ebusinessforum

Ο ΔΕΚΑΛΟΓΟΣ

ΓΙΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΠΙΧΕΙΡΕΙΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΒΙΟΜΗΧΑΝΙΑΣ

ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ, ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΠΟΚΕΝΤΡΩΣΗΣ
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
"ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ"

ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ
ΕΥΡΩΠΑΪΚΟ ΤΑΜΕΙΟ
ΠΕΡΙΦΕΡΕΙΑΚΗΣ ΑΝΑΠΤΥΞΗΣ

Το e-Business Forum αποτελεί έργο του Ε.Π. Κοινωνία της Πληροφορίας (Μέτρο 3.1), υλοποιείται από την ΕΔΕΤ Α.Ε. και συγχρηματοδοτείται κατά 75% από το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης και κατά 25% από εθνικούς πόρους.

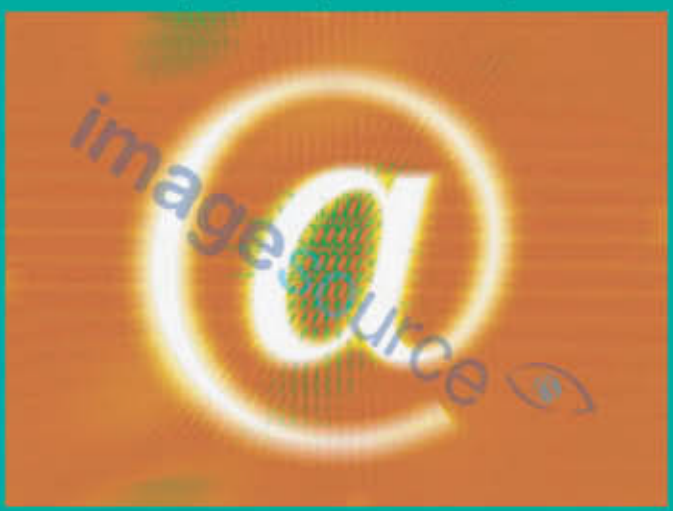
Ο ΔΕΚΑΛΟΓΟΣ ΓΙΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΠΙΧΕΙΡΕΙΝ

▶ 1. Ποιές είναι οι συνήθεις απαιτήσεις ασφάλειας (security requirements) που έχουν οι οργανισμοί και οι συναλλασσόμενοι, στα πλαίσια μιας ηλεκτρονικής δοσοληψίας και με ποιόν τρόπο αυτές μπορούν να ικανοποιηθούν;

Πρωταρχική σημασία για την αντιμετώπιση και επίλυση των προβλημάτων ασφάλειας (security) έχει η αναγνώριση εκ μέρους ενός οργανισμού των πραγματικών απαιτήσεων ασφάλειας που παρουσιάζει. Υπάρχουν τρεις κύριες πηγές για το σκοπό αυτό:

- Η αποτίμηση των κινδύνων (risk assessment) που αντιμετωπίζει ο οργανισμός: Μέσω αυτής της διαδικασίας, αναγνωρίζονται οι πιθανές απειλές προς τον οργανισμό, υπολογίζεται η ευπάθεια του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποίησής τους και το κόστος που θα έχουν για τον οργανισμό.
- Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.
- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες στη λειτουργία του.

Ένας αριθμός απαιτήσεων ελέγχου και προστασίας θεωρούνται θεμελιώδεις για την ασφάλεια πληροφοριών σε κάθε οργανισμό. Αυτές, είτε βασίζονται σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική σε θέματα ασφάλειας. Απαιτήσεις απαραίτητες σε έναν οργανισμό, που βασίζονται στη νομοθεσία, είναι η διαφύλαξη των προσωπικών δεδομένων, η διαφύλαξη των δεδομένων του οργανισμού και τα δικαιώματα πνευματικής ιδιοκτησίας. Απαιτήσεις που έχουν καθιερωθεί ως κοινή πρακτική είναι η εκπόνηση πολιτικής ασφάλειας, ο καταμερισμός καθηκόντων σχετικών με την ασφάλεια, η εκπαίδευση σε θέματα ασφάλειας, η αναφορά συμβάντων και η διαχείριση της επιχειρησιακής συνέχειας.



