ΛΗΨΗ ΚΑΤΑΛΛΗΛΩΝ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

ΣΧΕΔΙΑΣΤΙΚΑ

Σχεδιασμός εφαρμογών του πληροφοριακού συστήματος

Διαμόρφωση περιβάλλοντος υπολογιστών - φορητά μέσα

Διαχείριση δικαιωμάτων χρηστών

ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Έλεγχος φυσικής πρόσβασης

Προστασία από φυσικές καταστροφές

ΑΡΧΕΙΟΘΕΤΙΚΑ

Αρχεία καταγραφής

Αντίγραφα ασφαλείας

ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Ανωνυμοποίηση δεδομένων προσωπικού χαρακτήρα

Αναγνώριση και αυθεντικοποίηση

ΜΕΙΩΣΗ ΕΥΠΑΘΕΙΩΝ

Μείωση ευπαθειών του λογισμικού

Μείωση ευπαθειών που συνδέονται με τα υποστηρικτικά υλικά αγαθά

Μείωση ευπαθειών αναφορικά με τα δίκτυα επικοινωνίας

Αντιμετώπιση κακόβουλων λογισμικών

ΔΙΚΤΥΑΚΗ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ

Ασφάλεια επικοινωνιών

Ειδικά μέτρα για κινητές ή απομακρυσμένες συσκευές

Ενδεικτικές εφαρμογές και μηχανισμοί για διαδικτυακή ασφάλεια

ΔΙΚΤΥΟΓΡΑΦΙΑ - ΠΗΓΕΣ

ΠΡΟΛΟΓΟΣ

Τα μέτρα προστασίας, που λαμβάνει ο υπεύθυνος επεξεργασίας, είναι υποχρεωτικό να επιλέγονται με την ανάλογη προσοχή και καταλληλότητα της εκάστοτε περίστασης. Βασικό είναι να ελέγχονται οι πιο πρόσφατες εξελίξεις κυρίως νομικές και τεχνολογικές, με σκοπό την ετοιμότητα σε επιθέσεις και ευπάθειες πληροφοριακών συστημάτων, καθώς και τη βέλτιστη συμμόρφωση με τους νομικούς κανονισμούς και οδηγίες, ιδίως των κρατών μελών που ανήκει ο φορέας. Άλλος αξιοσημείωτος παράγοντας λήψης των μέτρων είναι τα χαρακτηριστικά της επεξεργασίας, όπως το πλαίσιο και οι σκοποί της επεξεργασίας, η φύση και το πεδίο εφαρμογής και το κόστος της. Ταυτόχρονα, πρέπει να λαμβάνονται υπόψη και οι κίνδυνοι διαφορετικής πιθανότητας επέλευσης και σοβαρότητας των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων από την επεξεργασία. Αυτό είναι πολύ κρίσιμο ζήτημα, το οποίο χρήζει σωστής αξιολόγησης των πιθανών συνεπειών για τα συσχετιζόμενα υποκείμενα.

Οι υπεύθυνοι επεξεργασίας και οι υπεύθυνοι προστασίας μπορούν να παραδειγματίζονται, εκτός από το παρόν, από τα πρότυπα ασφάλειας πληροφοριών ISO / IEC. Αυτά δημοσιεύονται από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και από τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC), με τίτλο «Τεχνολογία πληροφοριών - Τεχνικές ασφαλείας - Κώδικας πρακτικής για ελέγχους ασφάλειας πληροφοριών». Φερειπείν, το πρότυπο ISO / IEC 27002: 2013 παρέχει κατευθυντήριες γραμμές για τα πρότυπα ασφαλείας των οργανωτικών πληροφοριών και τις πρακτικές διαχείρισης της ασφάλειας των πληροφοριών, συμπεριλαμβανομένης της επιλογής, της υλοποίησης και της διαχείρισης των ελέγχων, λαμβάνοντας υπόψη τα περιβάλλοντα κινδύνου της ασφάλειας του οργανισμού. Είναι σχεδιασμένο να εφαρμόζεται από οργανισμούς, που σκοπεύουν να κάνουν ελέγχους στο πλαίσιο της διαδικασίας εφαρμογής ενός συστήματος διαχείρισης ασφάλειας πληροφοριών βάσει του ISO / IEC 27001, να εφαρμόζουν κοινώς αποδεκτούς ελέγχους ασφάλειας πληροφοριών, να αναπτύξουν τις δικές τους κατευθυντήριες γραμμές διαχείρισης της ασφάλειας των πληροφοριών.

ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

ΣΧΕΔΙΑΣΤΙΚΑ

Πολιτική ασφάλειας

Η πολιτική ασφάλειας υφίσταται ως το θεμέλιο του φορέα ή της εταιρείας/επιχείρησης, για τις αρχές προστασίας προσωπικών δεδομένων που ακολουθούνται και εφαρμόζονται. Ειδικότερα, περιγράφει με σαφήνεια τους ρόλους και τις αρμοδιότητες του προσωπικού, αλλά και των εξωτερικών συνεργατών ως εκτελούντες την επεξεργασία. Αυτή επανεξετάζεται και ενημερώνεται, ή όταν απαιτείται ή σε προγραμματισμένα χρονικά διαστήματα. Ακόμη, προσδιορίζει τα οργανωτικά και τεχνικά μέτρα προστασίας, αναφορικά με:

α) τη διαχείριση των χρηστών του πληροφοριακού συστήματος

β) την αναγνώριση και αυθεντικοποίηση των χρηστών

γ) την ασφάλεια των επικοινωνιών

δ) τη λειτουργία των αρχείων καταγραφής του πληροφοριακού συστήματος

ε) την εξαγωγή αντιγράφων ασφαλείας

στ) τη διαχείριση περιστατικών ασφαλείας

ζ) τη θεμιτή και εσκεμμένη καταστροφή των προσωπικών δεδομένων

η) τα μέτρα φυσικής ασφάλειας

Ένα άλλο περιεχόμενό της είναι το σχέδιο ασφάλειας, το οποίο περιγράφει την υλοποίηση των αρχών της πολιτικής ασφάλειας στα επιμέρους συστήματα επεξεργασίας προσωπικών δεδομένων του υπεύθυνου επεξεργασίας. Οι εκτελούντες την επεξεργασία οφείλουν, να έχουν υποβάλει την πολιτική ασφάλειας πληροφοριών στον υπεύθυνο επεξεργασίας πριν την ανάθεση επεξεργασίας.

Σχέδιο ανάκαμψης από καταστροφές

Μία ακόμη αξιοπρόσεκτη διαδικασία είναι το σχέδιο ανάκαμψης από καταστροφές (φυσικές, ηλεκτρονικές, κτλ.). Το σχέδιο αυτό είναι εγκεκριμένο και περιγράφει τις κύριες διαδικασίες, που ακολουθούνται για:

α) την προστασία των προσωπικών δεδομένων σε περιπτώσεις εκτάκτων περιστατικών

β) τις συνθήκες και τα περιστατικά ασφαλείας, κάτω από τα οποία ενεργοποιείται

γ) τους σχετικούς ρόλους και αρμοδιότητες του προσωπικού

δ) τους τρόπους αντιμετώπισης των περιστατικών που καλύπτει

Επιπλέον, χρειάζεται να ανανεώνεται συχνά με βάση και ιδιαιτέρως μετά από κάθε σημαντική αλλαγή στο πληροφοριακό σύστημα. Δυο βασικές προϋποθέσεις είναι το να φέρει επίσημη ενυπόγραφη έγκριση της διοίκησης του υπεύθυνου επεξεργασίας και η εκτέλεση δοκιμών σεναρίων, που περιγράφονται και προβλέπονται από το σχέδιο.

ΔΙΑΧΕΙΡΙΣΤΙΚΑ

Διαχείριση πληροφοριακών αγαθών

Ο υπεύθυνος επεξεργασίας υποχρεούται να καταγράφει σε έναν κατάλογο τα πληροφοριακά αγαθά, ενώ θα εξασφαλίζει ένα επαρκές επίπεδο ανάλυσης. Μάλιστα, για κάθε αγαθό στον κατάλογο είναι ουσιαστικό, να έχει οριστεί ένας υπεύθυνος/ιδιοκτήτης. Ειδικότερα για τα αγαθά του υπεύθυνου επεξεργασίας είναι καλό, να υπάρχουν πολιτικές αποδεκτής χρήσης. Επομένως, ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει κατάλληλες γνώσεις και κατάλληλη διαδικασία για την καταγραφή των επιμέρους συστημάτων και εφαρμογών που χρησιμοποιούνται. Επιπροσθέτως, η καταγραφή των πληροφοριακών αγαθών χρειάζεται:

α) να περιλαμβάνει και τα εκτός παραγωγής συστήματα, φερειπείν τους εξυπηρετητές παλαιότερου πληροφοριακού συστήματος ενός νοσοκομείου

β) τακτική/σταθερή αναθεώρηση, λόγου χάρη σε ετήσια βάση

γ) να ελέγχεται από συγκεκριμένο εξουσιοδοτημένο πρόσωπο, όπως ο διαχειριστής του πληροφοριακού συστήματος ή ο υπεύθυνος ασφαλείας

δ) συγκεκριμένη διαδικασία που θα διασφαλίζει ότι τα αγαθά επιστρέφονται με τη λύση της εργασιακής σχέσης

Εφόσον τα προαναφερθέντα εκτελούνται με σωστό τρόπο, τα πληροφοριακά αγαθά υφίστανται υπό τον έλεγχο και την εποπτεία των κατάλληλων ατόμων, διασφαλίζοντας και ασφαλίζοντάς τα.

Διαχείριση χρηστών

Εκτός της πολιτικής ασφάλειας, μια εταιρία έχει ανάγκη και από συγκεκριμένη πολιτική διαχείρισης των χρηστών του πληροφοριακού συστήματος, η οποία απαιτείται να περιλαμβάνει τουλάχιστον τα εξής:

α) διαδικασία για εισαγωγή νέου χρήστη ή για μεταβολή των δικαιωμάτων των χρηστών (λ.χ. κατά τη μετάθεση υπαλλήλου) στο σύστημα

β) διαδικασία για τη διαγραφή μη ενεργού χρήστη (λ.χ. σε περίπτωση αποχώρησης υπαλλήλου από το νοσοκομείο)

γ) κατηγοριοποίηση των χρηστών σε ομάδες αναλόγως τα δικαιώματα πρόσβασης, που αυτοί έχουν στους πόρους του συστήματος

δ) μέθοδος για την έγκριση εξουσιοδότησης, όταν την αιτείται κάποιος χρήστης

Παράλληλα, η πολιτική είναι απαραίτητο να καλύπτει τόσο τους υπαλλήλους του υπεύθυνου επεξεργασίας, όσο και εξωτερικούς συνεργάτες, όπως για παράδειγμα τους υπαλλήλους εκτελούντων την επεξεργασία που έχουν πρόσβαση στο πληροφοριακό σύστημα. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να διασφαλίζει ότι οι χρήστες έχουν πρόσβαση αποκλειστικά στις εφαρμογές και στα δεδομένα, τα οποία απαιτούνται για την εκτέλεση της εργασίας τους, και όχι για επιπρόσθετους σκοπούς. Μολαταύτα, τα δικαιώματα πρόσβασης επανεξετάζονται σε περιοδική βάση. Λόγου χάριν, το τμήμα του λογιστηρίου δεν επιτρέπεται να έχει πρόσβαση στα δεδομένα των ιατρικών φακέλων. Τελευταίο, αλλά εξίσου σπουδαίο είναι να υφίσταται ειδική μέθοδος για τη διαχείριση των προνομιακών λογαριασμών (privileged accounts) και να τηρείται κατάλογος με προνομιακές βοηθητικές εφαρμογές (privileged utility programs).

