ΤΕΥΧΟΣ ΠΡΟΔΙΑΓΡΑΦΩΝ 12

(ΤΕΠ-12)

Πληροφορικό Σύστημα Εποπτείας και Ελέγχου (ΠΣΕΕ)

Έκδοση: 1.0

ΚΕΦΑΛΑΙΟ 1: ΠΕΡΙΒΑΛΛΟΝΤΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΟΣ

1.1 Φυσική ασφάλεια

1.1.1 Γενική απαίτηση

Όλα τα στοιχεία συστήματος πρέπει να είναι αρκετά ανθεκτικά, ώστε να ανθίστανται σε παραβιάσεις.

1.2 Ασφάλεια υλισμικού και παικτών

1.2.1 Γενική απαίτηση

Τα ηλεκτρικά και μηχανικά μέρη και οι αρχές σχεδιασμού του ηλεκτρονικού υλισμικού δεν πρέπει να εκθέτουν τον παίκτη σε οποιοδήποτε φυσικό κίνδυνο. Η πιστοποίηση του ηλεκτρονικού υλισμικού από ανεξάρτητο φορέα πιστοποίησης δεν περιλαμβάνει δοκιμές ή χορήγηση πιστοποιήσεων για θέματα σχετικά με την Ασφάλεια και την Ηλεκτρομαγνητική Συμβατότητα (ΗΜΣ), καθώς τέτοιες δοκιμές και πιστοποιήσεις αποτελούν ευθύνη του κατασκευαστή του υλισμικού ή των εξουσιοδοτημένων αντιπροσώπων του στην Ε.Ε., σύμφωνα με τις προβλέψεις των σχετικών κείμενων διατάξεων.

1.3 Περιβαλλοντικές επιδράσεις στην ακεραιότητα του συστήματος

1.3.1 Πρότυπο ακεραιότητας

Τα ανεξάρτητα εργαστήρια πιστοποίησης θα πραγματοποιούν συγκεκριμένες δοκιμές για να προσδιορίσουν αν εξωτερικοί παράγοντες μπορούν να επηρεάσουν τη φερεγγυότητα του παιγνίου ή να δημιουργήσουν τη δυνατότητα εξαπάτησης. Τα συστήματα πρέπει να αντεπεξέρχονται στις ακόλουθες δοκιμές, συνεχίζοντας τη λειτουργία τους χωρίς την παρέμβαση του χειριστή:

α) Ηλεκτρομαγνητική παρεμβολή. Τα συστήματα δεν πρέπει να προκαλούν ηλεκτρονικό θόρυβο που επηρεάζει την ακεραιότητα ή τη φερεγγυότητα του γειτονικού συνδεδεμένου εξοπλισμού, και

β) Ηλεκτροστατική παρεμβολή. Για την προστασία από ηλεκτροστατική εκκένωση απαιτείται γείωση του υλισμικού του συστήματος με τρόπο που η ενέργεια της ηλεκτροστατικής εκκένωσης να μην προκαλεί μόνιμη βλάβη ή να μην αναστέλλει μόνιμα την κανονική

λειτουργία των ηλεκτρονικών ή άλλων στοιχείων του συστήματος. Τα συστήματα, ενδέχεται να παρουσιάσουν προσωρινή διακοπή όταν υποβάλλονται σε σημαντική ηλεκτροστατική εκκένωση, μεγαλύτερη από την εκκένωση του ανθρώπινου σώματος, αλλά πρέπει να έχουν τη δυνατότητα να επανέρχονται και να ολοκληρώνουν όλες τις λειτουργίες που διακόπηκαν, χωρίς απώλειες ή αλλοίωση των πληροφοριών που αφορούν τον έλεγχο ή τα σημαντικά δεδομένα που σχετίζονται με το σύστημα. Οι δοκιμές εκκένωσης στον αέρα θα πραγματοποιούνται μέχρι το επίπεδο των 27 kV.

ΚΕΦΑΛΑΙΟ 2: ΑΠΑΙΤΗΣΕΙΣ ΠΛΗΡΟΦΟΡΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΠΟΠΤΕΙΑΣ ΚΑΙ ΕΛΕΓΧΟΥ

2.1 Πληροφορικό σύστημα εποπτείας και ελέγχου

2.1.1 Γενική απαίτησ

Αν το πληροφορικό σύστημα εποπτείας και ελέγχου αποτελείται από πολλαπλά συστήματα υπολογιστών σε διάφορες τοποθεσίες, τότε το πληροφορικό σύστημα εποπτείας και ελέγχου ως σύνολο, καθώς και η επικοινωνία μεταξύ των στοιχείων του πρέπει να πληρούν τις ακόλουθες απαιτήσεις.

2.1.2 Τερματισμός λειτουργίας και επαναφορά

Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να έχει τις ακόλουθες δυνατότητες τερματισμού λειτουργίας και επαναφοράς:

α) Να έχει τη δυνατότητα να επανέρχεται από μη αναμενόμενες επανεκκινήσεις των κεντρικών του υπολογιστών ή οποιουδήποτε εκ των λοιπών στοιχείων του,

β) Να είναι σε θέση να τερματίζει ομαλά τη λειτουργία του σε περίπτωση απλής διακοπής ρεύματος και να επιτρέπει την αυτόματη επανεκκίνηση μετά την επαναφορά του ρεύματος, μόνον αφού ολοκληρωθούν οι ακόλουθες διαδικασίες ως ελάχιστη απαίτηση:

i. Επιτυχής ολοκλήρωση της τυπικής διαδικασίας ή διαδικασιών συνέχισης προγράμματος, συμπεριλαμβανομένων των αυτοελέγχων,

ii. Επιβεβαίωση της ταυτότητας όλων των σημαντικών αρχείων του πληροφορικού συστήματος εποπτείας και ελέγχου μέσω εγκεκριμένης μεθόδου (π.χ. ΚΕΠ, MD5, SHA-

1, κτλ.), και

iii. Εγκατάσταση και αντίστοιχη επιβεβαίωση ταυτότητας των επικοινωνιών με όλα τα στοιχεία που απαιτούνται για τη λειτουργία του πληροφορικού συστήματος εποπτείας και ελέγχου.