Παράλληλα, λαμβάνοντας υπόψη και την οπτική των ηλεκτρονικά συναλασσομένων καταναλωτών, οι απαιτήσεις ασφάλειας στο χώρο του ηλεκτρονικού επιχειρείν αφορούν, κυρίως, δραστηριότητες στα πλαίσια επικοινωνίας ηλεκτρονικού ταχυδρομείου και μεταφοράς δεδομένων μέσω δημόσιων δικτύων, όπως το Internet. Τα μέτρα ασφάλειας για την προστασία των εμπλεκομένων σε ηλεκτρονικές συναλλαγές θα πρέπει να περιλαμβάνουν, μεταξύ άλλων, τις παρακάτω υπηρεσίες:

- Αυθεντικοποίηση (authentication), η οποία αφορά το επίπεδο εμπιστοσύνης που οι συναλλασσόμενοι απαιτούν σε σχέση με την ταυτότητα των εμπλεκόμενων μερών.
- Εξουσιοδότηση (authorization), που αφορά τα δικαιώματα καθορισμού των παραμέτρων των συναλλαγών (τιμοκατάλογοι, ψηφιακά έγγραφα κλπ.). Επίσης θα πρέπει οι συναλλασσόμενοι να γνωρίζουν ποιος έχει τέτοια δικαιώματα.
- Ακεραιότητα (integrity) στοιχείων που γνωστοποιούνται στους αγοραστές (πχ. του τιμοκαταλόγου και λοιπών στοιχείων), καθώς και προστασία πληροφοριών για ειδικές εκπτώσεις.
- Μη-αποποίηση (non-repudiation) αποστολής και λήψης μηνυμάτων στα πλαίσια της δοσοληψίας
- Διαδικασίες ελέγχου των πληροφοριών που παρέχει ο πελάτης για την πληρωμή των αγαθών.
- Μηχανισμούς για την προστασία των στοιχείων της δοσοληψίας, αναφορικά με την ακεραιότητα, την εμπιστευτικότητα (confidentiality) και την ιδιωτικότητα (privacy) των εμπλεκομένων.
- Καθορισμό των ευθυνών και ανάληψης κινδύνου για την περίπτωση απάτης.

Αρκετά από τα παραπάνω αντιμετωπίζονται με τη χρήση κρυπτογραφίας και των εφαρμογών της, σε συνδυασμό πάντοτε με τη σχετική νομοθεσία. Ιδιαιτέρως, σε θέματα αναγνώρισης ψηφιακών υπογραφών, έχει τεθεί σε ισχύ ήδη από τον Ιούνιο του 2001, το ΠΔ 150/2001 το οποίο αναφέρεται στη νομική ισοδυναμία των ιδιόχειρων με τις ψηφιακές υπογραφές. Ακρογωνιαίο λίθο για την αξιοποίηση των ψηφιακών υπογραφών, αποτελεί η αξιόπιστη λειτουργία των Παρόχων Υπηρεσιών Πιστοποίησης (Certification Service Providers), σύμφωνα με το πλαίσιο που οριστικοποιεί η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (www.eett.gr).

▶ 2. Με ποιόν τρόπο μπορούμε να επιβεβαιώσουμε την αυθεντικότητα μιας εμπορικής ιστοσελίδας που επισκεπτόμαστε; Πόσο υψηλό κίνδυνο διατρέχουμε όταν αποστέλλουμε ηλεκτρονικά τον αριθμό της πιστωτικής μας κάρτας, στα πλαίσια μιας ηλεκτρονικής δοσοληψίας διαμέσου του Internet;

Τα πλέον αξιόπιστα ηλεκτρονικά καταστήματα, που δείχνουν ιδιαίτερη μέριμνα για την ασφάλεια των διακινούμενων δεδομένων κατά τη διάρκεια μιας συναλλαγής, συνήθως αξιοποιούν ευρέως γνωστές υπηρεσίες ασφάλειας και αναφέρουν ρητά στην ιστοσελίδα τους, στα πλαίσια της ακολουθητέας πρακτικής τους, τις λύσεις ασφάλειας τις οποίες χρησιμοποιούν. Συνήθως συστήνεται σε όσους ετοιμάζονται να εμπλακούν σε μία ηλεκτρονική συναλλαγή να μελετήσουν προσεχτικά τις υπηρεσίες

