

Ασφαλής διαχείριση της πληροφορίας

Η ανάδειξη της πληροφορίας ως το σημαντικότερο ίσως κεφάλαιο των σύγχρονων επιχειρήσεων, σε συνδυασμό με τα αυστηρά κανονιστικά πλαίσια, καθιστούν την αποτελεσματική διαχείριση και την ασφάλεια των πληροφοριών ζωτικής σημασίας.

Του **Ανδρέα Λάλλου**, Professional Services Manager, BESECURE



Ανδρέας Λάλλου

Ένα από τα βασικότερα ζητήματα που επηρεάζει σημαντικά τις σύγχρονες εταιρείες και οργανισμούς, το οποίο δεν είναι πάντα άμεσα αναγνωρίσιμο, είναι ότι ζούμε πια στην εποχή της πληροφορίας. Και η διαχείριση της πληροφορίας πλέον βασίζεται στην τεχνολογία και σε σχέσεις εμπιστοσύνης όπως τη διαχειρίζονται. Η πληροφορία είναι ίσως το σημαντικότερο αγαθό για κάθε εταιρεία, αφού δρα ως κινητήριος δύναμη για την ανάπτυξη της, ενώ παράλληλα αποτελεί και ανεκτίμητης αξίας αγαθό αν περιέλθει στη διάθεση του ανταγωνισμού. Αν κάποτε ίσχυε ότι η διαχείριση της γνώσης είναι δύναμη, πλέον στην εποχή μας αυτό ισχύει για την διαχείριση της πληροφορίας.

Η ασφάλεια των πληροφοριών

Η πληροφορία μπορεί να σχετίζεται με τις δραστηριότητες της κάθε εταιρείας και να αφορά προϊόντα και υπηρεσίες που παράγει — εμπορεύεται αλλά μπορεί να αφορά και σε δεδομένα τρίτων που επεξεργάζεται όπως συμβαίνει στον κλάδο των Τραπεζών, Χρηματοοικονομικών Υπηρεσιών, Τηλεπικοινωνιών κ.λπ. Η ασφάλεια των πληροφοριών είναι ένα θέμα που προβληματίζει και καλούνται να αντιμετωπίσουν όλες οι σύγχρονες επιχειρήσεις και οργανισμοί. Άλλοτε το πετυχαίνουν, άλλοτε πάλι όχι, με αποτέλεσμα να πλήττεται

η δημόσια εικόνα τους, η αξιοπιστία τους και η ρευστότητά τους, με αντίκτυπο σε κάποιες περιπτώσεις έως και την μη δυνατότητα συνέχισης λειτουργίας τους. Η αναγνώριση της ασφάλειας πληροφοριών ως ένα σημαντικό και πραγματικό επιχειρηματικό πρόβλημα είναι πλέον επιβεβλημένη, λαμβάνοντας υπόψη τον έντονο ανταγωνισμό και πώς επηρεάζεται από τα οικονομικά δεδομένα της εποχής μας. Ορισμένες επιχειρήσεις το αντιλαμβάνονται εγκαίρως και επενδύουν ορθά στον τομέα της ασφάλειας πληροφοριών. Επειδή η ευαισθητοποίηση της κάθε επιχείρησης όταν αυτή διαχειρίζεται πληροφορίες που επηρεάζουν τρίτους όπως Τράπεζες, Τηλεπικοινωνιακοί Πάροχοι κ.λπ., δεν αρκεί για την προστασία αυτών, έχουν θεσμοθετηθεί σε επίπεδο κράτους ή σε ειδικότερο επίπεδο τομέα δραστηριοποίησης, κανονισμοί και νομοθεσίες που επιβάλλουν την ασφάλεια των πληροφοριών με επιβολή άλλων οικονομικών και άλλων ποινικών κυρώσεων.

