκμηριώνεται με σαφήνεια το πεδίο εφαρμογής της εργασίας;** Τι θα περιλαμβάνει ο πάροχος στο πεδίο εφαρμογής της εργασίας; Συνιστάται θερμά το πεδίο εφαρμογής της εργασίας να περιλαμβάνει ολόκληρο το φάσμα των επιχειρηματικών δραστηριοτήτων και την υποκείμενη υποδομή. Σε οποιαδήποτε άλλη περίπτωση είναι πιθανόν το συγκεκριμένο αποτέλεσμα να είναι ανεπαρκές ή ακόμα και παραπλανητικό.
- **Με ποιόν τρόπο πρόκειται να ικανοποιηθούν οι νομικές απαιτήσεις,** π.χ. νομοθεσία για την προστασία των δεδομένων;
- Ποιοι διακανονισμοί θα εφαρμοστούν ώστε να επιτρέψουν σε όλα τα εμπλεκόμενα στην εξωτερική ανάθεση μέρη, συμπεριλαμβανομένων και των υπεργολάβων, να έχουν επίγνωση των δικών τους ευθυνών ασφάλειας;
- Με ποιόν τρόπο πρόκειται **να διατηρηθούν και να ελεγχθούν η ακεραιότητα και η εμπιστευτικότητα των πόρων του φορέα;**

- **Ποιοι φυσικοί και λογικοί έλεγχοι θα χρησιμοποιηθούν ώστε να περιορίσουν και να θέσουν όρια στην πρόσβαση των εξουσιοδοτημένων χρηστών σ' ευαίσθητα επαγγελματικά δεδομένα του οργανισμού;**
- **Με ποιόν τρόπο πρόκειται να διατηρηθεί η διαθεσιμότητα των υπηρεσιών στο ενδεχόμενο μιας καταστροφής;**
- **Περιλαμβάνεται στους γενικούς και ειδικούς όρους το δικαίωμα ελέγχου των μέτρων ασφάλειας και προστασίας των πληροφοριών του προμηθευτή;**
- Δηλώνονται ρητά **οι ελάχιστοι πόροι, η ικανότητα και η επαγγελματική πιστοποίηση** του προμηθευτή;
- Καθορίζονται με σαφήνεια το περιεχόμενο, η συχνότητα και η δομή των υποβαλλόμενων εκθέσεων;

Σαφώς, οι οργανισμοί μπορούν να προβούν στην ανάθεση εντολής προς τους παρόχους να διενεργήσουν την εκτίμηση βάσει της μεθοδολογίας προσέγγισης διαχείρισης κινδύνων που προτείνεται στο παρόν (βλέπε Κεφάλαιο 5. Κατευθυντήριες γραμμές αυτοαξιολόγησης με δύο παραδείγματα). Υπό τον όρο ότι η ΜΜΕ κατανοεί το περιεχόμενο της προτεινόμενης προσέγγισης, αυτό θα της επιτρέψει να ελέξει καλύτερα τις δραστηριότητες του ανάδοχου.

3.3.3 Εν μέρει Εξωτερική Ανάθεση

Μια λύση μικτών πόρων **μπορεί να συνδυάσει τα οφέλη της εσωτερικής αλλά και της εξωτερικής ανάθεσης**. Σε μια λύση μικτών πόρων, ο οργανισμός συμμετέχει ενεργά σε μια διαδικασία αυτοαξιολόγησης χρησιμοποιώντας έναν τρίτο ως διαμεσολαβητή. Στο πλαίσιο αυτό, η εκτίμηση βασίζεται σ' ένα υπόδειγμα εκτίμησης κινδύνων που κατανοεί ο πελάτης, π.χ. την προσέγγιση εκτίμησης κινδύνων που παρουσιάζεται στο παρόν (βλ. κεφάλαιο 4. Μία απλουστευμένη προσέγγιση: επισκόπηση). Αυτή είναι μια αναγκαία **προϋπόθεση προκειμένου να επιτευχθεί η μεταφορά τεχνογνωσίας** μεταξύ αναδόχου και πελάτη.

Σ' αυτή την εκδοχή, η ΜΜΕ αναπτύσσει την ενδοεπιχειρησιακή της ικανότητα ώστε να εκτελεί ορισμένα σημαντικά καθήκοντα σχετικά με θέματα ασφάλειας όταν και όπου αυτό απαιτείται. Μπορούν να προκύψουν καθαρά οφέλη από το γεγονός ότι ο οργανισμός μπορεί να ρυθμίσει και να διαχειριστεί τα μελλοντικά έξοδα του αναδόχου, καθώς και να συνεισφέρει σημαντικά στην εμπειρογνωμοσύνη που παρέχεται από εξειδικευμένον τρίτον.

Το ακόλουθο σύνολο ερωτήσεων μπορεί να χρησιμοποιηθεί για να βοηθήσει να καθοριστεί εάν μία εκτίμηση κινδύνων πρέπει να ανατεθεί εν μέρει σε κάποιον ανάδοχο:

Ερωτήσεις για την λήψη απόφασης	**Απάντηση**	
	☺ **ΝΑΙ**	☹ **Όχι**
Θεωρείτε ότι είναι απαραίτητο να διατηρείται αυξημένη η προσοχή σας σε κύριες ικανότητες και στρατηγικές επιχειρηματικές διεργασίες, αλλά και να βελτιώνετε, επίσης, την ευαισθητοποίηση σε θέματα ασφάλειας εσωτερικών πληροφοριών, όπως και τις δεξιότητες σε θέματα ασφάλειας των πληροφοριών;		
Είναι πιθανό να καταστήσετε διαθέσιμα από ένα έως δύο άτομα στον οργανισμό σας, τα οποία έχουν ευρεία και βαθιά κατανόηση του οργανισμού σας και, επίσης, διαθέτουν τα περισσότερα από τα ακόλουθα προσόντα; ▫ **Ικανότητα κατανόησης των επιχειρηματικών διεργασιών και της υποκείμενης υποδομής του οργανισμού** ▫ Ικανότητα επίλυσης προβλημάτων		

▫ Ικανότητα αναλυτικής σκέψης ▫ Ικανότητα εργασίας σε ομάδα ▫ Ηγετικές ικανότητες ▫ Δυνατότητα δαπάνης λίγων ημερών απασχόλησης σ' αυτή την μέθοδο ▫ Δυνατότητα για μεγαλύτερης διάρκειας απασχόληση		
Έχετε μία εξαιρετικά πολύπλοκη και σχετικά μεγάλη υποδομή συστημάτων ΤΠ αλλά ένα σχετικά απλό επιχειρηματικό μοντέλο;		
Στις επιχειρηματικές δραστηριότητες και τις υπηρεσίες που παρέχετε περιλαμβάνονται και οικονομικές συναλλαγές;		
Εκμεταλλεύεστε επιχείρηση η οποία υπόκειται σε μεγάλο βαθμό σε αυστηρούς νομικούς και κανονιστικούς περιορισμούς και/ή εντολές της ΕΕ ή της χώρας δραστηριοποίησής σας;		

Όπως και στις προηγούμενες προσεγγίσεις, όσο περισσότερες ερωτήσεις έχουν απαντηθεί με ένα «ναι» τόσο περισσότερο η ΜΜΕ προσαρμόζεται καλύτερα στην εν λόγω προσέγγιση υλοποίησης εκτίμησης κινδύνων.

Η απόφαση για την εν μέρει εξωτερική ανάθεση μιας εκτίμησης κινδύνων απαιτεί την σύναψη μίας Συμφωνίας Επιπέδου Υπηρεσίας (ΣΕΥ) ως πρωταρχική βάση για την συνεργασία με τον ανάδοχο. Στα βασικά στοιχεία μιας ΣΕΥ περιλαμβάνονται η επαγγελματική πιστοποίηση των μηχανικών ασφάλειας του παρόχου, η εμπιστευτικότητα, το χρονοδιάγραμμα, η κατανομή πόρων, το κόστος και η μεθοδολογία που θα εφαρμοστεί. Και σε αυτή την περίπτωση, οι φορείς μπορούν να προβούν στην ανάθεση εντολής προς τους παρόχους τους να διενεργήσουν μια εκτίμηση βάσει της μεθοδολογίας του ENISA, η οποία προτείνεται στο παρόν (Βλέπε κεφάλαιο 4. Μία απλουστευμένη προσέγγιση: επισκόπηση).

Οι ακόλουθες ερωτήσεις πρέπει, κατ' ελάχιστο, να τεθούν στο πλαίσιο μιας ΣΕΥ στην περίπτωση της εξωτερικής ανάθεση της εκτίμησης κινδύνων για την ασφάλεια των πληροφοριών:

- Συμφωνεί ο ανάδοχος να χρησιμοποιήσει μια προκαθορισμένη προσέγγιση εκτίμησης κινδύνων που είναι εξίσου γνωστή και στον πελάτη (λ.χ. την προτεινόμενη προσέγγιση εκτίμησης κινδύνων);
- Καλύπτονται θέματα **αστικής ευθύνης;** Τι θα συμβεί, για παράδειγμα, αν κατά την διάρκεια της εκτίμησης, διακοπούν ή διαταραχθούν σημαντικές επιχειρηματικές δραστηριότητες εξαιτίας της ανικανότητας του παρόχου να διενεργήσει μια εκτίμηση της υποκείμενης υποδομής ΤΠ και δικτύων;
- Προσδιορίζονται με σαφήνεια **οι ευθύνες** από την ΣΕΥ; Ποιος θα είναι υπεύθυνος και για ποια ενέργεια/πράξη; Ποια θα είναι η συμμετοχή του οργανισμού όσον αφορά τους πόρους;
- Τεκμηριώνεται με σαφήνεια **το πεδίο εφαρμογής** της εργασίας**;** Τι θα περιλαμβάνει ο πάροχος στο πεδίο εφαρμογής της εργασίας; Συνιστάται θερμά το πεδίο εφαρμογής της εργασίας να περιλαμβάνει ολόκληρο το φάσμα των επιχειρηματικών δραστηριοτήτων και την υποκείμενη υποδομή. Σε οποιαδήποτε άλλη περίπτωση, είναι πιθανόν το αποτέλεσμα να είναι ανεπαρκές ή ακόμα και παραπλανητικό.
- Με ποιόν τρόπο πρόκειται να ικανοποιηθούν **οι νομικές απαιτήσεις,** π.χ. νομοθεσία για την προστασία των δεδομένων;
- Ποιοι διακανονισμοί θα εφαρμοστούν ώστε να επιτρέψουν σ' όλα τα εμπλεκόμενα στην εξωτερική ανάθεση μέρη, συμπεριλαμβανομένων και των υπεργολάβων, να έχουν επίγνωση των δικών τους ευθυνών ασφάλειας;

- Με ποιόν τρόπο πρόκειται να διατηρηθούν και να ελεγχθούν **η ακεραιότητα και η εμπιστευτικότητα των πόρων του φορέα;**
- Ποιοι **φυσικοί και λογικοί έλεγχοι** θα χρησιμοποιηθούν ώστε να περιορίσουν και να θέσουν όρια στην πρόσβαση των εξουσιοδοτημένων χρηστών σ' ευαίσθητα επαγγελματικά δεδομένα του οργανισμού;
- Με ποιόν τρόπο πρόκειται να διατηρηθεί **η διαθεσιμότητα των υπηρεσιών στο ενδεχόμενο μιας καταστροφής;**
- Περιλαμβάνεται στους γενικούς και ειδικούς όρους **το δικαίωμα ελέγχου** των μέτρων ασφάλειας και προστασίας των πληροφοριών **του προμηθευτή;**
- Δηλώνονται ρητά **οι ελάχιστοι πόροι, η ικανότητα και η επαγγελματική πιστοποίηση** του προμηθευτή;
- Καθορίζονται με σαφήνεια το περιεχόμενο, η συχνότητα και η δομή των υποβαλλόμενων εκθέσεων;

4. Μια απλουστευμένη προσέγγιση: επισκόπηση

Το παρόν κεφάλαιο εκθέτει το περιεχόμενο μιας απλουστευμένης προσέγγισης εκτίμησης και διαχείρισης κινδύνων, η οποία μπορεί να χρησιμοποιηθεί από ΜΜΕ για αυτοαξιολόγηση, ακόμη και στο πλαίσιο έργων εξωτερικής ανάθεσης, όπως επισημαίνεται στο Κεφάλαιο 3.

Οι περισσότερες από τις υφιστάμενες προσεγγίσεις για την εκτίμηση και την διαχείριση κινδύνων σε θέματα ασφάλειας, γενικά, επικεντρώνονται στις ανάγκες μεγάλων οργανισμών. Σήμερα, δεν υπάρχει μια απλή προσέγγιση σχεδιασμένη για μικρούς οργανισμούς, τουλάχιστον όχι με την μορφή δημοσιοποιημένων κατευθυντήριων γραμμών. Ορισμένες επιχειρήσεις συμβούλων έχουν αναπτύξει ορθές πρακτικές γι' αυτό τον σκοπό, αλλά τις χρησιμοποιούν σε έργα πελατών τους. Άλλες προσεγγίσεις, αν και υποστηρίζεται ότι αρμόζουν για ΜΜΕ, παραμένουν αρκετά πολύπλοκες για αυτοαξιολογήσεις (π.χ. η OCTAVE). Από την άλλη πλευρά, όπως έχει ήδη σχολιαστεί, οι περισσότερες ΜΜΕ δεν μπορούν να αντεπεξέλθουν στο κόστος μιας εξολοκλήρου εξωτερικής ανάθεσης της εν λόγω αποστολής σε εξωτερικούς φορείς.

Πρόθεσή μας είναι να παράσχουμε στους οργανισμούς αυτούς μια απλή, αποτελεσματική και φθηνή προσέγγιση για την αναγνώριση και διαχείριση των κινδύνων που συνδέονται με την ασφάλεια των πληροφοριών τους. **Η προκύπτουσα απλουστευμένη προσέγγιση παρέχει στους μικρούς οργανισμούς μία μέθοδο για την διενέργεια αυτοαξιολογήσεων. Βασίζεται στις αρχές, τα χαρακτηριστικά και τα αποτελέσματα της OCTAVE[2], είναι, δε, προσαρμοσμένη στα/τις αντιπροσωπευτικά(-ες) περιβάλλοντα και ανάγκες των ΜΜΕ. Ουσιαστικά, αυτή η προσέγγιση είναι, επίσης, συμβατή με άλλα υφιστάμενα πρότυπα, όπως, για παράδειγμα, το ISO 13335-2.**

Για έναν φορέα, ο οποίος προσβλέπει στην κατανόηση των αναγκών που συνδέονται με την ασφάλεια των πληροφοριών του, η παρούσα προσέγγιση αποτελεί αυτοαξιολόγηση βασισμένη στον προσδιορισμό του χαρακτηριστικού προφίλ κινδύνων και τεχνική προγραμματισμού για θέματα ασφάλειας. Αντίθετα με τυπικές εκτιμήσεις που εστιάζονται στην τεχνολογία και οι οποίες είναι στοχευμένες μόνο στον τεχνολογικό κίνδυνο, αυτή η μέθοδος στοχεύει στο γενικό πλαίσιο και τους εγγενείς κινδύνους και επικεντρώνεται σε στρατηγικά, πρακτικής φύσεως ζητήματα.

Το βασικό πλεονέκτημα της παρούσας προσέγγισης είναι ότι μπορεί να παράσχει ένα αποδεκτό επίπεδο ασφάλειας με μικρή προσπάθεια έργου όσον αυτό αφορά την διαδικασία εκτίμησης και διαχείρισης. Αυτό οφείλεται στις ακόλουθες πτυχές που ενισχύουν την πρακτικότητα:

- Το προφίλ κινδύνων του οργανισμού μπορεί να προσδιοριστεί εύκολα.
- Δίνονται τα τυπικά στοιχεία των πόρων για μικρούς οργανισμούς.
- Η προστασία των πόρων μέσω μέτρων (ελέγχων) προκαθορίζεται μέσα από κάρτες ελέγχου.

Αυτά τα πλεονεκτήματα μπορούν να οδηγήσουν σε αυτοαξιολόγηση χαμηλού κόστους από ομάδες με χαμηλού επιπέδου εμπειρογνωμοσύνη σε θέματα ασφάλειας. Αν αυτό γίνει προσεκτικά, θα προκύψει ένα αποδεκτό επίπεδο ασφάλειας.

Η προτεινόμενη προσέγγιση εκτίμησης μπορεί να εφαρμοστεί από μη ειδικούς. Κατά την διάρκεια μιας εκτίμησης, η ομάδα εκτίμησης δε χρειάζεται να αντιμετωπίσει διάφορες πτυχές απειλών σε ευπρόσβλητους πόρους. Αντιθέτως, προτείνεται ένα προκαθορισμένο επίπεδο προστασίας, σύμφωνα με τον τύπο του πόρου και του απαιτούμενου επιπέδου ασφάλειας.

Η εργασία, που πραγματοποιείται για την ανάπτυξη ενός προτύπου κινδύνων, στην οποία στηρίζεται αυτή η προσέγγιση, βασίζεται στις ακόλουθες παραδοχές/στοιχεία:

- **Εκτίμηση των εγγενών κινδύνων** – Συχνά, το περιβάλλον μπορεί να καθορίσει το γενικό πλαίσιο κινδύνων (εγγενείς κίνδυνοι) μέσα στο οποίο ασκείται η οικονομική δραστηριότητα ή η εκμετάλλευση μιας επιχείρησης. Για παράδειγμα, ένας μικρός οργανισμός, ο οποίος δραστηριοποιείται στην αρτοποιία, εντάσσεται σε ένα γενικό πλαίσιο σημαντικά μικρότερων

κινδύνων απ' ό,τι ένας μικρός οργανισμός που δραστηριοποιείται στην παροχή υπηρεσιών υγειονομικής περίθαλψης ή συγκέντρωσης επιχειρηματικών πληροφοριών. Ανεξάρτητα από τα μέτρα ασφάλειας, την υποδομή και τα έσοδα, οι δυο επιχειρήσεις λειτουργούν σε εξολοκλήρου διαφορετικό περιβάλλον κινδύνων, το οποίο πρέπει να ληφθεί σοβαρά υπόψη πριν καθοριστεί η στρατηγική ασφάλειας των πληροφοριών και επιλεγούν οι ανάλογοι έλεγχοι ασφάλειας.

- **Η ποικιλία των εκδοχών απειλών (προφίλ) που διαπιστώνονται στις ΜΜΕ**. Στο γενικό πλαίσιο των ΜΜΕ, παρά τη φυσικά αναμενόμενη διασπορά όσον αφορά τους εγγενείς κινδύνους, έχουμε παρατηρήσει ότι οι απειλές είναι μάλλον χαρακτηριστικές και, συχνότατα, όταν ομαδοποιηθούν, μπορούν να διαμορφώσουν προφίλ γενικών απειλών, τα οποία είναι εφαρμόσιμα στην συντριπτική πλειονότητα των ΜΜΕ. Στο πλαίσιο αυτό, η εργασία μας επικεντρώνεται στην προτυποποίηση των απειλών μέσω προφίλ γενικών απειλών. Τα αναπτυγμένα προφίλ κινδύνων βοηθούν στην αντανάκλαση του επιπέδου των εγγενών κινδύνων ενός οργανισμού. Κατά συνέπεια, προσδιορίστηκαν και ομαδοποιήθηκαν τα ανάλογα μέτρα προκειμένου να καλύψουν τις απειλές για τα αντίστοιχα προφίλ κινδύνων.

Η **προτεινόμενη προσέγγιση είναι αυτοκατευθυνόμενη**, πράγμα που σημαίνει ότι το ανθρώπινο δυναμικό ενός οργανισμού αναλαμβάνει την ευθύνη για την εκτίμηση των κινδύνων, την επιλογή των ελέγχων και τον καθορισμό, κατ' αυτόν τον τρόπο, της στρατηγικής ασφάλειας του οργανισμού. Αυτή η τεχνική διευρύνει την γνώση των ατόμων πάνω στις πρακτικές και τις διαδικασίες ασφάλειας του οργανισμού τους, έτσι ώστε: **(α) να αντιλαμβάνονται την τρέχουσα κατάσταση των πρακτικών ασφάλειας εντός του οργανισμού, (β) να αναγνωρίζουν τους κινδύνους για τους πλέον κρίσιμους πόρους, (γ) να δίνουν προτεραιότητα στους τομείς στους οποίους σημειώνεται βελτίωση και να ορίζουν την στρατηγική ασφάλειας για τον οργανισμό.** Κατά την διαδικασία αυτή, καλύπτεται ολόκληρος ο κύκλος ζωής της εκτίμησης και της διαχείρισης κινδύνων.

Κατά την εφαρμογή της προτεινόμενης προσέγγισης, μια μικρή ομάδα ατόμων από επιχειρησιακές (ή επιχειρηματικές) μονάδες συνεργάζεται με την τμήμα της τεχνολογίας των πληροφοριών (ΤΠ) για την αντιμετώπιση των αναγκών ασφάλειας του οργανισμού, εξισορροπώντας έτσι δύο βασικές πτυχές της ασφάλειας, δηλαδή τα οργανωτικά μέτρα και τα μέτρα βάσει πόρων.

Οι οργανισμοί ενθαρρύνονται σθεναρά να εφαρμόζουν τις κατευθυντήριες γραμμές και τις ορθές πρακτικές, που περιλαμβάνονται στην εν λόγω προσέγγιση, μόνο ως βραχυπρόθεσμο σχέδιο για την επίτευξη του στόχου το συντομότερο δυνατόν, καθώς και για την αποτελεσματική προστασία κρίσιμων και καθοριστικών συστατικών στοιχείων της επιχειρηματικής τους δραστηριότητας. Το περιεχόμενο της εν λόγω προσέγγισης καλύπτει σημαντικούς κινδύνους στους οποίους συχνά εκτίθενται οι ΜΜΕ. Ωστόσο, η προτεινόμενη προσέγγιση δεν αποτελεί οριστική αντικατάσταση της ολοκληρωμένης και ενδελεχούς εκτίμησης κινδύνων για κρίσιμους πόρους. Συνιστούμε θερμά τέτοιου τύπου «καταδύσεις στα βαθιά» για να εκτιμήσουμε καλύτερα τους κινδύνους ειδικότερα εφόσον χρησιμοποιούνται πολύπλοκα εξαρτήματα για εξαιρετικά πολύτιμους πόρους.

Οι στόχοι σχετικά με την καθιέρωση της εν λόγω προσέγγισης εκτίμησης και διαχείρισης κινδύνων είναι:

- **Η βελτίωση των υφιστάμενων ευρωπαϊκών κατωφλίων ασφάλειας των πληροφοριών**. Η προσέγγιση μπορεί να χρησιμοποιηθεί ως καταλύτης για την επιτάχυνση των προσπαθειών των ΜΜΕ προς την κατεύθυνση της διαχείρισης κινδύνων της ασφάλειας των πληροφοριών μέσω της αντιμετώπισης υψηλών κινδύνων. Επιπλέον, η στόχευση σε τυπικές περιπτώσεις απειλών, θα βελτιώσει, σε τελευταία ανάλυση, τα υπάρχοντα ευρωπαϊκά κατώφλια ασφάλειας των πληροφοριών.

- Η εκπλήρωση των επιχειρηματικών απαιτήσεων, καθώς και η ανταπόκριση στο γενικό πλαίσιο και τους περιορισμούς, που διαπιστώνονται κατ' εξοχήν στα περιβάλλοντα των ΜΜΕ, **αποφεύγοντας, ταυτόχρονα, την εξειδικευμένη ορολογία και εξαλείφοντας καθήκοντα υψηλών απαιτήσεων**, τα οποία ενσωματώνονται σχεδόν σε κάθε υφιστάμενη, ευρέως διαδεδομένη επαγγελματική μεθοδολογία και βιομηχανικό πρότυπο (δηλαδή την αξιολόγηση των πόρων, την ανάλυση επιχειρηματικού αντίκτυπου, τον προσδιορισμό απαιτήσεων διασφάλισης κτλ).

- **Η χρήση μιας αυτοκατευθυνόμενης προσέγγισης,** η οποία είναι προσαρμοσμένη στα μέσα, τους πόρους και την εμπειρογνωμοσύνη που διαπιστώνονται κατ' εξοχήν σ' ένα περιβάλλον ΜΜΕ.
- **Η επικέντρωση στους κρίσιμους πόρους και τους υψηλότερους κινδύνους**. Η μέθοδος αναπτύχθηκε ως ένας απλός και εύχρηστος οδηγός για τον προσδιορισμό και προστασία των πόρων που κρίνονται ότι είναι οι πλέον κρίσιμοι για έναν οργανισμό.
- Η ανάπτυξη μιας **αυτοτελούς** μεθόδου εκτίμησης και διαχείρισης κινδύνων. Για τον σκοπό της παραγωγής του πρώτου πρακτικού και ρεαλιστικού αποτελέσματος έχουν χρησιμοποιηθεί οι έλεγχοι OCTAVE. Ωστόσο, η μέθοδος μπορεί να χρησιμοποιήσει, στην ουσία, όλους τους ελέγχους προτύπων που είναι διαθέσιμοι σήμερα (ISO, BS7799, NIST, BSI).

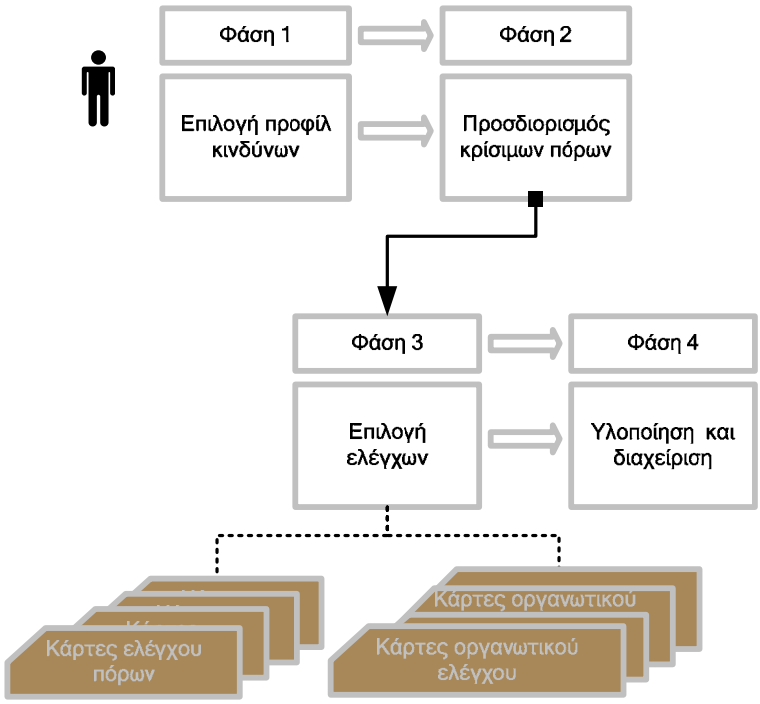
4.2 Παραδοχές εργασίας

Εκτός των προαναφερόμενων στόχων, έχουν γίνει ορισμένες θεωρήσεις/παραδοχές για την ανάπτυξη του παρόντος οδηγού και την προσέγγιση εκτίμησης κινδύνων που παρουσιάζει:

- Σε πολλές περιπτώσεις, η ΜΜΕ μπορεί να μην είναι εξοικειωμένη με την ασφάλεια των υπολογιστών και, κατά συνέπεια, μπορεί να ωφεληθεί από την πρόσβαση σε υλικό ευαισθητοποίησης, κατάρτισης και καθοδήγησης.
- Η δημιουργία ενός πλαισίου καθοδήγησης για την ασφάλεια μέσω των επαγγελματικών φορέων και ενώσεων ΜΜΕ θα βοηθήσει στην προώθηση της κατανόησης των θεμάτων ασφάλειας από εκείνους που διαθέτουν περιορισμένο εύρος γνώσεων στην ασφάλεια των πληροφοριών.
- Οι ΜΜΕ αποτελούν τομέα προτεραιότητας ενδιαφέροντος στον οποίο επικεντρώνεται η κυβερνητική οικονομική πολιτική και θεωρούνται μείζονος σημασίας για την κοινωνικοοικονομική ανάπτυξη στην Ευρωπαϊκή Ένωση.
- Οι ΜΜΕ συνήθως δημιουργούνται από επιχειρηματικό πάθος και ελλιπή χρηματοδότηση, με επιχειρησιακά συστήματα, τα οποία 'συρράπτονται ατάκτως' και, κατά συνέπεια, είναι ετερογενή και ανεξάρτητα.
- Οι πολιτικές και τα πλαίσια για τον προγραμματισμό της ασφάλειας των πληροφοριών και την ανάκτηση μετά από καταστροφή είναι, συνήθως, ανύπαρκτα. Επιπλέον, η βασική κατανόηση των κινδύνων για την ασφάλεια των πληροφοριών στις ΜΜΕ δεν επεκτείνεται πολύ πιο πέρα από τους ιούς και το αντιιικό λογισμικό.
- Οι περισσότεροι διευθυντές ΜΜΕ μόλις και μετά βίας κατανοούν την εξαιρετικά τεχνική και περίπλοκη επιστημονική ορολογία που σχετίζεται με την ασφάλεια των πληροφοριών.
- Οι εταιρείες μικρού μεγέθους συνήθως ασκούν τις εργασίες τους στο πλαίσιο ενός τυποποιημένου περιβάλλοντος επεξεργασίας δεδομένων, το οποίο όμως είναι σημαντικό για την επιχείρηση. Χρησιμοποιούν πακέτα όπως «ετοιμοπαράδοτα» προϊόντα, τα οποία συνίστανται εν μέρει ή εξολοκλήρου σ' ένα «μαύρο κουτί» (με όλους τους πιθανούς συσχετιζόμενους κινδύνους) και συνδέονται στο Διαδίκτυο, όπου ελλοχεύουν πολλές απειλές ασφάλειας ΤΠ.
- Οι ακούσιες απειλές θέτουν μερικούς από τους υψηλότερους κινδύνους για την ασφάλεια των πληροφοριών στις ΜΜΕ. Ωστόσο, η κατάρτιση του προσωπικού και τα προγράμματα ευαισθητοποίησης συχνά παραμελούνται. Ακόμα κι αν το προσωπικό των ΜΜΕ έχει εξειδικευμένη γνώση των πληροφοριακών συστημάτων, μπορεί να μην κατέχει ειδική τεχνογνωσία σε ζητήματα ασφάλειας ΤΠ. Ένας επιβαρυντικός παράγοντας είναι ότι, γενικά, οι εταιρείες δεν μπορούν να διαθέσουν τα απαραίτητα οικονομικά μέσα ώστε να επενδύσουν αρκετούς πόρους στην εκτίμηση και την διαχείριση κινδύνων.

4.3 Προσέγγιση τεσσάρων φάσεων

Η προτεινόμενη προσέγγιση εκτίμησης κινδύνων χρησιμοποιεί **τέσσερις φάσεις** για να εξετάσει οργανωτικά θέματα και ζητήματα ασφάλειας της τεχνολογίας, παρέχοντας έτσι μια περιεκτική ολιστική εικόνα των αναγκών για την ασφάλεια των πληροφοριών. Οι τέσσερις φάσεις για την προτεινόμενη μέθοδο απεικονίζονται στο Σχήμα 2.



Σχήμα 2: Οι τέσσερις φάσεις στις οποίες στηρίζεται η προτεινόμενη προσέγγιση εκτίμησης κινδύνων

Η προσέγγιση αξιολόγησης κινδύνων εξαρτάται από δυο βασικές πτυχές: **(1) το προφίλ επιχειρηματικών κινδύνων και (2) τον προσδιορισμό κρίσιμων πόρων**.

Την διαδικασία εκτίμησης κινδύνων διαχειρίζεται μια μικρή διεπιστημονική ομάδα αξιολόγησης (τρία έως πέντε άτομα, από το προσωπικό της ΜΜΕ, από εξωτερικό προσωπικό ή ένα μεικτό σχήμα των δύο σύμφωνα με τον τύπο υλοποίησης που αναφέρεται στο Κεφάλαιο 3.3 Με ποιόν τρόπο θα ενεργήσετε όσον αφορά την ασφάλεια των πληροφοριών), η οποία συγκεντρώνει και αναλύει πληροφορίες και εκπονεί σχέδια μετριασμού με βάση τους κινδύνους για την ασφάλεια του οργανισμού. Για την αποτελεσματική διενέργεια της εκτίμησης κινδύνων, η ομάδα πρέπει να διαθέτει ευρεία γνώση των επιχειρηματικών δραστηριοτήτων (αναφέρονται και ως επιχειρησιακές διαδικασίες) και της υποδομής ΤΠ του οργανισμού.

Ως σημείο εκκίνησης, η ομάδα ανάλυσης της ΜΜΕ **θα χρησιμοποιήσει τον πίνακα αξιολόγησης προφίλ κινδύνων ώστε να προσδιοριστεί το προφίλ των επιχειρηματικών κινδύνων**. Το επόμενο στάδιο περιλαμβάνει **τον προσδιορισμό κρίσιμων πόρων** και των συναφών **απαιτήσεων διασφάλισης** όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων.

Ακολούθως, επιλέγονται οι έλεγχοι (κάρτες ελέγχου). Η διαδικασία επιλογής είναι ριζικά απλοποιημένη με την χρήση τυποποιημένων καρτών ελέγχου. Οι ομάδες ολοκληρώνουν την διαδικασία επιλογής ελέγχων **απλώς «τραβώντας» τις κάρτες ελέγχου, που συνδέονται με κινδύνους** τόσο για τον οργανισμό όσο και για τους αναγνωρισμένους κρίσιμους πόρους, οι οποίες

έχουν δημιουργηθεί για κάθε επίπεδο του προφίλ κινδύνων, κατηγορία πόρου και απαίτηση διασφάλισης (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα).

Οι κάρτες ελέγχου περιλαμβάνουν ελέγχους από τον κατάλογο των πρακτικών που χρησιμοποιείται στην OCTAVE. Αυτή η απόφαση ελήφθη διότι οι εν λόγω έλεγχοι είναι αρκετά απλοί και πιο εύκολα κατανοητοί από μη ειδικούς σε θέματα ασφάλειας. Εναλλακτικά, μπορούν να χρησιμοποιηθούν άλλοι έλεγχοι ασφάλειας. Αυτό ενδεχομένως να είναι απαραίτητο στην περίπτωση που μία ΜΜΕ διαθέτει ήδη μια πολιτική ασφάλειας βάσει ενός άλλου προτύπου (π.χ. ISO 17799).

Κατά το τελευταίο στάδιο, η ομάδα ανάλυσης της ΜΜΕ απασχολείται με την ιεράρχηση των πόρων σύμφωνα με την κρισιμότητά τους, την επίδρασή τους στην επιχείρηση και το σχέδιο προστασίας τους.

Στις επόμενες παραγράφους περιγράφονται διεξοδικότερα οι φάσεις εκτίμησης κινδύνων.

4.3.1 Φάση 1 – Επιλογή προφίλ κινδύνων

Κατά την διάρκεια αυτής της φάσης, οι ομάδες αξιολόγησης αξιολογούν το προφίλ επιχειρηματικών κινδύνων τους χρησιμοποιώντας ένα σύνολο προκαθορισμένων **ποιοτικών κριτηρίων**. Χρησιμοποιώντας τον πίνακα αξιολόγησης προφίλ κινδύνων (Πίνακας 2), οι ομάδες αξιολόγησης είναι σε θέση να αναγνωρίσουν το γενικό πλαίσιο κινδύνων τους. Το γενικό πλαίσιο κινδύνων συνίσταται στο επιχειρηματικό και εξωτερικό περιβάλλον ενός οργανισμού και μπορεί να κατανεμηθεί σε **τέσσερις περιοχές κινδύνων: νομικής και κανονιστικής συμμόρφωσης, φήμη και εμπιστοσύνη πελατών, παραγωγικότητα και οικονομική σταθερότητα**.

Περιοχές κινδύνων	Υψηλού Επιπέδου	Μεσαίου Επιπέδου	Χαμηλού Επιπέδου
Νομικής και κανονιστικής συμμόρφωσης	Ο οργανισμός χειρίζεται πληροφορίες ευαίσθητης και προσωπικής φύσεως των πελατών συμπεριλαμβανομένων των ιατρικών δεδομένων και των προσωπικών δεδομένων κρίσιμης σημασίας όπως ορίζεται στην νομοθεσία της ΕΕ περί προστασίας των δεδομένων.	Ο οργανισμός χειρίζεται τις πληροφορίες προσωπικής αλλά όχι ευαίσθητης φύσεως των πελατών όπως ορίζεται στην νομοθεσία της ΕΕ περί προστασίας των δεδομένων.	Ο οργανισμός δεν χειρίζεται δεδομένα προσωπικού χαρακτήρα εκτός από εκείνα των ατόμων που απασχολούνται σε αυτόν.
Παραγωγικό-τητα	Ο οργανισμός απασχολεί περισσότερους από 100 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.	Ο οργανισμός απασχολεί περισσότερους από 50 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.	Ο οργανισμός απασχολεί λιγότερους από 10 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.
Οικονομική σταθερότητα	Τα ετήσια έσοδα του οργανισμού υπερβαίνουν τα 25 εκατ. ευρώ ή/και οι οικονομικές συναλλαγές με τρίτους ή πελάτες λαμβάνουν χώρα ως τμήμα της επιχειρηματικής δραστηριότητας ως συνήθης διαδικασία.	Τα ετήσια έσοδα του οργανισμού δεν υπερβαίνουν τα 25 εκατ. ευρώ.	Τα ετήσια έσοδα του οργανισμού δεν υπερβαίνουν τα 5 εκατ. ευρώ.
Φήμη και απώλεια εμπιστοσύνης πελατών	Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών έχουν άμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού ή/και πάνω από το 70% της βάσης πελατών έχουν	Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών έχουν έμμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού και/ή κάτω του 5% της βάσης πελατών έχουν ηλεκτρονική πρόσβαση σε	Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών δεν έχουν άμεση ή έμμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού ή καταλήγουν σε απώλεια εσόδων.

	ηλεκτρονική πρόσβαση σε προϊόντα και υπηρεσίες της επιχείρησης.	προϊόντα και υπηρεσίες της επιχείρησης.	

Πίνακας 2: Πίνακας αξιολόγησης προφίλ κινδύνων

Κάθε περιοχή ταξινομείται σε τρεις κατηγορίες: υψηλού, μεσαίου και χαμηλού επιπέδου κινδύνων. Αυτές οι κατηγορίες παριστούν ποσοτικά κριτήρια για τον εν λόγω οργανισμό όσον αφορά την περιοχή κινδύνων και βοηθούν στην αναγνώριση ενός επιπέδου κινδύνων. Η ομάδα αξιολογεί τους κινδύνους που αναγνωρίζονται σε κάθε περιοχή έτσι ώστε να δημιουργήσουν το **προφίλ κινδύνων του οργανισμού**.

Η πείρα λέει ότι ο υψηλότερος κίνδυνος που αναγνωρίζεται σε μια κατηγορία κινδύνων καθορίζει το συνολικό προφίλ επιχειρηματικών κινδύνων. Ένας υψηλός κίνδυνος που φέρεται στην κατηγορία οικονομικών κινδύνων οριοθετεί το προφίλ υψηλών κινδύνων. Επίσης, ένας κίνδυνος μεσαίου επιπέδου οδηγεί σ' ένα προφίλ μεσαίων κινδύνων και οι κίνδυνοι χαμηλού επιπέδου σε προφίλ χαμηλών κινδύνων. Για παράδειγμα, ένας κίνδυνος χαμηλού επιπέδου που φέρεται στην φήμη και την εμπιστοσύνη, στην νομική και κανονιστική συμμόρφωση και στην παραγωγικότητα αλλά είναι υψηλού επιπέδου στην κατηγορία κινδύνων της οικονομικής σταθερότητας καταλήγει σε προφίλ υψηλών κινδύνων για τον οργανισμό.