ασφάλειας που χρησιμοποιούνται. Κατά κανόνα, προηγείται ενημέρωση για την "ταυτότητα" της ιστοσελίδας του ηλεκτρονικού καταστήματος στη διεθνή βάση δεδομένων www.whois.net ή στη βάση των ελληνικών καταχωρήσεων www.hostmaster.gr/cgi-bin/webwhois. Στις ιστοθέσεις αυτές αναφέρεται σε ποιό νομικό ή φυσικό πρόσωπο έχει κατοχυρωθεί το συγκεκριμένο ηλεκτρονικό κατάστημα. Επίσης, σε αρκετές ιστοσελίδες υπάρχει σχετικό σήμα το οποίο μπορεί να αξιοποιηθεί για την πιστοποίηση της εταιρικής ταυτότητας μέσω σχετικής υπηρεσίας που διατίθεται από Παρόχους Υπηρεσιών Πιστοποίησης (Certification Service Provider). Επιπλέον, είναι αρκετές φορές χρήσιμο, πριν την ηλεκτρονική δοσοληψία, να επικοινωνεί κανείς με τον τηλεφωνικό αριθμό του φυσικού καταστήματος (η αναγραφή του αριθμού είναι υποχρεωτική), για εκ των προτέρων επιβεβαίωση της αυθεντικότητας του καταστήματος.

Σχετικά με την ηλεκτρονική αποστολή του αριθμού πιστωτικής κάρτας διαμέσου του Internet, παρά το γεγονός ότι αποτελεί υπαρκτό πρόβλημα η ενδεχόμενη υποκλοπή, έχει αναπτυχθεί υπερβολική σχετική φιλολογία, με αποτέλεσμα να μην περιγράφεται το πρόβλημα στις αληθινές του διαστάσεις. Κατά κανόνα, πλέον, τα ηλεκτρονικά καταστήματα αξιοποιούν τις εφαρμογές της κρυπτογραφίας με σκοπό την αποτελεσματική διασφάλιση της εμπιστευτικότητας των δεδομένων (π.χ. κρυπτογράφηση/αποκρυπτογράφηση δεδομένων), της ακεραιότητας των δεδομένων (π.χ. κώδικες αυθεντικοποίησης μηνυμάτων ή ψηφιακές υπογραφές), της αυθεντικοποίησης του αποστολέα ενός μηνύματος (π.χ. ψηφιακές υπογραφές) κλπ. Είναι σύνηθες το παράδειγμα της αξιοποίησης του πρωτοκόλλου SSL (Secure Socket Layer) κατά τη διάρκεια μιας συναλλαγής διαμέσου του Web, γεγονός το οποίο επιβεβαιώνεται από τη διαδικτυακή διεύθυνση που μεταβάλλεται πλέον σε https://

Σε κάθε περίπτωση, ακόμη και αν παρατηρηθεί σε μία πιστωτική κάρτα χρέωση που δεν ανταποκρίνεται στην πραγματικότητα, ο συναλασσόμενος διατηρεί το δικαίωμα να ζητήσει από την τράπεζα να ακυρώσει τη συναλλαγή, υπό την προϋπόθεση βεβαίως ότι το αίτημα θα υποβληθεί σε εύλογη προθεσμία που καθορίζεται από τη σύμβαση που υπογράφεται μεταξύ πελάτη-τράπεζας. Η τράπεζα υποχρεούται να διερευνήσει την καταγγελία και ακολούθως να ενεργήσει με τρόπο ανάλογο με εκείνον που ακολουθεί στις συμβατικές συναλλαγές. Σε περίπτωση που το αίτημα είναι εύλογο, τα χρήματα επιστρέφονται αφού η συναλλαγή θεωρείται ως μηδέποτε διεξαχθείσα.

▶ 3. Με ποιόν τρόπο μπορεί μία επιχείρηση να αποκτήσει ολοκληρωμένη εικόνα για τη σημαντικότητα των κινδύνων που αντιμετωπίζουν τα Πληροφοριακά Συστήματα της;

Σε περίπτωση που μία επιχείρηση ή ένας οργανισμός επιθυμεί να καταγράψει και αντιμετωπίσει τα προβλήματα ασφάλειας που υπάρχουν, μπορεί να ακολουθήσει διάφορες στρατηγικές.

Αν η επιχείρηση είναι μικρής κλίμακας, μπορεί να εφαρμόσει κατευθείαν τη βασική προσέγγιση (baseline approach), στα πλαίσια της οποίας επιλέγονται απευθείας βασικά μέτρα προστασίας, τα οποία είναι ευρέως γνωστά από υπάρχοντες κώδικες ακολουθητέας πρακτικής σε διεθνές επίπεδο.