γ) Να έχει τη δυνατότητα να ταυτοποιεί και να διαχειρίζεται καταλλήλως τις περιπτώσεις κεντρικής επαναφοράς σε άλλα πληροφορικά συστήματα εποπτείας και ελέγχου που επηρεάζουν το αποτέλεσμα του παιγνίου, το ποσό νίκης ή τις μετρήσεις,

δ) Να έχει τη δυνατότητα να επαναφέρει όλες τις σημαντικές πληροφορίες από τη στιγμή της τελευταίας δημιουργίας αντιγράφων ασφαλείας μέχρι τη στιγμή που συνέβη το σφάλμα ή η επαναφορά του πληροφορικού συστήματος εποπτείας και ελέγχου (χωρίς να ορίζεται συγκεκριμένο χρονικό όριο), και

ε) Να έχει τη δυνατότητα να εξασφαλίζει επαρκώς την αδιάλειπτη διάθεση των δικαιωμάτων του παίκτη και της δυνατότητας επιτήρησης.

2.1.3 <u>Φιλοξενία από τρίτα μέρη</u>

Με την επιφύλαξη των υπηρεσιών που παρέχονται βάσει του ΤΕΠ-3, όταν ένα ή περισσότερα στοιχεία του πληροφορικού συστήματος εποπτείας και ελέγχου φιλοξενούνται από τρίτους παρόχους υπηρεσιών, πρέπει να πληρούνται οι ακόλουθες απαιτήσεις:

α) Τα προσωπικά και τα οικονομικά στοιχεία όλων των παικτών δεν πρέπει να είναι προσβάσιμα από τους τρίτους παρόχους υπηρεσιών. Ωστόσο, αυτό δεν αποκλείει τη χρήση υπηρεσιών τρίτων μερών για τη δημιουργία αντιγράφων ασφαλείας και την αποθήκευση δεδομένων,

β) Καμία λειτουργικότητα παιγνίου δεν πρέπει να είναι προσβάσιμη από τρίτους παρόχους υπηρεσιών, και

γ) Απαγορεύεται η χρήση υπηρεσιών τρίτων παρόχων που απαιτούν συμμόρφωση του λογισμικού με κανόνες/κανονισμούς που αντίκεινται σε οποιοδήποτε στοιχείο του παρόντος τεύχους.

2.1.4 <u>Απενεργοποίηση στοιχηματισμού</u>

Οι χειριστές του συστήματος πρέπει να διασφαλίζουν διαρκώς την απρόσκοπτη επικοινωνία όλων των παιγνιομηχανημάτων με το ΠΣΕΕ μέσω του ΚΠΣ, επιτρέποντας την πραγματοποίηση ελέγχου

και εποπτείας σε πραγματικό χρόνο. Οι ακόλουθες απαιτήσεις αφορούν την απενεργοποίηση και ενεργοποίηση του στοιχηματισμού από το πληροφορικό σύστημα εποπτείας και ελέγχου:

α) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να έχει τη δυνατότητα να ενεργοποιεί και να απενεργοποιεί κάθε επιλογή στοιχηματισμού κατόπιν εντολής,

β) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να είναι σε θέση να ενεργοποιεί και να απενεργοποιεί μεμονωμένα παίγνια κατόπιν εντολής,

γ) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να είναι σε θέση να ενεργοποιεί και να απενεργοποιεί μεμονωμένες συνεδρίες του εκάστοτε παίκτη κατόπιν εντολής, και

δ) Σε περίπτωση απενεργοποίησης ή ενεργοποίησης οποιασδήποτε επιλογής στοιχηματισμού από το πληροφορικό σύστημα εποπτείας και ελέγχου, πρέπει να δημιουργείται αντίστοιχη καταχώριση στο αρχείο καταγραφής ελέγχου. Πρέπει να καταγράφεται η αιτία οποιασδήποτε απενεργοποίησης σε προστατευμένο αρχείο ελέγχου, το οποίο δεν απαιτείται να αποτελεί μέρος του πληροφορικού συστήματος εποπτείας και ελέγχου.

2.1.5 <u>Χρονικά όρια λήξης λόγω αδράνειας χρήστη</u>

Σε περίπτωση που το πληροφορικό σύστημα εποπτείας και ελέγχου δεν είναι σε θέση να πραγματοποιήσει σταθμοσκόπηση (polling) του παιγνιομηχανήματος για την επιβεβαίωση σύνδεσης, θα πρέπει να εφαρμόζει χρονικά όρια λήξης λόγω αδράνειας του χρήστη.

2.1.6 <u>Σταθμοσκόπηση παιγνιομηχανημάτων</u>

Σε περίπτωση που το πληροφορικό σύστημα εποπτείας και ελέγχου έχει τη δυνατότητα να πραγματοποιήσει σταθμοσκόπηση, πρέπει να δύναται να σταθμοσκοπεί άμεσα ή μέσω του ΕΣΠ τα παιγνιομηχανήματα βάσει συγκεκριμένου χρονοδιαγράμματος και κατόπιν εντολής από το χειριστή του πληροφορικού συστήματος εποπτείας και ελέγχου:

α) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να έχει τη δυνατότητα να αποθηκεύει την ώρα και την ημερομηνία της τελευταίας σταθμοσκόπησης,

β) Η αποτυχία απόκρισης ενός παιγνιομηχανήματος εντός χρονικού διαστήματος 30 λεπτών πρέπει να οδηγεί σε τερματισμό της συνεδρίας, και

γ) Το παιγνιομηχάνημα πρέπει να θεωρεί ότι η συνεδρία τερματίστηκε σε περίπτωση αποτυχίας λήψης απόκρισης από τον εξυπηρετητή εντός χρονικού διαστήματος 30 λεπτών.