Ο προσδιορισμός των χαρακτηριστικών (προφίλ) κινδύνων πρέπει να θεωρείται ως πολύ σημαντική απόφαση, η οποία, ακολούθως, οδηγεί στην επιλογή πόρων που σχετίζονται με κινδύνους και στην προστασία τους μέσω καρτών ελέγχου.

4.3.2 Φάση 2 – Προσδιορισμός κρίσιμων πόρων

Κατά τη διάρκεια αυτής της φάσης, η ομάδα αξιολόγησης επιλέγει τους κρίσιμους πόρους βάσει της σχετικής σημασίας για τον οργανισμό και ορίζει τις απαιτήσεις διασφάλισης για κάθε κρίσιμο πόρο.

Κατά κανόνα, η διεύθυνση ενός οργανισμού γνωρίζει ποιοι είναι οι **βασικοί πόροι του** και μπορεί να χρησιμοποιήσει τα περιορισμένα της μέσα ώστε να επικεντρωθεί στην προστασία αυτών των βασικών πόρων. Η ομάδα αξιολόγησης καθορίζει τι είναι σημαντικό για τον οργανισμό (π.χ. πόροι που συνδέονται με τις πληροφορίες) και επιλέγει εκείνους τους πόρους που είναι μείζονος σημασίας για τον οργανισμό, τα οποία ονομάζονται επίσης και **κρίσιμοι πόροι**.

Στον ακόλουθο πίνακας καθορίζονται οι κατηγορίες των πόρων και των τύπων που εξετάζονται κατά την επιλογή των κρίσιμων πόρων. Δίνεται προσοχή στους πόρους, οι οποίοι χρησιμοποιούνται για να βοηθήσουν τον οργανισμό να ασκήσει τις επιχειρηματικές του δραστηριότητες. Πρέπει να σημειωθεί ότι οι τύποι πόρων μπορούν να απαρτίζονται από άλλους τύπους πόρων. Για παράδειγμα, τα συστατικά μέρη μιας εφαρμογής μπορεί να είναι διακομιστές, σταθμοί εργασίας, δρομολογητές, τμήματα δικτύων κτλ.

Πρέπει, επίσης, να σημειωθεί ότι ο ακόλουθος κατάλογος είναι αντιπροσωπευτικός για τις περισσότερες μικρές επιχειρήσεις, δεν είναι, όμως, εξαντλητικός. Κατόπιν αιτήματος (π.χ. σε μελλοντικές εκδόσεις του παρόντος εγγράφου), είναι δυνατόν να παρουσιαστούν επιπρόσθετοι πόροι. Ακόμη, είναι δυνατόν ένας τύπος πόρων να χρησιμοποιεί άλλους πόρους για τις λειτουργίες του. Για παράδειγμα, μια εφαρμογή μπορεί να χρησιμοποιεί ως συστατικά της μέρη έναν διακομιστή, έναν μικρό αριθμό σταθμών εργασίας, μια συσκευή αποθήκευσης και ένα τμήμα δικτύου. Πρέπει να σημειωθεί, τέλος, ότι πέρα από την προστασία ενός πόρου, όλα τα συστατικά του μέρη πρέπει επίσης να προστατεύονται κατάλληλα.

Κατηγορία Πόρων	Περιγραφή	Πόρος (τύποι)
Συστήματα	Πληροφοριακά συστήματα που επεξεργάζονται και αποθηκεύουν πληροφορίες. Τα συστήματα αποτελούν ένα συνδυασμό πόρων πληροφοριών, λογισμικού, και υλικού. Κάθε ξενιστής Η/Υ, πελάτης Η/Υ, διακομιστής ή δίκτυο μπορεί να θεωρηθεί ως σύστημα. Κρίσιμα συστήματα είναι εκείνα που αναγνωρίζονται ως ουσιώδη για την συνεχή παροχή επιχειρηματικών υπηρεσιών και διάθεση προϊόντων, εκείνα που αποθηκεύουν κρίσιμες επιχειρηματικές πληροφορίες (ιδιοκτησίας πελατών ή επιχειρήσεων) ή αυτά που εκτίθενται στο εξωτερικό περιβάλλον για επιχειρηματικές λειτουργίες ή υπηρεσίες.	Διακομιστής Φορητός υπολογιστής Σταθμός εργασίας Αρχειοθέτηση και δημιουργία εφεδρικών αντιγράφων Αποθηκευτικά μέσα
Δίκτυο	Συσκευές σημαντικές για τα δίκτυα του οργανισμού. Οι δρομολογητές, οι μεταγωγείς και οι διαποδιαμορφωτές (μόντεμ) αποτελούν παραδείγματα αυτής της κατηγορίας εξαρτημάτων. Ασύρματα εξαρτήματα/συσκευές, όπως τα κινητά τηλέφωνα και τα σημεία ασύρματης πρόσβασης που χρησιμοποιεί το προσωπικό για να αποκτά πρόσβαση σε πληροφορίες (για παράδειγμα, το ηλεκτρονικό ταχυδρομείο). Κατά κανόνα, κρίσιμα δίκτυα είναι εκείνα που χρησιμοποιούνται για την υποστήριξη ουσιωδών κρίσιμων εφαρμογών ή συστημάτων ή εκείνα που διαμοιράζονται με τρίτους και συνήθως μη έμπιστα δίκτυα.	Δρομολογητές Καλωδίωση Πύλες δικτύου Σημεία ασύρματης πρόσβασης Τμήμα δικτύου (π.χ. καλωδίωση και εξοπλισμός μεταξύ δύο υπολογιστών) Λοιπά (SAT, Laser)
Άνθρωποι	Τα πρόσωπα που στελεχώνουν έναν οργανισμό, συμπεριλαμβανομένων των δεξιοτήτων, της κατάρτισης, των γνώσεων τους και της εμπειρίας τους. Κρίσιμα πρόσωπα είναι εκείνα που παίζουν ουσιαστικό ρόλο στις παραγωγικές ή επιχειρησιακές διεργασίες. Πρέπει να δοθεί σημασία στους καθοριστικούς πόρους (άτομα) που θεωρούνται αναντικατάστατα ή συνιστούν ένα μόνο σημείο αποτυχίας.	Διαχείριση επιχειρηματικών πόρων και ανθρώπινου δυναμικού Διαδικασίες και τεχνολογία Έρευνα και Ανάπτυξη Πωλήσεις και εμπορία (μάρκετινγκ) Ανάδοχοι και τρίτοι
Εφαρμογές	Κρίσιμες εφαρμογές: εφαρμογές που αποτελούν μέσο για ή συνιστούν μέρος της παροχής προϊόντων και υπηρεσιών. Τυχόν δυσλειτουργία των κρίσιμων εφαρμογών κατά κανόνα έχει ως κατάληξη την σοβαρή παρακώλυση ή ακόμη και την συμφόρηση των εξαρτωμένων από αυτές διαδικασιών.	Χρηματοοικονομικός έλεγχος Εξυπηρέτηση Πελατών Διαχειριστική υποστήριξη Ηλεκτρονικό εμπόριο Αντιμετώπιση καταστάσεων εκτάκτου ανάγκης

Πίνακας 3: Κατάσταση πόρων

Κατά την διαδικασία της αναγνώρισης, είναι ουσιώδες να ληφθούν υπόψη οι απόψεις των διευθυντικών στελεχών (ή του ιδιοκτήτη της επιχείρησης). Η συμμετοχή των υψηλά ιστάμενων στην ανάλυση διασφαλίζει ότι η επιχειρηματική αξία των επιχειρηματικών πόρων πληροφοριών επισημαίνεται δεόντως.

Στην συνέχεια, είναι αναγκαία η αξιολόγηση των απαιτήσεων διασφάλισης για τους πιο σημαντικούς πόρους. Οι απαιτήσεις διασφάλισης σκιαγραφούν τα ποιοτικά χαρακτηριστικά ενός πόρου, τα οποία είναι σημαντικό να προστατευθούν. Κατά την διαδικασία αξιολόγησης εξετάζονται οι ακόλουθες απαιτήσεις διασφάλισης:

- εμπιστευτικότητα – η ανάγκη διαφύλαξης του ιδιωτικού χαρακτήρα και της μη προσπέλασης από οποιοδήποτε μη εξουσιοδοτημένο άτομο των πληροφοριών ιδιοκτήτη, των ευαίσθητων πληροφοριών ή των προσωπικών δεδομένων
- ακεραιότητα – η γνησιότητα, η ακρίβεια και η πληρότητα ενός πόρου
- διαθεσιμότητα – η ιδιότητα ενός πόρου να είναι διαθέσιμη κατά τον χρόνο χρήσης του

Οι ομάδες αξιολόγησης πρέπει να χρησιμοποιούν τα κριτήρια επιλογής απαιτήσεων όπως δίνονται στον πίνακα 4 προκειμένου να προσδιορίσουν τις σημαντικότερες απαιτήσεις διασφάλισης για τις διαφορετικές κατηγορίες πόρων. Οι απαιτήσεις διασφάλισης των πόρων θα χρησιμοποιηθούν αργότερα κατά την επιλογή των καρτών ελέγχου πόρων. Η επιλογή των απαιτήσεων διασφάλισης έχει αναπτυχθεί ως ένας απλός και πρακτικός οδηγός ώστε να προσδιορίζονται οι ιδιότητες ασφάλειας των κρίσιμων πόρων που επιλέχθηκαν προηγουμένως. Οι απαιτήσεις αναδεικνύουν τη σημασία ενός πόρου και αποτελούν ένα δείκτη του απαιτούμενου επιπέδου προστασίας (π.χ. μέσω της χρήσης κατάλληλων ελέγχων).

Ο ακόλουθος πίνακας θα βοηθήσει τις ομάδες αξιολόγησης να προσδιορίσουν τις απαιτήσεις διασφάλισης για τις διαφορετικές κατηγορίες πόρων που αναφέρονται παραπάνω.

Κατηγορία Πόρων	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Συστήματα	Ένα σύστημα με απαιτήσεις εμπιστευτικότητας συχνά χειρίζεται εταιρικές πληροφορίες (έρευνας και ανάπτυξης) χαρακτηρισμένες ως ιδιόκτητες, πληροφορίες βάσης πελατών, ευαίσθητα δεδομένα πελατών ιατρικής ή προσωπικής φύσεως.	Συστήματα με απαιτήσεις ακεραιότητας κατά κανόνα χειρίζονται συναλλαγές χρηματοοικονομικής φύσεως, τις προμήθειες αγαθών ή το ηλεκτρονικό εμπόριο.	Οι απαιτήσεις διαθεσιμότητας ικανοποιούνται σε συστήματα που είναι ζωτικής σημασίας για καθημερινές επιχειρηματικές λειτουργίες και όπου ο χρόνος διακοπής λειτουργίας επισύρει συνήθως δαπάνες και έμμεσα έξοδα όσον αφορά την κατανομή των πόρων.
Δίκτυο	Ένα δίκτυο με απαιτήσεις εμπιστευτικότητας κατά κανόνα καλύπτει τις επικοινωνίες και την ανταλλαγή πληροφοριών σε μη ασφαλή και μη έμπιστα περιβάλλοντα.	Οι απαιτήσεις ακεραιότητας δικτύου είναι κατά κανόνα απαραίτητες όταν οι συναλλαγές λαμβάνουν χώρα σε δημόσιο και διαμοιρασμένο μητροπολιτικό δίκτυο ή σε παρόχους τηλεπικοινωνιών.	Οι απαιτήσεις διαθεσιμότητας είναι ιδιαιτέρως απαραίτητες όταν το δίκτυο χρησιμοποιείται ως τμήμα της εξυπηρέτησης πελατών ή για την παροχή υπηρεσιών και την διάθεση προϊόντων.
Άνθρωποι	Οι απαιτήσεις εμπιστευτικότητας ικανοποιούνται κατά κανόνα όταν οι άνθρωποι χειρίζονται οργανωτικές ιδιόκτητες και απόρρητες πληροφορίες οι οποίες όταν δημοσιοποιηθούν μπορούν να προκαλέσουν βλάβη στο εμπορικό σήμα και στην βάση πελατών του οργανισμού.	Οι απαιτήσεις ακεραιότητας, όταν αφορούν ανθρώπους, επιλαμβάνονται κοινών μυστικών όπως κλείδες κρυπτογράφησης ή συνθηματικά. Η κατοχή τέτοιων γνώσεων εισάγει απειλές, που οφείλονται στον ανθρώπινο παράγοντα, και πρέπει να αντιμετωπιστούν με ανάλογους ελέγχους.	Οι απαιτήσεις διαθεσιμότητας για ανθρώπινους πόρους είναι ιδιαίτερα σημαντικές όταν αυτοί οι άνθρωποι αποτελούν κρίσιμους πόρους για συνεχείς λειτουργίες που αφορούν στην παροχή υπηρεσιών και την διάθεση προϊόντων.
Εφαρμογές	Οι εφαρμογές με απαιτήσεις εμπιστευτικότητας συχνά χειρίζονται εταιρικές πληροφορίες (έρευνας και ανάπτυξης) χαρακτηρισμένες ως ιδιόκτητες, πληροφορίες βάσης πελατών, ευαίσθητα δεδομένα πελατών ιατρικής ή προσωπικής φύσεως.	Οι εφαρμογές με απαιτήσεις ακεραιότητας κατά κανόνα χειρίζονται συναλλαγές χρηματοοικονομικής φύσεως, τις προμήθειες αγαθών ή το ηλεκτρονικό εμπόριο.	Οι απαιτήσεις διαθεσιμότητας ικανοποιούνται σε εφαρμογές που είναι ζωτικής σημασίας για καθημερινές επιχειρηματικές λειτουργίες και όπου ο χρόνος διακοπής λειτουργίας επισύρει συνήθως δαπάνες και έμμεσα έξοδα όσον αφορά την κατανομή των πόρων.

Πίνακας 4: Πίνακας επιλογής απαιτήσεων διασφάλισης

Ως αποτέλεσμα αυτής της διαδικασίας, οι ομάδες αξιολόγησης πρέπει να έχουν έναν πίνακα κρίσιμων πόρων ταξινομημένων ανά κατηγορία πόρου και έναν κατάλογο αντίστοιχων απαιτήσεων διασφάλισης, παράλληλα με μία αιτιολόγηση ή συμπληρωματικές πληροφορίες που θα ληφθούν υπόψη κατά την αξιολόγηση.

Στην συνέχεια, το αποτέλεσμα θα χρησιμοποιηθεί ως δεδομένο εισόδου από την Φάση 3 – Επιλογή καρτών ελέγχου, όπως επισημαίνεται στο επόμενο κεφάλαιο.

4.3.3 Φάση 3 - Επιλογή Καρτών Ελέγχου

Κατά τη Φάση 3, η ομάδα αξιολόγησης επιλέγει τους κατάλληλους ελέγχους βάσει του προφίλ κινδύνων που επιλέγεται για κάθε κατηγορία κινδύνων και της κατάστασης των προσδιορισμένων κρίσιμων πόρων (συμπεριλαμβανομένων των απαιτήσεών τους). Οι έλεγχοι διαχωρίζονται σε δύο κατηγορίες: τους οργανωτικούς ελέγχους και τον έλεγχο βάσει πόρων.

Ολόκληρος ο οργανισμός υποτίθεται ότι αποτελεί ένα ενιαίο περιουσιακό στοιχείο που πρέπει να προστατευθεί. Οι οργανωτικοί έλεγχοι ασφάλειας είναι, κατά κανόνα, περιεκτικοί και εφαρμόζονται στην οργάνωση των πόρων κατά οριζόντιο τρόπο. Αντιθέτως, οι έλεγχοι βάσει πόρων στοχεύουν στην υλοποίηση της προστασίας που απαιτείται από τους πόρους (π.χ. ενισχύοντας τη διαθεσιμότητα ενός συστατικού μέρους ενός κρίσιμου δικτύου).

Οι έλεγχοι ομαδοποιούνται περαιτέρω σε κάρτες ελέγχου. Διατίθενται δυο τύποι καρτών ελέγχου για επιλογή από τις ομάδες που διεξάγουν την αξιολόγηση μιας ΜΜΕ:

- Κάρτες ελέγχου οι οποίες περιλαμβάνουν ελέγχους που εφαρμόζονται οριζόντια στον οργανισμό και σχετίζονται με πρακτικές και διαδικασίες διαχείρισης και
- Κάρτες ελέγχου που εφαρμόζονται σε κρίσιμους πόρους και ταξινομούνται σε συγκεκριμένες κατηγορίες πόρων. Οι κάρτες ελέγχου είναι κατά κύριο λόγο προεπιλεγμένοι - ομαδοποιημένοι έλεγχοι σύμφωνα με τα προφίλ κινδύνων και τις απαιτήσεις διασφάλισης των πόρων.

Ο Πίνακας 5 συγκαταριθμεί τις κατηγορίες ελέγχων, τη δομή τους και την ονομασία τους με τον τρόπο που θεωρούνται σε αυτή την προσέγγιση. Όπως έχει ήδη αναφερθεί, οι έλεγχοι αυτοί έχουν υιοθετηθεί από την OCTAVE . Η απόφαση για τη χρησιμοποίηση των ελέγχων αυτών βασίστηκε στην απλότητά τους. Μπορούν αντ᾽ αυτών να χρησιμοποιηθούν άλλοι έλεγχοι (π.χ. ISO 17799, IT-Grundschutz κτλ.). Στο παρόν δίνεται μία πιο λεπτομερής περιγραφή.

Κατηγορία Ελέγχων	Αρ. Ελέγχου.	Ονομασία ελέγχου
Οργανωτικοί	**SP1**	Ευαισθητοποίηση και κατάρτιση σε θέματα ασφάλειας
	SP2	Στρατηγική ασφάλειας
	SP3	Διαχείριση ασφάλειας
	SP4	Πολιτικές και κανονισμοί ασφάλειας
	SP5	Συγκεντρωτική διαχείριση ασφάλειας
	SP6	Σχεδιασμός έκτακτης ανάγκης/ Ανάκτηση μετά από καταστροφή
Βάσει πόρων	**OP1.1**	Σχέδια και διαδικασίες υλικής ασφάλειας
	OP1.2	Έλεγχος φυσικής πρόσβασης
	OP1.3	Παρακολούθηση και έλεγχος υλικής ασφάλειας
	OP2.1	Διαχείριση συστημάτων και δικτύων
	OP2.2	Εργαλεία διαχείρισης συστήματος
	OP2.3	Παρακολούθηση και έλεγχος ασφάλειας ΤΠ
	OP2.4	Επαλήθευση και εξουσιοδότηση
	OP2.5	Διαχείριση ευπάθειας
	OP2.6	Κρυπτογράφηση
	OP2.7	Σχεδιασμός και αρχιτεκτονική ασφάλειας

	OP3.1	Διαχείριση συμβάντων
	OP3.2	Γενικές πρακτικές προσωπικού

Πίνακας 5: Έλεγχοι που χρησιμοποιούνται στην εκτιθέμενη προσέγγιση

Αναλόγως, η Φάση 3 της προτεινόμενης προσέγγισης εκτίμησης αποτελείται από δύο ξεχωριστά αλλά εξίσου σημαντικά στάδια:

- Στάδιο Α, Επιλογή οργανωτικών ελέγχων
- Στάδιο Β, Επιλογή ελέγχων βάσει πόρων

Κατά τη διάρκεια αυτών των σταδίων, οι έλεγχοι ανατίθενται στον οργανισμό (ως ενιαίο σημαντικό περιουσιακό στοιχείο) και στους προσδιορισμένους κρίσιμους πόρους όπως επισημαίνονται παρακάτω.

Επιλογή καρτών οργανωτικού ελέγχου

Η επιλογή καρτών οργανωτικού ελέγχου διενεργείται κατά έναν αρκετά σαφή τρόπο: οι οργανωτικοί έλεγχοι είναι διαθέσιμοι για κάθε προφίλ κινδύνων (καθορίζονται στον πίνακα προσδιορισμού χαρακτηριστικού προφίλ κινδύνων). Ο παρακάτω πίνακας αναθέτει τους οργανωτικούς ελέγχους στα προφίλ κινδύνων, όπως αναφέρονται στο κεφάλαιο 4.3.1 Φάση 1 – Επιλογή προφίλ κινδύνων. Οι έλεγχοι που παρατίθενται παρακάτω συνιστώνται προκειμένου να μετριάσετε τους αντίστοιχους οργανωτικούς κινδύνους. Στο Παράρτημα Γ. Οργανωτικοί Έλεγχοι περιλαμβάνεται μία λεπτομερής περιγραφή των ελέγχων.

Περιοχές κινδύνων	**Υψηλού Επιπέδου**	**Μεσαίου Επιπέδου**	**Χαμηλού Επιπέδου**
Νομικής και κανονιστικής συμμόρφωσης	(SP1) (SP4)	(SP1) (SP4)	SP1.1
Παραγωγικότητα	(SP3) (SP4) (SP6) (SP5)	(SP4) (SP6)	SP4.1
Οικονομικές απώλειες	(SP2) (SP1) (SP4)	(SP4)	SP4.1
Φήμη και απώλεια εμπιστοσύνης πελατών	(SP1) (SP5)	(SP4) (SP1)	SP4.1

Πίνακας 6: Κάρτες οργανωτικού ελέγχου

Επιλογή καρτών ελέγχου βάσει πόρων

Βάσει του προφίλ κινδύνων και των απαιτήσεων διασφάλισης των πόρων, οι ομάδες αξιολόγησης ΜΜΕ μπορούν να χρησιμοποιούν τον πίνακα καρτών ελέγχου των πόρων (βλ. πίνακα 7) προκειμένου να προσδιορίσουν τους κατάλληλους ελέγχους για την προστασία των κρίσιμων πόρων.

Κάρτες ελέγχου πόρων			
Πόρος	**Κάρτες Υψηλών Κινδύνων**	**Κάρτες Μεσαίων Κινδύνων**	**Κάρτες Χαμηλών Κινδύνων**
Εφαρμογή	**CC-1A**	**CC-2A**	**CC-3A**
Σύστημα	**CC-1S**	**CC-2S**	**CC-3S**
Δίκτυο	**CC-1N**	**CC-2N**	**CC-3N**
Άτομα	**CC-1P**	**CC-2P**	**CC-3P**

Πίνακας 7: Κάρτες ελέγχου πόρων

Οι κάρτες ελέγχου πόρων ομαδοποιούνται κατά κύριο λόγο σε τρεις κατηγορίες, ανάλογα με το προφίλ κινδύνων του οργανισμού, την κατηγορία πόρων και την απαίτηση διασφάλισης. Για παράδειγμα, οι ομάδες αξιολόγησης που αντιμετωπίζουν ένα οργανωτικό προφίλ υψηλών κινδύνων θα έχουν διαφορετικές απαιτήσεις διασφάλισης απ' ότι τα προφίλ μεσαίων και χαμηλών κινδύνων. Κάθε κάρτα ελέγχου περιλαμβάνει έναν αριθμό ελέγχων πόρων (βλέπε Παράρτημα Β. Κάρτες ελέγχου πόρων) προκειμένου να αντιμετωπίσει ολόκληρο το εύρος των κινδύνων και των απαιτήσεων διασφάλισης, όπως απαιτείται στο συγκεκριμένο προφίλ και υπαγορεύεται από τις επιλεγμένες απαιτήσεις διασφάλισης. Στο Παράρτημα Δ, Έλεγχοι βάσει πόρων, μπορεί να βρεθεί μια πιο αναλυτική περιγραφή των ελέγχων που συμπεριλαμβάνονται στις κάρτες ελέγχου.

Χάριν της εν λόγω παρουσίασης, προσθέτουμε, σ' αυτό το σημείο, την κάρτα ελέγχου CC-1A. Όπως φαίνεται στον πίνακα, αυτή η κάρτα είναι κατάλληλη για την προστασία μιας εφαρμογής σε μία εκδοχή υψηλών κινδύνων (προφίλ υψηλών κινδύνων).

Αναγνωριστικό κάρτας ελέγχου βάσει πόρων					**CC-1A**					
Προφίλ Κινδύνων	**Υψηλού επιπέδου**									
Κατηγορία πόρων	**Εφαρμογή**									
Απαιτήσεις διασφάλισης	**Υλική ασφάλεια**	**Διαχείριση συστήματος και δικτύου**	**Εργαλεία Διαχείρισης Συστήματος**	**Παρακολούθηση και έλεγχος ασφάλειας ΤΠ**	**Επαλήθευση και εξουσιοδότηση**	**Διαχείριση ευπάθειας**	**Κρυπτογράφηση**	**Σχεδιασμός και αρχιτεκτονική ασφάλειας**	**Διαχείριση συμβάντων**	**Γενικές πρακτικές προσωπικού**
Εμπιστευτικότητα		2.1.3			2.4.2	2.5.1	2.6.1			
Ακεραιότητα		2.1.4			2.4.2	2.5.1	2.6.1			
Διαθεσιμότητα		2.1.6								

Πίνακας 8: Παράδειγμα κάρτας ελέγχου για τον πόρο εφαρμογή σε προφίλ υψηλών κινδύνων

Οι ομάδες αξιολόγησης, χρησιμοποιώντας τις προηγούμενες προσδιορισμένες απαιτήσεις διασφάλισης και την κάρτα ελέγχου μπορούν, στην συνέχεια, να προσδιορίσουν ειδικότερους ελέγχους (π.χ. τους ελέγχους για διαθεσιμότητα, εμπιστευτικότητα ή ακεραιότητα). Πρέπει να σημειωθεί ότι σε περιπτώσεις όπου επιλέγονται περισσότερες από μία απαιτήσεις, οι έλεγχοι που εφαρμόζονται στον πόρο αποτελούν το άθροισμα των ελέγχων για κάθε απαίτηση.

4.3.4 Φάση 4 – Υλοποίηση και Διαχείριση

Κατά την φάση 4 και βάσει της αξιολογηθέντων πληροφοριών, η ομάδα αξιολόγησης δημιουργεί σχέδια μετριασμού προκειμένου να αντιμετωπίσει τους κινδύνους για τους κρίσιμους πόρους.

Απ' την στιγμή που έχουν προσδιοριστεί: (1) το προφίλ κινδύνων του οργανισμού, (2) οι κρίσιμοι πόροι και (3) οι κάρτες ελέγχου, η ομάδα αξιολόγησης σχεδιάζει την εφαρμογή των επιλεγμένων ελέγχων. Είναι αναμενόμενο ότι λόγω των περιορισμένων μέσων τους, οι ΜΜΕ δεν θα είναι σε θέση να εφαρμόσουν όλους τους καθορισμένους ελέγχους για όλους τους κρίσιμους πόρους μια κι έξω. Από την άποψη αυτή, η ιεράρχηση προτεραιοτήτων αποτελεί βασικό στοιχείο για επιτυχημένες προσπάθειες μετριασμού των κινδύνων.

Ένα σχέδιο υλοποίησης ορίζει τον τρόπο με τον οποίον ένας οργανισμός προτίθεται να αυξήσει ή να διατηρήσει το υφιστάμενο επίπεδο ασφάλειάς του. Στόχος του είναι να παράσχει μια κατεύθυνση για μελλοντικές προσπάθειες σχετικά με την ασφάλεια των πληροφοριών μάλλον παρά να βρει μια άμεση λύση σε κάθε ευπάθεια και μέλημα ασφάλειας.

Παρακάτω, μπορούν να βρεθούν ορισμένα κριτήρια για την ιεράρχηση ενεργειών προκειμένου για την υλοποίηση προσδιορισμένων καρτών ελέγχου. Αν και δεν μπορούν όλες να εφαρμοστούν σε όλες τις εταιρείες, μπορούν, ωστόσο, να χρησιμεύσουν ως γενικός οδηγός:

- **Στρατηγική ευθυγράμμιση με τους στόχους του οργανισμού**: Αυτός ο πόρος υποστηρίζει άμεσα τους στόχους του σχεδίου τεκμηριωμένης οργάνωσης και/ή τομεακής εργασίας; Ποιοι σκοποί και/ή στόχοι του σχεδίου εργασίας θα υποστηριχθούν και με ποιόν τρόπο;
- **Συνεχείς προσπάθειες βελτίωσης**: Ο εν λόγω πόρος υποστηρίζει την προσπάθεια συνεχούς βελτίωσης του πόρου ενός τομέα; Ποιος είναι ο πόρος συνεχούς βελτίωσης; Με ποιόν τρόπο ο εν λόγω πόρος υποστηρίζει σκοπούς συνεχούς βελτίωσης;
- **Νομικές ή κανονιστικές εντολές**: Εφόσον είναι απαραίτητο ένας πόρος να ικανοποιεί κανονιστικές απαιτήσεις, αυτό θα αντικατοπτρίζεται στην ιεράρχηση προτεραιοτήτων.
- **Οφέλη του όλου συστήματος**: Τα οφέλη του όλου συστήματος περιλαμβάνουν βελτιωμένη εξυπηρέτηση πελατών για αρκετές ομάδες πελατών. Θα δοθεί μεγαλύτερη προτεραιότητα στις ομάδες πελατών που θεωρούνται κρίσιμες, αλλά όσο μεγαλύτερη είναι η επηρεαζόμενη ομάδα πελατών τόσο μεγαλύτερο θα είναι το όφελος
- **Εξοικονόμηση κόστους/χρόνου**: Οι εκτιμήσεις εξοικονόμησης κόστους και/ή χρόνου περιλαμβάνουν την δαπάνη χρόνου του προσωπικού, την εξοικονόμηση χρόνου των πελατών, την δημιουργία εσόδων και τις άμεσες μειώσεις προϋπολογισμού/κόστους.
- **Μείωση κινδύνων**: Ως αποτέλεσμα ενός έργου, οι πληροφορίες και/ή οι υπηρεσίες θα αποτρέψουν την απώλεια εσόδων και/ή την μη συμμόρφωση με πολιτικές, νομικές και ελεγκτικές απαιτήσεις.

Το επόμενο στάδιο είναι η διαδικασία σχεδιασμού, που υποδεικνύει και παρακολουθεί το ακριβές χρονοδιάγραμμα των εργαλείων ασφάλειας και την υλοποίηση των διαδικασιών.

Μια βασική ερώτηση, σχεδόν σε κάθε υλοποίηση, είναι αν οι ενδοεπιχειρησιακοί πόροι επαρκούν για να εκπληρώσετε το σχέδιο υλοποίησης. Με άλλα λόγια, ενδεχομένως να είναι απαραίτητη η λήψη απόφασης είτε για την εσωτερική είτε για την εξωτερική ανάθεση της σχετικής εργασίας υλοποίησης και διαχείρισης.

5. Κατευθυντήριες γραμμές αυτοαξιολόγησης με δύο παραδείγματα

Σε αυτό κεφάλαιο, θα παρουσιαστεί μια πιο λεπτομερής ανάλυση των τεσσάρων φάσεων σε λογικά στάδια. Αυτό θα βοηθήσει τις ΜΜΕ: (1) να προσδιορίσουν το προφίλ κινδύνων του οργανισμού τους, (2) να προσδιορίσουν τους κρίσιμους πόρους που είναι ανάγκη να διασφαλιστούν, (3) να επιλέξουν ελέγχους και λύσεις για βελτιωμένη ασφάλεια και, εν τέλει, (4) να αναπτύξουν σχέδια περαιτέρω βελτίωσης. Ωστόσο, ενέργειες και λύσεις που μπορεί να εφαρμοστούν στις ΜΜΕ δεν αφορούν αποκλειστικά και δεν περιορίζονται σε αυτές που παρέχονται στο παρόν.

Για μια ακόμη φορά, οι οργανισμοί ενθαρρύνονται σθεναρά να ακολουθούν τις κατευθυντήριες γραμμές και να τηρούν τις ορθές πρακτικές που συμπεριλαμβάνονται σε αυτήν τη μέθοδο μόνο ως βραχυπρόθεσμο σχέδιο, επιδιώκοντας την γρήγορη και αποτελεσματική προστασία κρίσιμων και καθοριστικών συστατικών στοιχείων των επιχειρήσεών τους. Ωστόσο, η διαδικασία αυτή δεν αντικαθιστά μια ολοκληρωμένη και ενδελεχή προσέγγιση εκτίμησης κινδύνων, η οποία συνίσταται θερμά ως βάση για μια μακροπρόθεσμη στρατηγική διαχείρισης κινδύνων.

Πριν επιχειρήσουμε να χρησιμοποιήσουμε τη μέθοδο, οι ΜΜΕ είναι ανάγκη να κατανοήσουν τις ακόλουθες τρεις μοναδικές πτυχές αυτής της μεθόδου:

- Μια μικρή διεπιστημονική ομάδα ανάλυσης τριών έως πέντε ατόμων διαχειρίζεται την διαδικασία εκτίμησης κινδύνων. Τα μέλη της ομάδας ανάλυσης πρέπει να διαθέτουν, συλλογικά, ευρεία αντίληψη για τις επιχειρηματικές διαδικασίες και τις διαδικασίες ασφάλειας του οργανισμού, σε τέτοιο βαθμό επάρκειας ώστε να είναι σε θέση να διεξάγουν όλες τις δραστηριότητες εκτίμησης κινδύνων. Γι' αυτό το λόγο, η μέθοδος δεν απαιτεί επίσημα εργαστήρια συλλογής δεδομένων για την έναρξη της αξιολόγησης.
- Η μέθοδος περιλαμβάνει μια περιορισμένη διερεύνηση της υποδομής των πληροφορικών συστημάτων. Από τη στιγμή που οι μικροί οργανισμοί συχνά προβαίνουν σε εξωτερική ανάθεση των υπηρεσιών και λειτουργιών ΤΠ που τους αφορούν, κατά κανόνα δεν έχουν αναπτύξει οργανωτικές ικανότητες για τη διαχείριση και την ερμηνεία των αποτελεσμάτων των εργαλείων εκτίμησης ευπάθειας. Ωστόσο, η έλλειψη οργανωτικής ικανότητας για την διαχείριση τέτοιων εργαλείων δεν αποκλείει έναν οργανισμό από τη εδραίωση μιας στρατηγικής για την προστασία των πληροφοριών του.
- Αντί να χρησιμοποιεί δεδομένα ευπάθειας για τη βελτίωση της άποψής του σχετικά με τις τρέχουσες πρακτικές ασφάλειας, ένας οργανισμός που διενεργεί μία αξιολόγηση εξετάζει τις εφαρμοζόμενες διαδικασίες προκειμένου να διαμορφώσει και να διατηρήσει την υποδομή των πληροφορικών συστημάτων του.

Το έγγραφο διαρθρώνεται σε φάσεις και στάδια σύμφωνα με την δομή των οικοδομικών τετραγώνων. Παρέχονται δύο παραδείγματα για κάθε φάση. Τα παραδείγματα χρησιμοποιούν τα παρακάτω εταιρικά σενάρια:

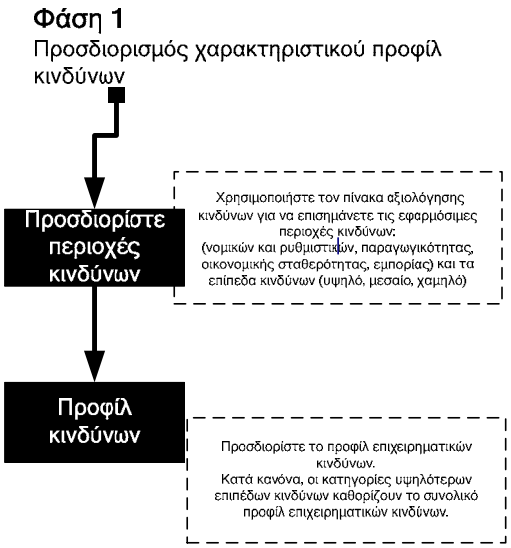
- **Εταιρία στο παράδειγμα Α.** Στο παράδειγμα Α, εξετάζουμε την ειδική περίπτωση μιας μεσαίου μεγέθους εταιρίας, η οποία παρέχει υπηρεσίες υγειονομικής περίθαλψης μέσω ηλεκτρονικής πρόσβασης, παρέχοντας ιατρική υποστήριξη μέσω του διαδικτύου σε γιατρούς που χρειάζονται συμβουλές για τους ασθενείς τους και πληροφορίες σχετικά με πρόσφατες προόδους στην ιατρική. Στο πλαίσιο αυτό, η βάση δεδομένων που υποστηρίζει την εφαρμογή, αποθηκεύει κρίσιμα και εμπιστευτικά δεδομένα προσωπικού χαρακτήρα. Η εταιρεία απασχολεί 100 άτομα και διαθέτει τρία τμήματα, το τμήμα ιατρικής και φαρμακευτικής υποστήριξης, το τμήμα ιατρικής επιστήμης και το τμήμα διαχείρισης, το οποίο περιλαμβάνει δραστηριότητες που αφορούν το ανθρώπινο δυναμικό και τον χρηματοοικονομικό έλεγχο.

- **Εταιρία στο παράδειγμα Β.** Στο παράδειγμα Β, η εταιρεία είναι μία δικηγορική εταιρία μικρού μεγέθους. Σ' αυτήν την περίπτωση, τα συστήματα ΤΠ χρησιμοποιούνται ευρέως για αποθήκευση πληροφοριών σχετικά με τις υποθέσεις της εταιρίας, την ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου, την προετοιμασία και επεξεργασία των απαραίτητων εγγράφων. Η εταιρεία απασχολεί πέντε δικηγόρους και ένα/μία γραμματέα.

Παρέχονται επίσης σχήματα (διαγράμματα ροής εργασίας) για κάθε φάση και υποδείξεις υλοποίησης για κάθε στάδιο στα περιγεγραμμένα με διακοπτόμενες γραμμές πλαίσια για κάθε μία από τις επικείμενες περιγραφές φάσης.

Φάση 1 – Επιλέξτε το Προφίλ Κινδύνων

Η ομάδα ανάλυσης λαμβάνει υπόψη της τις πτυχές επιχειρηματικών κινδύνων που αφορούν στην προστασία πληροφοριών, οι οποίες μπορούν: (α) να επηρεάσουν άμεσα ή έμμεσα ή να βλάψουν τη φήμη και την εμπιστοσύνη των πελατών, (β) να έχουν ως αποτέλεσμα τη νομική και ρυθμιστική μη συμμόρφωση, (γ) να επιφέρουν οικονομική απώλεια και (δ) να μειώσουν την παραγωγικότητα. Η ομάδα, στην συνέχεια, επιλέγει το κατάλληλο επίπεδο κινδύνων για κάθε περιοχή κινδύνων με τη χρήση ενός πίνακα αξιολόγησης προφίλ κινδύνων. Οι συγκεκριμένες περιοχές είναι οι ακόλουθες: νομικών και ρυθμιστικών κινδύνων, κινδύνων για την παραγωγικότητα, την οικονομική σταθερότητα, την φήμη και απώλεια εμπιστοσύνης πελατών. Όπως παρουσιάζεται στο σχήμα 3, η φάση περιλαμβάνει δύο στάδια.



Σχήμα 3: Φάση 1 – Ροή εργασίας επιλογής προφίλ κινδύνων

Για τον προσδιορισμό του τρέχοντος ή πιθανού επιπέδου κινδύνων, τα μέλη της ομάδας ανάλυσης πρέπει να επισημάνουν την περιοχή κινδύνων και να διαβάσουν την περιγραφή σε κάθε στήλη. Επιλέγονται οι περιοχές κινδύνων που είναι πιο κοντά στο προφίλ της επιχείρησής τους. Η διαδικασία ακολουθείται για κάθε περιοχή κινδύνων. Στο τέλος, πρέπει να υπάρχει ένας ΠΙΝΑΚΑΣ που επισημαίνει το εφαρμόσιμο επίπεδο κινδύνου σε κάθε περιοχή κινδύνων.