Αν η επιχείρηση είναι μεγαλύτερη και τα πληροφοριακά συστήματα έχουν ιδιαίτερη σημασία για τη λειτουργία της, για την αποτελεσματική και ολοκληρωμένη καταγραφή των προβλημάτων ασφάλειας που δυνητικά αντιμετωπίζει, ως επαρκέστερη επιστημονικά μέθοδος προτείνεται η εκπόνηση λεπτομερούς μελέτης ανάλυσης και διαχείρισης επικινδυνότητας (detailed risk analysis and management review) με χρήση πρότυπης αυτοματοποιημένης μεθοδολογίας, από έμπειρους μελετητές. Στα πλαίσια της μελέτης αυτής, αρχικά καταγράφονται λεπτομερώς και αποτιμώνται συγκριτικά τα αγαθά (assets) που περιλαμβάνονται στο πληροφοριακό σύστημα, μελετώνται διεξοδικά οι απειλές (threats) που υφίσταται το σύστημα και τα σημεία ευπάθειας που αυτό παρουσιάζει (vulnerabilities) και ακολούθως υπολογίζεται ο βαθμός επικινδυνότητας (risk factor) του συστήματος. Τελικά, αναπτύσσεται ένα ολοκληρωμένο σχέδιο ασφάλειας (Security Plan) για τον οργανισμό, το οποίο περιλαμβάνει τόσο τα προτεινόμενα αντίμετρα (countermeasures), όσο και την πολιτική ασφάλειας (Security Policy) του οργανισμού.

Τα προτεινόμενα αντίμετρα μπορεί να είναι κυρίως τεχνικά, αλλά και διοικητικά και οργανωτικά.

Η πολιτική ασφάλειας περιγράφει το σύνολο των κανόνων που καθορίζουν τον τρόπο με τον οποίο ένας οργανισμός προστατεύει τα πληροφοριακά του συστήματα, έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας. Η πολιτική ασφάλειας συντάσσεται λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά του οργανισμού και του τομέα της οικονομίας στον οποίο δραστηριοποιείται, βασίζεται στα αποτελέσματα της μελέτης ανάλυσης επικινδυνότητας, καθώς και στις βασικές διαστάσεις των στρατηγικών κατευθύνσεων του οργανισμού, σε σχέση με την αξιοποίηση των τεχνολογιών Πληροφορικής και Επικοινωνιών. Αξίζει να σημειωθεί, ότι η πολιτική ασφάλειας αποτελεί υπηρεσιακό κείμενο και θα πρέπει να λαμβάνεται μέριμνα, ώστε όλα τα μέλη του προσωπικού που έχουν ρόλο στη λειτουργία των συστημάτων, είτε ως χρήστες, είτε ως διαχειριστές, είτε ως διοικητικά στελέχη, να λάβουν γνώση της.

▶ 4. Με ποιόν τρόπο μπορούν να διασφαλιστούν τα συστήματα μιας επιχείρησης, στη συνήθη πλέον περίπτωση που η ανάπτυξη του πληροφοριακού συστήματος ή/και η επεξεργασία των δεδομένων έχουν ανατεθεί σε άλλον εξωτερικό φορέα (outsourcing);

Οι απαιτήσεις ασφάλειας μιας επιχείρησης, η οποία αναθέτει την ανά-πτυξη του πληροφοριακού της συστήματος ή/και την επεξεργασία των δεδομένων σε εξωτερικό φορέα, θα πρέπει να συμφωνηθούν με τη μορφή συμβάσεως ανάμεσα στα

εμπλεκόμενα μέρη. Γενικά, τα ζητήματα σχετικά με την προσπέλαση και επεξεργασία στο σύστημα εξωτερικών φορέων, θα πρέπει να ρυθμίζονται με ειδικές συμβάσεις, οι οποίες και θα διασφαλίζουν ότι οι τρόποι προσπέλασης και η επεξεργασία των δεδομένων είναι σύμφωνοι με την πολιτική ασφάλειας της επιχείρησης. Οι συμβάσεις θα πρέπει να προβλέπουν και σχετικές αποζημιώσεις για τα δύο μέρη, ενώ πρέπει να περιλαμβάνουν, μεταξύ άλλων, τα ακόλουθα:

- Τη γενική πολιτική σχετικά με την ασφάλεια των πληροφοριών.
- Τις ευθύνες των μερών της σύμβασης.
- Τον τρόπο με τον οποίο θα ικανοποιούνται οι απαιτήσεις της σχετικής νομοθεσίας και τις ευθύνες που απορρέουν από αυτήν.
- Τον τρόπο με τον οποίο θα διασφαλιστεί η ορθή και σαφής κατανομή αρμοδιοτήτων σε όλα τα εμπλεκόμενα μέρη.
- Την προστασία των διαφόρων πόρων συμπεριλαμβανομένων των διαδικασιών μέσω των οποίων οι πόροι αυτοί θα προστατεύονται, των διαδικασιών με βάση τις οποίες θα ελέγχεται η ασφάλεια τους, των μηχανισμών ελέγχου και προστασίας, τους κανόνες διαθεσιμότητας και ακεραιότητας, όπως και τους περιορισμούς σχετικά με την αντιγραφή πληροφοριών, την εμπιστευτικότητα τους και την απαιτούμενη εχεμύθεια.
- Τον τρόπο ελέγχου πρόσβασης στα δεδομένα του οργανισμού.
- Τα επίπεδα φυσικής ασφάλειας.
- Την περιγραφή των υπηρεσιών που θα είναι διαθέσιμες, το απαιτούμενο επίπεδο ποιότητας τους, καθώς και τη διαθεσιμότητα των απαραίτητων υπηρεσιών σε περίπτωση ανάγκης.
- Τα δικαιώματα ελέγχου και ιχνηλάτησης (audit).
- Τις διαδικασίες χειρισμού, επίλυσης και αναφοράς συμβάντων.
- Τις σχέσεις των τρίτων μερών με λοιπούς υπεργολάβους.

Σε κάθε περίπτωση, θα πρέπει στην υπογραφείσα σύμβαση να περιλαμβάνεται ένα ολοκληρωμένο σχέδιο ασφάλειας (security plan) στο οποίο θα πρέπει να έχουν συμφωνήσει τα εμπλεκόμενα μέρη.

5. Τι ακριβώς εννοούμε με τον όρο "Σχέδιο Επιχειρησιακής Συνέχειας" ("Business Continuity Plan"), ποιά η σημαντικότητα του και ποιές οι κυριότερες παράμετροι κατά τη διαχείριση του;

Το "Σχέδιο Επιχειρησιακής Συνέχειας" ("Business Continuity Plan") ενός οργανισμού αποτελεί ένα λεπτομερή οδηγό τόσο για την αντιμετώπιση εκτάκτων περιστατικών που θέτουν σε κίνδυνο την εύρυθμη λειτουργία ενός οργανισμού, όσο και για την ανάκαμψη (recovery) συστημάτων έπειτα από οποιαδήποτε ζημία ή καταστροφή.

Σκοπός της εκπόνησης ενός Σχεδίου Επιχειρησιακής Συνέχειας, είναι η αποτροπή εμποδίων στις επιχειρηματικές δραστηριότητες του οργανισμού και η προστασία των κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών στα συστήματα του. Μια διαδικασία διαχείρισης της επιχειρησιακής συνέχειας του οργανισμού (business continuity management process) θα πρέπει να αξιοποιείται για τη μείωση, σε ανεκτό επίπεδο, των επιπτώσεων από καταστροφές και συμβάντα σχετικά με την ασφάλεια του οργανισμού. Τέτοιες καταστροφές μπορεί να είναι αποτέλεσμα φυσικών καταστροφών, αστοχίας υλικών ή σκόπιμων ενεργειών. Επιπλέον θα πρέπει να περιλαμβάνονται και μέτρα για την αποκατάσταση της ομαλής λειτουργίας του οργανισμού. Ο σχεδιασμός για την αντιμετώπιση απρόοπτων γεγονότων θα πρέπει να εξασφαλίζει την αποκατάσταση των επηρεαζόμενων λειτουργιών μέσα σε ένα ρεαλιστικό και αποδεκτό χρονικό πλαίσιο.

6. Από τη νομοθεσία για την προστασία προσωπικών δεδομένων απορρέουν νέες/πρόσθετες δεσμεύσεις για μία επιχείρηση που συναλλάσσεται ηλεκτρονικά;

Η συλλογή και επεξεργασία προσωπικών δεδομένων εξελίσσεται σε συστατικό στοιχείο των ενδοδικτυακών συναλ-λαγών. Προσωπικά δεδομένα συλλέγονται συνήθως ήδη κατά την αρχική φάση σύνδεσης του ενδιαφερόμενου καταναλωτή με το δικτυακό χώρο της επιχείρησης, συχνά μέσω εντύπων που συμπληρώνει ψηφιακά ο πλοηγός-αγοραστής. Η συλλογή δεδομένων, συνήθως με απώτερο σκοπό τη δημιουργία του προφίλ του "πελάτη", γίνεται συχνά και με άλλους τρόπους, όπως εγκατάσταση cookies, τεχνικές εξόρυξης δεδομένων κλπ.. Η χρήση τέτοιων τεχνικών παρουσιάζεται συνήθως ως αναγκαιότητα για τη διαμόρφωση των πολιτικών και της στρατηγικής των επιχειρήσεων.