δ) Το παιγνιομηχάνημα πρέπει να ειδοποιεί τον παίκτη για τον τερματισμό της συνεδρίας.

ε) Το παίγνιο πρέπει να διακόπτεται μέχρι τη δημιουργία μιας νέας συνεδρίας μεταξύ του

πληροφορικού συστήματος εποπτείας και ελέγχου και του παιγνιομηχανήματος.

2.2 Πληροφορίες στοιχηματισμού που πρέπει να διατηρούνται στο πληροφορικό σύστημα εποπτείας και ελέγχου

2.2.1 Γενική απαίτηση

Ο Φορέας εκμετάλλευσης και η Ε.Ε.Ε.Π. πρέπει να διατηρούν τις πληροφορίες στοιχηματισμού για χρονικό διάστημα δέκα ετών σε ασφαλές μέσο ή μέσα, τα οποία θα καθιστούν δυνατή την ακριβή αναπαραγωγή των αποθηκευμένων δεδομένων εποπτείας από την Ε.Ε.Ε.Π.. Αυτές οι πληροφορίες μπορούν να αποθηκεύονται εκτός σύνδεσης (offline). Η χρονική σήμανση πρέπει να πραγματοποιείται με βάση μια συγκεκριμένη ζώνη ώρας και, εάν αυτή η ζώνη ώρας δεν είναι η Συντονισμένη Παγκόσμια Ώρα (Coordinated Universal Time, UTC), τότε πρέπει να είναι εμφανής η διαφορά με τη UTC.

2.2.2 Στοιχεία λογαριασμού παίκτη

Τα στοιχεία των λογαριασμών παικτών που πρέπει να διατηρούνται και να διατίθενται προς συμπερίληψη στις αναφορές του πληροφορικού συστήματος εποπτείας και ελέγχου και για τις οποίες πρέπει να δημιουργούνται αντίγραφα ασφαλείας είναι οι εξής:

α) Στοιχεία ταυτότητας χρήστη (συμπεριλαμβανομένης της μεθόδου επαλήθευσης),

β) Συγκατάθεση παίκτη ως προς τους Όρους και Προϋποθέσεις και την Πολιτική Απορρήτου του Φορέα εκμετάλλευσης,

γ) Στοιχεία λογαριασμού και τρέχον υπόλοιπο,

δ) Μέγιστα επίπεδα απώλειας στοιχήματος και κατάσταση αποκλεισμού,

ε) Προηγούμενοι λογαριασμοί και αιτίες απενεργοποίησης, και

στ) Πληροφορίες τρέχουσας συνεδρίας.

2.2.3 Πληροφορίες συνεδρίας

Για κάθε συνεδρία παιγνίου (δηλαδή από τη στιγμή της σύνδεσης ως τη στιγμή της αποσύνδεσης του παίκτη), οι πληροφορίες που πρέπει να διατηρούνται και να διατίθενται προς συμπερίληψη στις αναφορές του πληροφορικού συστήματος εποπτείας και ελέγχου και για τις οποίες πρέπει να δημιουργούνται αντίγραφα ασφαλείας είναι οι εξής:

α) Μοναδικό αναγνωριστικό παίκτη,

β) Ώρα έναρξης και λήξης της συνεδρίας,

γ) Στοιχεία σχετικά με τη συσκευή του παίκτη, όπως π.χ. η διεύθυνση IP και η έκδοση προγράμματος περιήγησης και/ή πελάτη,

δ) Συνολικό ποσό που στοιχηματίστηκε στη συνεδρία,

ε) Συνολικό ποσό που κερδήθηκε στη συνεδρία,

στ) Κεφάλαια που προστέθηκαν στο λογαριασμό για τη συνεδρία (με χρονική σήμανση),

ζ) Κεφάλαια που αποσύρθηκαν από το λογαριασμό για τη συνεδρία (με χρονική σήμανση),

η) Σε περίπτωση εφαρμογής σταθμοσκόπησης, την ώρα της τελευταίας επιτυχημένης σταθμοσκόπησης για τη συνεδρία,

θ) Αιτία τερματισμού της συνεδρίας,

ι) Σε περίπτωση εφαρμογής σταθμοσκόπησης, τα στοιχεία παιγνίου για τη συνεδρία (π.χ. παρτίδες που διεξήχθησαν, ποσά που στοιχηματίστηκαν, ποσά που κερδήθηκαν, Jackpot που κερδήθηκαν κ.λπ.),

ια) Υπόλοιπο λογαριασμού παίκτη κατά την έναρξη της συνεδρίας,

ιβ) Τρέχουσες ενεργές συνεδρίες (π.χ. σε εξέλιξη, ολοκληρώθηκε κ.λπ.), και

ιγ) Ώρα και ημερομηνία διακοπής.