Η διαχείριση της ασφάλειας πληροφοριών

Η διαχείριση της ασφάλειας πληροφοριών δεν περιορίζεται σε εφαρμογή τεχνολογιών ελέγχου πρόσβασης και προστασίας αυτών από κακόβουλους εξωγενείς παράγοντες, όπως συστήματα firewalls, antivirus, intrusion detection κ.λπ. έναντι κακόβουλων "hackers", αλλά επεκτείνεται και στη διαχείριση όπως έχουν πρόσβαση σε αυτήν. Και η απρόβλεπτη ανθρώπινη συμπεριφορά δεν αντιμετωπίζεται με τεχνολογικά μέτρα, όπως ενδεικτικά υπάλληλος που χρηματίζεται για να "διαρρεύσει" πληροφορίες ή ως άληπτε αναφέρεται σε ορισμένες περιπτώσεις: "there is no patch for human stupidity". Τα μέτρα που απαιτείται να εφαρμοσθούν σε κάθε σύγχρονη εταιρεία και οργανισμό

για την προστασία των πληροφοριών της, είναι πρωτίστως διοικητικά και εν συνεχεία τεχνολογικά. Ενημέρωση και εκπαίδευση για τους κινδύνους και τις απειλές που αντιμετωπίζουν οι εταιρείες είναι το πρώτο μέτρο προκειμένου να υπάρξει η αναγνώριση του προβλήματος και να αντιμετωπισθεί ως ένα πραγματικό επιχειρηματικό πρόβλημα. Η δέσμευση της διοίκησης σχετικά με τα ζητήματα της ασφάλειας, η ανάπτυξη και υποστήριξη μίας ολοκληρωμένη στρατηγικής που έχει ως αποτέλεσμα τη διάθεση των απαιτούμενων πόρων και χρημάτων είναι λύσεις που επέρχονται εφόσον υπάρχει πραγματική κατανόηση και αναγνώριση του κινδύνου. Η διάθεση πόρων είτε είναι σε ανθρώπινο δυναμικό είτε είναι σε επένδυση τεχνολογιών επιφέρει επίσης κόστος για την εταιρεία. Κόστος που δεν είναι πάντα μετρήσιμο, κόστος που αν δεν είναι δικαιολογημένο εγκυμονεί σοβαρούς κινδύνους να είναι μεγαλύτερο και του κόστους απώλειας της ίδιας της πληροφορίας που καλείται να προστατεύσει η εταιρεία. Αυτός είναι σε πολλές περιπτώσεις και ο πιο σημαντικός ανασταλτικός παράγοντας για την πραγματική αναγνώριση και αντιμετώπιση του προβλήματος.

Ο κύκλος ζωής των πληροφοριών

Η BESECURE αποτελεί την πλέον εξειδικευμένη στην Ελλάδα εταιρεία, με αποκλειστικό αντικείμενο την παροχή υπηρεσιών ασφαλείας και διαχείρισης κινδύνου πληροφοριών. Έχοντας την υποστήριξη συνεργατών, όπως της McAfee και της Checkpoint και διαθέτοντας στις τάξεις της έμπειρα στελέχη από ελληνικές και πολυεθνικές εταιρείες Πληροφορικής, η BESECURE έρχεται να καλύψει τις συνεχώς αυξανόμενες απαιτήσεις για πραγματικές λύσεις ασφάλειας πληροφοριών. Η

BESECURE καλύπτει όλο το φάσμα των υπηρεσιών και λύσεων που σχετίζονται με την ασφάλεια των πληροφορικών συστημάτων και την εφαρμογή συστημάτων διαχείρισης ασφάλειας πληροφοριών.