Ωστόσο, όσοι δραστηριοποιούνται στο πεδίο των ηλεκτρονικών συναλλαγών οφείλουν να γνωρίζουν πως ό,τι είναι τεχνικά

δυνατό δεν είναι αυτονόητα και νόμιμο ή θεμιτό. Η συλλογή και επεξεργασία προσωπικών δεδομένων στο πλαίσιο του ηλεκτρονικού επιχειρείν υπόκειται στις ρυθμίσεις, τις προϋποθέσεις και απαγορεύσεις των νόμων 2472/97 για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων και 2774/99 για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα και τις επιμέρους ερμηνευτικές Οδηγίες που έχει εκδώσει η Αρχή Προστασίας Προσωπικών Δεδομένων (http://www.dpa.gr).

Ένα κρίσιμο στοιχείο είναι ότι η συλλογή και επεξεργασία προσωπικών δεδομένων επιτρέπεται καταρχήν μόνο με συγκατάθεση του χρήστη-πελάτη ή στο πλαίσιο της εκπλήρωσης μιας σύμβασης που ήδη συνδέει την επιχείρηση με αυτόν. Σε άλλη περίπτωση η συλλογή τέτοιων δεδομένων είναι νόμιμη εφόσον αυτά προέρχονται από καταλόγους και πηγές δημόσια προσβάσιμες που απευθύνονται στο ευρύ κοινό καθώς και προηγούμενες συναλλακτικές επαφές στο πλαίσιο συναφών σκοπών. Τα προσωπικά δεδομένα των αντισυμβαλλόμενων ή των ενδιαφερόμενων επισκεπτών των ιστοσελίδων μιας επιχείρησης πρέπει να συλλέγονται με τρόπο νόμιμο, θεμιτό και διαφανή. Όπως τονίζεται στην νέα Οδηγία 2002/58/ΕΚ "σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών" λογισμικό παρακολούθησης, δικτυακοί "κοριοί" (web bugs), κρυφά αναγνωριστικά στοιχεία και άλλες παρόμοιες διατάξεις που μπορούν να εισέλθουν στο τερματικό του χρήστη εν αγνοία του με σκοπό την πρόσβαση σε πληροφορίες, την αποθήκευση αθέατων πληροφοριών ή την ανίχνευση των δραστηριοτήτων του χρήστη, συνιστούν ενδεχόμενη σοβαρή παραβίαση της ιδιωτικής ζωής του χρήστη. Η χρησιμοποίηση τέτοιων διατάξεων θα πρέπει να επιτρέπεται μόνο για θεμιτούς σκοπούς και εφόσον το γνωρίζουν οι χρήστες αυτοί.

▶ 7. Υπάρχουν περιορισμοί στην αποστολή διαφημιστικών μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου;

Μία συνήθης μέθοδος προσέγγισης του παρόντος ή μελλοντικού πελάτη είναι η αποστολή διαφημιστικών μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου. Η χρήση, ωστόσο, αυτής της μεθόδου επικοινωνίας υπόκειται σε περιορισμούς που επιβάλλει η νομοθεσία για την προστασία του καταναλωτή.

Η εμπορική επικοινωνία πρέπει καταρχήν να είναι σαφώς αναγνωρίσιμη, να είναι δηλαδή προφανής στον παραλήπτη του ηλεκτρονικού μηνύματος ο επιδιωκόμενος εμπορικός/επιχειρηματικός σκοπός. Εξάλλου, όπως ορίζεται στον νόμο 2774/99, η χρησιμοποίηση ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης προϊόντων και υπηρεσιών είναι επιτρεπτή μόνον εφόσον ο συνδρομητής έχει δώσει εκ των προτέρων τη ρητή συγκατάθεσή του για τη λήψη τέτοιων μηνυμάτων. Το λεγόμενο opt in επιβεβαιώθηκε ως βασική επιλογή από την πρόσφατη Οδηγία για την επεξεργασία προσωπικών δεδομένων και την προστασία της ιδιωτικότητας στον τομέα των ηλεκτρονικών επικοινωνιών. Η ίδια Οδηγία, η οποία όμως δεν έχει ενσωματωθεί ακόμη στο ελληνικό δίκαιο και συνεπώς δεν ισχύει ακόμη στην Ελλάδα, προβλέπει ωστόσο ότι η αποστολή εμπορικών και διαφημιστικών μηνυμάτων από μία επιχείρηση σε συνδρομητές και χρήστες που είναι ήδη πελάτες της, επιτρέπεται εφόσον αυτοί είχαν τη δυνατότητα να εκφράσουν την αντίθεσή τους στη λήψη τέτοιων μηνυμάτων.