2.2.4 <u>Πληροφορίες σημαντικών συμβάντων</u>

Οι ακόλουθες απαιτήσεις αφορούν την καταγραφή των πληροφοριών σημαντικών συμβάντων από το πληροφορικό σύστημα εποπτείας και ελέγχου:

α) Οι πληροφορίες σημαντικών συμβάντων που πρέπει να διατηρούνται και να διατίθενται προς συμπερίληψη στις αναφορές του πληροφορικού συστήματος εποπτείας και ελέγχου και για τις οποίες πρέπει να δημιουργούνται αντίγραφα ασφαλείας είναι οι εξής:

i. Πολύ υψηλά ποσά νίκης, τα οποία υπερβαίνουν την αξία που ορίζεται από την Ε.Ε.Ε.Π.,

ii. Μεταφορά πολύ μεγάλου όγκου κεφαλαίων (μεμονωμένα και συλλογικά για προκαθορισμένη χρονική περίοδο) που υπερβαίνει την αξία που ορίζεται από την Ε.Ε.Ε.Π.,

iii. Αλλαγές των παραμέτρων του παιγνίου που έγιναν από τον Φορέα Εκμετάλλευσης ή/και τους Παραχωρησιούχους,

iv. Αλλαγές των παραμέτρων Jackpot που έγιναν από τον Φορέα Εκμετάλλευσης ή/και τους Παραχωρησιούχους,

v. Νέα Jackpot που δημιουργήθηκαν,

vi. Περιστατικά νίκης Jackpot,

vii. Jackpot που αποσύρθηκαν,

viii. Αποκλεισμοί παίκτη (συμπεριλαμβανομένων της αιτίας αποκλεισμού, των αιτημάτων άρσης του αποκλεισμού και των άρσεων του αποκλεισμού),

ix. Συμβάντα εξωτερικών πληροφορικών συστημάτων εποπτείας και ελέγχου που επηρεάζουν το αποτέλεσμα του παιγνίου και των ποσών νίκης (π.χ. εξωτερικοί κεντρικοί υπολογιστές Jackpot),

x. Μη αναστρέψιμη απώλεια δεδομένων που αφορούν τους παίκτες, και

xi. Σημαντικές περίοδοι μη διαθεσιμότητας του πληροφορικού συστήματος εποπτείας και ελέγχου,

β) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να έχει τη δυνατότητα να παρέχει το κατάλληλο μέσο προβολής των σημαντικών συμβάντων, συμπεριλαμβανομένης της δυνατότητας αναζήτησης συγκεκριμένων τύπων συμβάντων, και

γ) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να έχει τη δυνατότητα να ταξινομεί τα συμβάντα κατά προτεραιότητα, βάσει του βαθμού σπουδαιότητάς τους (π.χ. αν απαιτείται καταγραφή συμβάντος, ενεργοποίηση συναγερμού ή απενεργοποίηση του παιγνίου).

2.2.5 *Δημιουργία αντιγράφων ασφαλείας*

Πρέπει να υφίσταται κατάλληλη μέθοδος δημιουργίας αντιγράφων ασφαλείας όλων των σημαντικών δεδομένων (δηλαδή των οικονομικών στοιχείων και των πληροφοριών ασφάλειας και συμβάντων) ανά εύλογα χρονικά διαστήματα, καθιστώντας δυνατή την ανάκτηση σε περίπτωση διακοπής.

ΚΕΦΑΛΑΙΟ 3: ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (INFORMATION SYSTEMS SECURITY - ISS)

3.1 Πολιτική ασφάλειας πληροφοριών

3.1.1 *Γενική απαίτηση*

Ένα έγγραφο πολιτικής ασφάλειας πληροφοριών πρέπει να εγκρίνεται από την Ε.Ε.Ε.Π., να δημοσιεύεται και να κοινοποιείται στο σύνολο των υπαλλήλων της και των εμπλεκόμενων

εξωτερικών φορέων. Η πολιτική ασφάλειας πληροφοριών πρέπει να πληροί τις ακόλουθες απαιτήσεις:

α) Η πολιτική ασφάλειας πληροφοριών πρέπει να υποβάλλεται σε αναθεώρηση ανά τακτά χρονικά διαστήματα και/ή κάθε φορά που πραγματοποιούνται σημαντικές αλλαγές, ώστε να διασφαλίζεται η αδιάλειπτη καταλληλότητα, επάρκεια και αποτελεσματικότητά της, και

β) Η προσέγγιση της Ε.Ε.Ε.Π. στη διαχείριση ασφάλειας και την εφαρμογή της (δηλαδή στόχοι ελέγχου, έλεγχοι, πολιτικές, διαδικασίες και μέθοδοι ασφάλειας πληροφοριών) πρέπει να ελέγχεται ανεξάρτητα ανά τακτά χρονικά διαστήματα ή κάθε φορά που πραγματοποιούνται σημαντικές αλλαγές στην εφαρμογή ασφάλειας. Μεταξύ των παραδειγμάτων «σημαντικών αλλαγών» μπορεί να συγκαταλέγεται η αναβάθμιση σε λειτουργικό σύστημα που επιτρέπει την πρόσβαση στο πληροφορικό σύστημα εποπτείας και ελέγχου από εξωτερικές πηγές, η προσθήκη νέων στοιχείων στο πληροφορικό σύστημα εποπτείας και ελέγχου και οι αλλαγές παραμετροποίησης του δικτύου, όπως π.χ. η προσθήκη νέων υποδικτύων (subnets).

3.2 Φυσικοί και περιβαλλοντικοί έλεγχοι

3.2.1 Ασφαλείς περιοχές

α) Τα πληροφορικά συστήματα εποπτείας και ελέγχου και τα σχετικά συστήματα επικοινωνιών πρέπει να βρίσκονται σε εγκαταστάσεις που παρέχουν φυσική προστασία από πιθανή πρόκληση βλάβης λόγω πυρκαγιάς, πλημμύρας, τυφώνα, σεισμού και άλλων φυσικών ή ανθρωπογενών καταστροφών,

β) Πρέπει να χρησιμοποιούνται περίμετροι ασφάλειας (φράγματα, όπως π.χ. τοίχοι, είσοδοι ελεγχόμενες μέσω κάρτας ή στελεχωμένα γραφεία υποδοχής) για την προστασία των περιοχών όπου βρίσκονται τα συστήματα επεξεργασίας πληροφοριών,

γ) Οι ασφαλείς περιοχές πρέπει να προστατεύονται μέσω κατάλληλων ελέγχων εισόδου, διασφαλίζοντας ότι η πρόσβαση επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό,

δ) Κάθε περιστατικό πρόσβασης πρέπει να καταγράφεται σε ασφαλές αρχείο, και

ε) Οι ασφαλείς περιοχές πρέπει να διαθέτουν σύστημα ανίχνευσης εισβολέων, ενώ θα πρέπει να καταγράφονται οι προσπάθειες τυχόν μη εξουσιοδοτημένης πρόσβασης.