Παράδειγμα Α. (Προφίλ Υψηλών Κινδύνων)

Στο παράδειγμα Α, η ομάδα χρησιμοποιεί τον **πίνακα αξιολόγησης προφίλ κινδύνων** προκειμένου να προσδιορίσει το γενικό πλαίσιο κινδύνων της εταιρίας. Μ' αυτόν τον τρόπο, η ομάδα προσδιορίζει ένα επίπεδο υψηλών κινδύνων (που επισημαίνεται με κόκκινο χρώμα) στην περιοχή νομικών και ρυθμιστικών κινδύνων εφόσον η επιχείρηση χειρίζεται πληροφορίες ευαίσθητης και προσωπικής φύσεως. Ταυτόχρονα, διαπιστώνει επίπεδο υψηλών κινδύνων στην παραγωγικότητα εφόσον απασχολεί 100 άτομα, ένα επίπεδο μεσαίων κινδύνων (που επισημαίνεται με πορτοκαλί χρώμα) στην οικονομική σταθερότητα και ένα επίπεδο χαμηλών κινδύνων (σημειώνεται με μπλε) στη φήμη και την απώλεια εμπιστοσύνης πελατών, όπως παρουσιάζεται στον ακόλουθο πίνακα αξιολόγησης προφίλ κινδύνων.

Περιοχές κινδύνων	Υψηλού Επιπέδου	Μεσαίου Επιπέδου	Χαμηλού Επιπέδου
Νομικών και ρυθμιστικών	**Η επιχείρηση χειρίζεται πληροφορίες ευαίσθητης και προσωπικής φύσεως των πελατών συμπεριλαμβανομένων των ιατρικών δεδομένων και των προσωπικών δεδομένων κρίσιμης σημασίας όπως ορίζεται στην νομοθεσία της ΕΕ περί προστασίας των δεδομένων.**	Η επιχείρηση χειρίζεται τις πληροφορίες προσωπικής αλλά όχι ευαίσθητης φύσεως των πελατών όπως ορίζεται στην νομοθεσία της ΕΕ περί προστασίας των δεδομένων.	Η επιχείρηση δεν χειρίζεται δεδομένα προσωπικού χαρακτήρα εκτός από εκείνα των ατόμων που απασχολούνται σε αυτόν.
Παραγωγι-κότητας	**Η επιχείρηση απασχολεί περισσότερους από 100 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.**	Η επιχείρηση απασχολεί περισσότερους από 50 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.	Η επιχείρηση απασχολεί λιγότερους από 10 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.
Οικονομικής σταθερότητας	Τα ετήσια έσοδα υπερβαίνουν τα 25 εκατ. ευρώ ή/και οι οικονομικές συναλλαγές με τρίτους ή πελάτες λαμβάνουν χώρα ως τμήμα της επιχειρηματικής δραστηριότητας ως συνήθης διαδικασία.	**Τα ετήσια έσοδα του οργανισμού δεν υπερβαίνουν τα 25 εκατ. ευρώ.**	Τα ετήσια έσοδα του οργανισμού δεν υπερβαίνουν τα 5 εκατ. ευρώ.
Φήμης και απώλειας εμπιστοσύ-νης πελατών	Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών έχουν άμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού ή/και πάνω από το 70% της βάσης πελατών έχουν ηλεκτρονική πρόσβαση σε προϊόντα και υπηρεσίες της επιχείρησης.	Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών έχουν έμμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού και/ή κάτω του 5% της βάσης πελατών έχουν ηλεκτρονική πρόσβαση σε προϊόντα και υπηρεσίες της επιχείρησης.	**Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών δεν έχουν άμεση ή έμμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού ή καταλήγουν σε απώλεια εσόδων.**

Πίνακας 9: Πίνακας αξιολόγησης προφίλ κινδύνων - Παράδειγμα Α

Κατόπιν, υπολογίζεται το προφίλ επιχειρηματικών κινδύνων. Οι περιοχές κινδύνων εκφράζουν ολόκληρο το συνολικό πλαίσιο επιχειρηματικών κινδύνων. **Συνίσταται ότι το προφίλ κινδύνων πρέπει να ισοδυναμεί με το υψηλότερο επίπεδο που έχει προσδιοριστεί στις δευτερεύουσες περιοχές κινδύνων στον πίνακα κινδύνων.**

Ο παρακάτω πίνακας απεικονίζει τα επίπεδα προσδιορισμένων κινδύνων στις προκαθορισμένες περιοχές κινδύνων και δείχνει πού πρέπει να επικεντρώσει τις προσπάθειές του ο οργανισμός για την εφαρμογή των κατάλληλων ελέγχων ασφάλειας. Ο πίνακας μπορεί να χρησιμοποιηθεί επίσης για την ιεράρχηση προτεραιοτήτων. Τα υψηλά επίπεδα κινδύνων υποδεικνύουν την επιτακτική ανάγκη για βελτίωση ενώ τα χαμηλά επίπεδα κινδύνων υπογραμμίζουν τις ενέργειες που πρέπει να ληφθούν υπόψη για μελλοντική βελτίωση.

Περιοχές κινδύνων	Επίπεδο κινδύνων	Προφίλ κινδύνων
Νομικών και ρυθμιστικών	**Υψηλό**	**Υψηλό**
Παραγωγικότητας	**Υψηλό**	
Οικονομικής σταθερότητας	**Μεσαίο**	
Φήμης και απώλειας εμπιστοσύνης πελατών	**Χαμηλό**	

Πίνακας 10: Προφίλ κινδύνων οργανισμού – παράδειγμα Α

Παράδειγμα Β. (Προφίλ Μεσαίων Κινδύνων)

Στο παράδειγμα Β, η ομάδα χρησιμοποιεί τον **Πίνακα Αξιολόγησης Προφίλ Κινδύνων** για την αναγνώριση του περιβάλλοντος κινδύνων της εταιρείας. Η ομάδα ανάλυσης ενεργεί αναγνωρίζοντας ένα χαμηλό επίπεδο κινδύνων (σημειώνεται με μπλε) στην νομική και ρυθμιστική περιοχή εφόσον η εταιρεία δεν χειρίζεται προσωπικά δεδομένα εκτός από εκείνα των υπαλλήλων του οργανισμού, ένα χαμηλό επίπεδο κινδύνων στην παραγωγικότητα (σημειώνεται με μπλε), ένα χαμηλό επίπεδο κινδύνων (σημειώνεται με μπλε) στην οικονομική σταθερότητα και ένα μεσαίο επίπεδο κινδύνων (σημειώνεται με πορτοκαλί) στην φήμη και την απώλεια εμπιστοσύνης πελατών, όπως παρουσιάζεται στον παρακάτω πίνακα αξιολόγησης προφίλ κινδύνων.

Περιοχές Κινδύνων	Υψηλού επιπέδου	Μεσαίου επιπέδου	Χαμηλού επιπέδου
Νομικής και κανονιστικής συμμόρφωσης	Η επιχείρηση χειρίζεται πληροφορίες ευαίσθητης και προσωπικής φύσεως των πελατών συμπεριλαμβανομένων των ιατρικών δεδομένων και των προσωπικών δεδομένων κρίσιμης σημασίας όπως ορίζεται στην νομοθεσία της ΕΕ περί προστασίας των δεδομένων.	Η επιχείρηση χειρίζεται τις πληροφορίες προσωπικής αλλά όχι ευαίσθητης φύσεως των πελατών όπως ορίζεται στην νομοθεσία της ΕΕ περί προστασίας των δεδομένων.	**Η επιχείρηση Δεν χειρίζεται δεδομένα προσωπικού χαρακτήρα εκτός από εκείνα των ατόμων που απασχολούνται σε αυτόν.**
Παραγωγικότητα	Η επιχείρηση απασχολεί περισσότερους από 100 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.	Η επιχείρηση απασχολεί περισσότερους από 50 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.	**Η επιχείρηση απασχολεί λιγότερους από 10 εργαζόμενους, οι οποίοι είναι υποχρεωμένοι καθημερινά να έχουν πρόσβαση σε εφαρμογές και υπηρεσίες της επιχείρησης.**
Οικονομική σταθερότητα	Τα ετήσια έσοδα του οργανισμού υπερβαίνουν τα 25 εκατ. ευρώ ή/και οι οικονομικές συναλλαγές με τρίτους ή πελάτες λαμβάνουν χώρα ως τμήμα της επιχειρηματικής δραστηριότητας ως συνήθης διαδικασία.	Τα ετήσια έσοδα δεν υπερβαίνουν τα 25 εκατ. ευρώ.	**Τα ετήσια έσοδα δεν υπερβαίνουν τα 5 εκατ. ευρώ.**
Φήμη και απώλεια εμπιστοσύνης πελατών	Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών έχουν άμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού ή/και πάνω από το 70% της βάσης πελατών έχουν ηλεκτρονική πρόσβαση σε προϊόντα και υπηρεσίες της επιχείρησης.	**Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών έχουν έμμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού και/ή κάτω του 5% της βάσης πελατών έχουν ηλεκτρονική πρόσβαση σε προϊόντα και υπηρεσίες της επιχείρησης.**	Η μη διαθεσιμότητα ή η ποιότητα των υπηρεσιών δεν έχουν άμεση ή έμμεση επίδραση στις επιχειρηματικές δραστηριότητες του οργανισμού ή καταλήγουν σε απώλεια εσόδων.

Πίνακας 11:Πίνακας αξιολόγησης προφίλ κινδύνων - Παράδειγμα Β

Κατόπιν, υπολογίζεται το προφίλ επιχειρηματικών κινδύνων. Οι περιοχές κινδύνων εκφράζουν ολόκληρο το συνολικό πλαίσιο επιχειρηματικών κινδύνων. **Συνίσταται ότι το προφίλ κινδύνων πρέπει να ισοδυναμεί με το υψηλότερο επίπεδο που έχει προσδιοριστεί στις δευτερεύουσες περιοχές κινδύνων στον πίνακα κινδύνων.**

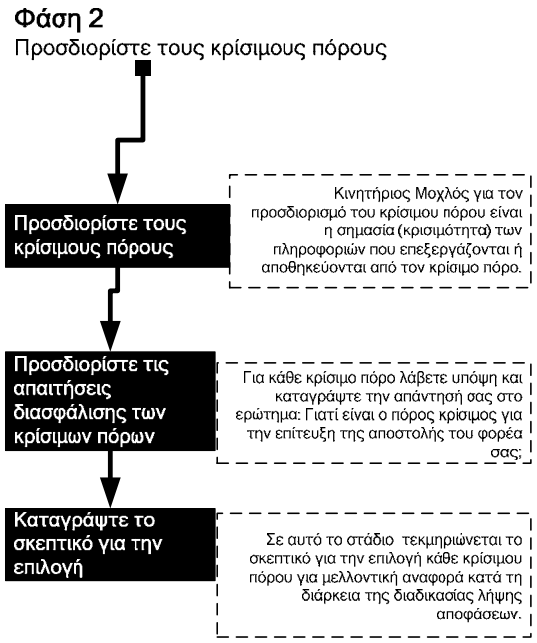
Ο παρακάτω πίνακας απεικονίζει τα επίπεδα προσδιορισμένων κινδύνων στις προκαθορισμένες περιοχές κινδύνων και δείχνει που πρέπει να επικεντρώσει τις προσπάθειές του ο οργανισμός για την εφαρμογή των κατάλληλων ελέγχων ασφάλειας. Ο πίνακας μπορεί να χρησιμοποιηθεί επίσης για την ιεράρχηση προτεραιοτήτων. Τα υψηλά επίπεδα κινδύνων υποδεικνύουν την επιτακτική ανάγκη για βελτίωση ενώ τα χαμηλά επίπεδα κινδύνων μπορούν να θεωρηθούν ως μια παρατήρηση ασφάλειας, που πρέπει να ληφθεί υπόψη για μελλοντική βελτίωση.

Περιοχές κινδύνων	Επίπεδο κινδύνων	Προφίλ κινδύνων
Νομικών και ρυθμιστικών	Χαμηλό	Μεσαίο
Παραγωγικότητας	Χαμηλό	
Οικονομική σταθερότητας	Χαμηλό	
Φήμης και απώλειας εμπιστοσύνης πελατών	Μεσαίο	

Πίνακας 12: Προφίλ κινδύνων Οργανισμού – Παράδειγμα Β

Φάση 2 - Προσδιορίστε τους κρίσιμους πόρους

Η Φάση 2 απαιτεί αποφάσεις που διαμορφώνουν τα δευτερεύοντα στοιχεία της αξιολόγησης— την διαδικασία επιλογή των κρίσιμων πόρων της επιχείρησης. Ανάλογα με το μέγεθος του φορέα, ο αριθμός των πόρων πληροφοριών που προσδιορίζονται κατά την διάρκεια αυτής της φάσης, θα μπορούσε να υπερβεί μ' ευκολία τους εκατό. Προκειμένου να καταστεί διαχειρίσιμη η ανάλυση, οι ΜΜΕ είναι ανάγκη να περιορίζουν το επίκεντρο της αξιολόγησης, επιλέγοντας μικρό αριθμό πόρων που είναι οι πλέον κρίσιμοι για την επίτευξη της αποστολής και την κάλυψη των επιχειρηματικών στόχων του φορέα. Αυτοί είναι οι μόνοι πόροι που θα αναλυθούν κατά τις μετέπειτα δραστηριότητες. Όπως απεικονίζεται στο σχήμα 4, η φάση αυτή περιλαμβάνει τρία στάδια.



Σχήμα 4: Φάση 2 – Προσδιορισμός ροής εργασίας των κρίσιμων πόρων

Στάδιο 1. Επιλέξτε τους πέντε κρισιμότερους πόρους του οργανισμού σας

Όταν επιλέγονται κρίσιμοι πόροι, οι ομάδες δεν περιορίζονται στο να επιλέξουν μόνο πέντε. Κανονικά, πέντε πόροι είναι αρκετοί για να δώσουν την δυνατότητα στους φορείς να αναπτύξουν ένα ικανοποιητικό σύνολο σχεδίων μετριασμού κατά την διάρκεια της φάσης 4. Ωστόσο, τα μέλη της ομάδας ανάλυσης πρέπει να χρησιμοποιούν την κρίση τους για το εάν θα χρησιμοποιήσουν περισσότερους ή λιγότερους από πέντε. Κατά την διάρκεια της διαδικασίας επιλογής των κρίσιμων πόρων, τα μέλη της ομάδας πρέπει να εξετάσουν ποιοι πόροι θα έχουν δυσμενή επίδραση στον φορέα, σ' ένα από τα ακόλουθα σενάρια:

- **Δημοσιοποίηση** πληροφοριών σε μη εξουσιοδοτημένα άτομα

- **Τροποποίηση** των πληροφοριών χωρίς εξουσιοδότηση
- **Απώλεια ή καταστροφή** του πόρου
- **Διακοπτόμενη πρόσβαση** στον πόρο ή τις αποθηκευμένες πληροφορίες

Σε περιπτώσεις όπου οι κρίσιμοι πόροι είναι δύσκολο να προσδιοριστούν, οι ομάδες πρέπει να λάβουν υπόψη τους τις επιχειρηματικές λειτουργίες/τομείς εντός του οργανισμού. Αυτές μπορεί να είναι διαφορετικά έργα, ομάδες εργασίας (ομάδες ατόμων με διαφορετική περιγραφή εργασίας) ή ακόμα και ξεχωριστά οργανωτικά τμήματα (τμήμα ανθρώπινου δυναμικού, λογιστικό τμήμα, τμήμα εμπορίας, τμήμα πωλήσεων κτλ.). Στην συνέχεια, αυτοί οι πόροι πρέπει να συνταχθούν υπό την μορφή καταλόγου κατά επίπεδο σημασίας στην επιχειρηματική διαδικασία. Αφού προσδιοριστούν οι τομείς που απαιτούν διασφάλιση ή αναδιοργανωθούν οι πόροι του φορέα, το επόμενο στάδιο είναι να συνταχθούν υπό την μορφή καταλόγου όλοι οι πόροι σύμφωνα με τον αντίκτυπό τους στην επιχειρηματική διαδικασία. Ένας πιο εφικτός τρόπος για να πραγματοποιηθεί αυτό, είναι να ομαδοποιήσουμε τους πόρους κατά τμήμα ή λειτουργία οργανωτικής δομής.

Ο κινητήριος μοχλός κατά τον προσδιορισμό των κρίσιμων πόρων είναι η βαρύτητα (κρισιμότητα) των πληροφοριών που επεξεργάζονται ή αποθηκεύονται από αυτόν. Μέσα από την διεξαγωγή της ανάλυσης διάσπασης, τα μέλη της ομάδας μπορούν εύκολα να προσδιορίσουν που και πως αποθηκεύονται ή χρησιμοποιούνται οι κρίσιμες πληροφορίες.

Στάδιο 2. Καταγράψτε το σκεπτικό για την επιλογή κάθε κρίσιμου πόρου

Ενώ επιλέγουμε τους κρίσιμους πόρους στο στάδιο 1, αναλύεται ένας αριθμός ζητημάτων που σχετίζονται με αυτούς τους πόρους. Σ' αυτό το στάδιο, το σκεπτικό για την επιλογή καθενός κρίσιμου πόρου τεκμηριώνεται για μελλοντική παραπομπή κατά την διαδικασία λήψης αποφάσεων. Επιπρόσθετα, κατανοώντας γιατί ένας πόρος είναι κρίσιμος μπορεί να επιτρέψει ευκολότερα τον ορισμό των απαιτήσεων διασφάλισης κατά το επόμενο στάδιο. Για κάθε κρίσιμο πόρο, οι ακόλουθες ερωτήσεις πρέπει να ληφθούν υπόψη και οι απαντήσεις να καταχωρίζονται:

- Γιατί είναι κρίσιμος ο πόρος για την επίτευξη της αποστολής του οργανισμού;
- Ποιος έχει τον έλεγχό του;
- Ποιος είναι υπεύθυνος γι' αυτόν;
- Ποιος τον χρησιμοποιεί;
- Πώς χρησιμοποιείται;

Αυτές οι ερωτήσεις επικεντρώνονται στον τρόπο με τον οποίο χρησιμοποιούνται οι πόροι και στο γιατί είναι σημαντικοί. Αν δεν παρέχονται απαντήσεις σ' όλα αυτά τα ερωτήματα, πρέπει να εντοπιστούν και να συμπεριληφθούν στην ομάδα ανάλυσης άτομα εκείνα του οργανισμού που μπορούν να παράσχουν τις απαντήσεις. Οι πληροφορίες που εξάγονται από τις απαντήσεις σε αυτά τα ερωτήματα θα είναι χρήσιμες αργότερα σ' αυτή την διαδικασία. Από αυτή την άποψη, οι πληροφορίες που συγκεντρώνονται σε αυτό το στάδιο πρέπει να καταχωρίζονται προσεκτικά.

Στάδιο 3. Αναγνωρίστε τις απαιτήσεις διασφάλισης ενός κρίσιμου πόρου

Γενικά, όταν περιγράφουμε μια απαίτηση διασφάλισης για έναν πόρο, απαιτείται να κατανοηθεί ποια πτυχή του πόρου είναι σημαντική. Για πόρους πληροφοριών, οι απαιτήσεις διασφάλισης θα επικεντρωθούν στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών.

Οι απαιτήσεις διασφάλισης μπορούν να ποικίλουν για διαφορετικές κατηγορίες πόρων στο πλαίσιο μιας ΜΜΕ, αλλά η προσεκτική επιλογή απαιτήσεων είναι ζωτικής σημασίας για την εργασία επιλογής ελέγχων που ακολουθεί. Με άλλα λόγια, οι απαιτήσεις υψηλής διαθεσιμότητας απαιτούν ελέγχους υψηλής διαθεσιμότητας κτλ.

Οι ομάδες ανάλυσης χρησιμοποιούν τα παρεχόμενα **κριτήρια επιλογής απαιτήσεων** προκειμένου να προσδιορίσουν τις πιο σημαντικές απαιτήσεις διασφάλισης. **Οι απαιτήσεις διασφάλισης των πόρων**

θα χρησιμοποιηθούν αργότερα κατά την επιλογή καρτών ελέγχου πόρων. Τα κριτήρια αξιολόγησης των απαιτήσεων διασφάλισης έχουν αναπτυχθεί ως ένας απλός και πρακτικός οδηγός για την αξιολόγηση των απαιτήσεων διασφάλισης όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των επιλεγμένων κρίσιμων πόρων. Η αξιολόγηση υπογραμμίζει την σημασία των χαρακτηριστικών διασφάλισης των πόρων και υποδεικνύει τους κατάλληλους ελέγχους για την προστασία τους.

Ως αποτέλεσμα αυτής της διαδικασίας, οι ομάδες ανάλυσης πρέπει να διαθέτουν **έναν πίνακα υπό τη μορφή καταλόγου κρίσιμων πόρων παράλληλα με μια σύντομη περιγραφή της σημασίας τους για την επίτευξη της επιχειρηματικής αποστολής της επιχείρησης, τα βασικά στοιχεία της και τις απαιτήσεις διασφάλισης**.

Για όλα, και τα τρία στάδια που αναλύθηκαν παραπάνω, μπορούν να χρησιμοποιηθούν οι πίνακες της ενότητας 4.3.2 για τον προσδιορισμό των συναφών πόρων και των απαιτήσεών τους (βλέπε Πίνακας 3 και Πίνακας 4).

Παράδειγμα Α. (Προφίλ κινδύνων: υψηλού επιπέδου, κρίσιμος πόρος: εφαρμογή - Φάση 2.)

[Στάδιο 1] Στο παράδειγμα Α, η Εφαρμογή Ιστού αναγνωρίζεται ως ο κρισιμότερος πόρος, που παρέχει ηλεκτρονική υποστήριξη στους πελάτες – τους γιατρούς. Η εν λόγω εφαρμογή είναι ουσιώδης για την επιχείρηση, καθώς αντιπροσωπεύει το πλέον σημαντικό στοιχείο των παρεχόμενων υπηρεσιών και επομένως, επιλέγεται ως ο κρισιμότερος πόρος.

[Στάδιο 2] Στο επόμενο στάδιο, τα μέλη της ομάδας τεκμηριώνουν τα στοιχεία που συνιστούν τον πόρο και το σκεπτικό για την επιλογή τους. Με αυτόν τον τρόπο, εν τέλει προσδιορίζουν την Βάση Δεδομένων που αποθηκεύει τις πληροφορίες των πελατών, το τμήμα δικτύου που υποστηρίζει την συνδεσιμότητα με εσωτερικά και εξωτερικά δίκτυα, τον εξυπερετητή ιστού και τους τοίχους προστασίας ως βασικά συστατικά στοιχεία του πόρου.

[Στάδιο 3] Στη συνέχεια, προσδιορίζονται οι απαιτήσεις διασφάλισης. Χρησιμοποιώντας τον ακόλουθο πίνακα (Πίνακας 13), οι ομάδες αναγνωρίζουν τα πλαίσια που προσαρμόζονται στις απαιτήσεις τους. Στο παράδειγμα Α, η ομάδα επιλέγει να έχει η βάση δεδομένων απαιτήσεις εμπιστευτικότητας εφόσον τα αποθηκευμένα δεδομένα αφορούν τους πελάτες της εταιρείας. Επιλέγουν το δίκτυο να έχει απαιτήσεις διαθεσιμότητας και εμπιστευτικότητας, εφόσον το δίκτυο μεταδίδει πληροφορίες που πρέπει να παραμείνουν άθικτες και απόρρητες για την ολοκλήρωση των συναλλαγών ή της παροχής ενημέρωσης.

Πόροι	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Συστήματα	Ένα σύστημα με απαιτήσεις εμπιστευτικότητας συχνά χειρίζεται εταιρικές πληροφορίες (έρευνας και ανάπτυξης) χαρακτηρισμένες ως ιδιόκτητες, πληροφορίες βάσης πελατών, ευαίσθητα δεδομένα πελατών ιατρικής ή προσωπικής φύσεως.	Συστήματα με απαιτήσεις ακεραιότητας κατά κανόνα χειρίζονται συναλλαγές χρηματοοικονομικής φύσεως, την προμήθεια αγαθών ή το ηλεκτρονικό εμπόριο.	Οι απαιτήσεις διαθεσιμότητας ικανοποιούνται σε συστήματα που είναι ζωτικής σημασίας για καθημερινές επιχειρηματικές λειτουργίες και όπου ο χρόνος διακοπής λειτουργίας επισύρει συνήθως δαπάνες και έμμεσα έξοδα όσον αφορά την κατανομή των πόρων.
Δίκτυο	Ένα δίκτυο με απαιτήσεις εμπιστευτικότητας κατά κανόνα καλύπτει τις επικοινωνίες και την ανταλλαγή πληροφοριών σε μη ασφαλή και μη έμπιστα περιβάλλοντα.	Οι απαιτήσεις ακεραιότητας δικτύου είναι κατά κανόνα απαραίτητες όταν οι συναλλαγές λαμβάνουν χώρα σε δημόσια και διαμοιρασμένα μητροπολιτικά δίκτυα ή σε παρόχους τηλεπικοινωνιακών υπηρεσιών.	Οι απαιτήσεις διαθεσιμότητας είναι ιδιαιτέρως απαραίτητες όταν το δίκτυο χρησιμοποιείται ως τμήμα της εξυπηρέτησης πελατών ή για την παροχή υπηρεσιών και την διάθεση προϊόντων.
Άνθρωποι	Οι απαιτήσεις εμπιστευτικότητας ικανοποιούνται κατά κανόνα όταν οι άνθρωποι χειρίζονται οργανωτικές ιδιόκτητες και απόρρητες πληροφορίες οι οποίες όταν δημοσιοποιηθούν μπορούν να προκαλέσουν βλάβη στο εμπορικό σήμα και στην βάση πελατών του οργανισμού.	Οι απαιτήσεις ακεραιότητας, όταν αφορούν ανθρώπους, επιλαμβάνονται κοινών μυστικών όπως κλείδες κρυπτογράφησης ή συνθηματικά. Η γνώση αυτών των στοιχείων εισάγει απειλές, που οφείλονται στον ανθρώπινο παράγοντα, και πρέπει να αντιμετωπιστούν με ανάλογους ελέγχους.	Οι απαιτήσεις διαθεσιμότητας για ανθρώπινους πόρους είναι ιδιαίτερα σημαντικές όταν αυτοί οι άνθρωποι αποτελούν κρίσιμους πόρους για συνεχείς λειτουργίες που αφορούν στην παροχή υπηρεσιών και την διάθεση προϊόντων.

Εφαρμογές	**Οι εφαρμογές με απαιτήσεις εμπιστευτικότητας συχνά χειρίζονται εταιρικές πληροφορίες (έρευνας και ανάπτυξης) χαρακτηρισμένες ως ιδιόκτητες, πληροφορίες βάσης πελατών, ευαίσθητα δεδομένα πελατών ιατρικής ή προσωπικής φύσεως.**	**Οι εφαρμογές με απαιτήσεις ακεραιότητας κατά κανόνα χειρίζονται συναλλαγές χρηματοοικονομικής φύσεως, την προμήθεια αγαθών ή το ηλεκτρονικό εμπόριο.**	**Οι απαιτήσεις διαθεσιμότητας ικανοποιούνται σε εφαρμογές που είναι ζωτικής σημασίας για καθημερινές επιχειρηματικές λειτουργίες και όπου ο χρόνος διακοπής λειτουργίας επισύρει συνήθως δαπάνες και έμμεσα έξοδα όσον αφορά στην κατανομή των πόρων.**

Πίνακας 13:Πίνακας επιλογής απαιτήσεων διασφάλισης – Παράδειγμα Α

Ως αποτέλεσμα της εν λόγω διαδικασίας, οι ομάδες ανάλυσης τεκμηριώνουν και συντάσσουν έναν πίνακα με τους κρίσιμους πόρους, υπό τη μορφή καταλόγου παράλληλα με το σκεπτικό για την επιλογή, τα βασικά στοιχεία του σκεπτικού και τις απαιτήσεις διασφάλισης για τις παρεχόμενες υπηρεσίες. Ο παρακάτω πίνακας περιέχει τα αποτελέσματα του παραδείγματος Α για την Φάση 1 (βλέπε Πίνακα 14).

Κρίσιμος πόρος	Κατηγορία πόρου	Συστατικά μέρη	Απαιτήσεις διασφάλισης	Σκεπτικό επιλογής
Εφαρμογή ηλεκτρονικού εμπορίου	Εφαρμογή	Βάση δεδομένων Τοίχος προστασίας Τμήμα Δικτύου Διακομιστής	**Εμπιστευτικότητα** **Ακεραιότητα** **Διαθεσιμότητα**	Η εφαρμογή είναι ουσιώδης για την επιχείρηση, καθώς αντιπροσωπεύει το πιο σημαντικό στοιχείο της παροχής υπηρεσιών.

Πίνακας 14: Σκεπτικό απαιτήσεων διασφάλισης

Παράδειγμα Β. (Προφίλ κινδύνων: μεσαίου επιπέδου, κρίσιμος πόρος: σύστημα - Φάση 2.)

[Στάδιο 1] Στο παράδειγμα Β, οι σταθμοί εργασίας αναγνωρίζονται ως ο κρισιμότερος πόρος που χρησιμοποιείται για την άσκηση καθημερινών δραστηριοτήτων συμπεριλαμβανομένης της αλληλογραφίας με τους πελάτες, τις πληροφορίες που σχετίζονται με υποθέσεις των πελατών και των βασικών λογιστικών πληροφοριών όσον αφορά στην τιμολόγηση και στους εισπρακτέους λογαριασμούς.

[Στάδιο 2] Στο επόμενο στάδιο, τα μέλη της ομάδας τεκμηριώνουν τα στοιχεία που συνιστούν τον πόρο και το σκεπτικό για την επιλογή τους. Ως εκ τούτου, προσδιορίζουν τέσσερους σταθμούς εργασίας, το εσωτερικό δίκτυο και τον διακομιστή αρχείων.

[Στάδιο 3] Στη συνέχεια, προσδιορίζονται οι απαιτήσεις διασφάλισης. Χρησιμοποιώντας τον ακόλουθο πίνακα, οι ομάδες αναγνωρίζουν τα πλαίσια τα οποία προσαρμόζονται στις απαιτήσεις τους. Στο παράδειγμα Β, η ομάδα επιλέγει τους σταθμούς εργασίας με τις απαιτήσεις διαθεσιμότητας όπως εκείνους που χρησιμοποιούνται για τις καθημερινές επιχειρηματικές δραστηριότητες και που, πρέπει, επομένως, να παραμένουν λειτουργικοί.

Κρίσιμοι πόροι	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Συστήματα	Ένα σύστημα με απαιτήσεις εμπιστευτικότητας συχνά χειρίζεται εταιρικές πληροφορίες (έρευνας και ανάπτυξης) χαρακτηρισμένες ως	Συστήματα με απαιτήσεις ακεραιότητας κατά κανόνα χειρίζονται συναλλαγές χρηματοοικονομικής φύσεως, την προμήθεια αγαθών ή το	**Οι απαιτήσεις διαθεσιμότητας ικανοποιούνται σε συστήματα που είναι ζωτικής σημασίας για**

	ιδιόκτητες, πληροφορίες βάσης πελατών, ευαίσθητα δεδομένα πελατών ιατρικής ή προσωπικής φύσεως.	ηλεκτρονικό εμπόριο.	**καθημερινές επιχειρηματικές λειτουργίες και όπου ο χρόνος διακοπής λειτουργίας επισύρει συνήθως δαπάνες και έμμεσα έξοδα όσον αφορά την κατανομή των πόρων.**
Δίκτυο	Ένα δίκτυο με απαιτήσεις εμπιστευτικότητας κατά κανόνα καλύπτει τις επικοινωνίες και την ανταλλαγή πληροφοριών σε μη ασφαλή και μη έμπιστα περιβάλλοντα.	Οι απαιτήσεις ακεραιότητας δικτύου είναι κατά κανόνα απαραίτητες όταν οι συναλλαγές λαμβάνουν χώρα σε δημόσια και διαμοιρασμένα μητροπολιτικά δίκτυα ή σε παρόχους τηλεπικοινωνιακών υπηρεσιών.	Οι απαιτήσεις διαθεσιμότητας είναι ιδιαιτέρως απαραίτητες όταν το δίκτυο χρησιμοποιείται ως τμήμα της εξυπηρέτησης πελατών ή για την παροχή υπηρεσιών και την διάθεση προϊόντων.
Άνθρωποι	Οι απαιτήσεις εμπιστευτικότητας ικανοποιούνται κατά κανόνα όταν οι άνθρωποι χειρίζονται οργανωτικές ιδιόκτητες και απόρρητες πληροφορίες οι οποίες όταν δημοσιοποιηθούν μπορούν να προκαλέσουν βλάβη στο εμπορικό σήμα και στην βάση πελατών του οργανισμού.	Οι απαιτήσεις ακεραιότητας, όταν αφορούν ανθρώπους, επιλαμβάνονται κοινών μυστικών όπως κλείδες κρυπτογράφησης ή συνθηματικά. Η γνώση αυτών των στοιχείων εισάγει απειλές, που οφείλονται στον ανθρώπινο παράγοντα, και πρέπει να αντιμετωπιστούν με ανάλογους ελέγχους.	Οι απαιτήσεις διαθεσιμότητας για ανθρώπινους πόρους είναι ιδιαίτερα σημαντικές όταν αυτοί οι άνθρωποι αποτελούν κρίσιμους πόρους για συνεχείς λειτουργίες που αφορούν στην παροχή υπηρεσιών και την διάθεση προϊόντων.
Εφαρμογές	Οι εφαρμογές με απαιτήσεις εμπιστευτικότητας συχνά χειρίζονται εταιρικές πληροφορίες (έρευνας και ανάπτυξης) χαρακτηρισμένες ως ιδιόκτητες, πληροφορίες βάσης πελατών, ευαίσθητα δεδομένα πελατών ιατρικής ή προσωπικής φύσεως.	Οι εφαρμογές με απαιτήσεις ακεραιότητας κατά κανόνα χειρίζονται συναλλαγές χρηματοοικονομικής φύσεως, την προμήθεια αγαθών ή το ηλεκτρονικό εμπόριο.	Οι απαιτήσεις διαθεσιμότητας ικανοποιούνται σε εφαρμογές που είναι ζωτικής σημασίας για καθημερινές επιχειρηματικές λειτουργίες και όπου ο χρόνος διακοπής λειτουργίας επισύρει συνήθως δαπάνες και έμμεσα έξοδα όσον αφορά στην κατανομή των πόρων.

Πίνακας 15: Πίνακας επιλογής απαιτήσεων διασφάλισης – Παράδειγμα Β

Ως αποτέλεσμα της εν λόγω διαδικασίας, οι ομάδες ανάλυσης τεκμηριώνουν και συντάσσουν έναν πίνακα με τους κρίσιμους πόρους, υπό τη μορφή καταλόγου, παράλληλα με το σκεπτικό επιλογής, τα βασικά στοιχεία του σκεπτικού και τις απαιτήσεις διασφάλισης για τις παρεχόμενες υπηρεσίες. Ο παρακάτω πίνακας περιέχει τα αποτελέσματα του παραδείγματος Β για την Φάση 3 (Πίνακας 16).

Κρίσιμος πόρος	Τύπος πόρου	Συστατικά μέρη	Απαιτήσεις διασφάλισης	Σκεπτικό επιλογής
Σταθμοί εργασίας	**Σύστημα**	**4 Σταθμοί εργασίας** **Τμήμα δικτύου** **Διακομιστής**	**Διαθεσιμότητα**	**Οι σταθμοί εργασίας είναι σημαντικοί για την εκτέλεση καθημερινών δραστηριοτήτων στις οποίες συμπεριλαμβά-νονται η αλληλογραφία με τους πελάτες, οι πληροφορίες για τις υποθέσεις των πελατών και βασικές λογιστικές πληροφορίες που αφορούν στην τιμολόγηση και στους εισπρακτέους λογαριασμούς.**

Πίνακας 16: Σκεπτικό απαιτήσεων διασφάλισης

Φάση 3 – Επιλέξτε τις Κάρτες Ελέγχου

Κατά την Φάση 3, τα μέλη της ομάδας ανάλυσης είναι σε θέση να «τραβήξουν» τις κάρτες ελέγχου που σχετίζονται με τις ήδη καθορισμένες (στην φάση 1) εφαρμόσιμες περιοχές κινδύνων και τον αναλυτικό κατάλογο με τους προσδιορισμένους κρίσιμους πόρους. Όπως απεικονίζεται στο σχήμα 5, η φάση αυτή περιλαμβάνει τρία στάδια.

Σχήμα 5: Φάση 3 – Ροή εργασίας επιλογής καρτών ελέγχου

Οι κάρτες ελέγχου περιέχουν ελέγχους από τον κατάλογο των πρακτικών που χρησιμοποιούνται στην προσέγγιση OCTAVE. Αυτός ο κατάλογος αποτελεί μια συλλογή καλών πρακτικών στρατηγικής και λειτουργικής διασφάλισης. Ένας οργανισμός που διενεργεί αξιολόγηση κινδύνων για την ασφάλεια των πληροφοριών αυτοαξιολογείται σε σχέση με αυτόν τον κατάλογο πρακτικών. Ο κατάλογος χρησιμοποιείται ως μέτρο του τι πράττει ορθά ο οργανισμός, όσον αφορά την ασφάλεια, κατά την παρούσα περίοδο (τις τρέχουσες πρακτικές ασφάλειάς του) και τι δεν πράττει ορθά (τα τρωτά σημεία της οργανωτικής δομής του).

Ο κατάλογος των πρακτικών χωρίζεται, σκόπιμα, σε **δυο τύπους ελέγχου**: **τους οργανωτικούς ελέγχους και τους ελέγχους βάσει πόρων**:

- **Οι οργανωτικοί έλεγχοι** επικεντρώνονται σε οργανωτικά ζητήματα σε επίπεδο πολιτικής και παρέχουν ορθές πρακτικές γενικής διαχείρισης. Οι οργανωτικοί έλεγχοι περιλαμβάνουν ζητήματα που άπτονται επιχειρηματικών δραστηριοτήτων, καθώς και ζητήματα που απαιτούν σχεδιασμό και συμμετοχή από ολόκληρο τον οργανισμό.
- Οι πρακτικές **ελέγχων βάσει πόρων** επικεντρώνονται σε ζητήματα που προκαλούν ανησυχίες σχετικά με την τεχνολογία. Περιλαμβάνουν, δε, ζητήματα, τα οποία συνδέονται με τον τρόπο που οι άνθρωποι χρησιμοποιούν, αλληλεπιδρούν και προστατεύουν την τεχνολογία.

Ο κατάλογος των πρακτικών είναι ένας γενικός κατάλογος. Δεν ειδικεύεται σε κάποιο τομέα, φορέα ή σύνολο κανονισμών. Μπορεί να τροποποιηθεί ώστε να προσαρμοστεί σε κάποιο πρότυπο δέουσας επιμέλειας συγκεκριμένου τομέα ή σύνολο κανονισμών (π.χ. τους κανονισμούς της ιατρικής κοινότητας και της HIPPA [Health Insurance Portability and Accountability Act of 1996]). Μπορεί, επίσης, να διευρυνθεί προκειμένου να συμπεριλάβει ειδικά πρότυπα για κάποιον φορέα ή μπορεί να τροποποιηθεί έτσι ώστε να αντικατοπτρίζει την ορολογία ενός συγκεκριμένου τομέα. **Επιπλέον,**

μπορεί να αντικατασταθεί με οποιονδήποτε αναλυτικό κατάλογο συμβατών με πρότυπα ελέγχων.