Διαχείριση φυσικού αρχείου

Ένα ακόμη καθήκον του υπεύθυνου επεξεργασίας αποτελεί και ο ορισμός αρμόδιων ατόμων για τη διαχείριση του φυσικού αρχείου, όπως επίσης και ορισμός συγκεκριμένων ατόμων μέσω των οποίων πραγματοποιείται η πρόσβαση σε αυτό. Μάλιστα είναι ουσιαστικό, ο χώρος του φυσικού αρχείου να είναι απομονωμένος με ελεγχόμενη πρόσβαση και να τηρείται κατάλληλη διαδικασία καταγραφής των προσβάσεων στο φυσικό αρχείο, μεγιστοποιώντας έτσι την προστασία και από τρίτες κακόβουλες οντότητες και ενέργειες αυτών. Παράλληλα, ο υπεύθυνος επεξεργασίας οφείλει να ορίζει επίσημα συγκεκριμένη φυσική περίμετρο ασφαλείας. Επιπροσθέτως, έχει ευθύνη για την πρόνοια της διασύνδεσης των

διαφορετικών αρχείων, όπως για παράδειγμα μέσω συσχετισμού με τους αντίστοιχους κωδικούς.

Διαχείριση αλλαγών

Επιπλέον καθήκον για την καλύτερη οργάνωση είναι η διαδικασία διαχείρισης αλλαγών των συστημάτων επεξεργασίας προσωπικών δεδομένων, όπου περιέχει τουλάχιστον τα παρακάτω:

α) καταγραφή των αιτημάτων αλλαγής

β) καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών

γ) καθορισμό των κριτηρίων αποδοχής αλλαγών και χρονοδιάγραμμα υλοποίησης

Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων

Είναι στοιχειώδης υποχρέωση ο εντοπισμός και η αντιμετώπιση περιστατικών παραβίασης προσωπικών δεδομένων. Ως παραβίαση δεδομένων νοείται η παραβίαση της ασφάλειας, που οδηγεί στην ακούσια ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα, που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται σε άλλη επεξεργασία. Εκτός άλλων, η διαδικασία αυτή χρήζει ορισμού ή/και υλοποίησης των:

α) περιστάσεων που θεωρούνται και υφίστανται περιστατικά παραβίασης προσωπικών δεδομένων, καθώς και των μεθόδων περιγραφής και αναφοράς των περιστατικών από υπαλλήλους του υπεύθυνου επεξεργασίας ή/και εκτελούντες την επεξεργασία

β) διεργασιών λήψης μέτρων για την καταπολέμηση των συμβάντων παραβίασης

γ) ενδεχόμενων διαδικασιών για την ενημέρωση των θιγόμενων ατόμων ανάλογα με την έκταση του περιστατικού, αλλά και αναφοράς του συμβάντος στην αρμόδια εποπτική Αρχή στο χρονικό πλαίσιο που ορίζει ο Κανονισμός

δ) εργαζομένων που είναι υπεύθυνοι για τη διαχείριση παραβιάσεων προσωπικών δεδομένων

ε) καταχωρήσεων των περιστατικών σε ειδικό αρχείο (έντυπο ή ηλεκτρονικό), συμπεριλαμβανομένων των βασικών χαρακτηριστικών του περιστατικού, καθώς και τον τρόπο με τον οποίο αντιμετωπίστηκε

στ) εφαρμογών για τους μηχανισμούς εκτίμησης, του πιθανού κινδύνου για τα υποκείμενα

ζ) παρακολουθήσεων και καταγραφών του τύπου, του όγκου και του κόστους των συμβάντων, για τον εντοπισμό των αιτιών και την αποτροπή αυτών, όπως επίσης και των κατάλληλων μέτρων για την αποτροπή της επανάληψης εμφάνισής τους.

Επίσης, δύναται να προβεί στην ανάπτυξη σχεδίου δράσης ή/και ανάδρασης, σε περίπτωση παραβίασης προσωπικών δεδομένων για κάθε υψηλό ή μη εκτιμημένο κίνδυνο. Σε κάθε ενδεχόμενο, οφείλει να βρίσκεται σε ετοιμότητα για την αποκατάσταση και διόρθωση των παραβιάσεων που διεξήχθησαν.

<u>Διαχείριση τρίτων με εξουσιοδότηση πρόσβασης στα προσωπικά δεδομένα</u>

Ένας ακόμη στόχος του υπεύθυνου επεξεργασίας είναι να περιορίσει τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, που ενέχει η επεξεργασία δεδομένων από τρίτες οντότητες. Συνεπώς ο υπεύθυνος ή/και ο εκτελών την επεξεργασία έχει χρέος:

α) να προσδιορίσει και να τεκμηριώσει σε κατάλληλη μορφή τα δικαιώματα και τις απαιτήσεις των τρίτων, βάσει της νομικής δομής και της γεωγραφικής θέσης των

β) να καταγράψει τη σύμβαση υπεργολαβίας, τις ρήτρες συνεργασίας και τους δεσμευτικούς εταιρικούς κανόνες (BCR)

γ) να προσδιορίσει όλα τα τρίτα μέρη που έχουν ή θα μπορούσαν να έχουν νόμιμη πρόσβαση σε προσωπικά δεδομένα, τα οποία τυγχάνουν επεξεργασίας για λογαριασμό του, όπως:

i) ορισμένες κατηγορίες εργαζομένων

ii) πάροχοι υπηρεσιών

iii) τεχνικοί συντήρησης

iv) επιχειρηματικοί εταίροι

v) εξουσιοδοτημένοι εξωτερικοί συνεργάτες

δ) να καθορίσει το ρόλο των τρίτων αυτών στη διαδικασία επεξεργασίας, βάσει των ενεργειών που θα εκτελέσουν. Για παράδειγμα, εάν ένας υπεύθυνος ή/και εκτελών την επεξεργασία συνεργάζεται με έναν πάροχο υπηρεσιών υπολογιστικού νέφους (cloud provider), ο τρίτος αυτός θεωρείται γενικά ως πάροχος υπηρεσιών, αν και σε ορισμένες περιπτώσεις μπορεί να θεωρηθεί ως εκτελών την επεξεργασία.

Καταστροφή δεδομένων

Εξίσου αξιόλογη είναι η λήψη κατάλληλων μέτρων, προτού καταστραφούν έντυπα ή ηλεκτρονικά αρχεία, τα οποία περιέχουν προσωπικά δεδομένα, καθώς και πριν την καταστροφή ή επαναχρησιμοποίηση εξοπλισμού, στου οποίου είναι αποθηκευμένα αρχεία με προσωπικά δεδομένα. Με αυτόν τον τρόπο, διασφαλίζεται η πλήρης και μόνιμη διαγραφή των δεδομένων. Ειδικότερα, επιβάλλεται:

α) να ακολουθούνται κατ' ελάχιστον, όσα προβλέπονται στην Οδηγία 1/2005 της Αρχής για το ασφαλές σβήσιμο των προσωπικών δεδομένων, ύστερα από το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας

β) ο υπεύθυνος επεξεργασίας να διαθέτει συγκεκριμένη γραπτή διαδικασία για την καταστροφή των δεδομένων και να ενημερώνει σχετικά τους υπαλλήλους του, τόσο όταν πρόκειται για προγραμματισμένη μαζική καταστροφή, όσο και όταν πρόκειται για καταστροφή σε καθημερινή βάση (π.χ. με χρήση καταστροφέων εγγράφων)

γ) να επιβεβαιωθεί η άνευ όρων χρησιμότητα των υπό διαγραφή δεδομένων. Φερειπείν, δεν χρειάζονται πλέον τα δεδομένα για την εκπλήρωση άλλων συμβατικών υποχρεώσεων του υπευθύνου επεξεργασίας, συνεπώς τίθενται υπό διαγραφή.

ΑΝΘΡΩΠΟΚΕΝΤΡΙΚΑ

Ρόλος υπευθύνου ασφαλείας

Σπουδαίο ρόλο στην οργάνωση των διαδικασιών, που είναι συναφείς με την ασφάλεια, κατέχει ο υπεύθυνος ασφάλειας, ο οποίος ορίζεται εγγράφως από τον υπεύθυνο επεξεργασίας. Ο υπεύθυνος ασφάλειας υποχρεούται κατ' ελάχιστον:

α) να έχει την επίβλεψη της κατάρτισης και της εφαρμογής της πολιτικής και του σχεδίου ασφαλείας

β) να προτείνει σχετικές αναθεωρήσεις και βελτιώσεις για την καλύτερη προσαρμογή στον κανονισμό, εφόσον αυτές καθίστανται αναγκαίες

γ) να διατηρεί τακτή επικοινωνία με τον υπεύθυνο επεξεργασίας, καθώς και με εξειδικευμένες ομάδες σε θέματα ασφάλειας πληροφοριακών συστημάτων (λ.χ. CERTs, εταιρείες λογισμικών ασφαλείας, λοιποί προμηθευτές εφαρμογών λογισμικού), με απώτερο σκοπό την επικαιροποίηση των σχετικών με την ασφάλεια διαδικασιών, συναρτήσει των νέων εξελίξεων

Στοιχειώδη επαγγελματικά προσόντα, που ευθύνεται να κατέχει, είναι τεχνικές γνώσεις πληροφορικής (βάσεις δεδομένων, λειτουργικά συστήματα, προγραμματισμό, δίκτυα) και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Οι αρμοδιότητες, που σχετίζονται με την ασφάλεια των συστημάτων, είναι καθορισμένες και κατανεμημένες σε συγκεκριμένα άτομα.