3.2.2 Ασφάλεια εξοπλισμού

α) Ο εξοπλισμός πρέπει να τοποθετείται σε κλειστό χώρο ή να προστατεύεται, ώστε να περιορίζονται οι κίνδυνοι από περιβαλλοντικές απειλές και καταστροφές, καθώς και οι πιθανότητες μη εξουσιοδοτημένης πρόσβασης,

β) Ο εξοπλισμός πρέπει να προστατεύεται από τυχόν διακοπές ρεύματος και άλλου είδους διαταραχές που ενδέχεται να προκληθούν λόγω σφαλμάτων στις υποστηρικτικές εφαρμογές/εγκαταστάσεις, και

γ) Τα καλώδια ισχύος ή τηλεπικοινωνιών που μεταφέρουν δεδομένα ή υποστηρίζουν τις υπηρεσίες πληροφοριών πρέπει να προστατεύονται από τυχόν υποκλοπή ή βλάβη.

3.2.3 Διαχείριση περιστατικών

Πρέπει να εφαρμόζονται κατάλληλες πολιτικές, σχέδια και διαδικασίες για την αντιμετώπιση τυχόν περιστατικών ασφάλειας.

3.3 Διοικητικοί έλεγχοι

3.3.1 Προστασία από το ανθρώπινο δυναμικό

α) Όλοι οι υπάλληλοι της Ε.Ε.Ε.Π. και, κατά περίπτωση, οι υπεργολάβοι/ανάδοχοι (contractors) και οι τρίτοι χρήστες πρέπει να λαμβάνουν επαρκή εκπαίδευση και τακτικές ενημερώσεις σχετικά με τις πολιτικές και τις διαδικασίες της Ε.Ε.Ε.Π., ανάλογα με τη θέση εργασίας που κατέχουν, και

β) Τα δικαιώματα πρόσβασης όλων των υπαλλήλων, των υπεργολάβων/αναδόχων και τρίτων χρηστών, στις πληροφορίες και τις εγκαταστάσεις επεξεργασίας των πληροφοριών πρέπει να αίρονται μετά τη λήξη της απασχόλησης, του συμβολαίου ή της σύμβασής τους, ή να προσαρμόζονται στην εκάστοτε αλλαγή.

3.3.2 Υπηρεσίες τρίτων μερών

α) Οι συμφωνίες με τρίτα μέρη, συμπεριλαμβανομένης της πρόσβασης, επεξεργασίας, κοινοποίησης ή διαχείρισης των πληροφοριών ή των εγκαταστάσεων επεξεργασίας των πληροφοριών, ή η προσθήκη προϊόντων ή υπηρεσιών στις εγκαταστάσεις επεξεργασίας πληροφοριών της Ε.Ε.Ε.Π. πρέπει να πληρούν το σύνολο των σχετικών απαιτήσεων ασφάλειας,

β) Οι υπηρεσίες, οι αναφορές και οι καταγραφές που παρέχονται από τρίτα μέρη πρέπει να τελούν υπό παρακολούθηση και αναθεώρηση, ενώ πρέπει να πραγματοποιούνται έλεγχοι

κατ' ελάχιστο σε ετήσια βάση, και

γ) Η διαχείριση τυχόν αλλαγών στην παροχή υπηρεσιών, συμπεριλαμβανομένης της διαχείρισης και της βελτίωσης των υπαρχόντων πολιτικών ασφάλειας πληροφοριών, διαδικασιών και ελέγχων, πρέπει να πραγματοποιείται συνυπολογίζοντας το βαθμό σπουδαιότητας των επιχειρησιακών συστημάτων και των εμπλεκόμενων διαδικασιών, καθώς και την επαναξιολόγηση των κινδύνων.

3.3.3 <u>Πολιτική δημιουργίας αντιγράφων ασφαλείας</u>

Πρέπει να δημιουργούνται αντίγραφα ασφαλείας των πληροφοριών και του λογισμικού, και να υποβάλλονται τακτικά σε έλεγχο, σε συμμόρφωση με τη συμφωνηθείσα πολιτική δημιουργίας αντιγράφων ασφαλείας.

3.3.4 <u>Διαχείριση μέσων</u>

α) Πρέπει να διατίθενται διαδικασίες διαχείρισης των αφαιρούμενων μέσων,

β) Όλα τα στοιχεία εξοπλισμού που περιλαμβάνουν μέσα αποθήκευσης πρέπει να υποβάλλονται σε έλεγχο για τη διασφάλιση της αφαίρεσης ή της ασφαλούς διαγραφής των ευαίσθητων δεδομένων και του αδειοδοτημένου λογισμικού πριν από την απόρριψή τους,

γ) Τα μέσα πρέπει να απορρίπτονται με ασφάλεια όταν διακόπτεται οριστικά η χρήση τους και σύμφωνα με τις επίσημες διαδικασίες,

δ) Πρέπει να καθιερώνονται διαδικασίες διαχείρισης και αποθήκευσης των πληροφοριών με σκοπό την προστασία των εν λόγω πληροφοριών από τυχόν μη εξουσιοδοτημένη αποκάλυψη ή κατάχρηση, και

ε) Η τεκμηρίωση του πληροφορικού συστήματος εποπτείας και ελέγχου πρέπει να προστατεύεται από τυχόν μη εξουσιοδοτημένη πρόσβαση.