▶ 8. Πρέπει να ενημερώνω τους επισκέπτες/συναλλασσόμενους ηλεκτρονικά με την επιχείρηση για τη συλλογή και επεξεργασία των δεδομένων που τους αφορούν;

Η ενημέρωση έχει κεφαλαιώδη σημασία για την προστασία των προσωπικών δεδομένων αλλά και για τη νομιμότητα της επεξεργασίας τους. Η ενημέρωση των χρηστών κατά το στάδιο της συλλογής των προσωπικών δεδομένων που τους αφορούν, δε συνιστά μόνο αυτοτελή υποχρέωση που έχει εισαγάγει η νομοθεσία για την προστασία προσωπικών δεδομένων, αλλά αποτελεί ταυτοχρόνως και προϋπόθεση για την έγκυρη συγκατάθεση του χρήστη. Η συγκατάθεση στην ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων νοείται ως "ενημερωμένη συγκατάθεση" (informed consent).

Η ενημέρωση πρέπει να αναφέρεται καταρχήν στο γεγονός καθεαυτό της συλλογής και επεξεργασίας προσωπικών δεδομένων και τη βάση στην οποία αυτή θεμελιώνεται (συγκατάθεση, σύμβαση). Οπωσδήποτε πρέπει να περιλαμβάνει την (online και offline) ταυτότητα αυτού που συλλέγει τα δεδομένα, το σκοπό για τον οποίο συλλέγονται τα δεδομένα, καθώς και για τους τυχόν περαιτέρω αποδέκτες των δεδομένων. Είναι επίσης αναγκαίο και σκόπιμο να ενημερώνονται οι επισκέπτες/συναλλασσόμενοι για τα δικαιώματά που τους παρέχει η νομοθεσία για την προστασία προσωπικών δεδομένων (δικαίωμα

πρόσβασης, διόρθωσης, αντίταξης κλπ.).
Εφόσον οι επιχειρήσεις έχουν εκπονήσει πολιτικές ασφάλειας της ιδιωτικότητας (privacy policies) είναι χρήσιμο και εξυπηρετεί ταυτόχρονα τους σκοπούς της ενημέρωσης να ανακοινώνονται σε εμφανή σημεία των αντίστοιχων ηλεκτρονικών σελίδων (privacy statement). Είναι αυτονόητο ότι αυτές οι πολιτικές πρέπει να είναι σύμφωνες και να εναρμονίζονται με το γράμμα και το πνεύμα της νομοθεσίας για την προστασία προσωπικών δεδομένων.
Η ενημέρωση είναι απαραίτητη και στην περίπτωση της εγκατάστασης "cookies" ή άλλων συναφών διατάξεων. Όταν οι δια-τάξεις αυτές προορίζονται για σκοπούς που η έννομη τάξη κρίνει ως θεμιτούς, η χρησιμοποίησή τους επιτρέπεται μόνο υπό τον όρον ότι παρέχονται στους χρήστες σαφείς και ακριβείς πληροφορίες για τον προορισμό των "cookies" ή τυχόν ανάλογων διατάξεων, ώστε να εξασφαλίζεται ότι είναι εν γνώσει του χρήστη οι πληροφορίες που αποθηκεύονται στον τερματικό υπολογιστή που χρησιμοποιεί και να παρέχεται στους χρήστες η δυνατότητα να αρνηθούν την αποθήκευση "cookies" ή παρόμοιων διατάξεων στον τερματικό τους εξοπλισμό. Οι τρόποι της παροχής πληροφοριών, της παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης θα πρέπει να είναι όσο το δυνατόν προσιτότεροι για το χρήστη.
Ο νόμος για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα επεκτείνει την υποχρέωση ενημέρωσης και στους κινδύνους παραβίασης της ασφάλειας του δικτύου. Τέτοιοι κίνδυνοι ενδέχεται να προκύψουν κυρίως για τις υπηρεσίες ηλεκτρονικών επικοινωνιών σε ένα ανοικτό δίκτυο, όπως το Internet ή η αναλογική κινητή τηλεφωνία. Οι πάροχοι υπηρεσιών που προσφέρουν διαθέσιμες στο κοινό υπηρεσίες επικοινωνιών μέσω του Internet, θα πρέπει να ενημερώνουν τους χρήστες και τους συνδρομητές και για τους τρόπους αποτροπής των κινδύνων, χρησιμοποιώντας συγκεκριμένους τύπους λογισμικού ή τεχνολογίες κρυπτογράφησης. Η απαίτηση να ενημερώνονται οι συνδρομητές για ιδιαίτερους κινδύνους ασφάλειας, δεν απαλλάσσει από την υποχρέωση να λαμβάνουν, με ίδιες δαπάνες, κατάλληλα και άμεσα μέτρα για να αποτρέπονται τυχόν νέοι, απρόβλεπτοι κίνδυνοι ασφάλειας και να αποκαθίσταται το κανονικό επίπεδο ασφάλειας της υπηρεσίας.