Οι έλεγχοι ομαδοποιούνται περαιτέρω σε κάρτες ελέγχου, οι οποίοι χωρίζονται σε δυο κατηγορίες / περιοχές ελέγχου: τις περιοχές οργανωτικού ελέγχου και τις περιοχές ελέγχου βάσει πόρων. Διατίθενται δύο τύποι καρτών ελέγχου προς επιλογή από τις ομάδες που διεξάγουν την ανάλυση μιας ΜΜΕ:

- **Κάρτες οργανωτικού ελέγχου,** οι οποίες περιέχουν ελέγχους που μπορούν να εφαρμοστούν οριζόντια στον οργανισμό και σχετίζονται με πρακτικές και διαδικασίες διαχείρισης. Οι κάρτες ελέγχου οργάνωσης ασφάλειας είναι, κατά κανόνα, απλές, στοχεύουν, δε, στον μετριασμό τυπικών πληροφοριακών κινδύνων που συνδέονται με το οργανωτικό προφίλ του φορέα.
- **Κάρτες ελέγχου βάσει πόρων,** οι οποίες εστιάζονται στους κρίσιμους πόρους και ειδικεύονται ανά κατηγορία πόρου. Οι κάρτες ελέγχου αποτελούν ουσιαστικά προκαθορισμένους – ομαδοποιημένους ελέγχους σύμφωνα με τα προφίλ κινδύνων και τις απαιτήσεις διασφάλισης πόρων. Όπως αναφέρθηκε παραπάνω, οι κυριότερες ομάδες πόρων ενός φορέα/οργανισμού είναι: οι πληροφορίες, το σύστημα/δίκτυο, οι άνθρωποι και οι εφαρμογές. Οι κάρτες ελέγχου βάσει πόρων δημιουργούνται με σκοπό την επικέντρωσή τους σε καθημερινές εργασίες και στοχεύουν σε ειδικούς για τον κάθε πόρο κινδύνους.

Μπορείτε να βρείτε μία αναλυτική περιγραφή των οργανωτικών ελέγχων στο Παράρτημα Γ. Οργανωτικοί Έλεγχοι

Στάδιο 1. Επιλέξτε τις κάρτες οργανωτικού ελέγχου

Κατά την διάρκεια αυτού του σταδίου, οι ομάδες ανάλυσης επιλέγουν τις κάρτες οργανωτικού ελέγχου για τις περιοχές κινδύνων που έχουν προσδιοριστεί στην φάση 1 (προσδιορισμός χαρακτηριστικών των προφίλ κινδύνων) και δι' αυτού καθορίζουν την κατεύθυνση των προσπαθειών που θα αναληφθούν για την ασφάλεια των πληροφοριών του οργανισμού. Ωστόσο, πρακτικοί λόγοι αποτρέπουν τις ΜΜΕ από το να υλοποιήσουν άμεσα όλες τις πρωτοβουλίες που αναλαμβάνονται μετά την αξιολόγηση. Οι οργανισμοί είναι πιθανό ότι διαθέτουν περιορισμένα κεφάλαια και διαθέσιμο προσωπικό για την υλοποίηση της στρατηγικής προστασίας. Μετά την αξιολόγηση, η ομάδα ανάλυσης ιεραρχεί τις δραστηριότητες που αφορούν στην στρατηγική προστασίας και κατόπιν επικεντρώνεται στην υλοποίηση των δραστηριοτήτων ύψιστης προτεραιότητας.

Είναι διαθέσιμοι οργανωτικοί έλεγχοι για κάθε προφίλ κινδύνων όπως καθορίζεται στον πίνακα προσδιορισμού προφίλ κινδύνων.

Στάδιο 2. Επιλέξτε ελέγχους βάσει πόρων

Βάσει του προφίλ κινδύνων και των απαιτήσεων διασφάλισης πόρων, οι ομάδες ανάλυσης των ΜΜΕ μπορούν να χρησιμοποιήσουν τον πίνακα καρτών ελέγχου πόρων (βλέπε Παράρτημα Γ. Οργανωτικοί Έλεγχοι) για τον προσδιορισμό των κατάλληλων ελέγχων πόρων. Οι κάρτες ελέγχου βάσει πόρων είναι στοιχειώδεις έλεγχοι, οι οποίοι ομαδοποιούνται σε τρεις κατηγορίες, σύμφωνα με το προφίλ κινδύνων, την κατηγορία πόρου και την απαίτηση διασφάλισης του οργανισμού. Για παράδειγμα, οι ομάδες ανάλυσης λόγω ενός προφίλ υψηλών κινδύνων ενός οργανισμού έχουν διαφορετικούς κινδύνους και απαιτήσεις διασφάλισης σε αντίθεση με προφίλ μεσαίων ή χαμηλών κινδύνων. Ομοίως, οι κάρτες ελέγχου περιλαμβάνουν περισσότερους ελέγχους για την αντιμετώπιση ενός μεγαλύτερου φάσματος κινδύνων και απαιτήσεων διασφάλισης.

Στάδιο 3. Τεκμηριώστε τον αναλυτικό κατάλογο των επιλεγμένων ελέγχων και το σκεπτικό

Ενόσω τραβάτε τις κάρτες ελέγχου κρίσιμων πόρων στο στάδιο 2, θα έχετε την δυνατότητα να αναλύσετε πολλά ζητήματα που σχετίζονται με τους εν λόγω ελέγχους. Σε αυτό το στάδιο τεκμηριώνετε το σκεπτικό σας για την επιλογή κάθε κάρτας ελέγχου και τις απαραίτητες ενέργειες για την υλοποίηση. Επιπλέον, κατανοώντας τις κάρτες ελέγχου, θα είστε σε προσφορότερη θέση προκειμένου να καθορίσετε καλύτερα τα σχέδια δράσης κατά τη διάρκεια του επόμενου σταδίου. Για

κάθε κάρτα ελέγχου, στοχαστείτε και καταγράψτε την απάντησή σας στο ακόλουθο ερώτημα: Τι απαιτείται, όσον αφορά τους πόρους και τις αλλαγές, για την υλοποίηση των επιλεγμένων ελέγχων; Αναλύστε τις λειτουργικές πτυχές του κάθε ελέγχου. Μελετήστε τα ακόλουθα ερωτήματα για κάθε έναν από αυτούς.

- Ποιος πρέπει να τον υλοποιήσει;
- Ποιος πρέπει να είναι υπεύθυνος γι' αυτόν;
- Ποιος πρέπει να ωφεληθεί απ' αυτόν;
- Πώς πρέπει να υλοποιηθεί;

Τα ερωτήματα αυτά επικεντρώνονται στον τρόπο με τον οποίο πρέπει να χρησιμοποιηθούν οι έλεγχοι και γιατί αυτοί είναι σημαντικοί. Αν δεν μπορείτε να απαντήσετε σε όλα αυτά τα ερωτήματα, μπορεί να χρειάζεται να ζητήσετε να το κάνουν άτομα του οργανισμού σας που μπορούν να απαντήσουν σε αυτά. Οι πληροφορίες που προσδιορίζετε απαντώντας σ' αυτά τα ερωτήματα θα σας φανούν χρήσιμες στην φάση 4 όταν θα εκπονήσετε τα σχέδια μετριασμού κινδύνων. Βεβαιωθείτε ότι αυτές οι πληροφορίες καταγράφονται.

Παράδειγμα Α. (Προφίλ κινδύνων: υψηλού επιπέδου, κρίσιμος πόρος: εφαρμογή)

[Στάδιο 1] Στο στάδιο 1, οι ομάδες ανάλυσης που χρησιμοποιούν τον **πίνακα αξιολόγησης προφίλ κινδύνων και τον πίνακα οργανωτικών ελέγχων (Πίνακας 17)** επιλέγουν κάρτες οργανωτικού ελέγχου για τις περιοχές κινδύνων που προσδιορίστηκαν στην φάση 1 (προσδιορισμός προφίλ κινδύνων), καθορίζοντας δι' αυτού την κατεύθυνση των προσπαθειών που θ' αναληφθούν για την ασφάλεια των πληροφοριών στον οργανισμό.

Στο παράδειγμα Α οι οργανωτικοί έλεγχοι για υψηλό επίπεδο νομικών και ρυθμιστικών κινδύνων εισηγούνται πρακτικές ασφάλειας (ελέγχους) που υπαγορεύονται από τους οργανωτικούς ελέγχους **SP1 και SP4**. Κατά τον ίδιο τρόπο, ένας υψηλός κίνδυνος στην κατηγορία κινδύνων παραγωγικότητας επιβάλει την ανάγκη για αντίμετρα και πρακτικές που εφαρμόζονται από τους οργανωτικούς ελέγχους **SP3, SP4, SP5** και **SP6.** Για μεσαίου επιπέδου κινδύνους στην οικονομική σταθερότητα, υπαγορεύεται ο έλεγχος SP4 και για το χαμηλό επίπεδο κινδύνων φήμης και απώλειας εμπιστοσύνης πελατών, ο SP4.1 (η ενότητα περιλαμβάνεται στους ελέγχους του SP4).

Περιοχές κινδύνων	Υψηλού επιπέδου	Μεσαίου επιπέδου	Χαμηλού επιπέδου
Νομικών και Ρυθμιστικών	**(SP1)**	(SP1)	SP1.1
	(SP4)	(SP4)	
Παραγωγικότητας	**(SP3)**	(SP4)	SP4.1
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Οικονομικής απώλειας	(SP2)	**(SP4)**	SP4.1
	(SP1)		
	(SP4)		
Φήμης και Απώλειας Εμπιστοσύνης Πελατών	(SP1)	(SP4)	**SP4.1**
	(SP5)	(SP1)	

Πίνακας 17: Επιλογή Οργανωτικών Ελέγχων– Παράδειγμα Α

[Στάδιο 2] Στο στάδιο 2, η ομάδα ανάλυσης επιλέγει την/τις κάρτα (κάρτες) ελέγχου βάσει πόρων χρησιμοποιώντας τον πίνακα καρτών ελέγχου βάσει πόρων. Στο παράδειγμα Α, δεδομένου του προφίλ υψηλών κινδύνων του οργανισμού που προσδιορίστηκε στη φάση 1 και του τύπου κρίσιμων πόρων που προσδιορίστηκαν στο στάδιο 2, επιλέγουν την κάρτα 1 για εφαρμογές προφίλ υψηλών κινδύνων, συγκεκριμένα την κάρτα CC-1A.

Πίνακας καρτών ελέγχου			
Κρίσιμοι πόροι	**Κάρτες υψηλών κινδύνων**	**Κάρτες μεσαίων κινδύνων**	**Κάρτες χαμηλών κινδύνων**
Εφαρμογή	**CC-1A**	CC-2A	CC-3A
Σύστημα	CC-1S	CC-2S	CC-3S
Δίκτυο	CC-1N	CC-2N	CC-3N
Άνθρωποι	CC-1P	CC-2P	CC-3P

Πίνακας 18: Επιλογή ελέγχων βάσει πόρων – παράδειγμα Α

Στο παράδειγμα Α, η επιλεγμένη κάρτα (βλέπε Παράρτημα Β. Κάρτες ελέγχου) παρουσιάζει τους απαραιτήτους ελέγχους για μια εφαρμογή που εκτελείται σε έναν οργανισμό με ένα προφίλ κινδύνων. Η ομάδα προσδιορίζει τους ελέγχους οι οποίοι ικανοποιούν τις απαιτήσεις διασφάλισης που προσδιορίζονται στη φάση 3. Σ' αυτό το παράδειγμα, χρησιμοποιούνται οι απαιτήσεις εμπιστευτικότητας και διαθεσιμότητας. Επιλέγονται οι ακόλουθοι έλεγχοι πόρων **2.1.3, 2.1.6, 2.4.2, 2.5.1**, και **2.6.1**.

Μοναδικό Αναγνωριστικό κάρτας ελέγχου βάσει πόρων					**CC-1A**					
Προφίλ κινδύνων					**Υψηλού επιπέδου**					
Κατηγορία πόρου					**Εφαρμογή**					
Απαιτήσεις διασφάλισης	**Υλική ασφάλεια**	**Διαχείριση Συστημάτων και Δικτύων**	**Εργαλεία Διαχείρισης Συστήματος**	**Ασφάλεια Παρακολούθησης και Ελέγχου ΤΠ**	**Επαλήθευση και Εξουσιοδότηση**	**Διαχείριση Ευπάθειας**	**Κρυπτογράφηση**	**Σχεδιασμός και αρχιτεκτονική ασφάλειας**	**Διαχείριση Συμβάντων**	**Γενικές Πρακτικές Προσωπικού**
Εμπιστευτικότητα		**2.1.3**			**2.4.2**	**2.5.1**	**2.6.1**			
Ακεραιότητα		**2.1.4**			**2.4.2**	**2.5.1**	**2.6.1**			
Διαθεσιμότητα		**2.1.6**								

Πίνακας 19: CC-1A Κάρτα ελέγχου βάσει πόρων – παράδειγμα Α

[Στάδιο 3] Στο στάδιο 3, οι ομάδες ανάλυσης ασχολούνται με την συγκέντρωση δεδομένων και την ανάλυση των αποτελεσμάτων που παρήχθησαν στα στάδια 1 και 2. Η τεκμηρίωση των αποτελεσμάτων των προηγούμενων σταδίων, τόσο των επιλεγμένων ελέγχων βάσει πόρων όσο και των οργανωτικών ελέγχων παρουσιάζονται σε μορφή αναλυτικού κατάλογου στον παρακάτω πίνακα.

Πόροι	Έλεγχος	Σκεπτικό επιλογής
Έλεγχοι βάσει πόρων	**2.1.3** **2.1.6**	Οι έλεγχοι διαχείρισης συστημάτων και δικτύων είναι ουσιώδεις για την διατήρηση της διαθεσιμότητας και της εμπιστευτικότητας του υπό εξέταση πόρου.
	2.1.4	Η ακεραιότητα της εφαρμογής είναι σημαντική διότι τα ιατρικά δεδομένα πρέπει να είναι ακριβή.
	2.4.2	Η επαλήθευση και η εξουσιοδότηση μπορούν να διασφαλίσουν ελεγχόμενη πρόσβαση στον υπό εξέταση πόρο είτε για εσωτερικούς και εξωτερικούς χρήστες είτε για τρίτους.
	2.5.1	Η διαχείριση της ευπάθειας, συμπεριλαμβανομένων της συνήθους εκτίμησης ευπάθειας και των απαραίτητων δραστηριοτήτων αποκατάστασης, είναι σημαντική προκειμένου να αξιολογήσουμε τα μέτρα και τα συστήματα ασφάλειας.
	2.6.1	Οι εμπιστευτικές πληροφορίες πρέπει να προστατεύονται κατά τη διάρκεια της μεταφοράς και της αποθήκευσης.
Οργανωτικοί έλεγχοι	**SP1**	Ευαισθητοποίηση και κατάρτιση σε θέματα σχετικά με την ασφάλεια.
	SP3	Διαχείριση ασφάλειας
	SP4	Πολιτική ασφάλειας
	SP5.	Συλλογική διαχείριση
	SP6	Ανάκτηση μετά από καταστροφή

Πίνακας 20: Πίνακας επιλεγμένων ελέγχων και σκεπτικό – παράδειγμα Α

Παράδειγμα Β. (Προφίλ κινδύνων: μεσαίου επιπέδου, κρίσιμος πόρος: σύστημα)

Στο στάδιο 1, οι ομάδες ανάλυσης, που χρησιμοποιούν τον **πίνακα οργανωτικών ελέγχων** (Πίνακας 21), επιλέγουν τις κάρτες οργανωτικού ελέγχου για τις περιοχές κινδύνων που προσδιορίστηκαν στο στάδιο 1 (Στάδιο 1 – **Πίνακας αξιολόγησης προφίλ κινδύνων**), καθορίζοντας την κατεύθυνση των προσπαθειών για την διασφάλιση των πληροφοριών στον οργανισμό.

Για το **παράδειγμα Β**, ο οργανωτικός έλεγχος, που επιβάλλεται για χαμηλού επιπέδου νομικούς και ρυθμιστικούς κινδύνους είναι ο SP1.1 ενώ για χαμηλού επιπέδου κινδύνους παραγωγικότητας και οικονομικής σταθερότητας είναι ο SP4.1. Οι κίνδυνοι μεσαίου επιπέδου της φήμης και της απώλειας εμπιστοσύνης πελατών επιβάλλουν την χρήση των οργανωτικών ελέγχων SP1 και SP4.

Ο Πίνακας 21 συνοψίζει τους ελέγχους αποτύπωσης για το προαναφερθέν παράδειγμα Β.

Περιοχές κινδύνων	Υψηλού επιπέδου	Μεσαίου επιπέδου	Χαμηλού επιπέδου
Νομικών και Ρυθμιστικών	(SP1) (SP4)	(SP1) (SP4)	**SP1.1**
Παραγωγικότητας	(SP3) (SP4)	(SP4)	**SP4.1**

	(SP6)	(SP6)	
	(SP5)		
Οικονομικής απώλειας	(SP2)	(SP4)	**SP4.1**
	(SP1)		
	(SP4)		
Φήμης και απώλειας εμπιστοσύνης πελατών	(SP1)	**(SP4)**	SP4.1
	(SP5)	**(SP1)**	

Πίνακας 21: Επιλογή οργανωτικών ελέγχων – παράδειγμα Β

[Στάδιο 2] Στο στάδιο 2, η ομάδα ανάλυσης επιλέγει την/τις κάρτα (κάρτες) ελέγχου βάσει πόρων χρησιμοποιώντας τον πίνακα καρτών ελέγχου βάσει πόρων. Στο παράδειγμα Β, δεδομένου του προφίλ μεσαίου επιπέδου κινδύνων του οργανισμού, που προσδιορίστηκε στην φάση 1 (Στάδιο 1) και του τύπου κρίσιμου πόρου, που προσδιορίστηκε στο στάδιο 2, επιλέγουν την κάρτα 2 για συστήματα προφίλ μεσαίου επιπέδου κινδύνων, δηλαδή την κάρτα CC-2S.

Πίνακας καρτών ελέγχου			
Κρίσιμοι πόροι	**Κάρτες υψηλών κινδύνων**	**Κάρτες μεσαίων κινδύνων**	**Κάρτες χαμηλών κινδύνων**
Εφαρμογή	CC-1A	CC-2A	CC-3A
Σύστημα	CC-1S	**CC-2S**	CC-3S
Δίκτυο	CC-1N	CC-2N	CC-3N
Άνθρωποι	CC-1P	CC-2P	CC-3P

Πίνακας 22:Επιλογή καρτών ελέγχου βάσει πόρων – παράδειγμα Β

Η κάρτα που επιλέχθηκε στο παράδειγμα Β (βλέπε Παράρτημα Β. Κάρτες ελέγχου πόρων) απεικονίζει τους απαραίτητους ελέγχους για πόρους του συστήματος σε έναν οργανισμό με προφίλ μεσαίου επιπέδου κινδύνων. Η ομάδα προσδιορίζει τους ελέγχους που επιλαμβάνονται των απαιτήσεων διασφάλισης οι οποίοι προσδιορίστηκαν στην φάση 3. Ακολουθώντας τα αποτελέσματα του παραδείγματος Β από την φάση 2 (στάδιο 3), χρησιμοποιούνται απαιτήσεις διαθεσιμότητας για τον προσδιορισμό των κατάλληλων ελέγχων από την **κάρτα** ελέγχου **CC-2S**. Συνεπώς, επιλέγονται οι έλεγχοι πόρων **2.1.7, 2.1.6**.

Μοναδικό Αναγνωριστικό κάρτας ελέγχου βάσει πόρων					**CC-2S**					
Προφίλ κινδύνων					**Μεσαίου επιπέδου**					
Κατηγορία πόρου					**Σύστημα**					
Απαιτήσεις Διασφάλισης	**Υλική ασφάλεια**	**Διαχείριση συστήματος και δικτύου**	**Εργαλεία Διαχείρισης Συστήματος**	**Παρακολούθηση και έλεγχος ασφάλειας ΤΠ**	**Επαλήθευση και εξουσιοδότηση**	**Διαχείριση ευπάθειας**	**Κρυπτογράφηση**	**Σχεδιασμός και αρχιτεκτονική ασφάλειας**	**Διαχείριση συμβάντων**	**Γενικές πρακτικές προσωπικού**
Εμπιστευτι-κότητα		**2.1.6** **2.1.7**			**2.4.1**					

Ακεραιότητα		**2.1.9**			**2.4.1**					
Διαθεσιμότητα		**2.1.6** **2.1.7**								

Πίνακας 23: Κάρτα ελέγχου CC-2S βάσει πόρων – Παράδειγμα Β

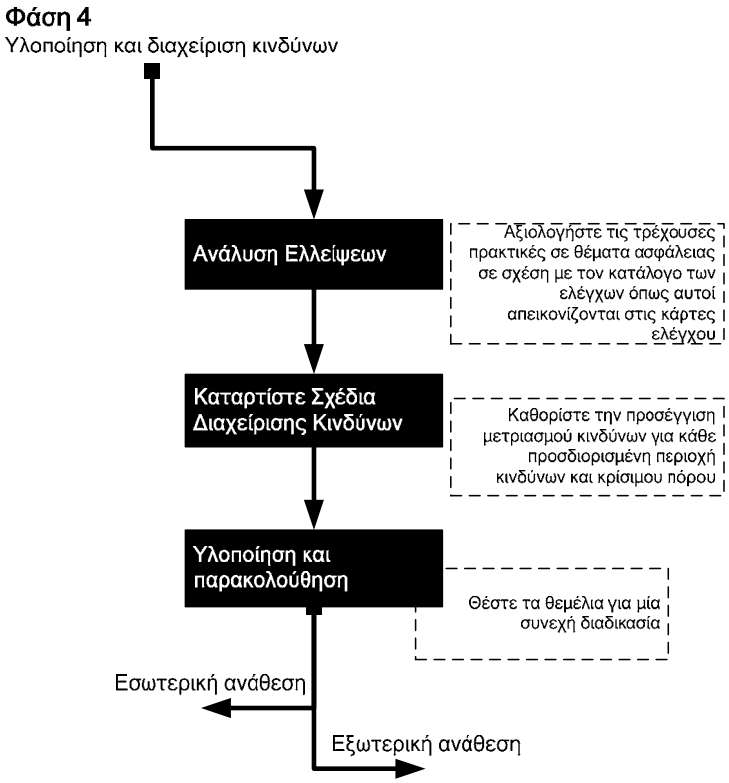
[Στάδιο 3] Στο στάδιο 3, οι ομάδες ανάλυσης ασχολούνται με την συγκέντρωση δεδομένων και την ανάλυση των αποτελεσμάτων που παρήχθησαν στα Στάδια 1 και 2. Τεκμηριώνοντας τα αποτελέσματα των προηγούμενων σταδίων, παρατίθενται, στην συνέχεια, στον παρακάτω πίνακα, υπό την μορφή αναλυτικού καταλόγου τόσο οι επιλεγμένοι βάσει πόρων έλεγχοι όσο και οι οργανωτικοί έλεγχοι.

Πόρος	**Έλεγχος**	**Σκεπτικό επιλογής**
Έλεγχοι βάσει πόρων	**2.1.6**	Οι έλεγχοι για την διαχείριση συστημάτων και δικτύων είναι ουσιώδεις για την διατήρηση της διαθεσιμότητας και της εμπιστευτικότητας του υπό εξέταση πόρου.
	2.1.7	
Οργανωτικοί έλεγχοι	**SP1**	Ευαισθητοποίηση και κατάρτιση σε θέματα σχετικά με την ασφάλεια.
	SP4	Πολιτική ασφάλειας
	SP1.1	Συμπεριλαμβάνεται στον SP1
	SP4.1	Συμπεριλαμβάνεται στον SP4

Πίνακας 24: Σκεπτικό επιλογής ελέγχων – Παράδειγμα Β

Φάση 4 – Υλοποίηση και Διαχείριση

Κατά την φάση 4, η ομάδα ανάλυσης προσδιορίζει τις ενέργειες και καταρτίζει έναν αναλυτικό κατάλογο ενεργειών, διακηρύσσοντας την κατεύθυνση για την βελτίωση της ασφάλειας. Για την επιτυχημένη υλοποίηση είναι ουσιώδης η εξεύρεση χρηματοδότησης για την συνεχή βελτίωση της ασφάλειας από τα ανώτατα στελέχη της επιχείρησης (υπεύθυνοι λήψεως αποφάσεων).



Σχήμα 6: Φάση 4 – Ροή εργασίας υλοποίησης και διαχείρισης

Στάδιο 1. Ανάλυση ελλείψεων

Η ανάλυση ελλείψεων είναι ουσιώδης προκειμένου για την βελτίωση του τρόπου με τον οποίο ένας οργανισμός χειρίζεται την ασφάλεια πληροφοριών, καθώς και για την εδραίωση της παρούσας κατάστασης ασφάλειας, πράγμα που σημαίνει εμπέδωση του ό,τι γίνεται με ορθό τρόπο, στις παρούσες συνθήκες, και πού απαιτείται βελτίωση.

Σ' αυτό το στάδιο, οι ομάδες ανάλυσης ασχολούνται με την αξιολόγηση των τρεχόντων πρακτικών σε θέματα ασφάλειας του οργανισμού σε σχέση με τους ελέγχους όπως αυτοί απεικονίζονται στις κάρτες ελέγχου. Οι ομάδες ανάλυσης διαβάζουν προσεκτικά τις επιλεγμένες κάρτες ελέγχου και εκμαιεύουν αναλυτικές πληροφορίες από αυτές για τις τρέχουσες πολιτικές, διαδικασίες και πρακτικές ασφάλειας του οργανισμού, παρέχοντας μ' αυτόν τον τρόπο ένα σημείο εκκίνησης για βελτίωση.

Κατά την διαδικασία της ανάλυσης ελλείψεων, οι ομάδες χρησιμοποιούν τις κάρτες ελέγχου σαν «απαιτήσεις» και αξιολογούν τις ελλείψεις μεταξύ αυτών και των τρεχόντων πρακτικών ασφάλειας, τόσο στο επίπεδο της οργάνωσης όσο και σε αυτό των κρίσιμων πόρων. Οι ομάδες ανάλυσης πρέπει να τεκμηριώσουν προσεκτικά τα αποτελέσματα με την μορφή δυο διακριτών σχεδίων – **(1) ένα για την οργανωτική βελτίωση** και **(2) ένα για την προστασία των πόρων.**

Το αποτέλεσμα αυτής της διαδικασίας μπορεί να αποτελέσει την βάση για την εργασία σχεδιασμού που έπεται. Αυτή διαχωρίζεται σε δυο κατηγορίες: **(α) τους οργανωτικούς ελέγχους**, όπου οι ομάδες ανάλυσης πρέπει να αναγνωρίσουν τι κάνουν και τι δεν κάνουν και να καθορίσουν τις ενέργειες για βελτίωση σε οργανωτικό επίπεδο και **(β) τους ελέγχους βάσει πόρων,** όπου οι ομάδες ανάλυσης αξιολογούν τα υφιστάμενα μέτρα προστασίας για τους προσδιορισμένους κρίσιμους πόρους.

Στάδιο 2. Καταρτίστε σχέδια μετριασμού κινδύνων

Σ' αυτό το στάδιο, τα μέλη των ομάδων ανάλυσης έχουν ήδη προσδιορίσει τους κρίσιμους πόρους, το προφίλ κινδύνων του οργανισμού τους, τις απαιτήσεις διασφάλισης και έχουν περαιτέρω επιλέξει κατάλληλους ελέγχους ενώ είναι έτοιμοι να καθορίσουν την προσέγγιση μετριασμού κινδύνων για κάθε προσδιορισμένη περιοχή κινδύνων και κάθε προσδιορισμένο κρίσιμο πόρο.

Λαμβάνοντας αυτά τα αρχικά μέτρα προς την κατεύθυνση της βελτίωσης της ασφάλειας, οι φορείς μπορούν να αρχίσουν να καταστρώνουν το δυναμικό που απαιτείται για την υλοποίηση της στρατηγικής για την προστασία τους.

Το αποτέλεσμα αυτής της εργασίας είναι το σχέδιο μετριασμού κινδύνων, το οποίο **οδηγεί σε μια σειρά μέτρων** που μπορεί να πάρει ένας οργανισμός για ν' αυξήσει ή να διατηρήσει το υφιστάμενο επίπεδο ασφάλειάς του. Στόχος του σχεδίου είναι μάλλον να παράσχει μια κατεύθυνση για την ανάληψη μελλοντικών προσπαθειών σχετικά με την ασφάλεια των πληροφοριών παρά να βρει μια άμεση λύση σε κάθε τρωτό σημείο της ασφάλειας ή σε κάθε σχετική ανησυχία. Δεδομένου ότι ένα σχέδιο μετριασμού παρέχει την οργανωτική κατεύθυνση όσον αφορά τις δραστηριότητες για την ασφάλεια των πληροφοριών, προτείνουμε η διάρθρωσή του να γίνει με βάση τις επιλεγμένες (φάση 3) κάρτες ελέγχου (οργανωτικές και βάσει κρίσιμων πόρων).

Στάδιο 3. Υλοποίηση, παρακολούθηση και έλεγχος

Μια απ' τις αρχές της μεθόδου εκτίμησης κινδύνων είναι να τεθούν τα θεμέλια για μια συνεχή διαδικασία. Αυτή η αρχή ικανοποιεί την ανάγκη υλοποίησης των αποτελεσμάτων μιας αξιολόγησης των κινδύνων που αφορούν στην ασφάλεια των πληροφοριών, παρέχοντας την βάση για βελτίωση της ασφάλειας. **Αν ένας οργανισμός δεν καταφέρει να υλοποιήσει τα αποτελέσματα μιας αξιολόγησης, δε θα καταφέρει να βελτιώσει επίσης και την στάση του απέναντι στην ασφάλειά του.**

Ένα από τα δυσκολότερα καθήκοντα σε κάθε δραστηριότητα βελτίωσης είναι η διατήρηση του δυναμικού που παράγεται κατά την διάρκεια μιας αξιολόγησης. Ωστόσο, πρακτικοί λόγοι αποτρέπουν τους περισσότερους φορείς από το να υλοποιήσουν άμεσα όλες τις πρωτοβουλίες μετά την αξιολόγηση. Ενδεχομένως, οι ΜΜΕ να διαθέτουν περιορισμένα κεφάλαια και προσωπικό για την υλοποίηση της στρατηγικής προστασίας.

Σε αυτό το στάδιο, οι ομάδες ανάλυσης ιεραρχούν τις δραστηριότητες και στην συνέχεια επικεντρώνονται στην υλοποίηση των δραστηριοτήτων ύψιστης προτεραιότητας.

Παρέχονται τρεις διακριτές δυνατότητες επιλογής:

- **Διαδικασία αποδοχής κινδύνων**. Όταν ένας κίνδυνος είναι αποδεκτός, δε λαμβάνει χώρα καμία ενέργεια για την μείωση των κινδύνων και οι συνέπειες γίνονται αποδεκτές στην περίπτωση που ο κίνδυνος αποκτήσει πραγματική υπόσταση.
- **Διαδικασία μετριασμού κινδύνων**. Όταν ένας κίνδυνος αμβλύνεται, προσδιορίζονται και ενισχύονται οι ενέργειες που έχουν σχεδιαστεί για την αντιμετώπιση της απειλής και μέσω αυτών ο κίνδυνος μειώνεται.

Τώρα που έχουν προσδιοριστεί τα ειδικά αντικείμενα ενεργειών, τα μέλη της ομάδας ανάλυσης επιβάλλεται να αναθέσουν ευθύνες για την αποπεράτωσή τους, καθώς και να ορίσουν μια ημερομηνία αποπεράτωσης. Πρέπει, δε, να επαναδιαταχθεί η σειρά των απαντήσεων για τις ακόλουθες ερωτήσεις – για κάθε επιμέρους αντικείμενο ενεργειών—:

- Ποιος θα είναι **υπεύθυνος** για κάθε επιμέρους αντικείμενο ενεργειών;
- Τι μπορεί να κάνει η διαχείριση για να **διευκολύνει** την αποπεράτωση αυτού του αντικειμένου ενεργειών;
- Πόσο θα **κοστίσει**;
- **Πόσο θα** διαρκέσει;
- **Μπορούμε να το κάνουμε μόνοι μας;**
- **Χρειαζόμαστε εξωτερική βοήθεια;**

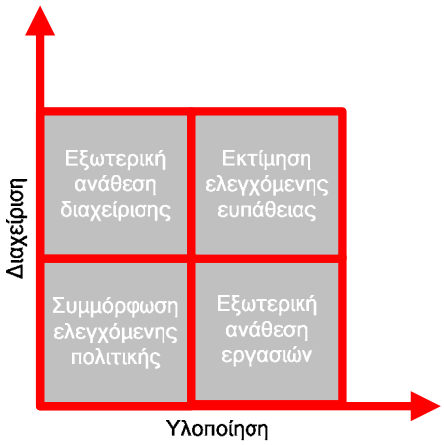
ΣΗΜΕΙΩΣΗ:

Οι δυο τελευταίες ερωτήσεις είναι ζωτικής σημασίας **για το εάν ένας οργανισμός μπορεί να χειριστεί την υλοποίηση των απαραίτητων ελέγχων μέσω εσωτερικής ανάθεσης.** Οι απαντήσεις

στις ερωτήσεις αυτές είναι εξίσου σημαντικές και πολύ δύσκολο να στοιχειοθετηθούν εφόσον έχουν και οι δυο διαδικασίες (η εξωτερική και η εσωτερική ανάθεση) οφέλη αλλά και μειονεκτήματα.

Η εξωτερική ανάθεση συνιστά για έναν οργανισμό **απόφαση «να δημιουργήσει ή να αγοράσει» και η οποία εφαρμόζεται στον εν λόγω πόρο.** Η εξωτερική ανάθεση, εφόσον γίνεται με ορθό τρόπο, μπορεί να προσφέρει σαφή πλεονεκτήματα. Οι κύριοι στόχοι για την εξωτερική ανάθεση είναι, πέρα από τις λειτουργίες υποστήριξης, η μείωση κόστους, η σμίκρυνση των συστημάτων και η επιθυμία του φορέα για την επικέντρωση του ενδιαφέροντος στις επιχειρηματικές δραστηριότητες του (βασική αυτάρκεια). Η έλλειψη αυτάρκειας στην ΤΟ, σε έναν οργανισμό, μπορεί, επίσης, να αποτελέσει αιτία για την εξωτερική ανάθεση της ΤΠ. Καθώς η ΤΠ γίνεται ολοένα και πιο σημαντική, οι εταιρείες συχνά αντιμετωπίζουν μια εκτεταμένη αναντιστοιχία μεταξύ των ικανοτήτων και των δεξιοτήτων που απαιτούνται για την πραγμάτωση του δυναμικού της ΤΠ και της πραγματικότητας της δικής τους εσωτερικής τεχνολογικής εμπειρογνωσίας.

Ωστόσο, υπάρχουν αρκετές εναλλακτικές επιλογές που πρέπει να μελετηθούν και οι οποίες συνδυάζουν τις βασικές ικανότητες του οργανισμού με την εξωτερική ή από τρίτους υποστήριξη (εν μέρει ή πλήρης εξωτερική ανάθεση). Όπως συνάγεται απ' το σχήμα 7, τόσο η διαχείριση όσο και η υλοποίηση μπορούν να εξωπριστούν. **Οι υπηρεσίες που κατά κανόνα διαπιστώνεται ότι μπορούν να προμηθεύσουν οι πάροχοι, μπορούν να συνοψιστούν ως ακολούθως**:



Σχήμα 7: Εναλλακτικές επιλογές εξωτερικής ανάθεσης διαχείρισης έναντι υλοποίησης

- **Εξωτερική Ανάθεση Διαχείρισης**. Στην εξωτερική ανάθεση της διαχείρισης, οι πάροχοι παρέχουν υπηρεσίες διαχείρισης στην ασφάλεια των πληροφοριών. Με άλλα λόγια, **ο πάροχος αναθέτει σ' έναν υπεύθυνο ασφάλειας** να διαχειριστεί το πρόγραμμα ασφάλειάς σας. Οι χρεώσεις, κατά κανόνα, υπολογίζονται σε ένα τριμηνιαίο τέλος ανάλογα με το μέγεθος και την πολυπλοκότητα του οργανισμού, τις απαραίτητες δεξιότητες και την κουλτούρα.
- **Συμμόρφωση ελεγχόμενης πολιτικής**. Στο πλαίσιο συμφωνιών/συμβάσεων τύπου συμμόρφωσης ελεγχόμενης πολιτικής, οι ειδικοί σύμβουλοι ασφαλείας **διενεργούν τακτικά προγραμματισμένους ελέγχους** προκειμένου να διασφαλίσουν την συνεχή συμμόρφωση με την εδραιωμένη πολιτική και τους καθιερωμένους ελέγχους για την ασφάλεια των πληροφοριών σας ώστε να προσδιοριστεί οιαδήποτε περίπτωση μη συμμόρφωσης. Ως αποτέλεσμα αυτής της τακτικής διαδικασίας, λαμβάνετε μία αναλυτική έκθεση για την συνολική κατάσταση των συστημάτων, τις περιοχές μη συμμόρφωσης, καθώς και καθοδήγηση για τον τρόπο με τον οποίο θα επαναφέρετε αυτά τα συστήματα σε κατάσταση συμμόρφωσης. Περιλαμβάνονται, επίσης, αναφορές και ανάλυση των σύγχρονων τάσεων που σας βοηθά να καθορίσετε αν η θεώρησή σας για την ασφάλεια βελτιώνεται ή όχι, και γιατί.
- **Εκτιμήσεις ελεγχόμενης ευπάθειας.** Σύμφωνα με αυτές τις μορφές συμφωνιών επιπέδου υπηρεσίας, **οι πάροχοι προμηθεύουν ένα μοναδικό σύνολο υπηρεσιών εκτίμησης**

ευπάθειας που μπορεί να προσαρμοστεί ανάλογα ώστε να επικεντρωθεί σε όλα τα πιθανά σημεία εισόδου των πληροφοριών ενός οργανισμού: το Διαδίκτυο, τα εσωτερικά δίκτυα, οι εφαρμογές, η τηλεπρόσβαση, και οι ασύρματες εφαρμογές. Βάσει των κινητήριων μοχλών της επιχείρησης, των τεχνικών της πόρων, και των παραγόντων απειλών, οι πάροχοι βοηθούν τους πελάτες να καθορίσουν το κατάλληλο χρονικό διάστημα για επαναλαμβανόμενες αξιολογήσεις και τον βέλτιστο βαθμό διερεύνησης του βάθους και του εύρους των.