3.3.5 <u>Διαχείριση ενημερώσεων κώδικα (patches) και λοιπών ενημερώσεων (updates)</u>

α) Η πολιτική για την εφαρμογή του συνόλου των ενημερώσεων κώδικα και λοιπών ενημερώσεων του λογισμικού πρέπει να διατίθεται σε γραπτή μορφή, και

β) Όλες οι ενημερώσεις κώδικα θα πρέπει, εφόσον είναι δυνατόν, να υποβάλλονται σε δοκιμές σε κάποιο πληροφορικό σύστημα εποπτείας και ελέγχου, πανομοιότυπα παραμετροποιημένο με το πληροφορικό σύστημα εποπτείας και ελέγχου στο οποίο πρόκειται να εγκατασταθούν. Σε περίπτωση αδυναμίας έγκαιρης πραγματοποίησης διεξοδικής δοκιμής των ενημερώσεων κώδικα για την τήρηση του χρονοδιαγράμματος για

το επίπεδο σοβαρότητας της ειδοποίησης, τότε η δοκιμή των ενημερώσεων κώδικα πρέπει να υποβάλλεται σε διαδικασίες διαχείρισης κινδύνου, είτε απομονώνοντας ή αφαιρώντας το μη δοκιμασμένο πληροφορικό σύστημα εποπτείας και ελέγχου από το δίκτυο είτε εφαρμόζοντας την ενημέρωση κώδικα και τη δοκιμή μετά το γεγονός.

3.3.6 <u>Διαδικασίες ελέγχου αλλαγής (change control)</u>

Οι διαδικασίες ελέγχου αλλαγής των προγραμμάτων πρέπει να είναι επαρκείς, ώστε να διασφαλίζεται η εφαρμογή μόνο κατάλληλα εγκεκριμένων και δοκιμασμένων εκδόσεων των προγραμμάτων στο παραγωγικό πληροφορικό σύστημα εποπτείας και ελέγχου. Μεταξύ των ελέγχων αλλαγών του παραγωγικού συστήματος πρέπει να περιλαμβάνονται τα εξής:

α) Κατάλληλη μέθοδος ή μηχανισμός ελέγχου της έκδοσης λογισμικού για το σύνολο των στοιχείων λογισμικού,

β) Λεπτομέρειες σχετικά με την αιτία της αλλαγής,

γ) Λεπτομέρειες σχετικά με το άτομο που πραγματοποιεί την αλλαγή, και

δ) Πλήρη αντίγραφα ασφαλείας προηγούμενων εκδόσεων του λογισμικού.

3.3.7 <u>Επιβεβαίωση ταυτότητας</u>

α) Το σύνολο των ατόμων (π.χ. χειριστές υπολογιστών, πάροχοι υπηρεσιών συντήρησης, λειτουργοί δικαιοδοσίας και αντιπρόσωποι κ.λπ.) και των υπολογιστικών συστημάτων (π.χ. ελεγκτές Jackpot, συστήματα οικονομικών πυλών, συστήματα αρχών πιστοποίησης κ.λπ.) που συνδέονται με το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να υποβάλλονται σε επιβεβαίωση ταυτότητας, με εξαίρεση το ακόλουθο στοιχείο (β),

β) Το Πληροφορικό Σύστημα Εποπτείας και Ελέγχου πρέπει να αυτό-υποβάλλεται σε επιβεβαίωση ταυτότητας στο σύνολο των ατόμων και των υπολογιστικών συστημάτων που πραγματοποιούν σύνδεση μαζί του, και

γ) Η επιβεβαίωση της ταυτότητας των ατόμων, των υπολογιστικών συστημάτων που ελέγχονται από την Ε.Ε.Ε.Π. και των πληροφορικών συστημάτων εποπτείας και ελέγχου τρίτων, πρέπει να βασίζεται σε πιστοποιημένη μέθοδο επιβεβαίωσης ταυτότητας, η οποία αναγνωρίζεται από την Ε.Ε.Ε.Π. ως ασφαλής.

3.3.8 <u>Ανάπτυξη, δοκιμή, υποστήριξη και συντήρηση λογισμικού</u>

Το λογισμικό πολλαπλών πλατφορμών πρέπει να φέρει ταυτόσημο κωδικό σε κάθε έκδοση, εξαιρουμένων των λειτουργιών που εξαρτώνται από το λειτουργικό σύστημα.

3.3.9 *Ασφάλεια κώδικα*

α) Λογισμικό κλειστού κώδικα. Ο κώδικας πρέπει να προστατεύεται όσο το δυνατόν περισσότερο από τον παίκτη, όπου κρίνεται κατάλληλο,

β) Λογισμικό ανοικτού κώδικα. Εάν το λογισμικό υποβάλλεται ως έργο ανοικτού κώδικα:

i. Η ομάδα ανάπτυξης του λογισμικού πρέπει να λάβει μια έγκυρη άδεια προγραμματισμού ανοικτού κώδικα, προκειμένου να ταξινομηθεί στην κατηγορία υποβολών ανοικτού κώδικα,

ii. Πρέπει να εφαρμόζεται κάποια έγκυρη διαδικασία, η οποία δεν θα παραβιάζει την αποκτηθείσα άδεια λογισμικού ανοικτού κώδικα, ώστε να αποτρέπεται τυχόν δημοσίευση των τροποποιήσεων κώδικα από τα ίδια τα άτομα που προέβησαν σε αυτές και οι οποίες μπορεί να έχουν ως αποτέλεσμα τη μεταβολή του επιπέδου ασφάλειας και ακεραιότητας του λογισμικού και του πληροφορικού συστήματος εποπτείας και ελέγχου, και

iii. Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να έχει τη δυνατότητα να ανιχνεύει με εύλογο τρόπο τυχόν τροποποιήσεις κώδικα που πραγματοποιήθηκαν από τον τελικό χρήστη και να αποτρέπει την εκτέλεση του λογισμικού, αν οι εν λόγω τροποποιήσεις μπορούν να μεταβάλλουν την ακεραιότητα του παιγνίου και/ή του πληροφορικού συστήματος εποπτείας και ελέγχου,