▶ 9. Είναι υποχρεωτικό να λαμβάνονται μέτρα ασφαλείας των προσωπικών δεδομένων;

Η ασφάλεια των πληροφοριακών συστημάτων είναι μία υποχρέωση που δεν αφορά μόνο την προστασία της επιχείρησης, αλλά και την προστασία των προσώπων, στοιχεία των οποίων έχουν καταχωριστεί στα συστήματα αυτά. Ήδη ο νόμος 2472/97 (άρθρο 10) έχει επιβάλει υποχρεώσεις προστασίας της εμπιστευτικότητας - μυστικότητας (secrecy) των πληροφοριών και λήψης μέτρων ασφάλειας: Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Τα μέτρα ασφαλείας που λαμβάνονται θα πρέπει να είναι ανάλογα προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Στις υποχρεώσεις μιας επιχείρησης περιλαμβάνεται η επιλογή συνεργατών που διαθέτουν όχι μόνο τεχνικές γνώσεις αλλά και προσωπική ακεραιότητα που διασφαλίζει την τήρηση του απορρήτου της επεξεργασίας.
Η Αρχή Προστασίας Προσωπικών Δεδομένων αποδίδει ιδιαίτερη σημασία στην εκπόνηση σχεδίου ασφάλειας (security plan) και έκτακτης ανάγκης από τον υπεύθυνο επεξεργασίας, αλλά και στη συνεχή αναθεώρηση των σχεδίων αυτών ώστε να ανταποκρίνεται στις τεχνολογικές εξελίξεις. Συχνά μάλιστα οι άδειες επεξεργασίας ευαίσθητων δεδομένων συνοδεύονται από την επιβολή όρων ασφαλείας των δεδομένων και την υποχρέωση επεξεργασίας τέτοιων σχεδίων Χωρίς να υπεισέρχεται σε λεπτομέρειες, η Αρχή Προστασίας Προσωπικών Δεδομένων έχει συντάξει ένα κείμενο οδηγιών, όπου αναφέρεται το βασικό περιεχόμενο των σχεδίων ασφαλείας και εκτάκτου ανάγκης, ώστε αυτά να κρίνονται επαρκή από την άποψη της προστασίας της εμπιστευτικότητας (http://www.dpa.gr/secure.htm).

▶ 10. Ποιες συνέπειες έχει η μη τήρηση αυτών των υποχρεώσεων;

Η τήρηση των επιταγών και απαγορεύσεων που σχετίζονται με την επεξεργασία αλλά και την ασφάλεια των προσωπικών δεδομένων επιβάλλεται από την οικεία νομοθεσία. Τυχόν παράβαση των υποχρεώσεων αυτών για προστασία και ασφάλεια των δεδομένων ενδέχεται να έχει ως αποτέλεσμα την επιβολή διοικητικών κυρώσεων από την Αρχή Προστασίας Προσωπικών Δεδομένων (όπως πρόστιμα, αναστολή επεξεργασίας, καταστροφή αρχείων κλπ.) ή/και τη γέννηση αξιώσεων και υποχρεώσεων αποζημίωσης ή χρηματικής ικανοποίησης των προσώπων που θίγονται από τις παραβάσεις των νομοθετικών διατάξεων και των υποχρεώσεων ασφαλείας. Συγκεκριμένες παραβάσεις συνιστούν μάλιστα ποινικά αδικήματα και επισύρουν και ποινικές κυρώσεις.

Ωστόσο, η μεγαλύτερη κύρωση είναι η δυσπιστία των συναλλασσομένων! Πολλές πρόσφατες μελέτες έχουν αποδείξει ότι πολλοί άνθρωποι απέχουν από ηλεκτρονικές συναλλαγές από φόβο για τη μεταχείριση και την τύχη των προσωπικών τους δεδομένων. Η επένδυση σε τεχνολογίες ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies), η ύπαρξη, τήρηση και διαφήμιση πολιτικών για την προστασία της ιδιωτικότητας δεν είναι απλά συμμόρφωση προς το νόμο. Είναι ανταγωνιστικό πλεονέκτημα! Είναι προϋπόθεση για να αποκτηθεί η εμπιστοσύνη των καταναλωτών!