- **Υποστήριξη ελεγχόμενων λειτουργιών**. Η διαρκής παροχή υπηρεσιών υποστήριξης λειτουργιών ασφάλειας παρέχει τους πόρους στους οργανισμούς - πελάτες προκειμένου να καλύψουν τις **εσωτερικές λειτουργίες ασφάλειας** σε καθημερινή βάση. Κατά κανόνα, οι πάροχοι προσφέρουν διαφορετικά και αρθρωτά επίπεδα υποστήριξης από απλές συμβουλές/προπαίδευση για την υλοποίηση λύσεων και πολιτικών ασφάλειας έως την μηχανίκευση και την τεχνική υλοποίηση της υποδομής ασφάλειας. Κατά κανόνα, οι λειτουργίες ασφάλειας περιλαμβάνουν εργασίες όπως σταθεροποίηση του διακομιστή, αλλαγές στην διάταξη ασφάλειας, επιδιορθώσεις ασφάλειας εφαρμογών κλπ.
- **Αντιμετώπιση καταστάσεων έκτακτης ανάγκης και συμβάντων**. Οι υπηρεσίες αντιμετώπισης καταστάσεων έκτακτης ανάγκης και συμβάντων διασφαλίζουν την υποστήριξη από ειδικευμένους μηχανικούς στις εγκαταστάσεις σας σε καταστάσεις έκτακτης ανάγκης ή κρίσης. Οι υπηρεσίες σε καταστάσεις έκτακτης ανάγκης και συμβάντα δίνουν την δυνατότητα σε οργανισμούς-πελάτες να **ανταποκρίνονται άμεσα και με αυτοπεποίθηση σε συμβάντα ασφάλειας που συνδέονται με υπολογιστές** – συμπεριλαμβανομένης της διακύβευσης συστημάτων, την προσβολή από ιούς και επιθέσεις άρνησης υπηρεσιών – βοηθώντας σας να ελαχιστοποιήσετε τον χρόνο διακοπής λειτουργίας λόγω βλάβης και την απώλεια εσόδων.

Οι συμφωνίες επιπέδου υπηρεσίας (ΣΕΥ) ανάμεσα στα ενδιαφερόμενα μέρη πρέπει να επιλαμβάνονται των απαιτήσεων διασφάλισης των οργανισμών, οι οποίοι προβαίνουν σε εξωτερική ανάθεση της διαχείρισης και του ελέγχου όλων ή μέρους των πληροφοριακών συστημάτων, των δικτύων και/ή των περιβαλλόντων εργασίας τους. Οποιαδήποτε ΣΕΥ για την εξωτερική ανάθεση της διαχείρισης και των λειτουργιών ασφάλειας των πληροφοριών πρέπει να επιλαμβάνεται των ακόλουθων ζητημάτων (ελέγχων):

Α. Επίπεδο εξωτερικής ανάθεσης και θέματα αστικής ευθύνης

Β. Παρακολούθηση Συμμόρφωσης

Γ. Ευθύνες Διαχείρισης

Δ. Πεδίο εφαρμογής της εργασίας

Ε. Τον τρόπο με τον οποίο ικανοποιούνται οι νομικές απαιτήσεις, π.χ. η νομοθεσία περί προστασίας δεδομένων

ΣΤ. Ποιοι διακανονισμοί θα εφαρμοστούν ώστε να επιτρέψουν σε όλα τα εμπλεκόμενα στην εξωτερική ανάθεση μέρη, συμπεριλαμβανομένων των υπεργολάβων, να έχουν επίγνωση των δικών τους ευθυνών ασφάλειας

Ζ. Με ποιόν τρόπο πρόκειται να διατηρηθούν και ελεγχθούν η ακεραιότητα και η εμπιστευτικότητα των επιχειρηματικών πόρων του φορέα

Η. Ποιοι φυσικοί και λογικοί έλεγχοι θα χρησιμοποιηθούν ώστε να περιορίσουν και να θέσουν όρια στην πρόσβαση των εξουσιοδοτημένων χρηστών σ' ευαίσθητα επαγγελματικά δεδομένα του οργανισμού

Θ. Με ποιόν τρόπο πρόκειται να διατηρηθεί η διαθεσιμότητα υπηρεσιών σε περίπτωση καταστροφής

Ι. Το δικαίωμα ελέγχου

Κ. Επάρκεια πόρων και επαγγελματική πιστοποίηση

Λ. Περιεχόμενο, συχνότητα και δομή υποβαλλόμενων εκθέσεων

Παράδειγμα Α. (Προφίλ Κινδύνων: Υψηλό, Κρίσιμοι Πόροι: Εφαρμογή)

[Στάδιο 1] Σ' αυτό το στάδιο, οι ομάδες ανάλυσης ασχολούνται με την αξιολόγηση των τρεχόντων πρακτικών ασφάλειας του οργανισμού σε σύγκριση με τους ελέγχους που περιγράφονται στις κάρτες ελέγχου. Οι ομάδες ανάλυσης διαβάζουν τους ελέγχους προσεκτικά και εκμαιεύουν αναλυτικές πληροφορίες για τις τρέχουσες πολιτικές, διαδικασίες και πρακτικές ασφάλειας του οργανισμού, παρέχοντας έτσι ένα σημείο εκκίνησης για βελτίωση.

Ο ακόλουθος πίνακας αναφέρεται στο παράδειγμα Α:

Πόρος	Έλεγχος	Ακολουθούμε, κατά την παρούσα περίοδο, τους ελέγχους που περιλαμβάνονται στις κάρτες ελέγχους;
Έλεγχοι βάσει πόρων	2.1.3	Όχι
	2.1.4	Εν μέρει
	2.1.6	Όχι
	2.4.2	Εν μέρει
	2.5.1	Όχι
	2.6.1	Όχι
Οργανωτικοί Έλεγχοι	SP1	Όχι
	SP3	Όχι
	SP4	Ναι
	SP5	Όχι
	SP6	Εν μέρει

Πίνακας 25: Αναλυτικός κατάλογος ανάλυσης ελλείψεων – παράδειγμα Α

[Στάδιο 2] Στο στάδιο 2, οι ομάδες ανάλυσης διαβάζουν τους ελέγχους (Παράρτημα Α, Β, Γ, Δ) και αποφασίζουν τις απαραίτητες ενέργειες.

Πόρος	Έλεγχος	Δράση
Έλεγχοι βάσει πόρων	2.1.3	Η ομάδα αποφασίζει να προστατεύσει ευαίσθητα δεδομένα με τη χρήση ασφαλών μεθόδων αποθήκευσης όπως καθορισμένες αλληλουχίες φύλαξης, δημιουργία εφεδρικών αντιγράφων, αποθηκευόμενων εκτός των εγκαταστάσεων της επιχείρησης, αφαιρούμενα μέσα αποθήκευσης, διαδικασία απόρριψης ευαίσθητων δεδομένων ή των μέσων αποθήκευσής τους.
	2.1.4	Η ομάδα αποφασίζει να προστατεύσει ευαίσθητα δεδομένα επαληθεύοντας τακτικά την ακεραιότητα της εγκατεστημένης βάσης λογισμικού για την εφαρμογή.
	2.1.6	Η ομάδα αποφασίζει να καθιερώσει ένα τεκμηριωμένο σχέδιο δημιουργίας εφεδρικών αντιγράφων ασφάλειας δεδομένων το οποίο ενημερώνεται σε τακτική βάση, ελέγχεται περιοδικά, επιβάλει τακτικά προγραμματισμένη δημιουργία εφεδρικών αντιγράφων όχι μόνον του λογισμικού αλλά και δεδομένων και απαιτεί περιοδικές δοκιμές και επαλήθευση της δυνατότητας επαναφοράς των δεδομένων από τα εφεδρικά αντίγραφα ασφάλειας.
	2.4.2	Η ομάδα αποφασίζει να καθιερώσει τεκμηριωμένες πολιτικές και διαδικασίες χρήσης πληροφοριών για ατομική και ομαδική πρόσβαση ώστε να: (Α) θεσπίζονται κανόνες για την εκχώρηση του κατάλληλου επιπέδου πρόσβασης, (Β) θεμελιωθεί το αρχικό δικαίωμα πρόσβασης, (Γ) τροποποιηθεί το δικαίωμα πρόσβασης (Δ) διακοπεί το δικαίωμα πρόσβασης και (Ε) να αναθεωρούνται και να επαληθεύονται περιοδικά τα δικαιώματα πρόσβασης.

	2.5.1	Η ομάδα αποφασίζει να επιλέξει εργαλεία αξιολόγησης ευπάθειας, καταλόγους ελέγχου και δέσμες ενεργειών (scripts), συμβαδίζοντας με γνωστούς τύπους ευπάθειας και μεθόδους προσβολής, αναθεωρώντας πηγές πληροφοριών για ανακοινώσεις ευπάθειας, συναγερμούς και προειδοποιήσεις ασφάλειας, αναγνωρίζοντας στοιχεία υποδομής προς αξιολόγηση, προγραμματίζοντας αξιολογήσεις ευπάθειας, ερμηνεύοντας και ανταποκρινόμενη στα αποτελέσματα, συντηρώντας την ασφαλή αποθήκευση και διάθεση των δεδομένων ευπάθειας.
	2.6.1	Η ομάδα αποφασίζει να ΜΗΝ υλοποιήσει κρυπτογράφηση των μεταδιδόμενων δεδομένων. Τα αποθηκευμένα δεδομένα προστατεύονται σε σχέση με την εμπιστευτικότητα με τη χρήση ενός συστήματος ελέγχου πρόσβασης.
Οργανωτικοί Έλεγχοι	**SP1**	Η ομάδα αποφασίζει να ξεκινήσει μια εκστρατεία βασικής ευαισθητοποίησης παρέχοντας εκπαίδευση σε όλους τους δικηγόρους σχετικά με τους κινδύνους που ενέχονται από τη χρήση του ηλεκτρονικού ταχυδρομείου, του διαδικτύου κλπ.
	SP3	Η λειτουργία διαχείρισης ασφάλειας πρέπει να καθιερωθεί. Η εργασία αυτή θα ανατεθεί σ΄ έναν υπεύθυνο ασφάλειας.
	SP4	Η ομάδα αποφασίζει, επίσης, να αναπτύξει μια γενική πολιτική ασφάλειας που καθορίζει την κυριότητα των πληροφοριών και τις ευθύνες για πληροφορίες.
	SP5	Αποφασίζονται οι διαδικασίες συλλογικής διαχείρισης που αφορούν τρίτους οι οποίοι είναι υπεύθυνοι για την συντήρηση της εφαρμογής.
	SP6	Το σχέδιο ανάκτησης από καταστροφή πρέπει να υλοποιείται και να ελέγχεται τακτικά.

Πίνακας 26: Αναλυτικός κατάλογος ενεργειών – Παράδειγμα Α

[Στάδιο 3] Στο στάδιο 3 για το παράδειγμα Α., οι ομάδες ανάλυσης ιεραρχούν τις δραστηριότητες και στην συνέχεια εστιάζονται στην υλοποίηση των δραστηριοτήτων ύψιστης προτεραιότητας. Αποφασίζουν να υλοποιήσουν τις ενέργειες υψηλής προτεραιότητας μέσα στο επόμενο τρίμηνο, τις ενέργειες μεσαίας προτεραιότητας για τους επόμενους έξι μήνες και τις ενέργειες χαμηλής προτεραιότητας πριν το τέλος του ερχόμενου χρόνου.

Τώρα που έχετε προσδιορίσει συγκεκριμένα αντικείμενα ενεργειών για τον αναλυτικό κατάλογο ενεργειών, πρέπει να αναθέσετε την ευθύνη της αποπεράτωσής τους, καθώς και μια ημερομηνία αποπεράτωσης. Απαντήστε τις παρακάτω ερωτήσεις για κάθε αντικείμενο ενεργειών στον αναλυτικό κατάλογό σας και καταγράψτε τα αποτελέσματα:

- Ποιος θα είναι υπεύθυνος για κάθε επιμέρους αντικείμενο ενεργειών;
- Μέχρι ροια ημερομηνία χρειάζεται να διευθετηθεί το αντικείμενο ενεργειών;
- Τι μπορεί να κάνει η διαχείριση για να διευκολύνει την αποπεράτωση αυτού του αντικειμένου ενεργειών;
- Πόσο θα κοστίσει;
- Πόσο θα διαρκέσει;
- Μπορούμε να το κάνουμε μόνοι μας;
- Χρειαζόμαστε εξωτερική βοήθεια;

Το αποτέλεσμα του σχεδίου τους συνοψίζεται στον παρακάτω πίνακα:

Πόρος	**Έλεγχος**	**Υπεύθυνος**	**Απαιτούμενη εξωτερική βοήθεια**	**Καμπή**	**Προτεραιότητα**
Έλεγχοι βάσει	**2.1.3**	Εργαζόμενος	Όχι	ΜΜ / ΗΗ	Υψηλή

πόρων		Α			
	2.1.4	Εργαζόμενος Α	Ναι		Μεσαία
	2.1.6	Εργαζόμενος Α	Ναι		Υψηλή
	2.4.2	Εργαζόμενος Α	Ναι		Μεσαία
	2.5.1	Εργαζόμενος Α	Ναι		Χαμηλή
	2.6.1	Εργαζόμενος Α	Όχι		Μεσαία
Οργανωτικοί έλεγχοι	**SP1**	Εργαζόμενος Β	Όχι		Χαμηλή
	SP3	Εργαζόμενος Β	Όχι		Μεσαία
	SP4	Εργαζόμενος Β	Ναι		Μεσαία
	SP5,	Εργαζόμενος Β	Όχι		Υψηλή
	SP6	Εργαζόμενος Β	Όχι		Υψηλή

Πίνακας 27: Σχέδιο υλοποίησης – Παράδειγμα Α

Παράδειγμα Β. (Προφίλ κινδύνων: μεσαίου επιπέδου, κρίσιμος πόρος: Σύστημα)

[Στάδιο 1] Σ' αυτό το στάδιο, οι ομάδες ανάλυσης ασχολούνται με την αξιολόγηση των τρεχόντων πρακτικών ασφάλειας του οργανισμού σε σχέση με τους ελέγχους που περιγράφονται στις κάρτες ελέγχου. Οι ομάδες ανάλυσης διαβάζουν προσεκτικά τους ελέγχους που εφαρμόζονται στο προφίλ τους (όπως απεικονίζεται στις επιλεγμένες κάρτες ελέγχου – Φάση 3, Στάδιο 3), και εκμαιεύουν αναλυτικές πληροφορίες για τις τρέχουσες πολιτικές, διαδικασίες και πρακτικές ασφάλειας ενός οργανισμού, παρέχοντας έτσι ένα σημείο εκκίνησης για βελτίωση.

Ο ακόλουθος πίνακας αναφέρεται στο Παράδειγμα Β:

Πόρος	**Έλεγχος**	**Ακολουθούμε, κατά την παρούσα περίοδο, τους ελέγχους που περιλαμβάνονται στις κάρτες ελέγχου;**
Έλεγχοι βάσει πόρων	**2.1.6**	Όχι
	2.1.7	Ναι
Οργανωτικοί έλεγχοι	**SP1**	Εν μέρει
	SP4	Ναι
	SP1.1	Όχι
	SP4.1	Ναι

Πίνακας 28: Αναλυτικός κατάλογος ανάλυσης ελλείψεων – παράδειγμα Β

[Στάδιο 2] Στο στάδιο 2, οι ομάδες ανάλυσης διαβάζουν τους ελέγχους (Παράρτημα Α, Β, Γ, Δ) και αποφασίζουν για τις απαραίτητες ενέργειες.

Πόρος	Έλεγχος	Ενέργειες
Έλεγχοι βάσει πόρων	**2.1.6**	Η ομάδα αποφασίζει να καθιερώσει ένα τεκμηριωμένο σχέδιο δημιουργίας εφεδρικών αντιγράφων ασφάλειας δεδομένων το οποίο ενημερώνεται σε τακτική βάση, ελέγχεται περιοδικά, επιβάλει τακτικά προγραμματισμένη δημιουργία εφεδρικών αντιγράφων όχι μόνον του λογισμικού αλλά και δεδομένων και απαιτεί περιοδικές δοκιμές και επαλήθευση της δυνατότητας επαναφοράς των δεδομένων από τα εφεδρικά αντίγραφα ασφαλείας.
	2.1.7	Η ομάδα αποφασίζει να ενημερώσει και να εκπαιδεύσει ολόκληρο το προσωπικό προκειμένου να κατανοήσει και να μπορέσει να ασκήσει τις αρμοδιότητές του σύμφωνα με τα σχέδια δημιουργίας εφεδρικών αντιγράφων.
Οργανωτικοί Έλεγχοι	**SP1**	Η ομάδα αποφασίζει να εκκινήσει μια βασική εκστρατεία ευαισθητοποίησης εκπαιδεύοντας όλους τους δικηγόρους σχετικά με τους κινδύνους που ενέχονται στην χρήση ηλεκτρονικού ταχυδρομείου, διαδικτύου κτλ..
	SP4	Η ομάδα αποφασίζει, επίσης, να αναπτύξει μια γενική πολιτική ασφάλειας καθορίζοντας την κυριότητα των πληροφοριών και τις ευθύνες για τις πληροφορίες.
	SP1.1	Περιλαμβάνονται στο SP1.
	SP4.1	Περιλαμβάνονται στην SP4.

Πίνακας 29: Αναλυτικός κατάλογος ενεργειών – παράδειγμα Β

[Στάδιο 3] Στο στάδιο 3 του παραδείγματος Β, οι ομάδες ανάλυσης ιεραρχούν τις δραστηριότητες και στην συνέχεια, επικεντρώνονται στην υλοποίηση των δραστηριοτήτων ύψιστης προτεραιότητας. Αποφασίζουν να υλοποιήσουν τις ενέργειες υψηλής προτεραιότητας μέσα στο επόμενο τρίμηνο, τις ενέργειες μεσαίας προτεραιότητας για τους επόμενους έξι μήνες και τις δραστηριότητες χαμηλής προτεραιότητας πριν το τέλος του ερχόμενου χρόνου.

Τώρα που έχετε αναγνωρίσει συγκεκριμένα αντικείμενα δράσεων για τον αναλυτικό κατάλογο ενεργειών, πρέπει να αναθέσετε την ευθύνη της αποπεράτωσής τους, καθώς και μια ημερομηνία αποπεράτωσης. Απαντήστε τις παρακάτω ερωτήσεις για κάθε αντικείμενο ενεργειών στον αναλυτικό κατάλογό σας και καταγράψτε τα αποτελέσματα:

- Ποιος θα είναι υπεύθυνος για κάθε επιμέρους αντικείμενο ενεργειών;
- Μέχρι ροια ημερομηνία χρειάζεται να διευθετηθεί το αντικείμενο ενεργειών;
- Τι μπορεί να κάνει η διαχείριση για να διευκολύνει την αποπεράτωση αυτού του αντικειμένου ενεργειών;
- Πόσο θα κοστίσει;
- Πόσο θα διαρκέσει;
- Μπορούμε να το κάνουμε μόνοι μας;
- Χρειαζόμαστε εξωτερική βοήθεια;

Τα αποτελέσματα του σχεδίου τους συνοψίζεται στον παρακάτω πίνακα:

Πόρος	Έλεγχος	Υπεύθυνος	Απαιτούμενη εξωτερική βοήθεια	Δείκτης	Προτεραιότητα
Έλεγχοι βάσει πόρων	**2.1.6**	Εργαζόμενος Α	Όχι	ΜΜ/ΗΗ	Υψηλή
	2.1.7	Εργαζόμενος Α	Όχι		Υψηλή
Οργανωτικοί Έλεγχοι	**SP1**	Εργαζόμενος Α	Όχι		Μεσαία
	SP4	Εργαζόμενος	Όχι		Χαμηλή

		A			
	SP1.1	Εργαζόμενος A	Όχι		Χαμηλή
	SP4.1	Εργαζόμενος A	Όχι		Υψηλή

Πίνακας 30: Σχέδιο υλοποίησης – Παράδειγμα Β

Παράρτημα Α. Κάρτες Οργανωτικού Ελέγχου

Ευαισθητοποίηση και κατάρτιση σε θέματα σχετικά με την ασφάλεια. (SP1)	
SP1	Η κάρτα ελέγχου ευαισθητοποίησης και κατάρτισης σε θέματα ασφάλειας περιλαμβάνει ελέγχους που απαιτούν την κατανόηση από μέρους των μελών του προσωπικού των ρόλων και των υπευθυνοτήτων τους σχετικά με την ασφάλεια. Πρέπει να παρέχονται σε ολόκληρο το προσωπικό ευαισθητοποίηση, κατάρτιση και περιοδικές υπομνήσεις για θέματα ασφάλειας. Η κατανόηση και οι ρόλοι του προσωπικού πρέπει να τεκμηριώνονται με σαφήνεια και η συμμόρφωση πρέπει να επαληθεύεται σε περιοδική βάση.
Στρατηγική Ασφάλειας (SP2)	
SP2	Η κάρτα ελέγχου στρατηγικής περιλαμβάνει ελέγχους που απαιτούν την συστηματική ενσωμάτωση των μελημάτων ασφάλειας στις επιχειρηματικές στρατηγικές του οργανισμού. Επίσης, οι πολιτικές και οι στρατηγικές ασφάλειας πρέπει να λαμβάνουν υπόψη τους τις στρατηγικές και τους στόχους του οργανισμού. Οι στρατηγικές, οι επιδιώξεις και οι στόχοι σε θέματα ασφάλειας πρέπει να τεκμηριώνονται, να ανανεώνονται, να ενημερώνονται και να κοινοποιούνται συστηματικά στον οργανισμό.
Διαχείριση Ασφάλειας (SP3)	
SP3	Η κάρτα ελέγχου διαχείρισης ασφάλειας περιλαμβάνει ελέγχους που απαιτούν την εφαρμογή στην πράξη της διαδικασίας διαχείρισης. Η εν λόγω διαδικασία οφείλει να αξιολογεί διαρκώς τα απαιτούμενα επίπεδα ασφάλειας των πληροφοριών και να καθορίζει τους κατάλληλους, αλλά και ισορροπημένους από την άποψη κόστους/κινδύνου(-ων), ελέγχους οι οποίοι πρέπει όχι μόνο να υλοποιούνται αλλά και να τεκμηριώνονται.
Πολιτικές και Κανονισμοί Ασφάλειας (SP4)	
SP4	Η κάρτα ελέγχου απαιτεί ο οργανισμός να διαθέτει ένα ολοκληρωμένο σύνολο τεκμηριωμένων, επίκαιρων πολιτικών για την ασφάλεια των πληροφοριών, οι οποίες θα ανανεώνονται και θα ενημερώνονται σε περιοδική βάση.
Συλλογική Διαχείριση Ασφάλειας (SP5)	
SP5	Οι κάρτες ελέγχου συλλογικής διαχείρισης περιλαμβάνουν ελέγχους ασφάλειας που εφαρμόζουν στην πράξη ελεγχόμενες και επιβεβλημένες διαδικασίες για την προστασία των πληροφοριών του οργανισμού όταν αυτός συνεργάζεται με εξωτερικούς φορείς (π.χ. τρίτους, συνεργάτες, υπεργολάβους ή εταίρους).
Σχεδιασμός Έκτακτης Ανάγκης / Ανάκτηση μετά από Καταστροφή (SP6)	
SP6	Οι κάρτες ελέγχου σχεδιασμού έκτακτης ανάγκης / ανάκτησης μετά από καταστροφή ενσωματώνουν ελέγχους ασφάλειας προκειμένου να διασφαλίσουν την συνέχιση των επιχειρηματικών δραστηριοτήτων στην περίπτωση καταστροφής ή μη διαθεσιμότητας των πληροφοριών. Τα βασικά στοιχεία της κάρτας ελέγχου είναι: ▫ τα σχέδια συνέχισης των επιχειρηματικών δραστηριοτήτων ή λειτουργίας έκτακτης ανάγκης, ▫ το/τα σχέδιο(-α) ανάκτησης μετά από καταστροφή και ▫ το/τα σχέδιο(-α) έκτακτης ανάγκης για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης.

Παράρτημα Β. Κάρτες ελέγχου πόρων[3]

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων										CC-1A
Προφίλ Κινδύνων										Υψηλού επιπέδου
Κατηγορία πόρου										Εφαρμογή
Απαιτήσεις Διασφάλισης	**Υλική ασφάλεια**	**Διαχείριση συστήματος και δικτύου**	**Εργαλεία Διαχείρισης Συστήματος**	**Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών**	**Επαλήθευση και εξουσιοδότηση**	**Διαχείριση ευπάθειας**	**Κρυπτογράφηση**	**Σχεδιασμός και αρχιτεκτονική ασφάλειας**	**Διαχείριση συμβάντων**	**Πρακτικές γενικού προσωπικού**
Εμπιστευτικότητα		2.1.3			2.4.2	2.5.1	2.6.1			
Ακεραιότητα		2.1.4			2.4.2	2.5.1	2.6.1			
Διαθεσιμότητα		2.1.6								

Οι έλεγχοι που βασίζονται στην εμπιστευτικότητα για ένα προφίλ οργανωτικής δομής υψηλών κινδύνων επιλαμβάνονται κατ' εξοχήν απαιτήσεων διασφάλισης στο επίπεδο μίας εφαρμογής, ενός συστήματος, ενός δικτύου και ανθρώπινων πόρων προκειμένου να διασφαλίσουν τον κύκλο ζωής κρίσιμων πληροφοριών. Οι έλεγχοι επιλέγονται κυρίως με στόχο την αποφυγή διαρροής πληροφοριών προς μη εξουσιοδοτημένες οντότητες ανεξάρτητα εάν αυτές είναι εξωτερικές ή εσωτερικές ως προς το περιβάλλον της επιχείρησης.

Απαραίτητοι έλεγχοι για την προστασία της εμπιστευτικότητας κρίσιμων πόρων είναι οι ακόλουθοι:

OP2.4.2 Ο έλεγχος απαιτεί τεκμηριωμένες πολιτικές και διαδικασίες χρήσης πληροφοριών για ατομική και ομαδική πρόσβαση ώστε να: (Α) θεσπίζονται κανόνες για την εκχώρηση του κατάλληλου επιπέδου πρόσβασης, (Β) θεμελιωθεί το αρχικό δικαίωμα πρόσβασης, (Γ) τροποποιηθεί το δικαίωμα πρόσβασης (Δ) διακοπεί το δικαίωμα πρόσβασης και (Ε) αναθεωρούνται και επαληθεύονται περιοδικά τα δικαιώματα πρόσβασης.

OP2.5.1 Ο έλεγχος απαιτεί την ύπαρξη ενός τεκμηριωμένου συνόλου διαδικασιών για την διαχείριση των τρωτών σημείων, συμπεριλαμβανομένης της επιλογής εργαλείων αξιολόγησης ευπάθειας, καταλόγων ελέγχου και δεσμών ενεργειών (scripts), συμβαδίζοντας με γνωστούς τύπους ευπάθειας και μεθόδους προσβολής, αναθεωρώντας πηγές πληροφοριών για ανακοινώσεις ευπάθειας, συναγερμούς και προειδοποιήσεις ασφάλειας, αναγνωρίζοντας στοιχεία υποδομής προς αξιολόγηση, προγραμματίζοντας αξιολογήσεις ευπάθειας, ερμηνεύοντας αποτελέσματα, συντηρώντας την ασφαλή αποθήκευση και διάθεση των δεδομένων ευπάθειας.

OP2.1.3 Ο έλεγχος απαιτεί να προστατεύονται οι ευαίσθητες πληροφορίες δια της ασφαλούς αποθήκευσης με μεθόδους όπως: καθορισμένες αλληλουχίες φύλαξης, δημιουργία εφεδρικών αντιγράφων αποθηκευόμενων εκτός των εγκαταστάσεων της επιχείρησης, αφαιρούμενα μέσα αποθήκευσης, διαδικασία απόρριψης ευαίσθητων δεδομένων ή των μέσων αποθήκευσής τους.

OP2.1.4 Ο έλεγχος απαιτεί την τακτική επαλήθευση της ακεραιότητας του εγκατεστημένου λογισμικού.

OP2.1.6 Ο έλεγχος απαιτεί την ύπαρξη ενός τεκμηριωμένου σχεδίου δημιουργίας εφεδρικών αντιγράφων δεδομένων, το οποίο ενημερώνεται σε τακτική βάση, ελέγχεται περιοδικά, επιβάλει τακτικά προγραμματισμένη δημιουργία εφεδρικών αντιγράφων όχι μόνον του λογισμικού αλλά και των δεδομένων και προϋποθέτει περιοδικό έλεγχο και επαλήθευση της ικανότητας επαναφοράς των δεδομένων από τα εφεδρικά αντίγραφα.

OP2.6.1 Ο έλεγχος απαιτεί κατάλληλους ελέγχους ασφάλειας, οι οποίοι πρέπει να χρησιμοποιούνται για την προστασία των ευαίσθητων δεδομένων ενόσω αυτά βρίσκονται σε κατάσταση αποθήκευσης και κατά την μετάδοση, συμπεριλαμβανομένων της κρυπτογράφησης των δεδομένων, της κρυπτογράφησης κατά την μετάδοση, της κρυπτογράφησης δεδομένων κατά την εγγραφή σε δίσκο, της

χρήσης δημόσιου κλειδιού, της τεχνολογίας ιδεατού ιδιωτικού δικτύου και της κρυπτογράφησης για οποιαδήποτε μετάδοση μέσω διαδικτύου.

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων										CC-1S
Προφίλ κινδύνων										Υψηλού επιπέδου
Κατηγορία πόρου										Σύστημα
Απαιτήσεις Διασφάλισης	**Υλική ασφάλεια**	**Διαχείριση συστήματος και δικτύου**	**Εργαλεία Διαχείρισης Συστήματος**	**Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών**	**Επαλήθευση και εξουσιοδότηση**	**Διαχείριση ευπάθειας**	**Κρυπτογράφηση**	**Σχεδιασμός και αρχιτεκτονική ασφάλειας**	**Διαχείριση συμβάντων**	**Γενικές πρακτικές προσωπικού**
Εμπιστευτικότητα		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Ακεραιότητα		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Διαθεσιμότητα		2.1.6 2.1.7 2.1.9			2.4.6					

Ένα υψηλό προφίλ κινδύνων υποδηλώνει απειλές που λαμβάνουν χώρα κατά την μη διαθεσιμότητα του συστήματος και που οδηγούν στη έλλειψη διαθεσιμότητας της υπηρεσίας στην επιχείρηση. Τα συστήματα δεν είναι σε θέση να φιλοξενήσουν επιχειρηματικές εφαρμογές ή μπορεί να προκαλέσουν απώλεια κρίσιμων πληροφοριών. Η πηγή προέλευσης των απειλών μπορεί να είναι η αστάθεια του συστήματος οφειλόμενη σε μηχανική δυσλειτουργία ή εσφαλμένη εγκατάσταση και χρήση.

Οι συστημικοί έλεγχοι περί εμπιστευτικότητας για προφίλ υψηλού επιπέδου κινδύνων οργανωτικής δομής περιλαμβάνουν μεθόδους που διασφαλίζουν την κατάλληλη διαμόρφωση και λειτουργικότητα του συστήματος. Οι συστημικοί έλεγχοι περί ακεραιότητας για ένα προφίλ υψηλών κινδύνων οργανωτικής δομής επιλαμβάνονται κατ' εξοχήν απαιτήσεων διασφάλισης στο επίπεδο εφαρμογής ή συστήματος ή δικτύου ή ανθρώπινων πόρων προκειμένου να διασφαλίσουν τη σταθερότητα του συστήματος και την ακεραιότητα των κρίσιμων πληροφοριών. Η συνεχής διαθεσιμότητα του συστήματος αποτελεί προϋπόθεση για την συνέχιση των επιχειρηματικών δραστηριοτήτων. Οι έλεγχοι επιλέγονται κυρίως για να επιλαμβάνονται πληροφοριών όσον αφορά την δημοσιοποίησή τους σε μη εξουσιοδοτημένες οντότητες ανεξάρτητα εάν αυτές είναι εξωτερικές ή εσωτερικές ως προς το περιβάλλον του οργανισμού.

Απαραίτητοι έλεγχοι για την διασφάλιση της ακεραιότητας των κρίσιμων πόρων είναι οι ακόλουθοι:

OP2.1.3 Ο έλεγχος απαιτεί να προστατεύονται οι ευαίσθητες πληροφορίες δια της ασφαλούς αποθήκευσης με μεθόδους όπως: καθορισμένες αλληλουχίες φύλαξης, δημιουργία εφεδρικών αντιγράφων, που αποθηκεύονται εκτός των εγκαταστάσεων της επιχείρησης, αφαιρουμένων μέσων αποθήκευσης, διαδικασίας απόρριψης ευαίσθητων δεδομένων ή των μέσων αποθήκευσής τους.

OP2.1.4 Ο έλεγχος απαιτεί την τακτική επαλήθευση της ακεραιότητας του εγκατεστημένου λογισμικού.

OP2.1.5 Ο έλεγχος απαιτεί την ενημέρωση όλων των συστημάτων σε σχέση με αναθεωρήσεις, προγράμματα επιδιόρθωσης (patches) και συμβουλές για την ασφάλεια.

OP2.1.6 Ο έλεγχος απαιτεί την ύπαρξη ενός τεκμηριωμένου σχεδίου δημιουργίας εφεδρικών αντιγράφων δεδομένων, το οποίο ενημερώνεται σε τακτική βάση, ελέγχεται περιοδικά, επιβάλει τακτικά προγραμματισμένη δημιουργία εφεδρικών αντιγράφων όχι μόνον του λογισμικού αλλά και των δεδομένων και προϋποθέτει περιοδικό έλεγχο και επαλήθευση της ικανότητας επαναφοράς των δεδομένων από τα εφεδρικά αντίγραφα.

OP 2.1.7 Ο έλεγχος απαιτεί ολόκληρο το προσωπικό να κατανοεί και να είναι σε θέση να ασκεί τις αρμοδιότητές του σύμφωνα με τα σχέδια δημιουργίας εφεδρικών αντιγράφων.

OP2.1.8 Ο έλεγχος απαιτεί οι μεταβολές στο υλικό και το λογισμικό ΤΠ να είναι προγραμματισμένες , ελεγχόμενες και τεκμηριωμένες.

OP2.1.9 Ο έλεγχος απαιτεί τα μέλη του προσωπικού ΤΠ να ακολουθούν διαδικασίες κατά την έκδοση, την αλλαγή και την διακοπή χρήσης συνθηματικών, των λογαριασμών και των προνομίων των χρηστών. Απαιτείται αναγνώριση μοναδικού χρήστη για όλους τους χρήστες των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των χρηστών τρίτων. Προτερόθετοι (default) λογαριασμοί και προτερόθετα συνθηματικά αφαιρούνται από τα συστήματα.

OP2.1.10 Ο έλεγχος απαιτεί να «εκτελούνται» μόνο οι απαραίτητες υπηρεσίες στα συστήματα – όλες οι μη απαραίτητες υπηρεσίες έχουν αφαιρεθεί.

OP2.2.1 Ο έλεγχος απαιτεί να επανεξετάζονται, σε τακτική βάση, όλα τα νέα εργαλεία, όλες οι νέες διαδικασίες και όλοι οι νέοι μηχανισμοί ασφάλειας ως προς την εφαρμοσιμότητά τους σχετικά με την ανταπόκρισή τους στις στρατηγικές ασφάλειας του οργανισμού.

OP2.2.2 Ο έλεγχος απαιτεί να χρησιμοποιούνται, να επανεξετάζονται, να ενημερώνονται ή να αντικαθιστώνται, σε τακτική βάση, τα εργαλεία και οι μηχανισμοί για την ασφαλή διαχείριση του συστήματος και του δικτύου. Παραδείγματα: διατάξεις ελέγχου ακεραιότητας δεδομένων, κρυπτογραφικά εργαλεία, διαγνώστες ευπάθειας, εργαλεία ελέγχου ποιότητας συνθηματικών, ανιχνευτές ιών, εργαλεία διαχείρισης διαδικασιών, συστήματα ανίχνευσης παρείσδυσης, ασφαλείς διαδικασίες τηλεδιαχείρησης, εργαλεία εξυπηρέτησης δικτύου, αναλυτές κίνησης, εργαλεία αντιμετώπισης συμβάντων, εργαλεία ανάλυσης δεδομένων για την πρόληψη εγκληματικών ενεργειών.

OP2.3.1 Ο έλεγχος απαιτεί να χρησιμοποιούνται, τακτικά, από τον οργανισμό τα εργαλεία ελέγχου και παρακολούθησης των συστημάτων και των δικτύων. Η δραστηριότητα παρακολουθείται από το προσωπικό ΤΠ , η δραστηριότητα των δικτύων και των συστημάτων καταχωρίζεται σε ημερολόγιο / καταγράφεται, οι καταχωρήσεις σε ημερολόγιο ανασκοπούνται σε τακτική βάση, η ασυνήθιστη δραστηριότητα περιγράφεται σύμφωνα με την κατάλληλη πολιτική ή διαδικασία, τα, δε, εργαλεία επανεξετάζονται και ενημερώνονται περιοδικά.

OP2.4.1 Ο έλεγχος απαιτεί να χρησιμοποιούνται οι κατάλληλοι έλεγχοι πρόσβασης και η κατάλληλη επιβεβαίωση γνησιότητας των χρηστών (π.χ. έγκριση μετατροπής αρχείων, διαμόρφωση δικτύου) που συνάδει με την σχετική πολιτική για τον περιορισμό της πρόσβασης των χρηστών σε πληροφορίες, προγράμματα γενικής-κοινής χρήσης συστήματος, σε κώδικα πηγής προγράμματος, ευαίσθητα συστήματα, ειδικές εφαρμογές και διατάξεις ελέγχου, συνδέσεις δικτύου μέσα στον οργανισμό, συνδέσεις δικτύου εκτός του οργανισμού.

OP2.4.3 Ο έλεγχος απαιτεί οι μέθοδοι/μηχανισμοί ελέγχου πρόσβασης να περιορίζουν την πρόσβαση σε πόρους σύμφωνα με τα δικαιώματα πρόσβασης που καθορίζονται από τις πολιτικές και τις διαδικασίες.

OP2.4.6 Ο έλεγχος απαιτεί να χρησιμοποιούνται μηχανισμοί επιβεβαίωσης γνησιότητας για την προστασία της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των ευαίσθητων δεδομένων. Τέτοια παραδείγματα είναι οι ψηφιακές υπογραφές και η βιομετρική.

OP2.6.1 Ο έλεγχος απαιτεί κατάλληλους ελέγχους ασφάλειας, που πρέπει να χρησιμοποιούνται για την προστασία των ευαίσθητων δεδομένων ενόσω αυτά βρίσκονται σε κατάσταση αποθήκευσης και κατά τη διάρκεια της μετάδοσης, συμπεριλαμβανομένων της κρυπτογράφησης κατά τη διάρκεια της μετάδοσης, της κρυπτογράφησης δεδομένων κατά την εγγραφή σε δίσκο, της χρήσης υποδομής δημόσιου κλειδιού, της τεχνολογίας ιδεατού ιδιωτικού δικτύου και της κρυπτογράφησης για οποιαδήποτε μετάδοση μέσω διαδικτύου.

OP2.7.1 Ο έλεγχος απαιτεί η αρχιτεκτονική και ο σχεδιασμός του συστήματος για καινούρια και μη αναθεωρημένα συστήματα να συμπεριλαμβάνει προβληματισμούς για στρατηγικές, πολιτικές και διαδικασίες ασφάλειας, το ιστορικό διαρροών ασφάλειας και τα αποτελέσματα αξιολογήσεων κινδύνων ασφάλειας.

OP2.7.2 Ο έλεγχος απαιτεί να διαθέτει ο οργανισμός ενημερωμένα διαγράμματα, τα οποία απεικονίζουν την αρχιτεκτονική ασφάλειας που διατρέχει το σύνολο του οργανισμού και την τοπολογία δικτύου.

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων					CC-1N					
Προφίλ κινδύνων					Υψηλού επιπέδου					
Κατηγορία πόρου					Δίκτυο					
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα					2.4.6	2.5.3	2.6.1			
Ακεραιότητα	1.1.4	2.1.1 2.1.10			2.4.1 2.4.3 2.4.4 2.4.6	2.5.3		2.7.2		
Διαθεσιμότητα	1.1.4				2.4.6					

Ένα προφίλ υψηλών κινδύνων υποδηλώνει απειλές, οι οποίες λαμβάνουν χώρα σε τρωτά σημεία του δικτύου που μπορεί να οδηγήσουν σε εξωτερικές προσβολές ή σε εσωτερική μη εξουσιοδοτημένη πρόσβαση σε ορισμένες περιοχές υψηλού ενδιαφέροντος ή κινδύνων του δικτύου.