γ) Δυνατότητες παραμετροποίησης μέσω αλλαγών κώδικα: Εάν το τοπικά εγκατεστημένο λογισμικό (client software) επιτρέπει την παραμετροποίηση από το χρήστη (π.χ. προσαρμόσιμες τράπουλες), πρέπει να πληρούνται οι παρακάτω απαιτήσεις:

i. Το παίγνιο που είναι εγκατεστημένο στο τερματικό (game client) δύναται να επιτρέπει την παραμετροποίηση από το χρήστη (π.χ. αλλαγή εμφάνισης του περιβάλλοντος εργασίας, προσαρμόσιμες τράπουλες κτλ). Ωστόσο, εάν η παραμετροποίηση εφαρμόζεται μέσω αλλαγών του κώδικα, ο κώδικας πρέπει να αποτελείται αποκλειστικά από γλώσσες σήμανσης (markup languages), και

ii. Απαγορεύεται η χρήση οποιασδήποτε γλώσσας προγραμματισμού για το συγκεκριμένο σκοπό, η οποία μπορεί να εκτελέσει εντολές σε επίπεδο πληροφορικού συστήματος εποπτείας και ελέγχου, και

δ) Τυχόν πακέτα θεμάτων με δυνατότητα δημόσιας εγκατάστασης πρέπει να φιλοξενούνται και να παρακολουθούνται από το ΚΠΣ ή/και τον ΕΣΠ του Φορέα Εκμετάλλευσης ή Παραχωρησιούχου, ενώ όλα τα θέματα που φορτώνονται πρέπει να επαληθεύονται, ώστε να διασφαλίζεται ότι δεν περιέχουν προγράμματα εκμετάλλευσης ευπαθών ατόμων ή κακόβουλο λογισμικό.

3.4 Τεχνικοί έλεγχοι

3.4.1 Εξυπηρετητές διαμεσολάβησης (Proxy servers)

Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να έχει τη δυνατότητα να λειτουργεί μέσω πολλαπλών εξυπηρετητών διαμεσολάβησης. Η ορθή λειτουργία των παιγνίων δεν πρέπει να εξαρτάται από οποιοδήποτε αίτημα ανανέωσης (refresh request) που αποστέλλεται από το παιγνιομηχάνημα στο πληροφορικό σύστημα εποπτείας και ελέγχου.

3.4.2 Αυτο-παρακολούθηση

α) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να εφαρμόζει αυτό-παρακολούθηση στα σημαντικά στοιχεία (π.χ. κεντρικοί υπολογιστές, συσκευές δικτύου, τείχη προστασίας, σύνδεσμοι σε τρίτα μέρη κ.λπ.), και

β) Τα σημαντικά στοιχεία που αποτυγχάνουν στις δοκιμές αυτο-παρακολούθησης πρέπει να τίθενται αμέσως εκτός λειτουργίας. Το στοιχείο δεν πρέπει να τίθεται εκ νέου σε λειτουργία μέχρι να αποδειχθεί επαρκώς ότι το σφάλμα έχει διευθετηθεί.

3.4.3 Προστασία από επιθέσεις

α) Για την προστασία του πληροφορικού συστήματος εποπτείας και ελέγχου από επιθέσεις, που βασίζονται στην αναπαραγωγή αυθεντικών ή μη αυθεντικών μηνυμάτων (π.χ. επίθεση κατανεμημένης άρνησης υπηρεσίας – DDoS attack), πρέπει να λαμβάνονται όλες οι εύλογες προφυλάξεις,

β) Το λογισμικό πρέπει να έχει τη δυνατότητα να ανιχνεύει ευλόγως και/ή να προλαμβάνει τις επιθέσεις τύπου ενδιάμεσης οντότητας (man-in-the-middle), χωρίς να παραβιάζεται το απόρρητο του τελικού χρήστη,

γ) Σε περίπτωση υποψίας επίθεσης τύπου ενδιάμεσης οντότητας (man-in-the-middle), το σύνολο των επικοινωνιών μεταξύ του ύποπτου πελάτη και του εξυπηρετητή πρέπει να διακόπτεται με την εμφάνιση ενός μηνύματος στο τελικό χρήστη, το οποίο θα εξηγεί την

αιτία τερματισμού της επικοινωνίας,

δ) Μετά τον τερματισμό της επικοινωνίας πελάτη-εξυπηρετητή, πρέπει να ακολουθούνται τα κατάλληλα βήματα προκειμένου να διαπιστωθεί κατά πόσο ο τελικός χρήστης πραγματοποιούσε ή όχι επίθεση τύπου ενδιάμεσης οντότητας (man-in-the-middle). Εάν διαπιστωθεί ότι πραγματοποιήθηκε απόπειρα επίθεσης οντότητας, πρέπει να πραγματοποιηθούν οι κατάλληλες ενέργειες ως προς την απάτη,

ε) Πρέπει να λαμβάνονται όλες οι εύλογες προφυλάξεις, ώστε να διασφαλίζεται ότι τα δεδομένα που φυλάσσονται στο σύστημα εποπτείας και ελέγχου ή μεταφέρονται μέσω αυτού, δεν πρόκειται να μολυνθούν από τυχόν ιούς (viruses), δούρειους ίππους (Trojan Horses), ιούς τύπου worm ή άλλου είδους κακόβουλο λογισμικό, και

στ) Το πληροφορικό σύστημα εποπτείας και ελέγχου πρέπει να υποβάλλεται σε δοκιμή παρείσφρησης (penetration testing) κατ' ελάχιστο μία φορά ανά εξάμηνο.