Εκτελούντες την επεξεργασία

Οι εκτελούντες την επεξεργασία δεσμεύονται να περιλαμβάνουν στις συμβάσεις τους κατ' ελάχιστον:

α) την περιγραφή των προσωπικών δεδομένων

β) το σκοπό και τον τόπο της επεξεργασίας

γ) τον τρόπο/διαδικασία της επεξεργασίας

δ) τα επίπεδα των υπηρεσιών, που έχει καθήκον να επιτυγχάνει ο εκτελών την επεξεργασία (σε επίπεδο ασφάλειας και ποιότητας δεδομένων)

ε) τις διαδικασίες ελέγχου συμμόρφωσης των διαδικασιών του εκτελούντα με τα προβλεπόμενα στη σύμβαση (οι έλεγχοι δεν γίνονται από τον ίδιο τον εκτελούντα)

στ) τις υποχρεώσεις τους για εμπιστευτικότητα και διαγραφή δεδομένων

ζ) τεκμήρια για τα μέσα (έλεγχοι ασφαλείας, επισκέψεις στις εγκαταστάσεις, κτλ), εκ των οποίων θα εξασφαλιστεί η αποτελεσματικότητα των εγγυήσεων που παρέχει ο εκτελών

η) ρήτρες αναφορικά με παραβιάσεις όρων της σύμβασης, σε συνάρτηση με όλα τα ανωτέρω

Είναι χρέος του υπεύθυνου επεξεργασίας να εξασφαλίζει ότι άπαντες οι εκτελούντες την επεξεργασία τηρούν τους όρους της πολιτικής ασφάλειας (του υπεύθυνου), στο μέτρο που αυτή τους αφορά (τους εκτελούντες) και ταυτόχρονα

ότι υλοποιούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας. Στις περιπτώσεις, όπου η επεξεργασία γίνεται εκτός των εγκαταστάσεων του υπεύθυνου επεξεργασίας, ο υπεύθυνος υποχρεούται να εξασφαλίζει ότι ο εκτελών παρέχει επίπεδο ασφαλείας τουλάχιστον ανάλογο με αυτό, που ορίζεται στην πολιτική ασφάλειας του υπευθύνου. Λοιπά σημεία άξια προσοχής είναι ότι οι υπάλληλοι του εκτελούντος έχουν χρέος να δεσμεύονται εγγράφως με κατάλληλη δήλωση εμπιστευτικότητας, υπάρχει ειδικός όρος για ασφάλεια στα συμβόλαια συντήρησης, έχει οριστεί πρόσωπο του υπευθύνου επεξεργασίας αρμόδιο να επιτηρεί εργασίες που γίνονται από τρίτους.

Υποχρέωση εμπιστευτικότητας του προσωπικού

Οι υπάλληλοι (μόνιμοι, συμβασιούχοι, εποχικοί), καθώς και οι εξωτερικοί συνεργάτες, που εξουσιοδοτούνται να έχουν πρόσβαση σε προσωπικά δεδομένα, οφείλουν να δεσμεύονται εγγράφως σχετικά με την τήρηση της εχεμύθειας και της εμπιστευτικότητας. Αυτό προορίζεται να γίνεται κατά τη διάρκεια της απασχόλησης και έπειτα από την αποχώρησή τους, όπως επίσης και πριν την ενεργοποίηση της σχετικής πρόσβασης. Η δέσμευση προσδιορίζει:

α) την ανάθεση σταθμού εργασίας

β) τη δημιουργία ενός λογαριασμού IT και τον ορισμό προφίλ χρήστη με συγκεκριμένα δικαιώματα

γ) την παροχή φυσικών και ηλεκτρονικών μέσων πρόσβασης και συνθηματικών

δ) τη διαδικασία που επιτάσσεται να ακολουθείται συστηματικά, όταν αποσύρεται η εξουσιοδότηση από ένα άτομο για πρόσβαση σε δεδομένα προσωπικού χαρακτήρα ή όταν ο ρόλος του μεταβληθεί

Κάθε άτομο με εξουσιοδοτημένη πρόσβαση και άλλα δικαιώματα σε δεδομένα προσωπικού χαρακτήρα, προκειμένου να εξασφαλιστεί η εμπιστευτικότητά του, δεσμεύεται ότι:

α) δεν θα χρησιμοποιήσει τα δεδομένα, στα οποία έχει πρόσβαση, για σκοπούς άλλους από εκείνους, που προβλέπονται σε σχέση με τις ευθύνες και τις αρμοδιότητές του

β) δεν θα αποκαλύψει τα δεδομένα αυτά σε τρίτους (φυσικά ή νομικά πρόσωπα δημόσιου ή ιδιωτικού συμφέροντος), οι οποίοι δεν είναι εξουσιοδοτημένοι να έχουν πρόσβαση σε αυτά

γ) δεν θα δημιουργήσει αντίγραφα αυτών των δεδομένων, εκτός αν η αντιγραφή αυτή είναι απαραίτητη για την εκτέλεση των καθηκόντων του

δ) θα λαμβάνει όλα τα προβλεπόμενα μέτρα σε σχέση με τις ευθύνες και τις αρμοδιότητές του, με απώτερο στόχο να αποτρέπει την ακατάλληλη ή δόλια χρήση αυτών των δεδομένων

ε) θα διασφαλίζει ότι στο πλαίσιο των αρμοδιοτήτων του, θα μπορούν να ασκούνται τα δικαιώματα των υποκειμένων των δεδομένων, με τη μέθοδο όπου αυτά ορίζονται στον Κανονισμό και απορρέουν από αυτόν

στ) σε περίπτωση τερματισμού των καθηκόντων του, θα επιστρέφει όλα τα δεδομένα, αρχεία ηλεκτρονικών υπολογιστών και μέσα ενημέρωσης, που σχετίζονται με αυτά τα δεδομένα

Κώδικας δεοντολογίας

Ο υπεύθυνος επεξεργασίας καταρτίζει τον κώδικα δεοντολογίας με τις βασικές αρχές προστασίας προσωπικών δεδομένων, όπου πρέπει να ακολουθούν οι υπάλληλοι (μόνιμοι, συμβασιούχοι, εποχικοί) και οι εξωτερικοί συνεργάτες. Ο κώδικας δεοντολογίας είναι βασικό:

α) να φέρει την έγκριση της διοίκησης του υπεύθυνου επεξεργασίας και να είναι δεσμευτικός για τους υπαλλήλους (λ.χ. ως πράξη της διοίκησης που εξειδικεύει τα καθήκοντα των υπαλλήλων ή ως τμήμα της σύμβασης των υπαλλήλων με τον υπεύθυνο επεξεργασίας)

β) να καθορίζει πιθανές κυρώσεις σε περίπτωση παραβίασής του και να περιλαμβάνει πειθαρχική διαδικασία, η οποία προβλέπει τη δίωξη εργαζομένων, όπου παραβιάζουν την πολιτική ασφαλείας πληροφοριών

γ) να ορίζει τις υποχρεώσεις του προσωπικού αναφορικά με την ασφάλεια, οι οποίες παραμένουν σε ισχύ ακόμα και μετά τη λύση ή τροποποίηση της σύμβασης εργασίας (λ.χ. μετάθεση σε άλλη θέση εργασίας) μέσω νομικά δεσμευτικών συμβάσεων/κειμένων. Εν τούτοις, υπάρχει χρέος για επιτακτική εποπτεία του προσωπικού, όπως επίσης και καταγραφή των ενεργειών του (λ.χ. δια των αρχείων καταγραφής)

Εκπαίδευση του προσωπικού

Ο υπεύθυνος επεξεργασίας ή/και ο εκτελών αυτήν είναι σημαντικό να παρέχει συνεχή εκπαίδευση και ενημέρωση στους υπαλλήλους σε θέματα

προστασίας προσωπικών δεδομένων και ασφάλειας, συναρτήσει των νομικών και τεχνολογικών εξελίξεων. Αυτό αποσκοπεί στην ελάττωση των λαθών και την καλύτερη απόδοση του προσωπικού της επιχείρησης/εταιρίας. Κατά την εκπαίδευση αυτή δύναται:

α) να κοινοποιεί στους υπαλλήλους την πολιτική ασφάλειας και τον κώδικα δεοντολογίας κατά την πρόσληψη αυτών

β) να ενημερώνει για τα ειδικά αιτήματα ασφάλειας, αναλόγως του ρόλου και των αρμοδιοτήτων των εκπαιδευομένων μέσα στον οργανισμό και να χορηγεί εξειδικευμένη κατάρτιση για το προσωπικό με εξειδικευμένα καθήκοντα

γ) να ενημερώνει τους υπαλλήλους για σημασιολογικού χαρακτήρα αλλαγές, των διαδικασιών ασφάλειας για ζητήματα προστασίας προσωπικών δεδομένων και ασφάλειας (π.χ. η ενημέρωση για την προστασία του συστήματος από κακόβουλο λογισμικό)

δ) να παρέχει διαρκή εκπαίδευση, γύρω από τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών, στους διαχειριστές των συστημάτων και στους υπαλλήλους του τμήματος πληροφορικής

Η εκπαίδευση μπορεί να γίνει με πολλούς τρόπους, όπως με τη διανομή κειμένων μέσω του εσωτερικού δικτύου, με εγκυκλίους, με ενημερώσεις ομάδων, διεξαγωγή ημερίδων από ειδικούς στο χώρο της ασφάλειας, χωρίς να περιορίζεται σε κάποια συγκεκριμένη μορφή.

ΛΟΙΠΑ

Χώροι εγκατάστασης πληροφορικού εξοπλισμού

Τα μέτρα φυσικής ασφάλειας είναι από τα πιο αξιοσημείωτα μέτρα, επειδή έχουν άμεσο και εμφανέστατο αντίκτυπο, τόσο στο ανθρώπινο δυναμικό, όσο και στις διάφορες εγκαταστάσεις του φορέα (πληροφοριακές, οικοδομικές, κλπ). Κύρια προστασία έχουν ανάγκη οι χώροι εγκατάστασης πληροφορικού εξοπλισμού. Συνεπώς, πρέπει να βρίσκονται σε απομονωμένο χώρο με ελεγχόμενη πρόσβαση και να αποτρέπουν τους φυσικούς κινδύνους, πιθανούς και (σε σχετικό βαθμό) μη. Δηλαδή να διαθέτουν πόρτα ασφαλείας, κλιματισμό (για άρση υπερθέρμανσης), πυρανίχνευση-πυρασφάλεια, ανιχνευτές υγρασίας και πλημμύρας. Παραπλήσια μέτρα που λαμβάνονται υπόψη σχετίζονται με:

α) την ασφάλεια των κωδικών για τον συναγερμό και των κλειδιών των πορτών ασφαλείας

β) τη διασφάλιση της συνεχούς λειτουργίας του συστήματος, σε περιπτώσεις διακοπής της παροχής ενέργειας και των επικοινωνιών

γ) τις τακτικές συντηρήσεις στον σχετικό εξοπλισμό (π.χ. συστήματα πυρόσβεσης, συστήματα κλιματισμού, κτλ)

δ) τις διαδικασίες για την εισαγωγή και εξαγωγή εξοπλισμού (check in, check out) από τις περιμέτρους ασφαλείας

ε) τους κανόνες για το προσωπικό που χρησιμοποιεί αγαθά (είτε πληροφοριακά, είτε σχετικά με τον εξοπλισμό) εκτός των εγκαταστάσεων

στ) τον ενημερωμένο κατάλογο των προσώπων ή των κατηγοριών προσώπων, στα οποία επιτρέπεται η είσοδος σε κάθε περιοχή, καθώς και τις εν λόγω προσβάσεις

ζ) την πολιτική του «καθαρού γραφείου» και γενικότερα της καθαριότητας, η οποία χρειάζεται να μην λησμονείται και να μη θεωρείται ασήμαντη ή άσχετη με την ασφάλεια

Αντίστοιχα, ο χώρος του φυσικού αρχείου χρήζει ασφάλειας με, αν όχι όλα, τα περισσότερα προαναφερθέντα μέσα.