Η απουσία ασφάλειας δικτύου έχει άμεσο και απευθείας αποτέλεσμα σε εκτελούμενες εφαρμογές και στην ροή των πληροφοριών.

Οι βασιζόμενοι στο δίκτυο έλεγχοι εμπιστευτικότητας για ένα οργανωτικό προφίλ υψηλών κινδύνων πρέπει να προστατεύει τις κρίσιμες εσωτερικές πληροφορίες από δυνητική απώλεια ή παράνομη χρήση. Επιπρόσθετα, οι πληροφορίες που αποθηκεύονται σε δίκτυο πρέπει να είναι διαθέσιμες και εύκολα προσβάσιμες ενώ πρέπει, επίσης, να διαχωρίζονται σύμφωνα με το επίπεδο κρισιμότητας.

Απαραίτητοι έλεγχοι για την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας σε ένα δίκτυο είναι οι ακόλουθοι:

OP2.6.1 Ο έλεγχος απαιτεί κατάλληλους ελέγχους ασφάλειας, που πρέπει να χρησιμοποιούνται για την προστασία των ευαίσθητων δεδομένων ενόσω αυτά βρίσκονται σε κατάσταση αποθήκευσης και κατά τη διάρκεια της μετάδοσης, συμπεριλαμβανομένων της κρυπτογράφησης δεδομένων κατά τη διάρκεια της μετάδοσης, της κρυπτογράφησης δεδομένων κατά την εγγραφή σε δίσκο, της χρήσης υποδομής δημόσιου κλειδιού, της τεχνολογίας ιδεατού ιδιωτικού δικτύου και της κρυπτογράφησης για οποιαδήποτε μετάδοση μέσω διαδικτύου.

OP2.4.6 Ο έλεγχος απαιτεί να χρησιμοποιούνται μηχανισμοί επιβεβαίωσης γνησιότητας για την προστασία της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των ευαίσθητων δεδομένων. Τέτοια παραδείγματα είναι οι ψηφιακές υπογραφές και η βιομετρική.

OP2.7.2 Ο έλεγχος απαιτεί να διαθέτει ο οργανισμός ενημερωμένα διαγράμματα, τα οποία απεικονίζουν την αρχιτεκτονική ασφάλειας που διατρέχει το σύνολο του οργανισμού και την τοπολογία δικτύου.

OP2.1.1 Ο έλεγχος απαιτεί να υπάρχουν τεκμηριωμένο(-α) σχέδιο(-α) ασφάλειας για την προστασία των συστημάτων και των δικτύων.

OP2.4.1 Ο έλεγχος απαιτεί να χρησιμοποιούνται οι κατάλληλοι έλεγχοι πρόσβασης και η κατάλληλη επιβεβαίωση γνησιότητας χρηστών (π.χ. έγκριση μετατροπής αρχείων, διαμόρφωση δικτύου) που συνάδει με την σχετική πολιτική για τον περιορισμό της πρόσβασης των χρηστών σε πληροφορίες, προγράμματα γενικής-κοινής χρήσης συστήματος, σε κώδικα πηγής προγράμματος, ευαίσθητα

συστήματα, ειδικές εφαρμογές και διατάξεις ελέγχου, συνδέσεις δικτύου μέσα στον οργανισμό, συνδέσεις δικτύου εκτός του οργανισμού.

OP2.4.3 Ο έλεγχος απαιτεί οι μέθοδοι/μηχανισμοί ελέγχου πρόσβασης να περιορίζουν την πρόσβαση σε πόρους σύμφωνα με τα δικαιώματα πρόσβασης που καθορίζονται από τις πολιτικές και τις διαδικασίες.

OP2.1.10 Ο έλεγχος απαιτεί μόνο οι απαραίτητες υπηρεσίες να «εκτελούνται» στα συστήματα – όλες οι μη απαραίτητες υπηρεσίες έχουν αφαιρεθεί.

OP 2.5.3 Ο έλεγχος απαιτεί οι αξιολογήσεις τρωτών σημείων της τεχνολογίας να διενεργούνται σε περιοδική βάση και τα τρωτά σημεία να αντιμετωπίζονται αφότου αναγνωρίζονται.

OP1.1.4 Ο έλεγχος απαιτεί να υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για την διαχείριση επισκεπτών, συμπεριλαμβανομένων των καταγραφών στοιχείων εισόδου, συνοδείας, πρόσβασης, υποδοχής και φιλοξενίας.

OP2.4.6 Ο έλεγχος απαιτεί να χρησιμοποιούνται μηχανισμοί επιβεβαίωσης γνησιότητας για την προστασία της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των ευαίσθητων δεδομένων. Τέτοια παραδείγματα είναι οι ψηφιακές υπογραφές και η βιομετρική.

Μοναδικό αναγνωριστικό καρτών ελέγχου πόρων										CC-1P
Προφίλ κινδύνων										Υψηλού επιπέδου
Κατηγορία πόρου										Ανθρώπινο δυναμικό
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα										3.2.1 3.2.2 3.2.3
Ακεραιότητα	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Διαθεσιμότητα										

Ένα προφίλ υψηλών κινδύνων υποδηλώνει απειλές, οι οποίες λαμβάνουν χώρα κατά την διαχείριση του ανθρώπινου δυναμικού και των ανθρώπινων πόρων γενικά. Το επίπεδο δέσμευσης του προσωπικού σχετικά με την χρήση των κατάλληλων ελέγχων ασφάλειας στους δικτυακούς πόρους καθορίζει το επίπεδο προστασίας που μπορεί να επιτευχθεί.

Ο χειρισμός των πληροφοριών και η επαναχρησιμοποίηση παλαιότερων εγγραφών μεγάλης αξίας για τον οργανισμό αποτελεί έναν κρίσιμο πόρο. Οι εσωτερικές ή εμπιστευτικές πληροφορίες από το προσωπικό πρέπει να αντιμετωπίζονται ευλαβικά. Η παρακολούθηση των πολιτικών προσωπικού για τις διαδικασίες αυτές διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών.

Απαραίτητοι έλεγχοι για την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών σε συνδυασμό με ένα πόρο ζωτικής σημασίας, όπως το ανθρώπινο δυναμικό, είναι οι ακόλουθοι:

OP3.2.1 Ο έλεγχος απαιτεί να ακολουθούν τα μέλη του προσωπικού ορθές πρακτικές ασφάλειας, που σημαίνει: να διασφαλίζουν τις πληροφορίες για τις οποίες είναι υπεύθυνοι· να μην αποκαλύπτουν ευαίσθητα δεδομένα σε τρίτους (αντίσταση στη χειραγώγηση)· να έχουν επαρκή ικανότητα χρήσης υλικού και λογισμικού πληροφορικής τεχνολογίας· να χρησιμοποιούν ορθές πρακτικές συνθηματικών· να κατανοούν και να ακολουθούν πολιτικές και να τηρούν κανονισμούς ασφάλειας· να αναγνωρίζουν και να αναφέρουν συμβάντα.

OP3.2.2 Ο έλεγχος απαιτεί ολόκληρο το προσωπικό, σε όλα τα επίπεδα ευθύνης, να εφαρμόζει τα καθήκοντα και την υπευθυνότητα που του έχει ανατεθεί σχετικά με την ασφάλεια των πληροφοριών.

OP3.2.3 Ο έλεγχος απαιτεί να υπάρχουν τεκμηριωμένες διαδικασίες για την εξουσιοδότηση και την επίβλεψη εκείνων που εργάζονται με ευαίσθητα δεδομένα ή που εργάζονται σε τοποθεσίες όπου αποθηκεύονται αυτά τα δεδομένα. Σε αυτούς συμπεριλαμβάνονται οι εργαζόμενοι, οι εργολάβοι, οι εταίροι, οι συνεργάτες και το προσωπικό από τρίτους, το προσωπικό συντήρησης συστημάτων ή το προσωπικό συντήρησης εγκαταστάσεων.

OP1.1.4 Ο έλεγχος απαιτεί να υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για την διαχείριση επισκεπτών, συμπεριλαμβανομένων των καταγραφών στοιχείων εισόδου, συνοδείας, των ημερολογίων πρόσβασης, της υποδοχής και φιλοξενίας.

OP1.3.2 Ο έλεγχος απαιτεί να μπορούν να καταγράφονται οι ενέργειες, είτε ενός ατόμου ή μίας ομάδας, όσον αυτό αφορά όλα τα φυσικά ελεγχόμενα μέσα.

Μοναδικό αναγνωριστικό καρτών ελέγχου πόρων					CC-2A					
Προφίλ κινδύνων					Μέτριου επιπέδου					
Κατηγορία πόρου					Εφαρμογή					
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα					2.4.2		2.6.1			
Ακεραιότητα					2.4.2					
Διαθεσιμότητα		2.1.6 2.1.7								

Ένα προφίλ μέτριων κινδύνων υποδηλώνει την αποθήκευση και επεξεργασία εσωτερικών ή μέτριας αξίας σχετικών με την ιδιοκτησία πληροφοριών που θα μπορούσε τυπικά να επισύρει την εμφάνιση ενός προφίλ γενικών απειλής που θα περιελάμβανε εξωτερικές κακόβουλες οντότητες που σκοπεύουν να παραβιάσουν ή να διακυβεύσουν την εμπιστευτικότητα ειδικών και μέτριας αξίας πληροφοριών. Οι έλεγχοι εμπιστευτικότητας που βασίζονται στις εφαρμογές για ένα οργανωτικό προφίλ μέτριων κινδύνων επιλαμβάνονται κατ' εξοχήν απαιτήσεων διασφάλισης στο επίπεδο μίας εφαρμογής, ενός συστήματος, ενός δικτύου και ανθρώπινων πόρων προκειμένου να διασφαλίσουν τον κύκλο ζωής κρίσιμων πληροφοριών. Οι έλεγχοι εμπιστευτικότητας που βασίζονται στην ακεραιότητα για ένα προφίλ οργανωτικής δομής μέτριου κινδύνων καθορίζουν το επίπεδο ακρίβειας των πληροφοριών μίας εφαρμογής ενώ η διαθεσιμότητα αφορά το επίπεδο προσβασιμότητας.

Απαραίτητοι έλεγχοι για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας στις εφαρμογές είναι οι ακόλουθοι:

OP2.4.2 Ο έλεγχος απαιτεί τεκμηριωμένες πολιτικές και διαδικασίες χρήσης πληροφοριών για ατομική και ομαδική πρόσβαση ώστε να καθιερωθούν κανόνες για την εκχώρηση του κατάλληλου επιπέδου πρόσβασης, θεμελιωθεί το αρχικό δικαίωμα πρόσβασης, τροποποιηθεί το δικαίωμα πρόσβασης, διακοπεί το δικαίωμα πρόσβασης και για να ανασκοπούνται και να επαληθεύονται περιοδικά τα δικαιώματα πρόσβασης.

OP2.6.1 Ο έλεγχος απαιτεί κατάλληλους ελέγχους ασφάλειας, που πρέπει να χρησιμοποιούνται για την προστασία των ευαίσθητων δεδομένων ενόσω αυτά βρίσκονται σε κατάσταση αποθήκευσης και κατά τη διάρκεια της μετάδοσης, συμπεριλαμβανομένων της κρυπτογράφησης των δεδομένων κατά τη διάρκεια της μετάδοσης, της κρυπτογράφησης δεδομένων κατά την εγγραφή σε δίσκο, της χρήσης υποδομής δημόσιου κλειδιού, της τεχνολογίας ιδεατού ιδιωτικού δικτύου και της κρυπτογράφησης για οποιαδήποτε μετάδοση μέσω διαδικτύου.

OP2.1.6 Ο έλεγχος απαιτεί την ύπαρξη ενός τεκμηριωμένου σχεδίου δημιουργίας εφεδρικών αντιγράφων δεδομένων, το οποίο ενημερώνεται σε τακτική βάση, ελέγχεται περιοδικά, επιβάλει τακτικά προγραμματισμένη δημιουργία εφεδρικών αντιγράφων όχι μόνον του λογισμικού αλλά και των δεδομένων και προϋποθέτει περιοδικό έλεγχο και επαλήθευση της ικανότητας επαναφοράς των δεδομένων από τα εφεδρικά αντίγραφα.

OP2.1.7 Ο έλεγχος απαιτεί ολόκληρο το προσωπικό να κατανοεί και να είναι σε θέση να ασκεί τις αρμοδιότητές του σύμφωνα με τα σχέδια δημιουργίας εφεδρικών αντιγράφων.

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων										CC-2S
Προφίλ κινδύνων										Μέτριου επιπέδου
Κατηγορία πόρου										Σύστημα
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας των τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα		2.1.6 2.1.7			2.4.1					
Ακεραιότητα		2.1.9			2.4.1					
Διαθεσιμότητα		2.1.6 2.1.7								

Ένα προφίλ μέτριων κινδύνων υποδηλώνει απειλές μέτριου επιπέδου που λαμβάνουν χώρα σε αστάθειες του συστήματος και που οδηγούν στη μη διαθεσιμότητα της υπηρεσίας στην επιχείρηση για ένα σύντομο χρονικό διάστημα. Τα συστήματα δεν είναι σε θέση να υποστηρίξουν δεόντως εφαρμογές ή λειτουργίες.

Οι βασισμένοι στο σύστημα έλεγχοι για ένα οργανωτικό προφίλ μέτριων κινδύνων περιλαμβάνουν μεθόδους που διασφαλίζουν την κατάλληλη διαμόρφωση και λειτουργικότητα του συστήματος για ενδεδειγμένη πρόσβαση.

Απαραίτητοι έλεγχοι για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας συστημάτων είναι οι ακόλουθοι:

OP2.4.1 Ο έλεγχος απαιτεί να χρησιμοποιούνται οι κατάλληλοι έλεγχοι πρόσβασης και η κατάλληλη επιβεβαίωση γνησιότητας χρηστών (π.χ. έγκριση μετατροπής αρχείων, διαμόρφωση δικτύου) που συνάδει με την σχετική πολιτική για τον περιορισμό της πρόσβασης των χρηστών σε πληροφορίες, προγράμματα γενικής-κοινής χρήσης συστήματος, σε πηγαίο κώδικα προγράμματος, ευαίσθητα συστήματα, ειδικές εφαρμογές και διατάξεις ελέγχου, συνδέσεις δικτύου μέσα στον οργανισμό, συνδέσεις δικτύου εκτός του οργανισμού.

OP2.1.6 Ο έλεγχος απαιτεί την ύπαρξη ενός τεκμηριωμένου σχεδίου δημιουργίας εφεδρικών αντιγράφων δεδομένων, το οποίο ενημερώνεται σε τακτική βάση, ελέγχεται περιοδικά, επιβάλει τακτικά προγραμματισμένη δημιουργία εφεδρικών αντιγράφων όχι μόνον του λογισμικού αλλά και των δεδομένων και προϋποθέτει περιοδικό έλεγχο και επαλήθευση της ικανότητας επαναφοράς των δεδομένων από τα εφεδρικά αντίγραφα.

OP2.1.7 Ο έλεγχος απαιτεί ολόκληρο το προσωπικό να κατανοεί και να είναι σε θέση να ασκεί τις αρμοδιότητές του σύμφωνα με τα σχέδια δημιουργίας εφεδρικών αντιγράφων.

OP2.1.9 Ο έλεγχος απαιτεί τα μέλη του προσωπικού της τεχνολογίας των πληροφοριών να ακολουθούν διαδικασίες κατά την έκδοση, την αλλαγή και την διακοπή χρήσης συνθηματικών, των λογαριασμών και των προνομίων κάθε χρήστη. Απαιτείται αναγνώριση μοναδικού χρήστη για όλους τους χρήστες των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των χρηστών τρίτων μερών. Προτερόθετοι λογαριασμοί και προτερόθετα συνθηματικά αφαιρούνται από τα συστήματα.

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων							CC-2N			
Προφίλ κινδύνων							Μέτριου επιπέδου			
Κατηγορία πόρου							Δίκτυο			
Απαιτήσεις Διασφάλισης	**Υλική ασφάλεια**	**Διαχείριση συστήματος και δικτύου**	**Εργαλεία Διαχείρισης Συστήματος**	**Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών**	**Επαλήθευση και εξουσιοδότηση**	**Διαχείριση ευπάθειας**	**Κρυπτογράφηση**	**Σχεδιασμός και αρχιτεκτονική ασφάλειας**	**Διαχείριση συμβάντων**	**Γενικές πρακτικές προσωπικού**
Εμπιστευτικότητα							2.6.1			
Ακεραιότητα					2.4.3					
Διαθεσιμότητα		2.1.5								

Ένα προφίλ μέτριων κινδύνων υποδηλώνει απειλές, οι οποίες λαμβάνουν χώρα σε τρωτά σημεία του δικτύου λόγω εσφαλμένης ή ανεπαρκώς εφαρμοζόμενης αρχιτεκτονικής δικτύου και που μπορεί να οδηγήσουν σε εξωτερικές απειλές ή εσωτερική μη εξουσιοδοτημένη πρόσβαση σε ορισμένες περιοχές του δικτύου ή μέτριου ενδιαφέροντος και μέτριας οργανωτικής αξίας.

Η απουσία ασφάλειας δικτύου έχει άμεσο και απευθείας αποτέλεσμα σε εκτελούμενες εφαρμογές και στην ροή των πληροφοριών. Ο κίνδυνος θεωρείται μέτριος όταν το σύστημα δεν επιτρέπει την πρόσβαση σε κρίσιμα συστατικά στοιχεία που θα μπορούσαν να επηρεάσουν άμεσα την φήμη ή την οικονομική υγεία του οργανισμού.

Απαραίτητοι έλεγχοι για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας σε ένα δίκτυο είναι οι ακόλουθοι:

OP2.6.1 Ο έλεγχος απαιτεί κατάλληλους ελέγχους ασφάλειας, που πρέπει να χρησιμοποιούνται για την προστασία των ευαίσθητων δεδομένων ενόσω αυτά βρίσκονται σε κατάσταση αποθήκευσης και κατά τη διάρκεια της μετάδοσης, συμπεριλαμβανομένων της κρυπτογράφησης των δεδομένων κατά τη διάρκεια της μετάδοσης, της κρυπτογράφησης δεδομένων κατά την εγγραφή σε δίσκο, της χρήσης υποδομής δημόσιου κλειδιού, της τεχνολογίας ιδεατού ιδιωτικού δικτύου και της κρυπτογράφησης για οποιαδήποτε μετάδοση μέσω διαδικτύου.

OP2.4.3 Ο έλεγχος απαιτεί οι μέθοδοι/μηχανισμοί ελέγχου πρόσβασης να περιορίζουν την πρόσβαση σε πόρους σύμφωνα με τα δικαιώματα πρόσβασης που καθορίζονται από τις πολιτικές και τις διαδικασίες.

OP2.1.5 Ο έλεγχος απαιτεί την ενημέρωση όλων των συστημάτων σε σχέση με αναθεωρήσεις, προγράμματα επιδιόρθωσης και συστάσεις για ελέγχους ασφάλειας.

Μοναδικό αναγνωριστικό καρτών ελέγχου πόρων										CC-2P
Προφίλ κινδύνων										Μέτριου επιπέδου
Κατηγορία πόρου										Ανθρώπινο δυναμικό
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα										3.2.1 3.2.2
Ακεραιότητα										3.2.1 3.2.2
Διαθεσιμότητα	1.1.4									

Ένα προφίλ μέτριων κινδύνων υποδηλώνει απειλές, οι οποίες λαμβάνουν χώρα κατά την διαχείριση των ανθρώπινων πόρων μεσαίου μεγέθους επιχειρήσεων όταν οι τρέχουσες πολιτικές ασφάλειας μπορούν να οδηγήσουν σε επιχειρηματικά προβλήματα μέτριας επίπτωσης.

Τα συμβάντα που προκύπτουν από την αδόκιμη χρήση των συνθηματικών ή των δικαιωμάτων πρόσβασης μπορεί να οδηγήσουν σε διαρροή των πληροφοριών. Ένα μέτριο επίπεδο εμπιστευτικότητας των πληροφοριών καθορίζει το επίπεδο κινδύνων ή την απώλεια χρημάτων για τον οργανισμό.

Η παρακολούθηση των πολιτικών προσωπικού για τις διαδικασίες αυτές διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών.

Απαραίτητοι έλεγχοι για την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών σε συνδυασμό με ένα κρίσιμο πόρο είναι οι ακόλουθοι:

OP3.2.1 Ο έλεγχος απαιτεί να ακολουθούν τα μέλη του προσωπικού ορθές πρακτικές ασφάλειας, που σημαίνει: να διασφαλίζουν τις πληροφορίες για τις οποίες είναι υπεύθυνοι· να μην αποκαλύπτουν ευαίσθητα δεδομένα σε τρίτους (αντίσταση στη χειραγώγηση)· να έχουν επαρκή ικανότητα χρήσης υλικού και λογισμικού πληροφοριακής τεχνολογίας· να χρησιμοποιούν ορθές πρακτικές συνθηματικών· να κατανοούν και να ακολουθούν πολιτικές και να τηρούν κανονισμούς ασφάλειας· να αναγνωρίζουν και να αναφέρουν συμβάντα.

OP3.2.2 Ο έλεγχος απαιτεί ολόκληρο το προσωπικό, σε όλα τα επίπεδα ευθύνης, να εφαρμόζει τα καθήκοντα και την υπευθυνότητα που τους έχει ανατεθεί σχετικά με την ασφάλεια των πληροφοριών.

OP1.1.4 Ο έλεγχος απαιτεί να υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για την διαχείριση επισκεπτών, συμπεριλαμβανομένων των καταγραφών στοιχείων εισόδου, συνοδείας, πρόσβασης, υποδοχής και φιλοξενίας.

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων										CC-3A
Προφίλ κινδύνων										Χαμηλού Επιπέδου
Κατηγορία πόρου										Εφαρμογή
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα					2.4.2					
Ακεραιότητα										
Διαθεσιμότητα										

Ένα προφίλ χαμηλών κινδύνων υποδηλώνει την αποθήκευση και την επεξεργασία δημόσιων ή εσωτερικών πληροφοριών αλλά χωρίς κρίσιμο επίπεδο σπουδαιότητας που θα συνεπαγόταν κάτι περισσότερο από μία ελάχιστη απώλεια χρημάτων. Η φήμη του οργανισμού δεν διακυβεύεται. Εν τούτοις, πρέπει να εφαρμόζονται οι έλεγχοι που θα αποσοβούσαν ακόμη και αυτού του τύπου την διαρροή πληροφοριών και που θα μπορούσαν να εξασφαλίσουν τον κύκλο ζωής των πληροφοριών.

Επιπρόσθετα, ακόμη και εάν δεν υφίσταται επίπτωση στην εμπιστευτικότητα, πρέπει να διασφαλίζεται η ακεραιότητα και η διαθεσιμότητα των πληροφοριών για κάθε εξουσιοδοτημένο χρήστη.

Απαραίτητος έλεγχος σχετικά με την εμπιστευτικότητα αυτού του περιουσιακού στοιχείου εφαρμογής είναι ο ακόλουθος:

OP2.4.2 Ο έλεγχος απαιτεί τεκμηριωμένες πολιτικές και διαδικασίες χρήσης πληροφοριών για ατομική και ομαδική πρόσβαση ώστε να καθιερωθούν κανόνες για την εκχώρηση του κατάλληλου επιπέδου πρόσβασης, να θεμελιωθεί το αρχικό δικαίωμα πρόσβασης, να τροποποιηθεί το δικαίωμα πρόσβασης, να διακοπεί το δικαίωμα πρόσβασης και να ανασκοπούνται και να επαληθεύονται περιοδικά τα δικαιώματα πρόσβασης.

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων										CC-3S
Προφίλ κινδύνων										Χαμηλού επιπέδου
Κατηγορία πόρου										Σύστημα
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα		2.1.9			2.4.1					
Ακεραιότητα					2.4.1					
Διαθεσιμότητα		2.1.6								

Ένα προφίλ χαμηλών κινδύνων υποδηλώνει το ελάχιστο επίπεδο απειλών που συνεπάγονται δυνητικές αστάθειες του συστήματος που οδηγούν σε μη διαθεσιμότητα της υπηρεσίας στην επιχείρηση για ένα σύντομο χρονικό διάστημα.

Οι βασισμένοι στο σύστημα έλεγχοι για οργανωτικό προφίλ ελάχιστων κινδύνων περιλαμβάνουν μεθόδους που διασφαλίζουν την κατάλληλη διάταξη και λειτουργικότητα του συστήματος για ενδεδειγμένη πρόσβαση.

Η επίπτωση στην μη διαθεσιμότητα του συστήματος δεν επηρεάζει την φήμη του οργανισμού δεδομένου ότι οι πληροφορίες δεν είναι ούτε ιδιωτικού χαρακτήρα ούτε καθοριστικές για τον οργανισμό.

Η μη διαθεσιμότητα του συστήματος δεν επηρεάζει την ποιότητα της υπηρεσίας ή του προϊόντος.

Απαραίτητος έλεγχος για την προστασία της εμπιστευτικότητας και της διαθεσιμότητας στα συστήματα είναι ο ακόλουθος:

OP2.4.1 Ο έλεγχος απαιτεί να χρησιμοποιούνται οι κατάλληλοι έλεγχοι πρόσβασης και η κατάλληλη επιβεβαίωση γνησιότητας χρηστών (π.χ. έγκριση μετατροπής αρχείων, διαμόρφωση δικτύου) που συνάδει με την σχετική πολιτική για τον περιορισμό της πρόσβασης των χρηστών σε πληροφορίες, προγράμματα γενικής-κοινής χρήσης συστήματος, σε κώδικα πηγής προγράμματος, ευαίσθητα συστήματα, ειδικές εφαρμογές και διατάξεις ελέγχου, συνδέσεις δικτύου μέσα στον οργανισμό, συνδέσεις δικτύου εκτός του οργανισμού.

OP2.1.6 Ο έλεγχος απαιτεί την ύπαρξη ενός τεκμηριωμένου σχεδίου δημιουργίας εφεδρικών αντιγράφων δεδομένων, το οποίο ενημερώνεται σε τακτική βάση, ελέγχεται περιοδικά, επιβάλει τακτικά προγραμματισμένη δημιουργία εφεδρικών αντιγράφων όχι μόνον του λογισμικού αλλά και των δεδομένων και προϋποθέτει περιοδικό έλεγχο και επαλήθευση της ικανότητας επαναφοράς των δεδομένων από τα εφεδρικά αντίγραφα.

OP2.1.9 Ο έλεγχος απαιτεί τα μέλη του προσωπικού της τεχνολογίας των πληροφοριών να ακολουθούν διαδικασίες κατά την έκδοση, την αλλαγή και την διακοπή χρήσης συνθηματικών, των λογαριασμών και των προνομίων κάθε χρήστη. Απαιτείται αναγνώριση μοναδικού χρήστη για όλους τους χρήστες των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των χρηστών τρίτων μερών. Προτερόθετοι λογαριασμοί και προτερόθετα συνθηματικά αφαιρούνται από τα συστήματα

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων							CC-3N			
Προφίλ κινδύνων							Χαμηλού επιπέδου			
Κατηγορία πόρου							Δίκτυο			
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα							2.6.1			
Ακεραιότητα										
Διαθεσιμότητα										

Ένα προφίλ χαμηλού επιπέδου κινδύνων υποδηλώνει απειλές που λαμβάνουν χώρα σε ελάσσονος σημασίας τρωτά σημεία του δικτύου ή σε μη διαθεσιμότητα λόγω εσφαλμένης ή ανεπαρκώς εφαρμοζόμενης αρχιτεκτονικής δικτύου. Η επίδραση ωστόσο μπορεί να θεωρηθεί αμελητέα από τη στιγμή που οι πληροφορίες δεν είναι μεγάλου ενδιαφέροντος ούτε υψηλού βαθμού εμπιστευτικότητας για τον οργανισμό. Κατά συνέπεια, η δυνητική οικονομική απώλεια για τον οργανισμό είναι μικρή.

Παρ' όλ' αυτά, συνιστώνται οι έλεγχοι ασφάλειας που επιλαμβάνονται κρυπτογραφημένων μεταβιβαζόμενων πληροφοριών.

Απαραίτητοι έλεγχοι για την διασφάλιση της εμπιστευτικότητας στο πλαίσιο ενός δικτύου είναι ο ακόλουθος ένας:

OP2.6.1 Ο έλεγχος απαιτεί κατάλληλους ελέγχους ασφάλειας, που πρέπει να χρησιμοποιούνται για την προστασία των ευαίσθητων δεδομένων ενόσω αυτά βρίσκονται σε κατάσταση αποθήκευσης και κατά τη διάρκεια της μετάδοσης, συμπεριλαμβανομένων της κρυπτογράφησης των δεδομένων κατά τη διάρκεια της μετάδοσης, της κρυπτογράφησης δεδομένων κατά την εγγραφή σε δίσκο, της χρήσης υποδομής δημόσιου κλειδιού, της τεχνολογίας ιδεατού ιδιωτικού δικτύου και της κρυπτογράφησης για οποιαδήποτε μετάδοση μέσω διαδικτύου.

Μοναδικό αναγνωριστικό καρτών ελέγχου βάσει πόρων										CC-3P
Προφίλ κινδύνων										Χαμηλού επιπέδου
Κατηγορία πόρου										Ανθρώπινο δυναμικό
Απαιτήσεις Διασφάλισης	Υλική ασφάλεια	Διαχείριση συστήματος και δικτύου	Εργαλεία Διαχείρισης Συστήματος	Παρακολούθηση και έλεγχος ασφάλειας τεχνολογίας των πληροφοριών	Επαλήθευση και εξουσιοδότηση	Διαχείριση ευπάθειας	Κρυπτογράφηση	Σχεδιασμός και αρχιτεκτονική ασφάλειας	Διαχείριση συμβάντων	Γενικές πρακτικές προσωπικού
Εμπιστευτικότητα										
Ακεραιότητα										
Διαθεσιμότητα	1.1.4									

Ένα προφίλ χαμηλού επιπέδου κινδύνων υποδηλώνει απειλές με μικρό αντίκτυπο στην διαχείριση των ανθρώπινων πόρων όταν οι τρέχουσες πρακτικές ασφάλειας θα μπορούσαν να οδηγήσουν στην δημιουργία προβλημάτων στην επιχείρηση αλλά με τον ελάχιστο κίνδυνο για τον οργανισμό.

Η κρισιμότητα των πληροφοριών δεν είναι υψηλού βαθμού/επιπέδου. Κατά συνέπεια, η επίπτωση, με οικονομικούς όρους, είναι χαμηλή και η απώλεια χρημάτων θεωρείται αμελητέα.

Ωστόσο, η παρακολούθηση των πολιτικών προσωπικού για τις διαδικασίες αυτές διασφαλίζει περαιτέρω την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών.

Απαραίτητοι έλεγχοι για την διασφάλιση της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών σε συνδυασμό με τους ανθρώπινους πόρους είναι ο ακόλουθος ένας:

OP1.1.4 Ο έλεγχος απαιτεί να υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για την διαχείριση επισκεπτών, συμπεριλαμβανομένων των καταγραφών στοιχείων εισόδου, συνοδείας, πρόσβασης, υποδοχής και φιλοξενίας.

Παράρτημα Γ. Οργανωτικοί Έλεγχοι

Ευαισθητοποίηση και κατάρτιση σε θέματα σχετικά με την ασφάλεια (SP1)	
SP1.1	Τα μέλη του προσωπικού κατανοούν τα ανατεθέντα καθήκοντα και αρμοδιότητές τους σε θέματα σχετικά με την ασφάλεια. Αυτό τεκμηριώνεται και επαληθεύεται.
SP1.2	Υπάρχει επαρκής αριθμός εσωτερικών εμπειρογνωμόνων για όλες τις υποστηριζόμενες υπηρεσίες, μηχανισμούς και τεχνολογίες (π.χ. τήρηση αρχείου ημερολογίου, παρακολούθηση ή κρυπτογράφηση), συμπεριλαμβανομένης της ασφαλούς λειτουργίας των παραπάνω. Το ζήτημα αυτό τεκμηριώνεται και επαληθεύεται.
SP1.3	Υπάρχει πρόβλεψη, για ολόκληρο το προσωπικό, ως προς την ευαισθητοποίηση και την κατάρτιση καθώς και για περιοδικές υπομνήσεις σε θέματα σχετικά με την ασφάλεια. Η κατανόηση των θεμάτων αυτών από το προσωπικό τεκμηριώνεται και η συμμόρφωση επαληθεύεται περιοδικά. Η κατάρτιση περιλαμβάνει τα παρακάτω θέματα:
	· στρατηγικές, σκοποί και στόχοι ασφάλειας
	· κανονισμοί, πολιτικές και διαδικασίες ασφάλειας
	· πολιτικές και διαδικασίες συνεργασίας με τρίτους
	· σχέδια έκτακτης ανάγκης και ανάκτησης μετά από καταστροφή
	· απαιτήσεις υλικής ασφάλειας
	· υπό το πρίσμα των χρηστών, όσον αφορά:
	- την διαχείριση του συστήματος και του δικτύου
	- τα εργαλεία διαχείρισης του συστήματος
	- την παρακολούθηση και τον έλεγχο για την υλική ασφάλεια και την ασφάλεια της τεχνολογίας ων πληροφοριών
	- την επιβεβαίωση γνησιότητας και την εξουσιοδότηση
	- την διαχείριση ευπάθειας
	- την κρυπτογράφηση
	- την αρχιτεκτονική και τον σχεδιασμό
	· την διαχείριση συμβάντων
	· τις γενικές πρακτικές προσωπικού
	· την συμμόρφωση, τις κυρώσεις και τα πειθαρχικά μέτρα για παραβιάσεις ασφάλειας
	· τον τρόπο με τον οποίο μπορούν να έχουν την ενδεδειγμένη πρόσβαση σε ευαίσθητα δεδομένα ή να εργάζονται σε περιοχές στις οποίες τα ευαίσθητα δεδομένα είναι προσβάσιμα
	· την οριστική λήξη των σχετικών με την ασφάλεια πολιτικών και διαδικασιών

Στρατηγική ασφάλειας (SP2)	
SP2.1	Οι επιχειρηματικές στρατηγικές του οργανισμού ενσωματώνουν, με προγραμματισμένο τρόπο, μελήματα ασφάλειας.
SP2.2	Οι στρατηγικές και πολιτικές ασφάλειας λαμβάνουν υπόψη τους τις/τους επιχειρηματικές(-ούς) στρατηγικές και σκοπούς του οργανισμού.
SP2.3	Οι στρατηγικές, σκοποί και στόχοι ασφάλειας τεκμηριώνονται και επανεξετάζονται, ενημερώνονται και γνωστοποιούνται στον οργανισμό.

Διαχείριση ασφάλειας (SP3)	
SP3.1	Η διεύθυνση διαθέτει επαρκή κονδύλια και επαρκείς πόρους σε ενέργειες για την ασφάλεια πληροφοριών.
SP3.2	Καθορίζονται τα ανατεθέντα καθήκοντα και οι σχετικές αρμοδιότητες για ολόκληρο το προσωπικό του οργανισμού.
SP3.3	Οι πρακτικές πρόσληψης και απόλυσης προσωπικού του οργανισμού λαμβάνουν υπόψη τους τα ζητήματα ασφάλειας των πληροφοριών.
SP3.4	Τεκμηριώνονται και επιβάλλονται τα απαιτούμενα επίπεδα ασφάλειας των πληροφοριών, καθώς και ο τρόπος εφαρμογής τους σε άτομα και ομάδες.
SP3.5	Ο οργανισμός διαχειρίζεται τους κινδύνους της ασφάλειας των πληροφοριών, συμπεριλαμβανομένων:
	· της εκτίμησης κινδύνων για την ασφάλεια των πληροφοριών, όχι μόνο σε περιοδική βάση, αλλά και σε απόκριση σε σημαντικές αλλαγές που συντελούνται στην τεχνολογία, καθώς και όσον αφορά τις εσωτερικές/εξωτερικές απειλές ή τα συστήματα και τις λειτουργίες του οργανισμού
	· της λήψης μέτρων για τον μετριασμό των κινδύνων σε ένα αποδεκτό επίπεδο
	· της διατήρησης ενός αποδεκτού επιπέδου κινδύνων
	· της αξιοποίησης των εκτιμήσεων των κινδύνων για την ασφάλεια των πληροφοριών προκειμένου αυτό να βοηθήσει στην επιλογή αποτελεσματικών από την άποψη κόστους/ασφάλειας μέτρων και την εξισορρόπηση του κόστους εφαρμογής έναντι δυνητικών απωλειών
SP3.6	Η διεύθυνση λαμβάνει συνήθεις εκθέσεις και ενεργεί βάσει συνήθων εκθέσεων που συνοψίζουν τα αποτελέσματα:
	· της επισκόπησης των ημερολόγιων των συστημάτων
	· της επισκόπησης διαδρομών ελέγχου
	· των εκτιμήσεων/αξιολογήσεων τρωτών σημείων της τεχνολογίας
	· των σχετικών με την ασφάλεια συμβάντων καθώς και των αποκρίσεων σε αυτά
	· των εκτιμήσεων κινδύνων
	· της επισκόπησης υλικής ασφάλειας
	· των σχεδίων και των συστάσεων για την βελτίωση της ασφάλειας

Πολιτικές και κανονισμοί ασφάλειας (SP4)	
SP4.1	Ο οργανισμός διαθέτει ολοκληρωμένο σύνολο τεκμηριωμένων, επίκαιρων πολιτικών για την ασφάλεια των πληροφοριών οι οποίες ανανεώνονται και ενημερώνονται σε περιοδική βάση. Οι πολιτικές αυτές επιλαμβάνονται των κυριότερων θεματικών πεδίων ασφάλειας, συμπεριλαμβανομένων:
	· της στρατηγικής και διαχείρισης ασφάλειας
	· της διαχείρισης κινδύνων ασφάλειας
	· της υλικής ασφάλειας
	· της διαχείρισης των συστημάτων και των δικτύων
	· των εργαλείων διαχείρισης του/των συστήματος/συστημάτων
	· της παρακολούθησης και του ελέγχου
	· της επιβεβαίωσης γνησιότητας και της εξουσιοδότησης
	· της διαχείρισης ευπάθειας
	· της κρυπτογράφησης
	· της αρχιτεκτονικής και του σχεδιασμού ασφάλειας

	· της διαχείρισης συμβάντων
	· των πρακτικών του προσωπικού ασφάλειας
	· της ισχύουσας νομοθεσίας και των κανονισμών
	· της ευαισθητοποίησης και της εκπαίδευσης
	· της συλλογικής ασφάλειας των πληροφοριών
	· του σχεδιασμού έκτακτης ανάγκης και της ανάκτησης μετά από καταστροφή
SP4.2	Υπάρχει τεκμηριωμένη διαδικασία για την διαχείριση των πολιτικών ασφάλειας, που περιλαμβάνει:
	· την δημιουργία
	· την διαχείριση (συμπεριλαμβανομένων περιοδικών ανασκοπήσεων και ενημερώσεων)
	· την επικοινωνία
SP4.3	Ο οργανισμός διαθέτει τεκμηριωμένη διαδικασία για περιοδική αξιολόγηση (τεχνική και μη) της συμμόρφωσης με τις πολιτικές ασφάλειας των πληροφοριών, την ισχύουσα νομοθεσία και τους κανονισμούς και τις απαιτήσεις ασφάλισης.
SP4.4	Ο οργανισμός διαθέτει τεκμηριωμένη διαδικασία για την συμμόρφωση με τις πολιτικές ασφάλειας των πληροφοριών, την ισχύουσα νομοθεσία και τους κανονισμούς και τις απαιτήσεις ασφάλισης.
SP4.5	Ο οργανισμός εφαρμόζει ομοιόμορφα τις πολιτικές ασφάλειάς του.
SP4.6	Η εξέταση και η αναθεώρηση των πολιτικών και των διαδικασιών ασφάλειας περιορίζεται στο εξουσιοδοτημένο προσωπικό.