Οι υπηρεσίες και λύσεις ασφάλειας πληροφοριών που παρέχονται έχουν αναπτυχθεί και καλύπτουν όλες τις φάσεις του κύκλου ζωής της ασφάλειας πληροφοριών, όπως τον ορίζουμε στην BESECURE. Κατά την προσέγγισή μας, οποιαδήποτε τεχνολογική λύση και αν υλοποιηθεί σε έναν οργανισμό, αν δεν έχει υπάρξει κατάλληλος σχεδιασμός, σωστή εφαρμογή, κατάλληλη διαχείριση και συνεχής επανέλεγχος λειτουργίας της σύμφωνα με τις απαιτήσεις που έχουν ορισθεί αρχικά ή σε επόμενες φάσεις βάσει των ρυθμών ανάπτυξης της εταιρείας, δεν μπορεί σε βάθος χρόνου να είναι το ίδιο λειτουργική αποτυγχάνοντας έτσι να διαφυλάξει το αρχικό κόστος επένδυσης. Επιπρόσθετα, ο Κύκλος Ζωής της Ασφάλειας της BESECURE προσεγγίζει το μοντέλο PDCA (Plan-Do-Check-Act) όπως ορίζεται και στο σύστημα διαχείρισης ασφάλειας πληροφοριών ISO 27001. Μέσω των υπηρεσιών μας, που προσαρμόζονται στον κύκλο ζωής ασφάλειας όπως τον έχουμε σχεδιάσει στην BESECURE, παρέχουμε συνοδικές λύσεις ασφάλειας πληροφοριών, συνδυάζοντας την εμπειρία, την εξειδικευμένη γνώση και τις στρατηγικές συνεργασίες που έχουμε συνάψει. Ενδεικτικές υπηρεσίες αφορούν Εκπόνησης Μελετών Επικινδυνότητας και Προσδιορισμού Απαιτήσεων Ασφάλειας στην φάση Σχεδιασμού, υπηρεσίες Σχεδιασμού Αρχιτεκτονικής Ασφάλειας Πληροφορικής Υποδομής, Σχεδιασμού και Ανάπτυξη Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών βάση προτύπου ISO/IEC 27001:2005 στην φάση Υλοποίησης, υπηρεσίες Διαχείριση & Παρακολούθηση Υποδομών Ασφαλείας στην φάση Διαχείρισης, υπηρεσίες Έλεγχου & Πιστοποίησης Ασφάλειας βάση διεθνών προτύπων και βέλτιστων πρακτικών, Διενέργειας Τεχνικών Ελέγχων Ασφάλειας και Δοκιμών Διείσδυσης σε πληροφορικά συστήματα και δίκτυα δεδομένων και επικοινωνιών στην φάση Ελέγχου και τέλος υπηρεσίες εκπαίδευσης στην Ασφάλεια Πληροφοριών στην φάση της Εκπαίδευσης.

Υπηρεσίες ασφάλειας

Η BESECURE με τις υπηρεσίες Managed Security, Secure Broadband και Secure Wireless που παρέχει, δίνει τη δυνατότητα στις επιχειρήσεις να αξιοποιήσουν κορυφαίες τεχνολογικές λύσεις ασφάλειας πληροφοριών με χαμηλό κόστος κτήσης και διαχείρισης, επιτρέποντάς τους να εστιάσουν σε άλλους τομείς όπως στην επιχειρηματική τους ανάπτυξη. Οι υπηρεσίες αυτές απευθύνονται σε μικρομεσαίες ή μεγάλες επιχειρήσεις που έχουν απομακρυσμένα σημεία πρόσβασης, όπως μη ελεγχόμενα υποκαταστήματα, απομακρυσμένους εργαζόμενους κ.λπ., σε παρόχους υπηρεσιών Διαδικτύου που επιθυμούν να παρέχουν σε πελάτες τους ολοκληρωμένες λύσεις ασφαλούς πρόσβασης στο Διαδίκτυο, υλοποίησης ιδεατών εικονικών δικτύων και υλοποίηση ασφαλών ασύρματων δικτύων. Οι υπηρεσίες Secure Broadband & Secure Wireless, υποστηρίζονται τεχνολογικά από Unified Threat Management Appliances της Checkpoint, τα οποία ενσωματώνουν την ίδια τεχνολογία που προστατεύει επίσης το 97% των Fortune 500 εταιρειών. Μέσω του Secure Operating Center της BESECURE αναλύουμε τα συμβάντα ασφάλειας που καταγράφονται παρέχοντας εκτενείς διοικητικές και τεχνικές αναφορές, με επιπρόσθετες δυνατότητες κεντρικής διαχείρισης και εφαρμογής πολιτικών ασφάλειας.