Εσωτερικός έλεγχος συμμόρφωσης

Ο υπεύθυνος ή/και ο εκτελών την επεξεργασία δύναται να δημιουργήσει μια διαδικασία παρακολούθησης και ελέγχου της συμμόρφωσης με την πολιτική ασφάλειας. Στο πλαίσιο της διαδικασίας αυτής:

α) θα ελέγχονται τακτικά τα μέτρα που περιγράφονται λεπτομερώς στο πλαίσιο της πολιτικής, ώστε να παρέχει διαβεβαιώσεις ότι εξακολουθούν να είναι αποτελεσματικά

β) θα διασφαλίζεται ότι η ευθύνη για την παρακολούθηση της συμμόρφωσης με την πολιτική είναι ανεξάρτητη από τα πρόσωπα που εφαρμόζουν την πολιτική, ώστε να είναι αμερόληπτη η παρακολούθηση

γ) θα καταγράφονται και θα αναφέρονται τα αποτελέσματα των ανωτέρω διαδικασιών στα υψηλότερα διευθυντικά στελέχη

δ) θα ελέγχονται και θα αναθεωρούνται τα αρχεία, όπου διατηρεί ο οργανισμός και τα οποία σχετίζονται άμεσα με την ικανοποίηση του καθεστώτος του Κανονισμού. Σίγουρα σε αυτά λαμβάνονται υπόψη τα από κάτω:

i) αρχείο δραστηριοτήτων

ii) μητρώο των αγαθών

iii) μελέτη εκτίμησης αντικτύπου

Αντίστοιχος έλεγχος υφίσταται και για την πολιτική της ιδιωτικότητας και προστασίας δεδομένων προσωπικού χαρακτήρα, αλλά και εν γένει η τήρηση του καθεστώτος του Κανονισμού.

ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

ΣΧΕΔΙΑΣΤΙΚΑ

Διαμόρφωση περιβάλλοντος υπολογιστών - φορητά μέσα

Σπουδαίας, επίσης, σημασίας είναι η διαμόρφωση του περιβάλλοντος των υπολογιστών. Άξια προσοχής είναι τα επόμενα σημεία:

α) η πολιτική για τη χρήση των φορητών υπολογιστών ή άλλων φορητών/αποσπώμενων μέσων, όπως οι εξωτερικοί δίσκοι ή τα USB φλασάκια, οι CD ή DVD δίσκοι, καθώς και άλλα. Για παράδειγμα, τα τερματικά και οι εξυπηρετητές, που χρησιμοποιούνται κυρίως για την επεξεργασία ευαίσθητων προσωπικών δεδομένων, δεν επιτρέπεται να εξάγουν δεδομένα με τη χρήση αποσπώμενων μέσων. Και αυτό, διότι αυξάνονται τα ενδεχόμενα μόλυνσης των συστημάτων με προσωπικά δεδομένα, καθώς και η υποκλοπή των δεδομένων. Ωστόσο, στην περίπτωση που χρησιμοποιούνται φορητά μέσα, που περιέχουν προσωπικά δεδομένα εκτός των εγκαταστάσεων του υπευθύνου, τα δεδομένα επιβάλλεται να είναι κρυπτογραφημένα.

β) η ύπαρξη διαδικασίας για τον έλεγχο της εγκατάστασης λογισμικού στα σχετικά συστήματα που είναι σε παραγωγική λειτουργία. Επίσης, καθίσταται αναγκαία η περιορισμένη πρόσβαση στον πηγαίο κώδικα των σχετικών με το σύστημα εφαρμογών, καθώς και στις σχετικές βιβλιοθήκες. Παρομοίως, και περιορισμένη πρόσβαση στα αρχεία ρύθμισης παραμέτρων (configuration files).

Για την τεχνική υποστήριξη τα εργαλεία απομακρυσμένης διαχείρισης θα πρέπει να συλλέγουν τη συγκατάθεση του χρήστη πριν την σύνδεση στο τερματικό.

Σχεδιασμός εφαρμογών του πληροφοριακού συστήματος

Αξιοπρόσεκτος χρειάζεται να είναι και ο σχεδιασμός των εφαρμογών ενός πληροφοριακού συστήματος, είτε αυτές αναπτύσσονται, είτε βελτιώνονται. Έτσι, συνεπάγεται περισσότερη αξιοπιστία στην ασφάλεια της ιδιωτικότητας και των συστημάτων. Επομένως, λαμβάνονται υπόψη:

α) η ελαχιστοποίηση των συλλεχθέντων δεδομένων προσωπικού χαρακτήρα και η συλλογή μόνο των απαραιτήτων δεδομένων για το σκοπό της επεξεργασίας τους

β) η ποιότητα και ακρίβεια των δεδομένων

γ) η δυνατότητα κωδικοποιημένης τήρησης χαρακτηρισμών ή ιδιαιτέρως ευαίσθητων δεδομένων

δ) η ικανότητα αυτοματοποιημένης ή/και χειροκίνητης διαγραφής δεδομένων μετά το χρονικό διάστημα, όπου επιβάλλεται για την πραγματοποίηση του σκοπού της επεξεργασίας

ε) η υλοποίηση όλων των ζητούμενων τεχνικών μηχανισμών ασφαλείας

στ) η τήρηση των αρχών της προστασίας δεδομένων και ασφάλειας, κατά τον προσδιορισμό των απαιτήσεων των εφαρμογών

Στις περιπτώσεις που πραγματοποιείται ανάπτυξη λογισμικού, αυτή οφείλεται να γίνεται σε επικαιροποιημένο περιβάλλον δοκιμών, απομονωμένο από το παραγωγικό σύστημα. Ορίζεται διαδικασία δοκιμής (testing) της υλοποίησης των αρχών προστασίας δεδομένων και ασφάλειας, περιγραφή του είδους του ελέγχου και με μοντελοποίηση των απειλών και ανάλυση επιθέσεων (π.χ. Penetration testing). Τόσο κατά την ανάπτυξη του λογισμικού όσο και κατά τη δοκιμή του, τα χρησιμοποιούμενα δεδομένα χρειάζεται να είναι μη πραγματικά (dummy data). Αν είναι αναγκαίο να χρησιμοποιηθούν πραγματικά δεδομένα, τότε μπορούν να χρησιμοποιηθούν μόνο σε ανωνυμοποιημένη μορφή. Γενικότερα, όμως, καθίσταται υποχρεωτική η χρήση εγκεκριμένων και μόνο μοντέλων και εργαλείων. Πριν την παραγωγική λειτουργία έχει οριστεί πλάνο αντιμετώπισης περιστατικών και έχει γίνει έλεγχος (review) ασφαλείας του λογισμικού, καθώς και η διαδικασία συντήρησής του.

Διαχείριση δικαιωμάτων χρηστών

Ο καθορισμός δικαιωμάτων στους διάφορους χρήστες του συστήματος είναι μια υποχρέωση του υπεύθυνου ή/ και του εκτελούντα την επεξεργασία, η οποία ισοδυναμεί με τη χορήγηση εξουσιοδότησής τους στα πληροφοριακά συστήματα. Ένα γιγάντιο μέρος της ασφάλειας στηρίζεται στην εξουσιοδότηση και για αυτό αποτελεί και βασικό στόχο των κακόβουλων ατόμων (π.χ. hackers). Κατά συνέπεια επιβάλλονται μέτρα, ικανά για τη σωστή λήψη των αρμοζουσών ενεργειών. Εν μέρει αυτά είναι:

α) καθορισμός προφίλ χρηστών του συστήματος με συγκεκριμένα δικαιώματα, όσον αφορά την επεξεργασία δεδομένων, όπως η δημιουργία, η πρόσβαση, η τροποποίηση, η μεταφορά και η διαγραφή δεδομένων. Οφείλει, επίσης, να αναθέσει σε κάθε άτομο ένα από τα καθορισμένα προφίλ κατά την έναρξη ισχύος του συμβολαίου εργασίας ή την αλλαγή θέσεων εργασίας.

β) διαχείριση των προφίλ των χρηστών, διαχωρίζοντας τα καθήκοντα και τους τομείς ευθύνης (κατά προτίμηση με κεντρικό τρόπο). Αυτό στοχεύει, να περιορίσει την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα αποκλειστικά σε εξουσιοδοτημένους χρήστες εφαρμόζοντας:

i) την αρχή των ελάχιστων δικαιωμάτων (least privilege principle), σύμφωνα με την οποία κάθε χρήστης έχει εξουσιοδότηση, να έχει πρόσβαση στα δεδομένα με το ελάχιστο επίπεδο προνομίων, που του επιτρέπει να εκτελεί τις απαραίτητες ενέργειες για την εκπλήρωση των καθηκόντων-αρμοδιοτήτων του

ii) την αρχή της αναγκαιότητας (need to know principle), σύμφωνα με την οποία κάθε χρήστης έχει εξουσιοδότηση, να έχει πρόσβαση μόνο στα δεδομένα, από τα οποία εξαρτάται η εκτέλεση των καθηκόντων-αρμοδιοτήτων του

γ) συσχέτιση κάθε χρήστη με εξουσιοδοτημένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, μέσω ενός μοναδικού αναγνωριστικού. Μια ενδεικτική μέθοδος ισχυρής εξακρίβωσης οντότητας, αποτελεί ο συνδυασμός τουλάχιστον δύο από τα παρακάτω:

i) αυθεντικοποίηση με κάτι που γνωρίζει ο χρήστης (π.χ. έναν κωδικό πρόσβασης)

ii) αυθεντικοποίηση με κάτι που έχει ο χρήστης (π.χ. μια έξυπνη κάρτα)

iii) αυθεντικοποίηση με κάποιο ειδικό ή μοναδικό χαρακτηριστικό για τον χρήστη (π.χ. δακτυλικό αποτύπωμα, ίριδα του ματιού)

δ) περιορισμός της χρήσης λογαριασμών, που έχουν αυξημένα δικαιώματα (π.χ. διαχειριστών συστημάτων), σε λειτουργίες που πραγματικά την έχουν ανάγκη. Μάλιστα, οι λογαριασμοί των διαχειριστών (administrator account) επιβάλλεται να είναι ατομικοί και να έχουν έναν προσωπικό κωδικό πρόσβασης.

ε) ανάκληση των δικαιωμάτων των εργαζομένων, των συμβαλλομένων και άλλων τρίτων, όταν δεν έχουν πλέον εξουσιοδότηση πρόσβασης στα δεδομένα ή όταν λήξει η σύμβαση εργασίας τους. Ακόμη, είναι σημαντικό να προσαρμόζονται τα δικαιώματα αυτών σε περίπτωση αλλαγής του ρόλου και των αρμοδιοτήτων ενός χρήστη.

στ) διεξαγωγή μιας ετήσιας αναθεώρησης της λίστας των δικαιωμάτων, για τον εντοπισμό και τη διαγραφή των ανενεργών λογαριασμών και την αναπροσαρμογή των δικαιωμάτων, όπου κρίνεται αναγκαίο. Για προσωρινούς λογαριασμούς (π.χ. για άτομο το οποίο κάνει πρακτική άσκηση στον οργανισμό ή

για κάποιο πάροχο υπηρεσιών ο οποίος θα πρέπει να έχει πρόσβαση στο σύστημα) θα πρέπει να καθοριστεί η ημερομηνία του λογαριασμού κατά την αρχική ανάθεση.

ζ) διατήρηση αρχείων καταγραφής (log files), που συνδέονται με τη διαχείριση των δικαιωμάτων των χρηστών.

ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Έλεγχος φυσικής πρόσβασης

Δε θα πρέπει να λησμονείται η φυσική ασφάλεια, από καμία λήψη μέτρων προστασίας. Μια βασική ενέργεια του υπεύθυνου επεξεργασίας είναι να αποτρέψει τις μη εξουσιοδοτημένες φυσικές προσβάσεις στις εγκαταστάσεις στις οποίες πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Πιο συγκεκριμένα, είναι υπεύθυνος για:

α) να κατηγοριοποιήσει και να διαχωρίσει τις περιοχές των κτιριακών εγκαταστάσεων ανάλογα με την κρισιμότητά τους. Λόγου χάριν, μπορούν να οριοθετηθούν οι ακόλουθες ζώνες:

i) περιοχή ανοικτή στο κοινό, όταν ο οργανισμός έχει ένα λειτουργικό καθήκον να επικοινωνεί με το κοινό, όπου εμπεριέχει αίθουσα υποδοχής, αίθουσα αναμονής, αίθουσα συνεδριάσεων

ii) περιοχή ελεγχόμενης πρόσβασης, συμπεριλαμβανομένων των γραφείων των υπαλλήλων και των χώρων αποθήκευσης

iii) περιοχή ασφαλείας στην οποία στεγάζονται οι διακομιστές (server room), σταθμοί διαχείρισης δικτύου, τα ενεργά συστατικά του δικτύου (ευαίσθητοι πόροι), όπως εξοπλισμός ενεργειακού εφοδιασμού και διανομής ή εξοπλισμός δικτύου και τηλεφωνίας

β) να διατηρεί έναν κατάλογο ατόμων (συμπεριλαμβανομένων επισκεπτών, υπαλλήλων, εξουσιοδοτημένων υπαλλήλων, διαχειριστών συστημάτων, διοικητικών στελεχών, εκπαιδευόμενων και παρόχων υπηρεσιών), που είναι εξουσιοδοτημένοι να εισέρχονται σε κάθε περιοχή. Ο κατάλογος είναι σημαντικό να επανεξετάζεται τακτικά, έτσι ώστε να είναι ενημερωμένος και συμβατός με τις απαιτήσεις του οργανισμού, σχετικά με τα δικαιώματα πρόσβασης στις περιοχές ασφαλείας.

γ) να επιλέγει και να υλοποιεί μεθόδους αυθεντικοποίησης για την εξακρίβωση της ταυτότητας των εργαζομένων, συμφώνως προς το μέγεθος των κινδύνων. Παρόμοιες μεθόδους, έχει χρέος να εφαρμόζει και για τους επισκέπτες. Ειδικότερα:

i) εάν οι κίνδυνοι είναι χαμηλοί, ένα άτομο που βρίσκεται στον χώρο υποδοχής, είναι επαρκές για τον έλεγχο της πρόσβασης

ii) εάν οι κίνδυνοι είναι μεγαλύτεροι, όπως στην περιοχή ελεγχόμενης πρόσβασης, συνιστάται η εφαρμογή μιας πιο ισχυρής μεθόδου αυθεντικοποίησης. Αυτή θα μπορούσε (ενδεικτικά) να είναι η επίδειξη μιας έξυπνης κάρτας, που να περιέχει τη φωτογραφία αναγνώρισης του κομιστή και τον αριθμό αναγνώρισης του εργαζομένου

iii) εάν οι κίνδυνοι είναι ιδιαιτέρως υψηλοί, συνιστάται η εφαρμογή μιας ιδιαιτέρως ισχυρής μεθόδου αυθεντικοποίησης, όπως η υλοποίηση βιομετρικών μεθόδων αυθεντικοποίησης με τη χρήση του δακτυλικού αποτυπώματος ή της ίριδας του ματιού

δ) να ορίσει τις ενέργειες που πρέπει να ακολουθηθούν σε περίπτωση αποτυχίας της διαδικασίας αυθεντικοποίησης. Λόγου χάρη, εάν δεν ισχύουν τα διαπιστευτήρια ή δεν υπάρχει εξουσιοδότηση για την είσοδο σε μια περιοχή ασφαλείας, να απαγορεύεται η είσοδος και να ειδοποιείται ο υπεύθυνος για τη φύλαξη του κτιρίου.

Προστασία από φυσικές καταστροφές

Αξιοσημείωτες είναι και οι φυσικές καταστροφές, γιατί οι επιπτώσεις τους ενδέχεται να είναι επιβλαβέστατες, δυσδιάκριτες και ανεπανόρθωτες. Σε αυτές συμπεριλαμβάνονται η πυρκαγιά, ο σεισμός, η πλημμύρα και άλλα. Επιβάλλεται λοιπόν:

α) η εγκατάσταση συστημάτων πυρανίχνευσης, πυροπροστασίας, καπνού και θερμότητας με συναγερμούς, που μεταδίδονται σε κεντρική βάση (επιτόπια ασφάλεια και εξωτερικές υπηρεσίες). Παρομοίως, επιβάλλεται και η τήρηση πυροσβεστήρων σκόνης, υγρών και αερίων.

β) η εγκατάσταση συστημάτων παρακολούθησης, ελέγχου και ρύθμισης της θερμοκρασίας. Φερειπείν, συστήματα κλιματισμού με τη δυνατότητα παροχής σημάτων ειδοποίησης και ενημέρωσης, σε περίπτωση υπέρβασης του ορίου θερμοκρασίας.

γ) τα συστήματα παρακολούθησης και διαχείρισης του ηλεκτρικού ρεύματος. Είναι βασική η προστασία των συστημάτων από διακυμάνσεις ισχύος της ηλεκτρικής τάσης και από διακοπές της ηλεκτροδότησης, μέσω γεννήτριας ή μετατροπέων του ρεύματος και εγκατάσταση συστημάτων ειδοποίησης σε περίπτωση βλάβης ή δυσλειτουργίας.

δ) ο καθορισμός του χρόνου ανταπόκρισης, σε περίπτωση αποτυχίας των συμβάσεων συντήρησης του εξοπλισμού, που χρησιμοποιείται για τη λειτουργία των βασικών λειτουργιών και των υπηρεσιών ασφαλείας. Στον εξοπλισμό συμπεριλαμβάνονται οι πυροσβεστήρες, τα κλιματιστικά, οι ανιχνευτές καπνού και θερμότητας, οι ανιχνευτές μη εξουσιοδοτημένης εισόδου, οι γεννήτριες παροχής ηλεκτρικής ενέργειας.

ε) ο καθορισμός διαδικασίων για την υποστήριξη αγαθών, μηχανημάτων και εξοπλισμού από πλημμύρα.

Επιπροσθέτως παίζει σπουδαίο ρόλο η οργάνωση των εγκαταστάσεων. Ειδικότερες υποπεριπτώσεις αποτελούν:

α) η αφαίρεση αχρησιμοποίητων κιβωτίων, αναλωσίμων και εύφλεκτων ουσιών,

β) η ανύψωση των αγαθών σε απόσταση τουλάχιστον 20 εκατοστών από το έδαφος, απομακρύνοντάς τα από εγκαταστάσεις νερού, που θα μπορούσαν να προκαλέσουν κίνδυνο πλημμύρας (υδραυλικά, κλιματιστικά, καλοριφέρ),

γ) η τήρηση των αγαθών, μακριά από ευπαθή σημεία και χώρους. Πιο συγκεκριμένα, καλό είναι η εγκατάσταση του server room, να γίνεται σε υψηλούς ορόφους στα κτίρια και όχι στο ισόγειο ή το υπόγειο, για την αποφυγή καταστροφής από σεισμούς.

δ) η αποθήκευση επικίνδυνων προϊόντων (συμπεριλαμβανομένων των εύφλεκτων, διαβρωτικών, εκρηκτικών, και υγρών αντικειμένων) σε κατάλληλες περιοχές αποθήκευσης και σε ασφαλή απόσταση από τις περιοχές, όπου γίνεται η επεξεργασία των προσωπικών δεδομένων.

ΑΡΧΕΙΟΘΕΤΙΚΑ

Αρχεία καταγραφής

Προκειμένου να υπάρχει πλήρης επίγνωση της εγγραφής, διόρθωσης και διαγραφής δεδομένων, οι δραστηριότητες αυτές καταγράφονται σε ενεργοποιημένα αρχεία που ονομάζονται αρχεία καταγραφής. Μάλιστα είναι χρέος, να επιβλέπονται ανά τακτά διαστήματα, από αρμόδιο υπάλληλο για ανίχνευση και αναγνώριση αθέμιτων ενεργειών. Επιπρόσθετα περιεχόμενα σε αυτά, είναι:

α) η καταγραφή επιτυχημένων και αποτυχημένων προσπαθειών σύνδεσης των χρηστών, τόσο σε επίπεδο λειτουργικού συστήματος όσο και σε επίπεδο εφαρμογών, καθώς και στις επιμέρους βάσεις δεδομένων των εφαρμογών

β) η πρόσβαση στα αρχεία καταγραφής με χρονοσφραγίδα

γ) οι ενέργειες των διαχειριστών των συστημάτων και τα χρονικά διαστήματα επεξεργασίας δεδομένων

δ) η ανίχνευση και η αναγνώριση αθέμιτων ενεργειών, ανά τακτά διαστήματα από αρμόδιο υπάλληλο του υπεύθυνου επεξεργασίας (π.χ. διαχειριστή ή/και υπεύθυνο ασφαλείας) και παράλληλα η διασφάλιση της ακεραιότητάς τους

ε) η μη εφικτή διαγραφή και αλλοίωση των αρχείων καταγραφής

Πολύ χρήσιμο θα ήταν να υπάρχει πρόβλεψη, ώστε το σύστημα να σταματά τη λειτουργία του, αν το σύστημα των αρχείων καταγραφής πάψει την καταγραφή συμβάντων/γεγονότων.

Αντίγραφα ασφαλείας

Τα αντίγραφα ασφαλείας (backup files) είναι διπλότυπα ηλεκτρονικών (μερικές φορές και φυσικών εντύπων) αρχείων και δεδομένων, που δίνουν τη δυνατότητα για άμεση ανάκτηση των πρωτότυπών τους σε περίπτωση διαγραφής, καταστροφής, απώλειάς τους. Τα αντίγραφα ασφαλείας αποθηκεύονται σε ασφαλή χώρο και φέρουν κατάλληλη σήμανση. Για αυτό ζητείται συγκεκριμένη πολιτική λήψης αντιγράφων ασφαλείας, η οποία, στο μικρότερο βαθμό της, θα ενσωματώνει τις επόμενες υποχρεώσεις για διατήρηση δεδομένων (data retention):

α) χρόνους λήψης των αντιγράφων και χρόνους κράτησής τους

β) μέτρα για την ασφαλή αποθήκευσή τους, όπως η κρυπτογράφησή τους ή ο ορισμός διαφορετικών τοποθεσιών που υποχρεωτικά αποθηκεύονται

γ) μέτρα για τον έλεγχο της ορθής εξαγωγής τους, όπως ο περιοδικός έλεγχος ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται

δ) υπεύθυνο εφαρμογής της πολιτικής λήψης αντιγράφων

ε) αποθήκευση σε ασφαλή χώρο, διαφορετικό από τον τόπο λήψη

στ) επαρκές επίπεδο ασφάλειας κατά την μεταφορά των αντιγράφων από μια εγκατάσταση σε μια άλλη

ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Ανωνυμοποίηση δεδομένων προσωπικού χαρακτήρα

Στόχος του υπεύθυνου επεξεργασίας με τη χρήση των μεθόδων ανωνυμοποίησης είναι η αφαίρεση των χαρακτηριστικών αναγνώρισης από τα προσωπικά δεδομένα. Δηλαδή, να καθίσταται αδύνατη η διασύνδεση μεταξύ των προσωπικών δεδομένων και του φυσικού προσώπου στο οποίο αναφέρονται. Συνεπώς, υπάρχει ανάγκη για:

α) προσδιορισμό εκείνων των δεδομένων που χρήζουν ανωνυμοποίησης, συναρτήσει του πλαισίου και της μορφής αποθήκευσης (συμπεριλαμβανομένων των πεδίων βάσεων δεδομένων ή αποσπασμάτων κειμένων) των προσωπικών δεδομένων, όπως επίσης και των ενδεχόμενων κινδύνων αυτών,

β) μόνιμη ανωνυμοποίηση των δεδομένων που την απαιτούν. Εάν, όμως, τα δεδομένα αυτά δε δύνανται να υποστούν μόνιμη ανωνυμοποίηση, θα χρειαστεί να επιλεγούν εργαλεία (συμπεριλαμβανομένης της μερικής διαγραφής, hashing κλειδιού και περιεχομένου), έτσι ώστε να ικανοποιούνται παράλληλα οι λειτουργικές ανάγκες του οργανισμού.