Συλλογική Διαχείριση Ασφάλειας (SP5)	
SP5.1	Ο οργανισμός διαθέτει τεκμηριωμένες, ελεγχόμενες και εφαρμοζόμενες στην πράξη διαδικασίες για την προστασία των πληροφοριών του κατά την συνεργασία του με εξωτερικούς φορείς (π.χ. τρίτους, συνεργάτες, υπεργολάβους ή εταίρους).
SP5.2	Ο οργανισμός διαθέτει ελεγμένες(-ους) υπηρεσίες, μηχανισμούς και τεχνολογίες που ανατίθενται σε τρίτους και που ανταποκρίνονται στις ανάγκες και εκπληρώνουν τις απαιτήσεις του.
SP5.3	Ο οργανισμός τεκμηριώνει, παρακολουθεί και εφαρμόζει στην πράξη στρατηγικές για την προστασία των πληροφοριών που ανήκουν σε εξωτερικούς φορείς, η πρόσβαση στις οποίες γίνεται μέσω των δικών του στοιχείων υποδομής ή οι οποίες χρησιμοποιούνται από το δικό του προσωπικό.
SP5.4	Ο οργανισμός παρέχει και εξακριβώνει την ευαισθητοποίηση για και την εκπαίδευση σε εφαρμόσιμες πολιτικές και διαδικασίες ασφάλειας εξωτερικών φορέων για το προσωπικό που σχετίζεται με αυτούς τους φορείς.
SP5.5	Υπάρχουν τεκμηριωμένες διαδικασίες για το εξωτερικό προσωπικό, του οποίου έχει καταγγελθεί η σύμβαση, που καθορίζουν τα κατάλληλα μέτρα ασφάλειας για τον τερματισμό της πρόσβασής του σε πληροφορίες. Οι διαδικασίες αυτές κοινοποιούνται στον εξωτερικό φορέα και συντονίζονται με αυτόν.

Σχεδιασμός έκτακτης ανάγκης / Ανάκτηση μετά από καταστροφή (SP6)	
SP6.1	Έχει γίνει ανάλυση των λειτουργιών, των εφαρμογών και της κρισιμότητας των δεδομένων.
SP6.2	Ο οργανισμός έχει τεκμηριώσει
	· την συνέχιση των επιχειρηματικών δραστηριοτήτων ή των σχεδίων λειτουργίας σε κατάσταση έκτακτης ανάγκης
	· το/τα σχέδιο(-α) ανάκτησης μετά από καταστροφή
	· το/τα σχέδιο(-α) έκτακτης ανάγκης για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης
SP6.3	Τα σχέδια έκτακτης ανάγκης, ανάκτησης μετά από καταστροφή και συνέχισης των επιχειρηματικών δραστηριοτήτων λαμβάνουν υπόψη τους τις απαιτήσεις και τους ελέγχους φυσικής και ηλεκτρονικής πρόσβασης.

SP6.4	Τα σχέδια έκτακτης ανάγκης, ανάκτησης μετά από καταστροφή και συνέχισης των επιχειρηματικών δραστηριοτήτων επανεξετάζονται, ελέγχονται και αναθεωρούνται περιοδικά.
SP6.5	Το σύνολο του προσωπικού:
	· είναι ενήμερο για τα σχέδια έκτακτης ανάγκης, ανάκτησης μετά από καταστροφή και συνέχισης των επιχειρηματικών δραστηριοτήτων
	· κατανοεί και είναι σε θέση να ασκήσει τις αρμοδιότητές του

Παράρτημα Δ. Έλεγχοι βάσει πόρων

Υλική ασφάλεια (OP1)	
Σχέδια και Διαδικασίες Υλικής ασφάλειας (OP1.1)	
OP1.1.1	Υπάρχει(-ουν) τεκμηριωμένο(-α) σχέδιο(-α) ασφάλειας των εγκαταστάσεων για την προστασία των χώρων, των κτιρίων και οποιωνδήποτε αυστηρά ελεγχόμενων περιοχών.
OP1.1.2	Τα σχέδια αυτά επανεξετάζονται, ελέγχονται και αναθεωρούνται περιοδικά.
OP1.1.3	Οι διαδικασίες και οι μηχανισμοί υλικής ασφάλειας επιθεωρούνται και αναθεωρούνται τακτικά.
OP1.1.4	Υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για την διαχείριση των επισκεπτών, που περιλαμβάνουν
	· την εισαγωγή στοιχείων αναγνώρισης
	· την συνοδεία
	· τα ημερολόγια πρόσβασης
	· υποδοχή και φιλοξενία
OP1.1.5	Υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για τον φυσικό έλεγχο υλικού και λογισμικού, συμπεριλαμβανομένων:
	· των σταθμών εργασίας, φορητών υπολογιστών, διααποδιαμορφωτών, ασύρματων εξαρτημάτων και όλων των άλλων μονάδων που χρησιμοποιούνται για την πρόσβαση σε πληροφορίες
	· της πρόσβασης, αποθήκευσης και ανάκτησης δεδομένων εφεδρικών αντιγράφων
	· της αποθήκευσης ευαίσθητων δεδομένων σε υλικά και ηλεκτρονικά μέσα
	· της διάθεσης ευαίσθητων δεδομένων ή των μέσων στα οποία αποθηκεύονται
	· της επαναχρησιμοποίησης και ανακύκλωσης χαρτιού και ηλεκτρονικών μέσων
Έλεγχος φυσικής πρόσβασης (OP1.2)	
OP1.2.1	Υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για ατομική και ομαδική πρόσβαση που καλύπτουν:
	· τους κανόνες για την παροχή του ενδεδειγμένου επιπέδου φυσικής πρόσβασης
	· τους κανόνες για τον καθορισμό ενός αρχικού δικαιώματος πρόσβασης
	· την τροποποίηση του δικαιώματος πρόσβασης
	· την διακοπή του επιπέδου πρόσβασης
	· την περιοδική αναθεώρηση και επαλήθευση των δικαιωμάτων πρόσβασης
OP1.2.2	Υπάρχουν τεκμηριωμένες πολιτικές διαδικασίες και μηχανισμοί για τον έλεγχο της φυσικής πρόσβασης σε καθορισμένες οντότητες. Συγκεκριμένα περιλαμβάνονται:
	· οι χώροι εργασίας
	· το υλικό (υπολογιστές, συσκευές επικοινωνίας κλπ) και μέσα λογισμικού
OP1.2.3	Υπάρχουν τεκμηριωμένες διαδικασίες για την εξακρίβωση της εξουσιοδότησης πρόσβασης πριν από την παροχή φυσικής πρόσβασης.
OP1.2.4	Οι σταθμοί εργασίας και άλλες μονάδες που επιτρέπουν την πρόσβαση σε ευαίσθητα δεδομένα όντως διασφαλίζονται προκειμένου να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση.
Παρακολούθηση και έλεγχος υλικής ασφάλειας (OP1.3)	
OP1.3.1	Τηρούνται αρχεία συντήρησης για την τεκμηρίωση των επισκευών και των τροποποιήσεων του υλικού.
OP1.3.2	Μπορούν να καταχωρίζονται οι ενέργειες ενός ατόμου ή ομάδας που αφορούν σε φυσικά ελεγχόμενα μέσα.
OP1.3.3	Τα αρχεία ελέγχου και παρακολούθησης εξετάζονται τακτικά για τυχόν ανωμαλίες και λαμβάνονται, ανάλογα με τις ανάγκες, διορθωτικά μέτρα.

Ασφάλεια της τεχνολογίας των πληροφοριών (OP2)	
Διαχείριση συστημάτων και δικτύων (OP2.1)	
OP2.1.1	Υπάρχει(-ουν) τεκμηριωμένο(-α) σχέδιο(-α) ασφάλειας για την διαφύλαξη των συστημάτων και των δικτύων.
OP2.1.2	Το/Τα σχέδιο(-α) ασφάλειας αναθεωρούνται, ελέγχονται και ενημερώνονται περιοδικά.
OP2.1.3	Τα ευαίσθητα δεδομένα προστατεύονται μέσω ασφαλούς αποθήκευσης, όπως, για παράδειγμα, μέσω:
	· καθορισμένων αλληλουχιών φύλαξης
	· εφεδρικών αντιγράφων που αποθηκεύονται εκτός οργανισμού
	· αφαιρούμενων μέσων αποθήκευσης
	· διαδικασίας απόρριψης των ευαίσθητων δεδομένων ή των μέσων αποθήκευσής τους
OP2.1.4	Επαληθεύεται τακτικά η ακεραιότητα του εγκατεστημένου λογισμικού.
OP2.1.5	Όλα τα συστήματα ενημερώνονται σε σχέση με αναθεωρήσεις, προγράμματα επιδιόρθωσης και συστάσεις για ελέγχους ασφάλειας.
OP2.1.6	Υπάρχει τεκμηριωμένο σχέδιο δημιουργίας εφεδρικών αντιγράφων δεδομένων, το οποίο:
	· ενημερώνεται τακτικά
	· ελέγχεται περιοδικά
	· επιβάλλει τον τακτικό προγραμματισμό δημιουργίας εφεδρικών αντιγράφων και του λογισμικού και των δεδομένων
	· απαιτεί τον/την περιοδικό(-ή) έλεγχο και επαλήθευση της ικανότητας επαναφοράς των δεδομένων από εφεδρικά αντίγραφα
OP2.1.7	Ολόκληρο το προσωπικό κατανοεί και είναι σε θέση να ασκήσει τις αρμοδιότητές σύμφωνα με τα σχέδια δημιουργίας εφεδρικών αντιγράφων.
OP2.1.8	Οι αλλαγές στο υλικό και το λογισμικό της τεχνολογίας των πληροφοριών προγραμματίζονται, ελέγχονται και τεκμηριώνονται.
OP2.1.9	Τα μέλη του προσωπικού της τεχνολογίας των πληροφοριών ακολουθούν διαδικασίες κατά την έκδοση, την αλλαγή και την διακοπή χρήσης συνθηματικών, των λογαριασμών και των προνομίων των χρηστών.
	· Απαιτείται αναγνώριση μοναδικού χρήστη για όλους τους χρήστες των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των χρηστών τρίτων.
	· Προτερόθετοι λογαριασμοί και προτερόθετα συνθηματικά αφαιρούνται από τα συστήματα.
OP2.1.10	Μόνο οι απαραίτητες υπηρεσίες «εκτελούνται» στα συστήματα – όλες οι μη απαραίτητες υπηρεσίες έχουν αφαιρεθεί.
Εργαλεία Διαχείρισης Συστήματος (OP2.2)	
OP2.2.1	Τα νέα εργαλεία, οι νέες διαδικασίες και νέοι μηχανισμοί ασφάλειας αναθεωρούνται ως προς την εφαρμοστικότητά τους σχετικά με την επίτευξη των στρατηγικών ασφάλειας του οργανισμού.
OP2.2.2	Χρησιμοποιούνται εργαλεία και μηχανισμοί για την ασφαλή διαχείριση των συστημάτων και των δικτύων, που αναθεωρούνται και ενημερώνονται ή αντικαθίστανται τακτικά. Παραδείγματα είναι:
	· διατάξεις ελέγχου ακεραιότητας δεδομένων
	· κρυπτογραφικά εργαλεία
	· διαγνώστες ευπάθειας
	· εργαλεία ελέγχου ποιότητας συνθηματικών
	· ανιχνευτές ιών
	· εργαλεία διαχείρισης διαδικασιών
	· συστήματα ανίχνευσης παρείσδυσης
	· ασφαλείς διαδικασίες τηλεδιαχείρησης

	· εργαλεία εξυπηρέτησης δικτύου
	· αναλυτές κίνησης
	· εργαλεία αντιμετώπισης συμβάντων
	· εργαλεία ανάλυσης δεδομένων για την πρόληψη εγκληματικών ενεργειών
Παρακολούθηση και έλεγχος της ασφάλειας της τεχνολογίας των πληροφοριών (OP2.3)	
OP2.3.1	Τα εργαλεία ελέγχου και παρακολούθησης των συστημάτων και των δικτύων χρησιμοποιούνται τακτικά από τον οργανισμό.
	· Η δραστηριότητα παρακολουθείται από το προσωπικό της τεχνολογίας των πληροφοριών.
	· Η δραστηριότητα των δικτύων και των συστημάτων καταχωρίζεται σε ημερολόγιο / καταγράφεται.
	· Τα ημερολόγια επισκοπούνται σε τακτική βάση.
	· Η ασυνήθιστη δραστηριότητα περιγράφεται σύμφωνα με την κατάλληλη πολιτική ή διαδικασία
	· Τα εργαλεία επανεξετάζονται και ενημερώνονται περιοδικά.
OP2.3.2	Ο τοίχος προστασίας και τα λοιπά συστατικά ασφάλειας ελέγχονται περιοδικά σχετικά με την συμμόρφωση με την ανάλογη πολιτική του οργανισμού.
Επιβεβαίωση Γνησιότητας και Εξουσιοδότηση (OP2.4)	
OP2.4.1	Χρησιμοποιούνται οι/η κατάλληλοι(-η) έλεγχοι πρόσβασης και η επιβεβαίωση γνησιότητας χρηστών (π.χ. έγκριση μετατροπής αρχείων, διαμόρφωση δικτύου) που συνάδει με την σχετική πολιτική για τον περιορισμό της πρόσβασης των χρηστών σε:
	· πληροφορίες
	· προγράμματα γενικής-κοινής χρήσης συστήματος
	· πηγαίο κώδικα προγράμματος
	· ευαίσθητα συστήματα
	· ειδικές εφαρμογές και διατάξεις ελέγχου
	· συνδέσεις δικτύου μέσα στον οργανισμό
	· συνδέσεις δικτύου εκτός του οργανισμού
OP2.4.2	Υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες χρήσης πληροφοριών για ατομική και ομαδική πρόσβαση ώστε να:
	· καθιερωθούν κανόνες για την εκχώρηση του κατάλληλου επιπέδου πρόσβασης
	· θεμελιωθεί το αρχικό δικαίωμα πρόσβασης
	· τροποποιηθεί το δικαίωμα πρόσβασης
	· διακοπεί το δικαίωμα πρόσβασης
	· να ανασκοπούνται και να επαληθεύονται περιοδικά τα δικαιώματα πρόσβασης
OP2.4.3	Οι μέθοδοι/μηχανισμοί ελέγχου πρόσβασης περιορίζουν την πρόσβαση σε πόρους σύμφωνα με τα δικαιώματα πρόσβασης που καθορίζονται από τις πολιτικές και τις διαδικασίες.
OP2.4.4	Οι μέθοδοι/μηχανισμοί ελέγχου πρόσβασης αναθεωρούνται και επαληθεύονται περιοδικά.
OP2.4.5	Παρέχονται μέθοδοι ή μηχανισμοί προκειμένου να διασφαλιστεί ότι δεν έχει υπάρξει πρόσβαση, αλλοίωση ή καταστροφή των ευαίσθητων δεδομένων κατά μη εξουσιοδοτημένο τρόπο.
OP2.4.6	Χρησιμοποιούνται μηχανισμοί επιβεβαίωσης γνησιότητας για την προστασία της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των ευαίσθητων δεδομένων. Παραδείγματα είναι:
	· οι ψηφιακές υπογραφές
	· η βιομετρική
Διαχείριση Ευπάθειας (OP2.5)	
OP2.5.1	Υπάρχει ένα τεκμηριωμένο σύνολο διαδικασιών για την διαχείριση τρωτών σημείων, που περιλαμβάνει:

	· την επιλογή εργαλείων αξιολόγησης ευπάθειας, καταλόγων ελέγχου και δεσμών ενεργειών
	· την συμπόρευση με γνωστούς τύπους ευπάθειας και μεθόδους προσβολής ευαισθησίας
	· την ανασκόπηση πηγών πληροφοριών για ανακοινώσεις, συναγερμούς και προειδοποιήσεις ασφάλειας
	· τον προσδιορισμό σημαντικών στοιχείων υποδομής προς αξιολόγηση
	· τον προγραμματισμό αξιολογήσεων ευπάθειας
	· την ερμηνεία και την ανταπόκριση σε αποτελέσματα
	· την συντήρηση της ασφαλούς αποθήκευσης και την διάθεση των δεδομένων ευπάθειας.
OP2.5.2	Τηρούνται οι διαδικασίες διαχείρισης ευπάθειας και αναθεωρούνται και ενημερώνονται περιοδικά.
OP2.5.3	Οι εκτιμήσεις ευπάθειας διενεργούνται σε περιοδική βάση και τα τρωτά σημεία αντιμετωπίζονται όταν προσδιορίζονται.
Κρυπτογράφηση (OP2.6)	
OP2.6.1	Χρησιμοποιούνται οι κατάλληλοι έλεγχοι ασφάλειας για την προστασία των ευαίσθητων δεδομένων ενόσω αυτά βρίσκονται σε κατάσταση αποθήκευσης αλλά και κατά την μετάδοση, που περιλαμβάνουν:
	· την κρυπτογράφηση των δεδομένων κατά την μετάδοση,
	· την κρυπτογράφηση δεδομένων κατά την εγγραφή σε δίσκο
	· την χρήση υποδομής δημόσιου κλειδιού
	· την τεχνολογία ιδεατού ιδιωτικού δικτύου
	· την κρυπτογράφηση για οποιαδήποτε μετάδοση μέσω διαδικτύου
OP2.6.2	Χρησιμοποιούνται κρυπτοθετημένα πρωτόκολλα κατά την τηλεδιαχείριση συστημάτων, δρομολογητών και τοίχων προστασίας.
OP2.6.3	Οι έλεγχοι και τα πρωτόκολλα κρυπτογράφησης ανασκοπούνται, επαληθεύονται και αναθεωρούνται τακτικά.
Σχεδιασμός και Αρχιτεκτονική Ασφάλειας (OP2.7)	
OP2.7.1	Η αρχιτεκτονική και ο σχεδιασμός των συστημάτων για καινούρια και μη αναθεωρημένα συστήματα συμπεριλαμβάνει:
	· προβληματισμούς για στρατηγικές, πολιτικές και διαδικασίες ασφάλειας
	· το ιστορικό διαρροών ασφάλειας
	· τα αποτελέσματα εκτιμήσεων κινδύνων ασφάλειας
OP2.7.2	Ο οργανισμός διαθέτει ενημερωμένα διαγράμματα, τα οποία απεικονίζουν την αρχιτεκτονική ασφάλειας που διατρέχει το σύνολο της επιχείρησης και την τοπολογία δικτύων.

Ασφάλεια Προσωπικού (OP3)	
Διαχείριση Συμβάντων (OP3.1)	
OP3.1.1	Υφίστανται τεκμηριωμένες διαδικασίες για την αναγνώριση, καταγραφή και αντιμετώπιση τυχόν συμβάντων και παραβιάσεων της ασφάλειας, οι οποίες περιλαμβάνουν:
	· βασισμένα στο Διαδίκτυο συμβάντα
	· συμβάντα φυσικής πρόσβασης
	· συμβάντα χειραγώγησης
OP3.1.2	Οι διαδικασίες διαχείρισης συμβάντων ελέγχονται, επαληθεύονται και αναθεωρούνται περιοδικά.
OP3.1.3	Υπάρχουν τεκμηριωμένες πολιτικές και διαδικασίες για την συνεργασία με υπηρεσίες εφαρμογής του νόμου
Γενικές Πρακτικές Προσωπικού (OP3.2)	
OP3.2.1	Τα μέλη του προσωπικού ακολουθούν ορθές πρακτικές ασφάλειας, όπως για παράδειγμα:
	· διασφαλίζοντας τις πληροφορίες για τις οποίες είναι υπεύθυνοι

	· μη αποκαλύπτοντας ευαίσθητα δεδομένα σε τρίτους (αντίσταση στη χειραγώγηση)
	· διαθέτοντας επαρκείς ικανότητες για την χρήση του υλικού και του λογισμικού της τεχνολογίας των πληροφοριών
	· χρησιμοποιώντας ορθές πρακτικές για τα συνθηματικά
	· κατανοώντας και τηρώντας τις πολιτικές και τους κανονισμούς ασφάλειας
	· αναγνωρίζοντας και αναφέροντας συμβάντα
OP3.2.2	Ολόκληρο το προσωπικό, σε όλα τα επίπεδα ευθύνης, εφαρμόζει τα καθήκοντα και την υπευθυνότητα που του έχει ανατεθεί σχετικά με την ασφάλεια των πληροφοριών
OP3.2.3	Υπάρχουν τεκμηριωμένες διαδικασίες για την εξουσιοδότηση και την επίβλεψη εκείνων που εργάζονται με ευαίσθητα δεδομένα ή που εργάζονται σε τοποθεσίες όπου αποθηκεύονται αυτά τα δεδομένα. Και πιο συγκεκριμένα για:
	· τους εργαζόμενους
	· τους εργολάβους, εταίρους, συνεργάτες και το προσωπικό από τρίτους
	· το προσωπικό συντήρησης συστημάτων
	· το προσωπικό συντήρησης εγκαταστάσεων

Παράρτημα Ε. Απλές συμβουλές[4]

ΣΗΜΑΝΤΙΚΕΣ ΥΠΟΔΕΙΞΕΙΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Τα ακόλουθα συνιστούν τις θεμελιώδεις προϋποθέσεις μέσων άμυνας για την εταιρία σας

- ☐ Διεξαγωγή διαδικασιών ελέγχου με φίλτρα ελέγχου για όλους τους εργαζόμενους και αναδόχους σας (π.χ. βάσει αναφορών ή εισηγήσεων)
- ☐ Γνώση και τεκμηρίωση των πολύτιμων πόρων του οργανισμού σας
- ☐ Διάθεση σύντομων, αποδοτικών και επαρκώς τεκμηριωμένων διαδικασιών ασφάλειας
- ☐ Διεξαγωγή βασικής εκπαίδευσης ευαισθητοποίησης σε θέματα ασφάλειας για τους εργαζόμενούς σας
- ☐ Ταχεία ή αυτόματη εφαρμογή προγραμμάτων επιδιόρθωσης τρωτών σημείων λογισμικού μετά από τον έλεγχο της λειτουργικότητάς τους
- ☐ Γνώση του διαθέτοντος πρόσβαση στα συστήματά σας και γιατί
- ☐ Χρήση δύσκολων συνθηματικών και τακτική αλλαγή τους
- ☐ Επιβεβαίωση περί της εφαρμογής αντιιικών διεργασιών σε όλους τους υπολογιστές και τις κινητές συσκευές σας, καθώς και περί της αυτόματης ενημέρωσης του συστήματος για αντιιική προστασία
- ☐ Χρήση διαφορετικών αντιιικών προϊόντων για τους διακομιστές και τους Η/Υ πελάτες του δικτύου σας
- ☐ Χρήση συστήματος φιλτραρίσματος για προστασία έναντι του περιεχομένου ανεπίκλητων ηλεκτρονικών μηνυμάτων, μηχανισμού εξαπάτησης, καθώς και κακόβουλου και απαγορευμένου περιεχομένου
- ☐ Χρήση τοίχου προστασίας, ιδιαίτερα εάν διαθέτετε ευρυζωνική πρόσβαση στο διαδίκτυο
- ☐ Χρήση ενός «όλα σε ένα» δικτυακού συστήματος άμυνας με ένα μικρό δίκτυο

Συνθηματικά

Αυτά είναι τα κλειδιά σας για πρόσβαση στις ηλεκτρονικές σας πληροφορίες. Οποιοσδήποτε μπορεί να προσπελάσει τις πληροφορίες που δεν προστατεύονται με συνθηματικό. Εάν επιλέγετε εύκολα συνθηματικά, είναι αρκετά πιθανό κάποιος να μπορέσει να τα μαντέψει ή να τα αποκρυπτογραφήσει. Στην συνέχεια παρέχονται ορισμένες υποδείξεις για δύσκολα συνθηματικά.

- Ανοίξτε ένα λεξικό σε μία τυχαία σελίδα και επιλέξτε μία μακροσκελή λέξη (ας πούμε με 4 συλλαβές). Χρησιμοποιήστε αυτή τη λέξη αλλά εισάγετε τον αριθμό σελίδας στο μέσο της. Για παράδειγμα εάν η λέξη <multifarious> βρίσκεται στην σελίδα 345 του λεξικού σας, το συνθηματικό σας θα είναι <multi345farious>. (Εάν ξεχάσετε το συνθηματικό, πρέπει να θυμάστε ποια σελίδα επιλέξατε.)

- Επιλέξτε μία «συνθηματική φράση» που σημαίνει κάτι για σας. Για παράδειγμα «η ζέβρα μου λέγεται Σποτ και είναι 9 χρονών". Η φράση αυτή μπορεί να μετασχηματιστεί στο συνθηματικό <mzicS&i9yo>. Αυτό είναι ένα δυσπροσπέλαστο συνθηματικό διότι εμπεριέχει γράμματα, αριθμούς και ειδικούς χαρακτήρες. Το «σπάσιμό» του είναι εξαιρετικά δύσκολο.

Απαράβατοι κανόνες για τα συνθηματικά είναι οι παρακάτω:

- χρησιμοποιείτε τουλάχιστον 8 χαρακτήρες για το συνθηματικό
- βεβαιωθείτε ότι αλλάζετε τακτικά συνθηματικά – π.χ. κάθε μήνα.
- εάν ένας εργαζόμενος αποχωρήσει, αλλάξτε το παλιό συνθηματικό του αμέσως.
- χρησιμοποιείτε ένα συνθηματικό για κάθε εφαρμογή - μη χρησιμοποιείτε το ίδιο συνθηματικό παντού.

Απ' την άλλη πλευρά, υπάρχουν ορισμένα πράγματα που δεν πρέπει να κάνετε με τα συνθηματικά.
Σε αυτά περιλαμβάνονται τα παρακάτω:

- μην γράφετε ένα συνθηματικό!
- μην χρησιμοποιείτε το όνομά σας, το όνομα του συντρόφου σας, τα ονόματα των παιδιών σας, τον αριθμό της άδειας κυκλοφορίας του αυτοκινήτου σας, ημερομηνίες γενεθλίων και ο,τιδήποτε άλλο για σας ή την οικογένειά σας που είναι ευρέως γνωστά ή που μπορεί εύκολα να αποκρυπτογραφηθούν με λίγο "χειραγώγηση"
- Μην χρησιμοποιείτε προσωπικούς ειδικούς κωδικούς, όπως, για παράδειγμα, τον αριθμό τηλεφώνου σας, τον αριθμό ταυτότητάς σας, τον αριθμό αδείας του λογισμικού, που όλα μπορεί να εντοπιστούν.
- Μην χρησιμοποιείτε τους ίδιους αριθμούς ή γράμματα, π.χ. <11111111> σε ένα συνθηματικό και μην χρησιμοποιείτε την λέξη συνθηματικό <password> διότι αυτό είναι ακριβώς το πρώτο που θα δοκιμάσει ένας ηλεκτρονικός πειρατής (χάκερ).
- Μην μοιράζεστε το συνθηματικό σας με άλλους
- Μην χρησιμοποιείτε ένα προτερόθετο συνθηματικό που παρέχεται με ένα στοιχείο του λογισμικού– αλλάξτε το
- Μην χρησιμοποιείτε λειτουργίες ερωτήσεων του τύπου «Θυμήσου το συνθηματικό» σε ένα υπολογιστή διότι τα συνθηματικά που αποθηκεύονται με αυτόν τον τρόπο είναι ευκόλως ανακτήσιμα με ελάχιστη απαιτούμενη δεξιότητα.

Εν συντομία, να μεταχειρίζεστε το συνθηματικό σας με προσοχή. Επιλέξετε ένα δύσκολο συνθηματικό, αλλάζετέ το τακτικά και διαφυλάξτε το.

Ιοί, Σκουλήκια και Δούρειοι Ίπποι

Οι γλωσσαμύντορες θα έλεγαν ότι όλα αυτά είναι διαφορετικά μεταξύ τους αλλά από επιχειρηματική άποψη μπορείτε να τα μεταχειρίζεστε με τον ίδιο τρόπο. Το κρίσιμο σημείο είναι ότι όλα αυτά μπορούν να προκαλέσουν, και όντως προκαλούν βλάβη, στους υπολογιστές και στις πληροφορίες που αποθηκεύονται σε αυτούς. Ωστόσο, η αποφυγή τους είναι πραγματικά απλή. Χρησιμοποιείστε αντιιικό λογισμικό. Οποιοδήποτε αντιιικό λογισμικό επαρκεί δεδομένου ότι όλα δουλεύουν, πάνω – κάτω, με τον ίδιο τρόπο και κάνουν την ίδια δουλειά. Το σημαντικότερο όλων είναι απλά η χρήση ενός λογισμικού προγράμματος.

Αυτό που οι περισσότεροι άνθρωποι δεν αντιλαμβάνονται είναι ότι το αντιιικό λογισμικό πρέπει να ενημερώνεται διαρκώς. Αυτό σημαίνει καθημερινές, ναι, καθημερινές ενημερώσεις, διότι οι συγγραφείς αυτού του λογισμικού ανακοινώνουν νέες εκδόσεις καθημερινά.

Εάν δεν εγκαταστήσετε το λογισμικό αυτό και δεν το ενημερώνετε τόσο τακτικά, είναι 100% εγγυημένο ότι θα «κολλήσετε» κάποιο ιό αργά ή γρήγορα.

Οποιοδήποτε αντιιικό λογισμικό χρησιμοποιείτε, πρέπει να το εγκαταστήσετε προκειμένου να ελέγχει αυτόματα οποιαδήποτε νέα δεδομένα. Μ' αυτόν τον τρόπο, εάν λάβετε καινούρια δεδομένα σε μία δισκέτα, ένα σύμπυκνο δίσκο (CD), ή από το Διαδίκτυο, οι πληροφορίες αυτές θα ελέγχονται για την ύπαρξη ή μη ιών πριν αυτοί προκαλέσουν κάποια βλάβη.

Ένας χρυσός κανόνας είναι ότι οποιαδήποτε προσβεβλημένα από ιούς αρχεία ή δεδομένα πρέπει να καταστρέφονται. Ορισμένα αντιιικά λογισμικά διατείνονται ότι απολυμαίνουν αρχεία αλλά αυτό δεν είναι ποτέ εγγυημένο. Η ασφαλέστερη άποψη είναι να καταστρέφετε το/τα αρχείο(-α) που έχουν προσβληθεί από ιό. Εάν πρόκειται για ηλεκτρονικό μήνυμα, το καταστρέφετε χωρίς να το ανοίξετε!

Ανεπίκλητα ηλεκτρονικά μηνύματα (spam)

Μπορεί να νομίζετε ότι τα μηνύματα αυτά είναι απλώς ένας κακός μπελάς, αλλά, δυστυχώς, κρύβουν εξίσου κινδύνους. Ανεπίκλητα ηλεκτρονικά μηνύματα μπορεί να:

- είναι ένα πρόσχημα γι' απάτη
- είναι ένα επικίνδυνο αλυσιδωτό μηνύματα ηλεκτρονικού ταχυδρομείου
- περιέχει έναν κρυφό κώδικα ο οποίος μπορεί να αλλάξει τις ρυθμίσεις του υπολογιστή σας (π.χ. να σας κατευθύνει σε έναν ιστότοπο πορνογραφικού περιεχομένου)
- περιέχει έναν κρυφό κώδικα ο οποίος μετατρέπει τον υπολογιστή σας σε φορέα αναμετάδοσης ανεπίκλητων μηνυμάτων (που σημαίνει ότι ένας μεγάλος όγκος ανεπίκλητων μηνυμάτων στέλνεται από τον υπολογιστή σας σε ολόκληρο τον κόσμο) και δι' αυτού στέλνονται οι διευθύνσεις των πελατών σας σε ολόκληρο τον κόσμο και με ένα καινούριο αντίγραφο ανεπίκλητων μηνυμάτων/σκουλικιού/δούρειου ίππου που επισυνάπτεται σε αυτόν!

Στην περίπτωση του κρυφού κώδικα, ο κώδικας αυτός, κατά πάσα πιθανότητα εμπίπτει στην κατηγορία 'Δούρειος Ίππος' και μπορεί να εντοπιστεί από το αντιιικό λογισμικό σας. Ωστόσο, υπάρχουν ορισμένοι κανόνες που χρειάζεται να ακολουθήσετε στην περίπτωση των ανεπίκλητων ηλεκτρονικών μηνυμάτων και εφόσον το κάνετε αυτό θα ελαχιστοποιήσετε οποιουσδήποτε κινδύνους.

- Εάν το ηλεκτρονικό μήνυμα δεν έχει προφανή αξία ούτε οποιαδήποτε σχέση με την επιχείρησή σας, είναι ημιαναλφάβητο κλπ. απλώς διαγράψτε το χωρίς να το ανοίξετε.
- Να μην αποκρίνεστε σε ανεπίκλητα ηλεκτρονικά μηνύματα. Η διεύθυνση ηλεκτρονικού ταχυδρομείου σας έχει εντοπιστεί, με τον ένα ή τον άλλο τρόπο, και οι αποστολείς ανεπίκλητων ηλεκτρονικών μηνυμάτων δεν γνωρίζουν εάν υπάρχετε πραγματικά.
- Εάν απαντήσετε, θα επιβεβαιώσετε την παρουσία σας και θα λάβετε πολύ περισσότερα τέτοια ηλεκτρονικά μηνύματα.
- Μην πατάτε το πλήκτρο "πατήστε εδώ για να αφαιρέσετε το όνομά σας από τον κατάλογο διευθύνσεών μας" που βρίσκεται στο ηλεκτρονικό μήνυμα.

Πρόκειται, συνήθως, για απάτη. Δεν θα αφαιρεθεί η διεύθυνσή σας, απλώς θα επιβεβαιώσετε την παρουσία σας.

- Μην γνωστοποιείτε την διεύθυνση του ηλεκτρονικού σας ταχυδρομείου παρά μόνον σε ανθρώπους που μπορείτε να εμπιστευθείτε.
- Αυτό είναι πολύ δύσκολο όταν ασκείτε επιχειρηματική δραστηριότητα διότι επιθυμείτε η διεύθυνση του ηλεκτρονικού σας ταχυδρομείου να είναι ευρέως διαθέσιμη. Εξετάστε το ενδεχόμενο να έχετε δύο διευθύνσεις ηλεκτρονικού ταχυδρομείου· μία δημοσιοποιημένη και μία για προσωπική χρήση, η οποία να ελέγχεται προσεκτικά.
- Εάν ένας ιστότοπος στο Διαδίκτυο σας ζητά την διεύθυνση του ηλεκτρονικού σας ταχυδρομείου κάντε μία γρήγορη εκτίμηση κινδύνων. Πρόκειται για ένα σύννομο οργανισμό που έχει αποδεδειγμένη φήμη; Ή είναι κάποιος για τον οποίο δεν έχετε ακουστά και ο οποίος δεν μνημονεύει μία φυσική επιχειρηματική διεύθυνση στον ιστότοπό του; Να θυμάστε ότι οι απατεώνες παριστάνουν ότι δραστηριοποιούνται ως σύννομες επιχειρήσεις.
- Οι ιστοσελίδες που σας υπόσχονται ότι θα σας αφαιρέσουν από καταλόγους διευθύνσεων ανεπίκλητων ηλεκτρονικών μηνυμάτων γενικά δεν το κάνουν. Μην τις χρησιμοποιείτε.

Το κλείδωμα ανεπίκλητων ηλεκτρονικών μηνυμάτων είναι ένα ενδεχόμενο. Διατίθεται ειδικό λογισμικό κλειδώματος αλλά μπορεί να είναι πολύ ακριβό για μικρές επιχειρήσεις. Είναι πιθανόν να συμφέρει να ζητήσετε από τον Πάροχό σας Υπηρεσιών Διαδικτύου (ISP) εάν μπορεί – έναντι μικρής πρόσθετης αμοιβής – να σας παράσχει κλείδωμα ανεπίκλητων ηλεκτρονικών μηνυμάτων χρησιμοποιώντας δικά του μέσα. Ωστόσο, μια χρήσιμη συμβουλή: το κλείδωμα ανεπίκλητων ηλεκτρονικών μηνυμάτων είναι τέχνη όσο και επιστήμη. Μπορείτε, το ίδιο εύκολα, να κλειδώσετε σύννομα ηλεκτρονικά μηνύματα εάν τα κριτήρια κατά των ανεπίκλητων ηλεκτρονικών μηνυμάτων είναι πολύ αυστηρά.

Υ.Γ. Εάν λάβετε ένα ηλεκτρονικό μήνυμα το οποίο θέτει σε άμεση απειλή την επιχείρησή σας, με τον ένα ή τον άλλο τρόπο, π.χ. εκβιαστικές απειλές, να έρθετε σε επαφή με την αρμόδια Αστυνομική αρχή της περιοχής σας και μάλιστα αμέσως. Θα παραπεμφθείτε γρήγορα σε μία ομάδα, η οποία έχει εκπαιδευτεί να διαχειρίζεται ηλεκτρονικές απειλές. Κάτι τέτοιο είναι πολύ πιθανό να μη σας συμβεί, αλλά για καλό και για κακό…

Κατασκοπευτικό λογισμικό (spyware)

Αυτά είναι μικρά προγράμματα που παρεισφρύουν στο υπολογιστικό σας σύστημα προκειμένου να συγκεντρώσουν λαθραία πληροφορίες για τον/την χρήστη/επιχείρηση χωρίς αυτός/αυτή να το γνωρίζουν. Το μεγαλύτερο μέρος αυτού του λογισμικού αφορά σε διαφημιστικούς σκοπούς αλλά μπορεί επίσης να συγκεντρώσει πληροφορίες για διευθύνσεις ηλεκτρονικού ταχυδρομείου, ακόμα και για συνθηματικά αλλά και στοιχεία για πιστωτικές κάρτες.

Πρόσφατα, δημοσιεύθηκαν επίσημες προειδοποιήσεις σχετικά με το κατασκοπευτικό λογισμικό το οποίο χρησιμοποιείται για την συγκέντρωση ευαίσθητων από εμπορική άποψη δεδομένων, π.χ. στοιχεία συμβάσεων.
Το κατασκοπευτικό λογισμικό δεν είναι ο,τι καλύτερο και ο προσεκτικός χρήστης προσπαθεί να το περιορίσει ή να το αφαιρέσει εντελώς. Διατίθενται δύο καλά πακέτα από το Διαδίκτυο τα οποία αφαιρούν το κατασκοπευτικό λογισμικό. Και τα δύο είναι για προσωπική χρήση, οι επιχειρήσεις, παρ' ολ' αυτά αναμένεται ότι θα τα αγοράσουν. Είναι τα:

- Lavasoft's <Ad-aware>
- Spybot

Συνιστάται να μεταφορτώσετε («κατεβάσετε») και τα δύο αυτά πακέτα και να τα εκτελείτε τουλάχιστον μία φορά τη βδομάδα. Θα εκπλαγείτε με το τι μπορούν να εντοπίσουν. (Και μην ξεχνάτε ότι πρέπει να ενημερώνονται επίσης!)