Εκπαιδευτικές υπηρεσίες

Η BESECURE στα πλαίσια των εκπαιδευτικών υπηρεσιών που παρέχει έχει συνάψει στρατηγικές συνεργασίες για τη διεξαγωγή αναγνωρισμένων σεμιναρίων που θέτουν τις κατάλληλες βάσεις για την ανάπτυξη Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών που θα υποστηρίξουν τις απαιτήσεις Εταιρικής Διακυβέρνησης & Διακυβέρνησης Ασφάλειας των εταιρειών, επιτρέποντας την υγιή ανάπτυξή τους και τη συμμόρφωσή τους με πρότυπα, κανονισμούς και νομοθεσίες που υπόκεινται. Στα πλαίσια αυτά διοργανώνεται δύο φορές το χρόνο, το πιστοποιημένο σεμινάριο HISP (Holistic Information Security Practitioner), με το επόμενο σεμινάριο να διενεργείται στις 14-18 Απριλίου σε συνεργασία με την Ελληνοαμερικανική Ένωση.

Το HISP Course παρέχει στους συμμετέχοντες τις απαραίτητες γνώσεις ώστε να εφαρμόσουν ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών που είναι συμβατό με τις απαιτήσεις Εταιρικής Διακυβέρνησης & Διακυβέρνησης Ασφάλειας, διεθνή πρότυπα, κανονισμούς και νομοθεσίες όπως ISO 27001, Sarbanes Oxley Act, EU Data Protection Act, FACT Act, HIPPA, VISA PCI Data Security κ.α. Αυτό πετυχαίνεται μέσω της αντιστοίχησης των απαιτήσεων αυτών σε διεθνή αναγνωρισμένα frameworks, όπως ISO 27002, ITIL, CobIT και COSO. Η πιστοποίηση HISP σε συνείδηση εξετάσεων, μετά την εκπαίδευση βεβαιώνει ότι ο επαγγελματίας έχει γνώσεις εφαρμογής βέλτιστων διεθνών πρακτικών σε θέματα Εταιρικής Διακυβέρνησης και Διακυβέρνησης Ασφάλειας, ότι κατέχει μια ολιστική προσέγγιση στη διαχείριση του ρίσκου ασφάλειας πληροφοριών και ότι μπορεί να αντιστοιχήσει τις βέλτιστες πρακτικές των ISO 27002, ITIL, CobIT και COSO σε υπάρχουσες αλλά και μελλοντικές απαιτήσεις συμμόρφωσης του οργανισμού σε κανονισμούς και νομοθεσίες. Η BESECURE, με το εύρος των λύσεων και υπηρεσιών που παρέχει καλύπτει ένα εύρος επιχειρήσεων ανεξαρτήτως κλάδου δραστηριοποίησης, δεδομένου ότι το θέμα της ασφάλειας των πληροφοριών δεν περιορίζεται σε συγκεκριμένους κλάδους αλλά προσαρμόζει σε κάθε εταιρεία που επιθυμεί να διαφυλάξει το πιο πολύτιμο αγαθό της, τις πληροφορίες που διαχειρίζεται. Ειδικότερα για τους κλάδους των Τραπεζών, Χρηματοοικονομικών Υπηρεσιών, Τηλεπικοινωνιών, παρέχονται εξειδικευμένες λύσεις κυρίως λόγω των ιδιαίτερων απαιτήσεων ασφάλειας βάσει αναγκών συμμορφώσεως με κανονισμούς και της κρισιμότητας των διαχειριζόμενων πληροφοριών.



Στοιχεία Επικοινωνίας
BESECURE
www.besecure.gr
τηλ. 210 3307440
fax. 210 3307441