γ) εντοπισμός των περιστάσεων όπου είναι εφικτό, αποφευχθεί η ανωνυμοποίηση με απλή διαγραφή ή κάλυψη μέρους των δεδομένων. Πράγματι, μερικές φορές υπάρχουν πιο απλοί μέθοδοι για να επιτευχθεί ο επιθυμητός στόχος. Για παράδειγμα:

i) η διατήρηση μόνο του έτους γέννησης και όχι της πλήρους ημερομηνίας γέννησης, έτσι ώστε να μη μπορεί να αναγνωριστεί το υποκείμενο των δεδομένων, εάν ο τόπος γέννησής του και το φύλο του είναι επίσης γνωστά

ii) η διαγραφή των τελευταίων δύο οκτάδων μιας διεύθυνσης Ipv4

iii) η αντικατάσταση των αναγνωριστικών προσωπικών δεδομένων με ουδέτερο κείμενο (αστέρια, μερικά πανομοιότυπα γράμματα ή ένα διαδοχικό αναγνωριστικό)

Σε περίπτωση, κατά την οποία τα εξουσιοδοτημένα πρόσωπα οφείλουν, να είναι σε θέση να επιβεβαιώνουν ότι, τα ανώνυμα δεδομένα αντιστοιχούν στα αρχικά δεδομένα που βρίσκονται στην κατοχή τους, δύνανται να χρησιμοποιούν μια συνάρτηση κατακερματισμού, όπως η SHA-256 με μυστικό κλειδί (HMAC), ή να εκτελούν διπλή ανωνυμοποίηση με δύο μυστικά κλειδιά, που τηρούν δύο διαφορετικές οντότητες.

Αναγνώριση και αυθεντικοποίηση

Κάθε λειτουργικό σύστημα, εφαρμογή και γενικότερα κάθε πληροφοριακό σύστημα, κινδυνεύει σε μεγάλο βαθμό από μη εξουσιοδοτημένες προσβάσεις και τροποποιήσεις, εάν δεν υφίστανται κατάλληλα μέτρα αυθεντικοποίησης οντοτήτων. Το πιο απλό ενδεχόμενο είναι το «σπάσιμο» ενός κωδικού ή με απλά λόγια, το να βρει ένας τρίτος το συνθηματικό πρόσβασης και να έχει πρόσβαση και εξουσιοδότηση στο σύστημα. Επομένως, η πολιτική των συνθηματικών, είναι βασικό να χαρακτηρίζεται από αυξημένη πολυπλοκότητα. Μερικές ιδιότητες, που εξασφαλίζουν αυτήν την ιδιότητα, είναι:

α) η απαγόρευση επαναχρησιμοποίησης ενός παλαιότερου συνθηματικού,

β) η αλλαγή των προκαθορισμένων (default) συνθηματικών (εφόσον υπάρχουν) και η γενικότερη τακτή ανανέωση/αντικατάσταση συνθηματικού ανά χρονική περίοδο,

γ) η εφαρμογή παρεμπόδισης πρόσβασης, έπειτα από κάποιον αριθμό διαδοχικών και αποτυχημένων προσπαθειών πρόσβασης. Αυτό κατορθώνεται με το κλείδωμα του λογαριασμού ή με την αύξηση του χρόνου αναμονής για την επόμενη δυνατή προσπάθεια εισόδου ή με άλλη διεργασία.

δ) η υποχρεωτική χρήση μεγάλου μήκους συνθηματικών, με αρκετούς διαφορετικούς χαρακτήρες (αριθμητικοί, αλφαβητικοί, ειδικά σύμβολα),

ε) η μη επιτρεπτή δημιουργία κωδικών χαμηλής εντροπίας, δηλαδή κωδικών που χρησιμοποιούνται συχνά ή είναι εύκολο να τους μαντέψει κάποιος, όπως ένα όνομα συνοδευόμενο από διαδοχικούς αριθμούς (π.χ. Maria123) ή από ημερομηνία γέννησης (π.χ. Nikos1997),

στ) το διαφορετικό συνθηματικό σε κάθε χρήστη του συστήματος και σε ομάδες χρηστών,

ζ) αυθεντικοποίηση βάσει ρόλου (κυρίως για τις εφαρμογές) και έλεγχος ορθής υλοποίησης των δικαιωμάτων πρόσβασης στο σύστημα,

η) η διαδικασία για τη διαχείριση των κλειδιών και των πιστοποιητικών, η οποία περιλαμβάνει την περίπτωση των ξεχασμένων συνθηματικών,

θ) η επιλογή μεθόδου αυθεντικοποίησης, συμφώνως προς το πλαίσιο της επεξεργασίας, την κρισιμότητα των δεδομένων και το επίπεδο των εντοπισθέντων κινδύνων. Πιο συγκριμένα, εάν οι κίνδυνοι είναι:

i) χαμηλού επιπέδου, μπορεί να υπάρχει ένας κωδικός πρόσβασης,

ii) μεσαίου επιπέδου, είναι δυνατό να χρησιμοποιούνται κωδικοί πρόσβασης μιας χρήσης, όπου θα αποστέλλονται μέσω μηνύματος SMS, σε κάρτα με κωδικό PIN, κτλ,

iii) υψηλού επιπέδου, καθίσταται απαραίτητη η εφαρμογή ισχυρής αυθεντικοποίησης, όπως είναι τα ψηφιακά πιστοποιητικά.

ι) η κρυπτογραφημένη αποθήκευση των κωδικών πρόσβασης, κατά την εισαγωγή τους σε προγράμματα, αρχεία, βάσεις δεδομένων και άλλα.

Ένας ισχυρός μηχανισμός εξακρίβωσης οντότητας, ο οποίος μάλιστα έχει αναφερθεί και στη «Διαχείριση δικαιωμάτων χρηστών», αποτελεί ο συνδυασμός τουλάχιστον δύο από τα παρακάτω:

α) αυθεντικοποίηση με κάτι που γνωρίζει ο χρήστης (π.χ. έναν κωδικό πρόσβασης)

β) αυθεντικοποίηση με κάτι που έχει ο χρήστης (π.χ. μια έξυπνη κάρτα)

γ) αυθεντικοποίηση με κάποιο ειδικό ή μοναδικό χαρακτηριστικό για τον χρήστη (π.χ. δακτυλικό αποτύπωμα, ίριδα του ματιού)

ΜΕΙΩΣΗ ΕΥΠΑΘΕΙΩΝ

Μείωση ευπαθειών του λογισμικού

Άλλο ουσιώδες καθήκον του υπεύθυνου επεξεργασίας είναι ο περιορισμός, ή ακόμα και η εξάλειψη των ευπαθειών, που σχετίζονται με το λογισμικό (λειτουργικά συστήματα, επιχειρηματικές εφαρμογές, συστήματα διαχείρισης βάσεων δεδομένων, κλπ) και οι οποίες είναι δυνατόν να εμφανίσουν κινδύνους για τα δεδομένα προσωπικού χαρακτήρα. Επομένως, ο υπεύθυνος ή/και ο εκτελών την επεξεργασία προϋποθέτει:

α) να διατηρεί τα συστήματα και τις εφαρμογές λογισμικού ενημερωμένα (εκδόσεις, ενημερώσεις ασφαλείας κ.λπ.). Όπου αυτό δεν είναι εφικτό (λ.χ. σε παλιές εφαρμογές που δεν υποστηρίζονται πλέον από τον κατασκευαστή τους), θα απομονώνει το μηχάνημα στο οποίο είναι εγκατεστημένη η εφαρμογή και θα παρακολουθεί προσεκτικά τα αρχεία καταγραφής.

β) να χρησιμοποιεί τις τελευταίες εκδόσεις, που χρησιμοποιούνται από τον προμηθευτή του λογισμικού ή από τρίτο μέρος, εφόσον έχει πραγματοποιήσει δοκιμές των ενημερώσεων, πριν την ανάπτυξή τους σε όλο το σύστημα, και να εξασφαλίζει ότι, οι ενημερώσεις μπορούν να απενεργοποιηθούν σε περίπτωση αποτυχίας,

γ) να ελέγχει τακτικά ότι οι άδειες λογισμικού είναι έγκυρες,

δ) να προστατεύει την ακεραιότητα, τη διαθεσιμότητα και, όπου απαιτείται, την εμπιστευτικότητα του λογισμικού και των πηγαίων κωδικών εφαρμογών που αναπτύσσονται εσωτερικά, ιδίως εάν είναι καινοτόμες ή σχετίζονται άμεσα με την επεξεργασία δεδομένων προσωπικού χαρακτήρα,

ε) να παρέχει ένα επαρκές επίπεδο ασφαλείας για τους διακομιστές(servers) με:

i) απομόνωση των διακομιστών κρίσιμων για τα δεδομένα από το υπόλοιπο δίκτυο σε μια αποστρατικοποιημένη ζώνη (DMZ)

ii) προστασία από ιούς, spyware και ανεπιθύμητα μηνύματα με την εφαρμογή πιστοποιημένων και ενημερωμένων προγραμμάτων

iii) εγκατάσταση ενημερωμένων εκδόσεων ασφαλείας του λειτουργικού συστήματος

iv) πιστοποίηση συσκευών με τη χρήση ψηφιακών πιστοποιητικών (digital certificates)

στ) να παρέχει ένα επαρκές επίπεδο ασφαλείας για τις βάσεις δεδομένων (databases) με:

i) τη μη χρήση των διακομιστών, που χρησιμοποιούνται για βάσεις δεδομένων και περιέχουν δεδομένα προσωπικού χαρακτήρα, για άλλους σκοπούς, όπως για περιήγηση στον ιστό (web browsing) ή πρόσβαση σε ηλεκτρονικό ταχυδρομείο (E-mail server)

ii) την εφαρμογή ή/και εγκατάσταση συστημάτων για την προστασία από επιθέσεις SQL INJECTION και SCRIPT INJECTION

iii) την απαγόρευση εισαγωγής μεγάλων όγκων δεδομένων

iv) την απαγόρευση εισαγωγής δεδομένων από πλευράς χρήστη, που δεν είναι εγκεκριμένου τύπου και με ένα γενικότερο φιλτράρισμα των δεδομένων που εισάγει ο χρήστης

v) την απενεργοποίηση της χρήσης των δεδομένων, που εισάγει ο χρήστης για την εκτέλεση οποιωνδήποτε εργασιών (π.χ. εντοπισμός και απόρριψη δεδομένων που ενδέχεται να εκκινήσουν μια εκτελέσιμη εντολή)