«Τοίχοι προστασίας» (firewalls)

Τα συστήματα αυτά πήραν τα όνομά τους από τα φυσικά φράγματα που κατασκευάζονται σε κτίρια για την καταπολέμηση της εξάπλωσης της φωτιάς. Με όρους πληροφορικής, ένας «τοίχος προστασίας» δρα ως φραγμός για την αποτροπή μη εξουσιοδοτημένης χρήσης προς/από ένα ιδιωτικό υπολογιστικό σύστημα. Δείτε το σαν ένα είδος πόρτας ασφάλειας και αντικλεπτικού συναγερμού για υπολογιστές. Βοηθά στον περιορισμό όλων εκείνων των εσκεμμένων απειλών που σκιαγραφήθηκαν προηγουμένως. Ένας «τοίχος προστασίας» θεωρείται σήμερα απαραίτητος εάν έχετε έναν ή περισσότερους υπολογιστές συνδεδεμένους με το Διαδίκτυο.

Ο «τοίχος προστασίας» είναι είτε ένα τμήμα λογισμικού είτε ένα είδος υλικού. Για την προστασία μεγάλων υπολογιστικών συστημάτων μπορεί να είναι ένας συνδυασμός λογισμικού και υλικού.

Βασικά ένας «τοίχος προστασίας» ελέγχει όλα τα δεδομένα που εισέρχονται ή ακόμη και όσα εξέρχονται από έναν υπολογιστή ώστε να διασφαλιστεί ότι αυτά είναι σύννομα. Συγκεκριμένα αυτό σημαίνει ότι: ο «τοίχος προστασίας» είναι η καλύτερη άμυνά σας έναντι ενός χάκερ. Για να δώσουμε ένα ζωντανό παράδειγμα, ένας «τοίχος προστασίας» μπορεί να αναχαιτίσει την ανάληψη του ελέγχου του υπολογιστή σας μέσω μίας έμπιστης τρίτης οντότητας και την ρύθμισή του ως αναμεταδότη ανεπίκλητων μηνυμάτων. Είναι άξιο μνείας ότι όταν συνδέετε τον υπολογιστή σας με το Διαδίκτυο, ανοίγετε 65.536 "πόρτες" – ή από τεχνική άποψη "θύρες" – μέσω των οποίων μπορούν να εισχωρήσουν δεδομένα στον υπολογιστή σας. Αυτό που πραγματικά χρειάζεται να κάνετε είναι να αφήνετε ανοιχτές μόνον τις απαραίτητες θύρες για να στέλνετε και να λαμβάνετε δεδομένα και να παραμένουν κλειστές κατά το υπόλοιπο του χρόνου που είστε συνδεδεμένοι με το Διαδίκτυο.

Πρόκειται για ένα εξαιρετικά περίπλοκο πεδίο της επιστήμης των υπολογιστών και το παρόν δεν αποτελεί τον χώρο όπου μπορούν να αναπτυχθούν διεξοδικά οι αρχές και οι πρακτικές του, οι οποίες αποτελούν αντικείμενο διδακτορικών διατριβών. Για καλή τύχη, οι τοίχοι προστασίας λογισμικού είναι σήμερα ανέξοδοι, εύκολοι στην χρήση και εύκολα διαθέσιμοι.
Εάν έχετε έναν υπολογιστή, αγοράστε ένα τοίχο προστασίας λογισμικού. Είναι εύκολος στην εγκατάστασή του. Εσείς απλώς αποδέχεστε τις προτερόθετες ρυθμίσεις του. Εάν έχετε δύο ή περισσότερους υπολογιστές συνδεδεμένους με το Διαδίκτυο, ένας τοίχος προστασίας υλικού αποτελεί την καλύτερη επένδυση και μπορεί να εγκατασταθεί ανάμεσα σε όλους τους υπολογιστές σας και στο καλώδιο το οποίο εξέρχεται προς το Διαδίκτυο. Οι τοίχοι προστασίας υλικού είναι πιο πολύπλοκοι και είναι προτιμότερο να βάλετε έναν ειδικό να τον εγκαταστήσει και να τον διαμορφώσει. Ένας επαγγελματίας θα διασφαλίσει το γεγονός ότι ο τοίχος σας δεν είναι τόσο ασφαλής έτσι ώστε να μην μπορείτε να συνδεθείτε με το Διαδίκτυο.

(Επιχειρήσεις που διαθέτουν έναν ή περισσότερους υπολογιστές θα μπορούσαν να αγοράσουν ένα συνδυασμό λογισμικών τύπου τοίχου προστασίας και αντιικού σε ένα πακέτο. Κάτι τέτοιο επιφέρει οικονομικά και τεχνικά πλεονεκτήματα για την μικρή επιχείρηση.)

Προγράμματα επιδιόρθωσης (patches)

Τα προγράμματα επιδιόρθωσης είναι λιγότερο γνωστά αλλά είναι πολύ σημαντικά και συνδέονται με ιούς και την ηλεκτρονική παρείσφρηση. Όλα τα προγράμματα λογισμικού παρουσιάζουν προβλήματα και ελαττώματα. Στις περισσότερες περιπτώσεις, τα ελαττώματα είναι τόσο επουσιώδη που μπορούν να αγνοηθούν και ενδεχομένως να μην έχουν κανένα αντίκτυπο στην οποιαδήποτε επιχείρηση. Ορισμένα, ωστόσο, ελαττώματα είναι εξαιρετικά σημαντικά για να αγνοηθούν.

Όλοι οι παραγωγοί λογισμικού παρέχουν προγράμματα επιδιόρθωσης - δηλαδή ενημερώσεις λογισμικού σχεδιασμένες ώστε να αφαιρούν προβλήματα από το λογισμικό τους. Εάν έχετε έναν και μοναδικό υπολογιστή που δεν είναι συνδεδεμένος με οτιδήποτε άλλο (όπως με έναν άλλον υπολογιστή, το Διαδίκτυο κλπ) ενδεχομένως να μην χρειάζεται να ανησυχείτε για τα προγράμματα επιδιόρθωσης εφόσον ο υπολογιστής σας δουλεύει άψογα.

Τα παρακάτω ζητήματα αφορούν κυρίως το λειτουργικό σύστημα του υπολογιστή σας. Αυτό είναι το βασικό πρόγραμμα που εκτελείται στην καρδιά του υπολογιστή σας. Μπορεί να χρησιμοποιείτε κάποια έκδοση του Microsoft Windows, ενδεχομένως Apple OSX ή ίσως Unix/Linux. Όλα αυτά τα λειτουργικά συστήματα χρειάζονται, κατά καιρούς, επιδιόρθωση. Παρ' όλ' αυτά πολλές εφαρμογές χρειάζονται επίσης σποραδική επιδιόρθωση. Οι φυλλομετρητές Διαδικτύου και τα πακέτα ηλεκτρονικού ταχυδρομείου συχνά χρειάζονται επιδιόρθωση και δεν είναι ασύνηθες για τα συνήθη λογιστικά πακέτα να χρειάζονται ένα πρόγραμμα επιδιόρθωσης.

Εάν δεν ενημερώνετε τα προγράμματα επιδιόρθωσης λογισμικού, διακινδυνεύετε να υποστεί βλάβη το λογισμικό σας ή, στην περίπτωση του φυλλομετρητή ή του ηλεκτρονικού ταχυδρομείου, να επιτρέψετε σε κακόβουλο λογισμικό να αλλοιώσει την λειτουργία του υπολογιστή σας ή σε κακόβουλους χρήστες να αποκτήσουν τον έλεγχο του υπολογιστή σας.

Οι περισσότεροι κατασκευαστές λογισμικού παρέχουν μία υπηρεσία ειδοποίησης μέσω ηλεκτρονικού ταχυδρομείου που ενημερώνει τους πελάτες τους όταν εκδίδονται νέα προγράμματα επιδιόρθωσης. Συνήθως διαβαθμίζουν σε μία κλίμακα αυτές τις ειδοποιήσεις από κρίσιμες έως αναμενόμενες. Εάν λάβετε μία προειδοποίηση για ένα πρόγραμμα επιδιόρθωσης ζωτικής σημασίας, το οποίο επηρεάζει ένα τμήμα του λογισμικού στο οποίο στηρίζεται η εύρυθμη λειτουργία της επιχείρησής σας, συνιστάται να το εγκαταστήσετε το συντομότερο δυνατό. Η συνέχιση των επιχειρηματικών δραστηριοτήτων σας ενδεχομένως να εξαρτάται από αυτό το γεγονός. Μπορείτε, επίσης, να ελέγχετε τον ιστότοπο του προμηθευτή του λογισμικού σας για ενδιαφέρουσες ειδήσεις ή ενημερώσεις.

Σήμερα οι περισσότεροι κατασκευαστές λογισμικού προσφέρουν αυτόματες ενημερώσεις μέσω του διαδικτύου.

Δημιουργία εφεδρικών αντιγράφων (backup)

Η δημιουργία εφεδρικών αντιγράφων είναι η διαδικασία με την οποία παίρνετε ένα αντίγραφο ηλεκτρονικών δεδομένων, όπως, για παράδειγμα, ενός αρχείου λογαριασμών. Γιατί να μπείτε στον κόπο; Διότι τα ηλεκτρονικά δεδομένα είναι πολύ εύκολο να χαθούν, εγκαταλειφθούν από αμέλεια ή να καταστραφούν. Εάν χάσετε το μοναδικό αντίγραφο των ηλεκτρονικών λογαριασμών σας, με ποιον τρόπο θα διαχειριστείτε την επιχείρησή σας την επόμενη μέρα;

Ένα τυπικό και αποτελεσματικό καθεστώς δημιουργίας εφεδρικών αντιγράφων θα αποτρέψει μεγάλο μέρος των φυσικών ή τυχαίων απειλών που αναφέρθηκαν προηγουμένως. Μπορείτε να αντιγράψετε θεμελιώδους σημασίας δεδομένα σε:

- μία μαγνητική ταινία (παλιότερη μέθοδος που, όμως, αξίζει να την εξετάσετε εξαιτίας του ότι μπορείτε να την επαναχρησιμοποιήσετε)
- μία μονάδα αντιγραφής δίσκου (κατά προτίμηση αφαιρέσιμη)
- ένα σύμπυκνο δίσκο (CD) (των περίπου 700 Mb) ή ένα ψηφιακό βιντεοδίσκο (DVD) (των περίπου 4.3 Gb)

Πρέπει να εξετάσετε το ενδεχόμενο του να δημιουργείτε πολλαπλά εφεδρικά αντίγραφα δεδομένων κρίσιμης σημασίας χρησιμοποιώντας μέσα τριών γενιών. Για παράδειγμα, κρατώντας τα δεδομένα «του τέλους της εβδομάδας» των τελευταίων τριών εβδομάδων με κυλιόμενο τρόπο έτσι ώστε να έχετε πάντοτε εφεδρικά αρχεία τριών εβδομάδων (ή γενιών) για κάθε ενδεχόμενο στην περίπτωση που χρειάζεται να ξαναδημιουργήσετε το σύστημα. Ένα ενδεδειγμένο καθεστώς δημιουργίας εφεδρικών αντιγράφων για μια επιχείρηση (ακόμη και μιας ατομικής επιχείρησης) είναι:

- στο τέλος κάθε εργάσιμης ημέρας – δημιουργία εφεδρικών αντιγράφων όλων των αρχείων που αλλάχθηκαν την ημέρα αυτή
- στο τέλος κάθε εβδομάδας - δημιουργία εφεδρικών αντιγράφων όλων των εφαρμογών (λογαριασμών, αλληλογραφίας κλπ)
- στο τέλος κάθε μήνα - δημιουργία εφεδρικών αντιγράφων και του λειτουργικού συστήματος επίσης

Εάν πρέπει να ανακατασκευάσετε τον υπολογιστή μετά από μία καταστροφική βλάβη, θα χρησιμοποιήσετε τα εφεδρικά αντίγραφα του "τέλους μήνα" για να επαναφέρετε το λειτουργικό σύστημα. Στην συνέχεια επαναφέρατε τα εφεδρικά αντίγραφα εφαρμογών του «τέλους εβδομάδας".
Στο τέλος, επαναφέρατε κάθε εφεδρικό αντίγραφο του "τέλους ημέρας" που δημιουργήθηκε μετά το τελευταίο του "τέλους εβδομάδας". Μ' αυτόν τον τρόπο, θα ανακατασκευάσετε ολόκληρο το σύστημα. Εάν δεν μπορεί να διαβαστεί κανένα από τα εφεδρικά αντίγραφα (ένα εκπληκτικά κοινό φαινόμενο ανεξάρτητα από το μέσο δημιουργίας εφεδρικών αντιγράφων), μπορείτε να επιστρέψετε στο προηγούμενο από τα τρία αντίγραφα και να ξεκινήσετε από εκεί. Εάν συμβεί αυτό, είναι μάλλον απίθανο να αποκαταστήσετε όλα τα αρχεία δεδομένων σας. Αναπόφευκτα κάτι θα χαθεί και στα μέσα που υπέστησαν βλάβη. Αυτό ωστόσο είναι προτιμότερο από το να χάσετε όλα τα πολύτιμα δεδομένα σας.

Αυτό το καθεστώς δημιουργίας εφεδρικών αντιγράφων χρησιμοποιείται από τότε που εφευρέθηκαν οι υπολογιστές και έχει αποδειχθεί ότι είναι αξιόπιστο με την πάροδο του χρόνου. Πιο περίπλοκα καθεστώτα δημιουργίας εφεδρικών αντιγράφων μπορούν να χρησιμοποιηθούν όπου οι αλλαγές δεδομένων γίνονται με ταχύ ρυθμό ή όταν υφίστανται δεδομένα υψηλής αξίας. Να είστε προετοιμασμένοι για την αλλαγή εάν οι κίνδυνοι που απειλούν την επιχείρησή σας μεταβληθούν.

Να διατηρείτε τα εφεδρικά σας αντίγραφα σε ασφαλή τοποθεσία. Είναι τόσο πολύτιμα όσο και τα πρωτότυπα δεδομένα σας, υπόκεινται, δε, στις ίδιες αρχές αναγνώρισης εξουσιοδότησης. Μην τα αφήνετε σε μέρη από όπου μπορούν να κλαπούν ή να υποστούν βλάβη. Και, φυσικά, μην τα αφήνετε πάνω στον υπολογιστή σας. Εάν αυτός καεί, τι θα συμβεί στα εφεδρικά σας αντίγραφα ασφάλειας; Στην ιδανική περίπτωση, να φυλάτε τα εφεδρικά σας αντίγραφα σε ένα εντελώς διαφορετικό κτίριο από αυτό στο οποίο βρίσκεται ο

υπολογιστής σας. Εάν το γραφείο σας υποστεί ολοσχερή καταστροφή από φωτιά, δεν θα θέλατε να έχουν την ίδια μοίρα τα εφεδρικά σας αντίγραφα!

Ένα μείζον πρόβλημα με τα εφεδρικά αντίγραφα λαμβάνει χώρα όταν ο ιδιοκτήτης λησμονεί να τα επισημάνει δεόντως με την ημερομηνία και το θέμα τους. Στην περίπτωση αυτή όταν το εφεδρικό αντίγραφο χρειαστεί σε συνθήκες βιάσης….

Μία εναλλακτική επιλογή, εάν έχετε μεγάλο αριθμό εφεδρικών αντιγράφων σε διαφορετικά μέσα, είναι να αγοράσετε ένα "πυρασφαλές χρηματοκιβώτιο". Ένα τέτοιο χρηματοκιβώτιο μπορεί να φυλάσσεται στις εγκαταστάσεις της επιχείρησης αλλά πρέπει να γνωρίζετε ότι μετά από μία πολύ δυνατή φλογερή φωτιά μπορεί να πρέπει να περάσουν 2/3 ημέρες πριν το χρηματοκιβώτιο έχει κρυώσει αρκετά για να ανοιχθεί.

Υποκλοπή πληροφοριών και ταυτότητας

Πρόκειται για μία από τις γρηγορότερα αναπτυσσόμενες αξιόποινες πράξεις τόσο στο Ηνωμένο Βασίλειο όσο και σε άλλες ανεπτυγμένες χώρες. Έχει δοθεί μεγάλη δημοσιότητα στο γεγονός αυτό αλλά το σημαντικό ζητούμενο δεν αναφέρεται. Η υποκλοπή πληροφοριών και στοιχείων ταυτότητας μπορεί να επηρεάσει εξίσου τις επιχειρήσεις και τους ιδιώτες.

Για μία επιχείρηση είναι ζωτικής σημασίας οι παλιές πληροφορίες να καταστρέφονται με ασφαλή τρόπο. Σε αυτό συμπεριλαμβάνονται και τα έγγραφα και τα ηλεκτρονικά αντίγραφα. Δεν είναι κάτι καινούριο για μικρές επιχειρήσεις, οι οποίες διαθέτουν δικές τους ιστοσελίδες, να υποκλέπτονται στοιχεία από τον ιστότοπό τους από κάποιον που έχει κλέψει παλιά επιστολόχαρτα με κεφαλίδες αποστολέα και έχει βρει σε αυτά υπογραφές διευθυντικών στελεχών. Αυτός ο τρόπος χρησιμοποιείται για να χαλκεύονται επιστολές στις υπηρεσίες καταχώρησης ονομασίας στο διαδίκτυο έτσι ώστε να επανακαταχωρηθεί ο ιστότοπος σε μία νέα φυσική διεύθυνση. Στην συνέχεια οργανώνεται μία δόλια επιχείρηση και χορηγούνται έτσι επιχειρηματικά δάνεια.

Μπορεί επίσης να κλαπούν στοιχεία ταυτότητας ιδιωτών με πρόθεση απάτης. Παρά το γεγονός ότι δεν θα καταστείτε υπόλογος για μία ξεκάθαρη απάτη που διαπράχθηκε από άλλους, το πρόβλημα με την κλοπή στοιχείων ταυτότητας είναι η ανάκτηση της αξιοπιστίας σας από τράπεζες και άλλους χρηματοοικονομικούς οργανισμούς και ιδιαίτερα από υπηρεσίες/φορείς πιστωτικής αναφοράς.
Ορισμένα πράγματα που πρέπει να κάνετε:

- Μην δίνετε προσωπικές πληροφορίες, μέσω του Διαδικτύου, ηλεκτρονικών μηνυμάτων, από το τηλέφωνο ή μέσα από επιστολές, σε οποιονδήποτε εκτός εάν είστε ήδη βέβαιοι ότι μπορείτε να τον/τη εμπιστευθείτε.
- Να θυμάστε ότι οι τράπεζες δεν ζητούν ποτέ να επιβεβαιώσουν οι πελάτες τους τα συνθηματικά ή τους κώδικες πρόσβασής τους μέσω ηλεκτρονικού ταχυδρομείου, οπότε μην δίνετε τέτοιες πληροφορίες.
- Μην πετάτε εμπιστευτικά επιχειρηματικά ή προσωπικά έγγραφα πριν τα τεμαχίσετε πρώτα και, στην ιδανική περίπτωση, χρησιμοποιήστε έναν καταστροφέα εγγράφων που έχει διπλή φορά κοπής (εγκάρσια και διαγώνια).
- Ηλεκτρονικό ή μαγνητικό υλικό, που δεν είναι πλέον χρήσιμο, πρέπει να καταστρέφεται με φυσικά τρόπο και έως του σημείου που δεν μπορεί να ξαναχρησιμοποιηθεί.

- Εάν έχετε ανενεργούς επιχειρηματικούς τραπεζικούς λογαριασμούς ή γραμμές συναλλαγής με παλιούς προμηθευτές, κλείστε τους/τες διότι θα μπορούσαν τύχουν εκμετάλλευσης με πρόθεση απάτης.

Σε κάθε περίπτωση, πρέπει να ελέγχετε εξονυχιστικά, γραμμή – γραμμή, αμέσως μόλις τα πάρετε στα χέρια σας, τα αντίγραφα κίνησης τραπεζικών λογαριασμών και άλλα οικονομικά έγγραφά σας. Οποιεσδήποτε ανεπιθύμητες πληρωμές ή χρεωστικές εγγραφές πρέπει να διερευνώνται άμεσα. Η τράπεζά σας δεν θα ενοχληθεί στην περίπτωση που έχετε οποιεσδήποτε απορίες. Ανησυχούν και αυτοί, το ίδιο με εσάς, προκειμένου για τον περιορισμό της απάτης. Ένα άλλο θέμα είναι να ελέγχετε περιοδικά τις προσωπικές ή επαγγελματικές πιστωτικές σας εγγραφές για οποιαδήποτε από τα ακόλουθα απροσδόκητα συμβάντα:

- ερωτήματα σχετικά με την πιστωτική σας επιφάνεια από εταιρίες με τις οποίες δεν είχατε ποτέ καμία συναλλαγή ή δοσοληψία,
- προσβλητικά σχόλια σχετικά με την πιστωτική σας επιφάνεια,
- ειδοποιήσεις αλλαγής διεύθυνσης, ή
- αναφορές σε αποφάσεις δικαστηρίων κλπ

Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα (WiFi εν συντομία) είναι πολύ ελκυστικά για μικρές επιχειρήσεις. Είναι ανέξοδα στην εγκατάσταση, εύκολα στην διαμόρφωση, παρέχουν ευελιξία και μετριάζουν την δυσκολία και την δαπανηρή διαδικασία καλωδίωσης. Δυστυχώς, είναι επίσης πολύ εύκολο να δημιουργηθεί ένα δίκτυο WiFi που επιτρέπει στον οποιονδήποτε και στον καθένα να διαβάσει τα εμπιστευτικά επιχειρηματικά σας στοιχεία.

Ο μεγάλος κίνδυνος είναι ότι οποιοσδήποτε εντός της ασύρματης περιοχής μπορεί να χρησιμοποιήσει το WiFi δίκτυό σας. Μπορεί να χρησιμοποιήσει την σύνδεσή σας στο Διαδίκτυο δωρεάν, να λάβει γνώση της μεταφοράς δεδομένων σας, π.χ. ηλεκτρονικών μηνυμάτων ή συνθηματικών, να έχει πρόσβαση σε αρχεία δεδομένων στους υπολογιστές σας ή ακόμη και να ξετρυπώσει τα στοιχεία του τραπεζικού σας λογαριασμού. Ένα μη ασφαλές δίκτυο WiFi συνιστά μεγάλο κίνδυνο βιομηχανικής κατασκοπίας.

Η δημιουργία δικτύου WiFi στην επιχείρησή σας απαιτεί προσεκτικό σχεδιασμό και ενδεχομένως να απαιτηθεί βοήθεια από ειδικούς. Η επεξηγηματική αυτή σημείωση δεν μπορεί να αποτελέσει πλήρη οδηγό για την δημιουργία ενός δικτύου. Το σημαντικό σημείο εδώ είναι ότι ένα δίκτυο WiFi μπορεί και πρέπει να δημιουργηθεί με ασφάλεια έτσι ώστε μόνο εσείς και το προσωπικό σας να μπορείτε να το χρησιμοποιείτε, να έχετε πρόσβαση σε και να διαμοιράζεστε δεδομένα. Ακολουθούν ορισμένες βασικές υποδείξεις.

Κατ' αρχήν, δυστυχώς, ορισμένες σημαντικές τεχνικές παρατηρήσεις. Κάθε WiFi πρέπει να συμμορφώνεται με το πρότυπο 802.11 του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE). Υπάρχουν επιμέρους υποσύνολα σε αυτό το πρότυπο. Τα σημαντικά για εσάς είναι τα 802.11 G και 802.11N. Το υποσύνολο 'G' αφορά στο εν λόγω ζήτημα ενώ το 'N' απομακρύνεται κάπως από αυτό. Για επιχειρηματικούς σκοπούς, επικεντρωθείτε στο 'G' τώρα, αν και, σήμερα πωλούνται τα ονομαζόμενα "προ N" εργαλεία, τα οποία όμως μπορεί να μην συμμορφώνονται πλήρως με το τελικό πρότυπο 'N'. Το 'N' προσφέρει πολύ μεγαλύτερες ταχύτητες μετάδοσης και δυνητικά καλύτερη ασφάλεια. Μην δελεαστείτε από τις παρωχημένες σήμερα παραλλαγές 'A' ή 'B' καθώς είναι βραδύτερες και λιγότερο ασφαλείς.

Μην βασίζεστε στην δήλωση επιδόσεων του κατασκευαστή. Γενικά θα έχετε τη μισή ταχύτητα μετάδοσης για τη μισή απόσταση εκτός εάν λειτουργείτε σε εργαστηριακές συνθήκες. Οι κτιριακές κατασκευές μπορεί να έχουν μία σαφή επίδραση στην επίδοση ενός WiFi ενώ τα πέτρινα κτίρια παρουσιάζουν τα περισσότερα προβλήματα.

Τι θα χρειαστείτε:

- Έναν ασύρματο δρομολογητή, ο οποίος μεταδίδει και λαμβάνει τα σήματα δεδομένων που εκπέμπονται σε ολόκληρο το γραφείο. Μπορεί να συντονιστούν πιο εξεζητημένοι δρομολογητές έτσι ώστε το σήμα να περιορίζεται τόσο όσο να καλύπτει απλώς το κτίριο σας.
- Ευρυζωνική σύνδεση , εάν δεν έχετε ήδη.
- Έναν ασύρματο προσαρμογέα για κάθε υπολογιστή. Οι περισσότεροι σύγχρονοι φορητοί υπολογιστές διατίθενται, σήμερα, με ενσωματωμένο προσαρμογέα αλλά οι υπολογιστές γραφείου χρειάζονται ξεχωριστό προσαρμογέα. Συνιστάται ένας ασύρματος προσαρμογέας ο οποίος συνδέεται απευθείας σε μία θύρα USB.

Στην περίπτωση όπου μία επιχείρηση διαθέτει έναν ήδη εγκατεστημένο κεντρικό διακομιστή αρχείων με αποκατεστημένη σύνδεση στο Διαδίκτυο, ο δρομολογητής θα είναι άμεσα συνδεδεμένος στον διακομιστή αρχείων. Τα μικρά γραφεία μπορούν να αγοράσουν ένα δρομολογητή με ενσωματωμένο ευρυζωνικό διαποδιαμορφωτή (μόντεμ). Μπορούν να αγοραστούν πιο εξεζητημένα "μαύρα κουτιά", τα οποία συνδυάζουν δρομολογητή με τοίχο προστασίας για πρόσθετη προστασία. Μία καλή υπόδειξη είναι να αγοράσετε ολόκληρο τον WiFi εξοπλισμό σας από τον ίδιο κατασκευαστή. Μην αναμειγνύετε και ταιριάζετε προϊόντα επειδή, εάν αυτή η επιλογή δεν έχει το επιδιωκόμενο αποτέλεσμα, όλοι οι προμηθευτές θα αλληλοκατηγορούνται. Και, φυσικά, μην αγοράζετε ένα άγνωστης εμπορικής ονομασίας προϊόν.

Οι παρακάτω τεχνικές παρατηρήσεις είναι ουσιώδεις για την ασφάλεια:

- Κάθε μετάδοση δεδομένων πρέπει να είναι κρυπτογραφημένη. Μην χρησιμοποιείτε κρυπτογράφηση προστασίας ασύρματου ισοδύναμης με ενσύρματη (WEP). Χρησιμοποιήστε, αντί γι' αυτή, ασύρματη προστατευόμενη πρόσβαση (WPA ή WPA2).
- Χρησιμοποιείτε προ-μοιρασμένα κλειδιά (PSK) για την δημιουργία μίας μορφής συνθηματικού ανάμεσα στους υπολογιστές και τον δρομολογητή σας. Συνιστάται η χρήση μίας μακροσκελούς κλείδας.
- Δημιουργήστε μία μοναδική ονομασία για το WiFi δίκτυο σας μέσω της αντίστοιχης υπηρεσίας .
- Θέστε αναγνωριστικά (SSID). Δημιουργήστε μία ασφαλή ονομασία.
- Διαμορφώστε τον WiFi δρομολογητή σας έτσι ώστε να μην εκπέμπεται το SSID σας.
- Μην χρησιμοποιείτε ποτέ την προτερόθετη ονομασία του SSID του κατασκευαστή.
- Καταχωρείστε τις διευθύνσεις ελέγχου πρόσβασης μέσων (MAC) των υπολογιστών του γραφείου σας στον δρομολογητή σας και δημιουργήστε έναν κανόνα όπου μόνο οι καταχωρημένες διευθύνσεις MAC μπορούν να συνδιαλέγονται με αυτόν.
- Βεβαιωθείτε ότι τα λειτουργικά συστήματα του διακομιστή και των λοιπών υπολογιστών σας υποστηρίζουν το WiFi πριν αγοράσετε το εξοπλισμό!

Εάν όλα αυτά ακούγονται κάπως δύσκολα, μην αποπειραθείτε να φτιάξετε μόνοι σας το δίκτυό σας. Ζητήστε από έναν ειδικό να σας εγκαταστήσει το WiFi δίκτυό σας. Μην ξεχνάτε

ότι τα δεδομένα σας είναι ενδεχομένως το σημαντικότερο περιουσιακό σας στοιχείο και είναι ανάγκη να προστατευθεί με ένα ασφαλές WiFi. Στο κάτω-κάτω, δεν θέλετε να μετατρέψετε το δίκτυό σας σε ένα σημείο ελεύθερης πρόσβασης για το κοινό.

Τρίτοι

Σε διάφορες επιχειρηματικές δραστηριότητες, που αφορούν τις ΜΜΕ, εμπλέκονται αρκετά συχνά τρίτοι. Στις συνήθεις δεσμεύσεις τους περιλαμβάνονται η παροχή συμβουλευτικών υπηρεσιών για την διαχείριση εμπορικών υποθέσεων και την εμπορία (μάρκετινγκ), καθώς και η υποστήριξη κρίσιμων συστημάτων της τεχνολογίας των πληροφοριών. Συχνότατα σε αυτούς παρέχεται πρόσβαση σε εμπιστευτικές εταιρικές πληροφορίες ή πρόσβαση σε συστήματα και υποδομή δικτύων για λόγους συντήρησης. Είναι απαραίτητο οι επιχειρήσεις να διασφαλίσουν την εμπιστευτικότητα αυτών των πληροφοριών όχι μόνο συμβατικά αλλά και μέσω μίας διαδικασίας διαχείρισης ελέγχου ενδεδειγμένης πρόσβασης. Οι ΜΜΕ πρέπει, κατ' ελάχιστο, να λάβουν υπόψη τους παρακάτω ελέγχους όταν συναλλάσσονται με τρίτους:

- Σύναψη συμφωνίας εμπιστευτικότητας και τήρησης του απορρήτου.
- Παροχή πρόσβασης σε πληροφορίες, εφόσον συντρέχει λόγος ενημέρωσης, που σημαίνει ότι πρέπει να παρέχεται πρόσβαση σε τρίτους σε πληροφορίες που είναι απολύτως απαραίτητες προκειμένου να εκτελέσουν την εργασία τους.
- ΔΕΝ πρέπει να παρέχεται πρόσβαση υποστήριξης τεχνολογίας της πληροφορίας σε τρίτους σε μόνιμη βάση εκτός εάν αυτό είναι αναγκαίο και προβλέπεται ρητά. Η πρόσβαση πρέπει να διακόπτεται άμεσα μετά την ολοκλήρωση των αναγκαίων δραστηριοτήτων. Οι διαδρομές ελέγχου πρέπει να εκτυπώνονται και να ανασκοπούνται προκειμένου να επαληθευθεί ότι οι δραστηριότητες που έλαβαν χώρα περιορίζονταν σε σύννομες διαδικασίες συντήρησης.
- Αιτηθείτε από το τρίτο μέρος το δικαίωμά σας να ελέγχετε τα μέτρα προστασίας ασφάλειάς του ιδιαίτερα σε περιπτώσεις όπου εταιρικές πληροφορίες χαρακτηρισμένες ως ιδιόκτητες και εμπιστευτικές υπόκεινται σε επεξεργασία στις κτιριακές εγκαταστάσεις του.

Πάροχοι Υπηρεσιών

Οι πάροχοι υπηρεσιών είναι βασικά οι πάροχοι υπηρεσιών διαδικτύου (ISP), οι πάροχοι υπηρεσιών εφαρμογών (ASP) και οι πάροχοι τηλεπικοινωνιακών υπηρεσιών. Πριν επιλέξετε έναν πάροχο, τα αρμόδια πρόσωπα πρέπει να ενημερωθούν για τους κανονισμούς που έχουν θεσπιστεί από τον εν δυνάμει υποψήφιο, για παράδειγμα εάν έχουν τεθεί ανώτατα όρια για το εύρος ζώνης , εάν φιλτράρονται τα ηλεκτρονικά μηνύματα και, εάν ναι, σύμφωνα με ποιους κανόνες.

Οι πάροχοι συνήθως αποθηκεύουν δεδομένα χρηστών για σκοπούς τιμολόγησης (επωνυμία, διεύθυνση, αναγνωριστικό χρήστη , τραπεζικό λογαριασμό) καθώς και δεδομένα σύνδεσης και μετάδοσης περιεχομένου (για μια δεδομένη χρονική περίοδο που ποικίλει από τον ένα πάροχο στον άλλο).

Οι χρήστες πρέπει να ζητούν από τους παρόχους τους για ποιο χρονικό διάστημα και ποια στοιχεία των δεδομένων τους παραμένουν αποθηκευμένα. Κατά την επιλογή ενός παρόχου, πρέπει να ληφθεί υπόψη ότι οι πάροχοι στην ΕΕ πρέπει να συμμορφώνονται με τις διατάξεις για την προστασία της ιδιωτικότητας των δεδομένων που ισχύουν για την επεξεργασία των πληροφοριών αυτών.

Μέσω της κρυπτογράφησης, οι χρήστες μπορούν να αποτρέψουν τους παρόχους από το να είναι σε θέση να διαβάσουν το περιεχόμενο των διαβιβαζόμενων δεδομένων.

Πρόσθετοι έλεγχοι:

- Σύμφωνα με ποια κριτήρια επιλέγεται ο πάροχος;
- Ποια μέτρα ασφάλειας εφαρμόζει ο πάροχος;
- Σύμφωνα με ποια κριτήρια φιλτράρονται τα ηλεκτρονικά μηνύματα από τον πάροχο (Πάροχοι Ηλεκτρονικού Ταχυδρομείου); Είναι το προσωπικό διαθέσιμο 24 ώρες το 24ωρο για την αντιμετώπιση τεχνικών προβλημάτων και πόσο ικανό είναι;
- Πόσο καλά προετοιμασμένος είναι ο πάροχος για την περίπτωση βλάβης ενός ή περισσότερων συστημάτων ΤΠ (σχεδιασμός έκτακτης ανάγκης, αντίληψη για τον τρόπο δημιουργίας αντιγράφων)?
- Ποιο επίπεδο διαθεσιμότητας μπορεί να εγγυηθεί ο πάροχος (μέγιστο διάρκειας διακοπής λειτουργίας); Ελέγχει τακτικά το ότι οι συνδέσεις των πελατών παραμένουν σταθερές και εάν έχουν ληφθεί τα μέτρα που απαιτούνται;
- Τι κάνει ο πάροχος για να διαφυλάξει την ασφάλεια των συστημάτων ΤΠ και των πελατών του;

Πρέπει να τηρείται η πολιτική ασφάλειας των πληροφοριών και να ακολουθούνται συστηματικά οι κατευθυντήριες γραμμές ασφάλειας κάθε παρόχου. Πρέπει, επίσης, να είναι εφικτό σε εξωτερικούς χρήστες να επιθεωρούν τις κατευθυντήριες γραμμές ασφάλειας. Το προσωπικό του παρόχου πρέπει να είναι ενημερωμένο για τα θέματα της ασφάλειας της τεχνολογίας των πληροφοριών (ΤΠ) και θα υποχρεώνεται να τηρεί τις κατευθυντήριες γραμμές ασφάλειας. Πρέπει, επίσης, να του παρέχεται τακτική εκπαίδευση (όχι μόνο σε θέματα ασφάλειας).

Προστασία και Ιδιωτικότητα Δεδομένων

Πέραν των ανθρώπων που απασχολείτε, τι θεωρείτε ως βασικό αγαθό της επιχειρηματικής σας οργάνωσης, το οποίο είναι αθέατο, κατά κύριο λόγο υποτιμημένο, που μπορεί να χρησιμοποιηθεί κατά εσφαλμένο τρόπο από λάθος αποδέκτη και να χαθεί αυτοστιγμεί;

Η πιθανότερη απάντηση είναι οι πληροφορίες. Οι επιχειρηματικές πληροφορίες υπόκεινται σε επιθεώρηση και επεξεργασία, από τα κατάλληλα άτομα τότε που τις χρειάζονται, με βάση την ορθή πολιτική ασφάλειας των πληροφοριών. Σήμερα, η νομοθεσία απαιτεί από εσάς να διασφαλίζετε ότι οι πληροφορίες που τηρούνται για τους ανθρώπους προστατεύονται επαρκώς.

Η νομοθετική πράξη του 1998 περί προστασίας των δεδομένων τέθηκε σε ισχύ την 1η Μαρτίου 2000. Αφορά σε προσωπικά δεδομένα, δηλαδή πληροφορίες σχετικά με αναγνωρίσιμα εν ζωή άτομα ή «υποκείμενα των δεδομένων».

Οι απαιτήσεις της εν λόγω νομοθετικής πράξης μπορούν να συνοψιστούν ως εξής:

- Αξιολόγηση των κινδύνων που αφορούν σε πληροφορίες προσωπικού και ευαίσθητου χαρακτήρα
- Αναγνώριση των αναγκαίων ελέγχων για την προστασία των δεδομένων και της ιδιωτικότητας
- Ανάπτυξη και εφαρμογή πολιτικής ασφάλειας των πληροφοριών

Παραπομπές

1. The fraud advisory Panel – Cyber crime what every SME should know about
2. Jack A. Jones, CISSP, CISM, CIS - An Introduction to Factor Analysis of Information Risk (FAIR) - A framework for understanding, analyzing, and measuring information risk
3. ENISA - Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)
4. ENISA - Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools
5. ISO 27001
6. DTI – Directors Guide for Information Security
7. Oxford Integrated Systems - Security in an Uncertain World SME's and a Level Playing Field
8. COMMISSION OF THE EUROPEAN COMMUNITIES - DIRECTORATE GENERAL - B6: Security of Telecommunications and Information Systems -Information Technology Security Evaluation Manual (ITSEM) Version 1.0
9. UK Department of Trade and Industry, Information Technology Security Evaluation Criteria (ITSEC)
10. Leeds Council - Information Assurance Guide and Questionnaire for Small & Medium Sized Businesses (SMEs)
11. Russell Morgan - Information Security for Small Businesses
12. Network and Information Security Report – ICTSB / NISSG
13. COMMISSION RECOMMENDATION of 3 April 1996 concerning the definition of small and medium-sized enterprises
14. The OCTAVE (SM) Method Implementation Guide Version 2.0
15. Charles A. Shoniregun, Impacts and Risk Assessment of Technology for Internet Security – Enabled Information Small-Medium Enterprises
16. Official Journal of the European Union (20.5.2003)
17. Risk Management among SMEs Executive report of discovery research by Alpa A. Virdi (November 2005) Institute of Chartered Accountants in England and Wales
18. Reputation: Risk of risks (An Economist Intelligence Unit white paper) December 2005
19. Risk management service for SMEs (Newsletter) International Accounting Bulletin: 3, May 24, 2006. ISSN: 0265-0223, Lafferty Publications Ltd
20. Information Security Guide for Small businesses (Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), INFOSEC of the office of Government Chief Information Officer (OGCIO) and the Technology Crime Division HK Police force of the HKSAR Government.)
21. http://sme.cordis.lu/home/index.cfm (SME TechWeb)
22. http://europa.eu.int/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm#top (Europe's Information Society – Thematic Portal)