ζ) να παρέχει ένα επαρκές επίπεδο ασφαλείας για τις υπηρεσίες ηλεκτρονικού ταχυδρομείου, με:

i) κρυπτογράφηση συνημμένων αρχείων που περιέχουν δεδομένα προσωπικού χαρακτήρα και χρήση λογισμικού κρυπτογράφησης μηνυμάτων ηλεκτρονικού ταχυδρομείου, όπως το PGP (Pretty Good Privacy) ή το S/MIME

ii) ενημέρωση των χρηστών για να μην ανοίγουν μηνύματα ηλεκτρονικού ταχυδρομείου με άγνωστη προέλευση και ιδιαίτερα επικίνδυνα συνημμένα (με επεκτάσεις όπως .pif, .com, .bat, .exe, .vbs και .lnk). Ακόμα, μπορεί να διαμορφώσει το σύστημα, με απώτερο σκοπό να καθίσταται αδύνατο, να ανοιχθούν αρχεία με τέτοιες επεκτάσεις

<u>Μείωση ευπαθειών που συνδέονται με τα υποστηρικτικά υλικά αγαθά</u>

Επιπρόσθετο χρέος του υπεύθυνου επεξεργασίας είναι ο περιορισμός, ή ακόμα και η εξάλειψη των ευπαθειών, που συνδέονται με τα υποστηρικτικά για τα δεδομένα υλικά αγαθά (σταθμοί εργασίας, μηχανήματα, δικτυακός και τηλεπικοινωνιακός εξοπλισμός, κ.λπ.), οι οποίες μπορούν να προκαλέσουν την εμφάνιση κινδύνων για τα δεδομένα προσωπικού χαρακτήρα. Συνεπώς ο υπεύθυνος ή/ και ο εκτελών την επεξεργασία χρειάζεται:

α) να διατηρεί έναν ενημερωμένο κατάλογο των πόρων και των υλικών αγαθών που χρησιμοποιούνται κατά τις πράξεις επεξεργασίας. Αυτός ο κατάλογος πρέπει να καθορίζει πληροφορίες σχετικά με τον εξοπλισμό, τον τύπο του λειτουργικού συστήματος, το δίκτυο (διεύθυνση IP, διεύθυνση MAC), τις προηγούμενες εκδόσεις και τις εγκατεστημένες ενημερωμένες εκδόσεις λογισμικού, που είναι εγκατεστημένες. Ενδεικτικά θα διατηρεί μια λίστα:

i) των σταθμών εργασίας και των χρηστών στους οποίους έχουν ανατεθεί

ii) των τοπικά διαχειριζόμενων διακομιστών

iii) του εξοπλισμού δικτύου και τηλεπικοινωνιών

iv) άλλων συσκευών, όπως εκτυπωτές, φαξ, κλπ

v) των κινητών συσκευών, όπως φορητοί υπολογιστές

β) να παρέχει ένα επαρκές επίπεδο ασφαλείας για τις κινητές συσκευές. Ενδεικτικά μπορεί να προβεί στις παρακάτω ενέργειες:

i) περιορισμός στο ελάχιστο, των προσωπικών δεδομένων που είναι αποθηκευμένα σε κινητές συσκευές (αυτή η αποθήκευση κατά τη διάρκεια ταξιδιού στο εξωτερικό απαγορεύεται)

ii) κρυπτογράφηση προσωπικών δεδομένων που είναι αποθηκευμένα σε κινητές συσκευές

iii) εξασφάλιση της διαθεσιμότητας των προσωπικών δεδομένων που είναι αποθηκευμένα σε κινητές συσκευές με την αντιγραφή τους σε άλλον υπολογιστή ή συσκευή το συντομότερο δυνατόν

iv) διαγραφή των προσωπικών δεδομένων από κινητές συσκευές, μόλις αυτά καταχωρηθούν στο σύστημα πληροφοριών του οργανισμού

Μείωση ευπαθειών αναφορικά με τα δίκτυα επικοινωνίας

Ένας άλλος περιορισμός, που οφείλει ο υπεύθυνος επεξεργασίας να εφαρμόσει, είναι ο περιορισμός, ή ακόμα και η εξάλειψη των ευπαθειών, αναφορικά με τα στοιχεία του δικτύου επικοινωνιών υπολογιστών (ενσύρματα δίκτυα, ασύρματα δίκτυα Wi-Fi, ραδιοκύματα, οπτικές ίνες, κλπ) και οι οποίες δύνανται να προκαλέσουν κινδύνους στα δεδομένα προσωπικού χαρακτήρα. Άρα, ο υπεύθυνος ή/και ο εκτελών την επεξεργασία έχει χρέος:

α) να διατηρεί ένα λεπτομερή και ενημερωμένο χάρτη του δικτύου του οργανισμού και να καταγράφει σε μητρώο όλα τα σημεία πρόσβασης (access points) στο Διαδίκτυο

β) να κατακερματίσει το δίκτυο σε ζώνες κρισιμότητας (υποδίκτυα), προκειμένου να ομαδοποιηθούν ορισμένα είδη υλικού, σύμφωνα με λογικά κριτήρια και να ελέγχει τις ροές δεδομένων που βασίζονται σε διευθύνσεις δικτύου, δημιουργώντας διακριτά φυσικά δίκτυα, ώστε να διαχωριστεί η κυκλοφορία του δικτύου μεταξύ των διαφόρων ομάδων εσωτερικού δικτύου, αποστρατικοποιημένης ζώνης (DMZ), περιμετρικού δικτύου, εξωτερικού δικτύου

γ) να απαγορεύει κάθε άμεση επικοινωνία μεταξύ εσωτερικών σταθμών εργασίας και εξωτερικών δικτύων

δ) να χρησιμοποιεί μόνο συνδέσεις που επιτρέπονται ρητά, με τη χρήση ενός τείχους προστασίας

ε) να παρακολουθεί διαρκώς τη δραστηριότητα του δικτύου μέσω συστημάτων ανίχνευσης εισβολής (IDS) ή συστημάτων πρόληψης εισβολής (IPS), προκειμένου να αναλύεται η κυκλοφορία δικτύου σε πραγματικό χρόνο και να

εντοπίζεται στο μέτρο του δυνατού, οποιαδήποτε ύποπτη δραστηριότητα που δύναται να προκαλέσει κάποιο περιστατικό παραβίασης των δεδομένων προσωπικού χαρακτήρα

στ) να αποτρέπει τη σύνδεση μη ελεγχόμενου υλικού στο εσωτερικό δίκτυο του οργανισμού

ζ) να επιτρέπει, μόνο στο υλικό (υπολογιστές, PDA, έξυπνες συσκευές κλπ) του οποίου η διαμόρφωση έχει εγκριθεί ρητά από τον υπεύθυνο ασφάλειας, να συνδεθεί ή να συγχρονιστεί με το δίκτυο ή τους σταθμούς εργασίας

η) να φροντίσει για την ύπαρξη μοναδικών αναγνωριστικών των καρτών δικτύου (διεύθυνση MAC) του υλικού ως μέσο αυθεντικοποίησης, με το οποίο θα ανιχνεύονται και θα αποκλείονται οι συνδέσεις

θ) να διαβιβάζει μυστικές πληροφορίες, συσχετισμένες με τη διατήρηση της εμπιστευτικότητας των προσωπικών δεδομένων (κλειδί αποκρυπτογράφησης, κωδικός πρόσβασης κλπ) σε κανάλι διαφορετικό από εκείνο που χρησιμοποιείται για τη μετάδοση δεδομένων ή εναλλακτικά με τη χρήση περισσοτέρων ασφαλών μεθόδων. Παραδείγματος χάριν, η αποστολή κρυπτογραφημένων αρχείων μέσω ηλεκτρονικού ταχυδρομείου και η παράδοση κωδικών μέσω τηλεφώνου ή σε γραπτό μήνυμα.

ΔΙΚΤΥΑΚΗ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ

Αντιμετώπιση κακόβουλων λογισμικών

Θεμελιώδες χρέος του υπεύθυνου επεξεργασίας είναι η προστασία των δεδομένων προσωπικού χαρακτήρα από τους κινδύνους, που προκύπτουν με την εισαγωγή κακόβουλου λογισμικού στις εφαρμογές και τα συστήματα του οργανισμού. Αυτό συνήθως γίνεται δια μέσου δημοσίων δικτύων ή μη ελεγχόμενων δικτύων (δίκτυα συνεργατών), σταθμών εργασίας και διακομιστών. Προγράμματα αντιμετώπισης των κακόβουλων λογισμικών, εκτός άλλων, αποτελούν τα αντι-ιϊκά προγράμματα (antivirus). Προϋποθέσεις για τη σωστή λειτουργία τους είναι:

α) η ενημέρωση των βάσεων δεδομένων των προγραμμάτων τουλάχιστον ανά ημέρα και των μηχανών προστασίας εβδομαδιαία. Αν και αυτό συνήθως αποτελεί αυτοματοποιημένη διαδικασία, χρειάζεται να εξασφαλιστεί ότι δεν είναι απενεργοποιημένη αυτή η διαδικασία.

β) η έλλειψη δυνατότητας απενεργοποίησης και τροποποίησης των παραμέτρων των αντι-ιϊκών προγραμμάτων, από τους χρήστες,

γ) διασφάλιση της ανάλυσης του συστήματος σε πραγματικό χρόνο, σύμφωνα με τους κανόνες που ορίζονται από το τμήμα πληροφορικής και προστασίας δεδομένων στο εσωτερικό του οργανισμού,

δ) η πλήρης και αυτόματη ανάλυση των τοπικών δίσκων τουλάχιστον εβδομαδιαίως, χωρίς να χρησιμοποιεί τους πόρους του συστήματος, διαταράσσοντας έτσι τις υπόλοιπες διεργασίας. Λόγου χάριν καλό είναι, να εκτελούνται κατά τη διάρκεια των μη εργάσιμων ωρών, ή να εκτελούνται με περιορισμό του φορτίου του συστήματος που κατανέμεται στην ανάλυση.

ε) οι πολιτικές και τα μέτρα φιλτραρίσματος, που μπορούν να υλοποιηθούν για τον έλεγχο των εισροών και εκροών δικτύων, καθώς και υλοποίηση τείχους προστασίας (firewall),

στ) η καταγραφή συμβάντων παραβίασης, για στατιστική (και όχι μόνο) ανάλυση και για την αντιμετώπιση ανάλογων κινδύνων στο μέλλον.

Παρόλα αυτά, οι κίνδυνοι ποικίλλουν και πολλές φορές δεν υπάρχει πλήρης προστασία μόνο από τα αντι-ιϊκά προγράμματα. Για αυτό και υπάρχουν και τα Anti-Malware και Anti-Spyware (αντικατασκοπευτικά) και άλλα προγράμματα ασφάλειας των υπολογιστών από κακόβουλα προγράμματα. Λίγα λόγια για τα Anti-Malware:

α) καταπολεμούν τα malware, ένα σύνολο από την πιο συχνή κατηγορία κακόβουλων λογισμικών. Αυτά καταλαμβάνουν εξουσιοδότηση στον υπολογιστή και μετέπειτα ο κακόβουλος χρήστης «εξυπηρετεί τα συμφέροντά του».

β) δεν ταυτίζονται με τα αντι-ιϊκά προγράμματα και τα συμπληρώνουν σε αξιόλογο (πολλές φορές) βαθμό, εις βάρος των υπολογιστικών πόρων,

γ) προτείνονται να χρησιμοποιούνται, κατ’ ελάχιστον στους υπολογιστές με τα περισσότερα δικαιώματα και εξουσιοδοτήσεις, οι οποίοι χρήζουν μεγαλύτερης ασφάλειας,

δ) οι προϋποθέσεις για την ορθή λειτουργία τους είναι παρόμοιες (αν όχι ίδιες) με των αντι-ιϊκών λογισμικών, όπως και με κάθε λογισμικό καταπολέμησης κακόβουλων προγραμμάτων.

Ασφάλεια επικοινωνιών

Η ασφάλεια των επικοινωνιών αποτελεί ένα από τα μεγαλύτερης αξίας θέματα ασφάλειας. Υπάρχουν επίσημες πολιτικές, διαδικασίες και μέτρα ασφάλειας για την προστασία της μετάδοσης πληροφοριών. Αυτή μπορεί να χωριστεί σε:

α) απομακρυσμένη πρόσβαση, η οποία επιτρέπεται μόνο σε συγκεκριμένα εξουσιοδοτημένα πρόσωπα. Αυτή είναι απαραίτητο να εδραιώνεται με εποπτεία και έλεγχο του υπεύθυνου επεξεργασίας, με χρήση ειδικού κωδικού χρήστη και με επαρκή καταγραφή. Ταυτόχρονα απαιτείται εφαρμογή VPN για απομακρυσμένη πρόσβαση και ισχυρό μηχανισμό αυθεντικοποίησης του χρήστη (smart card, συσκευή παραγωγής onetime password (OTP), κτλ).

β) ασύρματη πρόσβαση, όπου αναφέρεται σε συγκεκριμένους χρήστες και υπολογιστές βάσει των απαιτήσεών τους. Αυτή πρέπει να προστατεύεται από αξιόπιστους αλγόριθμους κρυπτογράφησης, όπως WPA3 με αλγόριθμο κρυπτογράφησης AES. Σε κάθε περίπτωση, ο κωδικός πρόσβασης χρειάζεται να είναι πολύπλοκος και όχι ο προκαθορισμένος (default). Άλλο ζήτημα είναι τα ασύρματα δίκτυα ανοικτά σε επισκέπτες, τα οποία χρήζουν διαχωρισμού από το εσωτερικό δίκτυο.

γ) web-based εφαρμογές (βασισμένες στον παγκόσμιο ιστό). Εκεί η επικοινωνία γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας, φερειπείν μέσω υλοποίησης πρωτόκολλου TLS σε όλους τους διαδικτυακούς τόπους, τουλάχιστον TLS 1.2, με αλγόριθμο κρυπτογράφησης AES-GCM, ή ιδανικά TLS 1.3.

<u>Ειδικά μέτρα για κινητές ή απομακρυσμένες συσκευές</u>

Επίσης, ο υπεύθυνος επεξεργασίας πρέπει να καταπολεμά τις απειλές της εξ αποστάσεως πρόσβασης στο εσωτερικό δίκτυο του οργανισμού, μέσω κινητών ή απομακρυσμένων συσκευών (φορητοί υπολογιστές, έξυπνα κινητά ή ταμπλέτες, κλπ.). Για παράδειγμα, ένας υπάλληλος ευρισκόμενος σε μία χώρα του εξωτερικού, επιθυμεί να συνδεθεί μέσω του φορητού υπολογιστή του στο εταιρικό εσωτερικό δίκτυο, με απώτερο σκοπό να διαβάσει ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή να προσπελάσει μια παρουσίαση. Κατά συνέπεια, υπάρχει ανάγκη για την αντιμετώπιση των κινδύνων αυτών, μέσω:

α) κρυπτογράφησης επικοινωνιών μεταξύ κινητών συσκευών και εσωτερικών συστημάτων πληροφοριών,

β) χρήσης ενός εικονικού ιδιωτικού δικτύου (Virtual Private Network VPN) με την εφαρμογή αποδεδειγμένα ισχυρών αλγορίθμων κρυπτογράφησης, όπως για παράδειγμα SSL 128-bit για υπηρεσίες Web,

γ) εγκατάστασης ενός τείχους προστασίας για την προστασία της κίνησης δικτύου από και προς τις κινητές συσκευές. Αυτό το τείχος προστασίας θα είναι ενεργοποιημένο μόλις μια κινητή συσκευή εγκαταλείψει τις εγκαταστάσεις του

οργανισμού. Δεν θα είναι δυνατή η απενεργοποίηση ή η αλλαγή των ρυθμίσεών του τείχους προστασίας από τους χρήστες.

Ενδεικτικές εφαρμογές και μηχανισμοί για διαδικτυακή ασφάλεια

Εφόσον η επικοινωνία και η ανταλλαγή δεδομένων στηρίζεται άμεσα ή/και κυρίως στο διαδίκτυο, η ασφάλειά του καθίσταται βαρυσήμαντη. Η ασφάλειά του στηρίζεται ιδίως σε τεχνικές δικτύων και κρυπτογράφησης. Παρόλο που (πολλές φορές) αυτά συνδέονται άρρηκτα μεταξύ τους, εκτός άλλων, το πρώτο χρειάζεται:

α) περιορισμό της πρόσβασης στο διαδίκτυο με αποκλεισμό μη βασικών υπηρεσιών, φερειπείν VoIP, peer to peer, κτλ,

β) περιορισμό της δικτυακής πρόσβασης στα απολύτως απαραίτητα, με ισχυρό φιλτράρισμα της εισερχόμενης/εξερχόμενης κίνησης (firewall, proxy servers, κτλ.),

γ) μέθοδο που δεν επιτρέπει στα μη αυθεντικοποιημένα συστήματα τη σύνδεση στο δίκτυο,

δ) να γίνονται μέσω πρωτοκόλλου οι μεταφορές αρχείων σε τρίτους. Αυτό εγγυάται την εμπιστευτικότητα και την αυθεντικοποίηση του εξυπηρετητή-λήπτη, π.χ SFTP, FTPS, χρήση του PGP.

Ως κρυπτογράφηση ορίζεται ο μετασχηματισμός των δεδομένων προσωπικού χαρακτήρα σε μια φαινομενικά ακατάληπτη μορφή. Κατά συνέπεια, περιορίζεται ο κίνδυνος της αποκάλυψης των δεδομένων σε μη εξουσιοδοτημένες οντότητες, κάνοντάς τα δεδομένα μη αναγνώσιμα, σε όσους δεν είναι εξουσιοδοτημένοι να έχουν πρόσβαση σε αυτά. Σχετικά καθήκοντα, εκτός άλλων, αποτελούν:

α) η υποχρεωτική κρυπτογράφηση ευαίσθητων εγγράφων και δεδομένων, όταν στέλνονται μέσω ηλεκτρονικού ταχυδρομείου ή όταν αποθηκεύονται σε μια βάση δεδομένων,

β) η εμπιστευτικότητα των κλειδιών κρυπτογράφησης, των συνθηματικών, κτλ, αξιοποιώντας διαφορετικό ασφαλές κανάλι επικοινωνίας,

γ) η χρησιμοποίηση αναγνωρισμένων και ασφαλών αλγορίθμων, όπως:

i) SHA-256, SHA-512 ή SHA-3 συναρτήσεις κατακερματισμού

ii) HMAC με μία εκ των ανωτέρω συνάρτηση κατακερματισμού, για την αυθεντικοποίηση μηνύματος

iii) AES για συμμετρική κρυπτογράφηση (όχι με τρόπο λειτουργίας ECB – ανά περίπτωση, θα πρέπει να εξετάζεται η καλύτερη επιλογή μεταξύ CBC, CTR, GCM, XTS)

iv) BCRYPT,SCRYPT OR PBKDF2 για αποθήκευση συνθηματικών

v) RSA-OAEP για ασύμμετρη κρυπτογράφηση

vi) RSASSA-PSS ή ECDSA σε ψηφιακές υπογραφές

δ) η εφαρμογή κατάλληλων μεγεθών κλειδιών: για AES 128 bits (ιδανικά, 256 bits), για τον RSA το δημόσιο κλειδί (ζεύγος «exponent – modulus») θα πρέπει να ικανοποιεί τα εξής: το “exponent” να είναι μεγαλύτερο από 65536 και το modulus να έχει μέγεθος τουλάχιστον 2048 bits (ιδανικά 3072 ή 4096 bits),

ε) τα μυστικά κλειδιά, τα οποία είναι σημαντικό να προστατεύονται τουλάχιστον μέσω περιορισμένων δικαιωμάτων πρόσβασης και ασφαλή συνθηματικά.

Να τονισθεί ότι τα παραπάνω αναφερθέντα δεν είναι απόλυτα, αλλά ενδεικτικά. Πάντοτε τα μέτρα ασφάλειας, αναφερθέντα και μη, πρέπει να εφαρμόζονται ανάλογα με την περίσταση, την οποία πρόκειται να αντιμετωπίσουν. Τέλος, για τη σωστή επίτευξη και οργάνωση των άνω μέτρων ασφάλειας, ο οργανισμός προϋποτίθεται να διαθέτει:

α) πολιτική για την άσκηση των κρυπτογραφικών μηχανισμών,

β) πολιτική για τη χρήση, προστασία και διαχείριση των κρυπτογραφικών κλειδιών σε όλο τον κύκλο ζωής τους,

γ) διαδικασία για την διαχείριση των ευπαθειών στο σύστημα,

δ) διαχωρισμό του δικτύου σε διαφορετικά τμήματα.

ΔΙΚΤΥΟΓΡΑΦΙΑ – ΠΗΓΕΣ

ENISA, Guidelines for SMEs on the security of personal data processing, DECEMBER 2016

https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Cnil pia Knowledge Bases, February 2018 edition

https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf

Ιδιωτικό και δημόσιο μαθησιακό υλικό του Μάγκου Εμμανουήλ, Επίκ. Καθηγητή Τμήματος Πληροφορικής, Ιονίου Πανεπιστημίου

https://opencourses.ionio.gr/courses/DDI140/
https://e-class.ionio.gr/courses/DCS101/
https://e-class.ionio.gr/courses/DCS132/

Ιδιωτικό μαθησιακό υλικό της Τσώχου Αγγελικής, Επίκ. Καθηγήτριας Τμήματος Πληροφορικής, Ιονίου Πανεπιστημίου

https://opencourses.ionio.gr/modules/document/?course=DDI127
https://opencourses.ionio.gr/courses/DDI135/
https://e-class.ionio.gr/courses/DCS265/

Ιδιωτικό υλικό της Αρχής Προστασίας Προσωπικών Δεδομένων