3.4.4 *<u>Διαχείριση ασφάλειας δικτύου</u>*

α) Τα δίκτυα πρέπει να υπόκεινται σε επαρκείς διαδικασίες διαχείρισης και ελέγχου, ώστε να προστατεύονται από τυχόν απειλές και να διασφαλίζουν την ασφάλεια των συστημάτων και των εφαρμογών που χρησιμοποιεί το σύστημα, συμπεριλαμβανομένων των μεταφερόμενων πληροφοριών,

β) Τα στοιχεία δικτύου πρέπει να υποβάλλονται σε σάρωση εσωτερικών ευπαθειών κατ' ελάχιστο μία φορά ανά εξάμηνο, και

γ) Τα χαρακτηριστικά ασφάλειας, τα επίπεδα συντήρησης και οι απαιτήσεις διαχείρισης του συνόλου των υπηρεσιών δικτύου πρέπει να ταυτοποιούνται και να περιλαμβάνονται σε όλες τις συμβάσεις υπηρεσιών δικτύου, ανεξάρτητα από το εάν οι εν λόγω υπηρεσίες παρέχονται εκ των έσω ή από άλλη εταιρία.

3.4.5 *<u>Έλεγχοι πρόσβασης δικτύου</u>*

α) Πρέπει να καθιερώνεται, να τεκμηριώνεται και να υποβάλλεται σε αναθεώρηση μια πολιτική ελέγχου πρόσβασης βάσει των επιχειρησιακών απαιτήσεων και των απαιτήσεων ασφάλειας ως προς την πρόσβαση,

β) Πρέπει να εφαρμόζεται μια επίσημη μέθοδος εγγραφής και διαγραφής χρηστών για την παροχή και την άρση πρόσβασης στο σύνολο των πληροφορικών συστημάτων και των πληροφοριών,

γ) Ο καταμερισμός των δικαιωμάτων χρήστη πρέπει να περιορίζεται και να ελέγχεται βάσει των επιχειρησιακών απαιτήσεων,

δ) Η Ε.Ε.Ε.Π. πρέπει να ελέγχει τα δικαιώματα πρόσβασης των χρηστών ανά τακτά χρονικά διαστήματα μέσω μιας επίσημης διαδικασίας,

ε) Οι χρήστες πρέπει να έχουν πρόσβαση μόνο στις υπηρεσίες για τις οποίες διαθέτουν συγκεκριμένη εξουσιοδότηση,

στ) Οι κωδικοί πρόσβασης πρέπει να υποβάλλονται σε έλεγχο μέσω μιας επίσημης διαδικασίας διαχείρισης,

ζ) Η επιλογή κωδικών πρόσβασης πρέπει να συμφωνεί με τις ορθές πρακτικές ασφάλειας,

η) Ο μη επιβλεπόμενος εξοπλισμός πρέπει να προστατεύεται επαρκώς και να αποσυνδέει αυτόματα το χρήστη μετά από ένα προκαθορισμένο χρονικό διάστημα,

θ) Πρέπει να χρησιμοποιούνται κατάλληλες μέθοδοι επιβεβαίωσης ταυτότητας για τον έλεγχο της πρόσβασης από απομακρυσμένους χρήστες,

ι) Η αυτόματη αναγνώριση εξοπλισμού πρέπει να εκλαμβάνεται ως μέσο επιβεβαίωσης της ταυτότητας των συνδέσεων από συγκεκριμένες τοποθεσίες και εξοπλισμούς,

ια) Πρέπει να υποβάλλεται σε έλεγχο η φυσική και λογική πρόσβαση στις θύρες διάγνωσης και παραμετροποίησης,

ιβ) Οι ομάδες υπηρεσιών πληροφόρησης, χρηστών και πληροφορικών συστημάτων πρέπει να διαχωρίζονται σε δίκτυα,

ιγ) Όσον αφορά τα κοινόχρηστα δίκτυα, ειδικά εκείνα που εκτείνονται πέραν των ορίων της Ε.Ε.Ε.Π., η δυνατότητα σύνδεσης των χρηστών στο δίκτυο πρέπει να είναι περιορισμένη, σύμφωνα με την πολιτική ελέγχου πρόσβασης και τις απαιτήσεις των εφαρμογών της Ε.Ε.Ε.Π., και

ιδ) Τα δίκτυα πρέπει να υποβάλλονται σε ελέγχους δρομολόγησης, ώστε να διασφαλίζεται ότι οι συνδέσεις υπολογιστών και η ροή πληροφοριών δεν παραβιάζουν την πολιτική ελέγχου πρόσβασης των εφαρμογών της Ε.Ε.Ε.Π..

3.4.6 <u>Έλεγχοι πρόσβασης λειτουργικού συστήματος</u>

α) Η πρόσβαση στα λειτουργικά συστήματα πρέπει να ελέγχεται από μια ασφαλή διαδικασία σύνδεσης,

β) Όλοι οι χρήστες πρέπει να διαθέτουν ένα μοναδικό αναγνωριστικό (ταυτότητα χρήστη) για

αποκλειστικά προσωπική χρήση, ενώ πρέπει να επιλεγεί μια κατάλληλη μέθοδος επιβεβαίωσης ταυτότητας για την τεκμηρίωση της ταυτότητας του εκάστοτε χρήστη,

γ) Τα συστήματα διαχείρισης κωδικών πρόσβασης πρέπει να είναι διαδραστικά και να διασφαλίζουν την παραγωγή ισχυρών κωδικών πρόσβασης,

δ) Η χρήση βοηθητικών προγραμμάτων, τα οποία ενδέχεται να έχουν τη δυνατότητα να παρακάμπτουν τους ελέγχους συστήματος και εφαρμογής, πρέπει να περιορίζεται και να υποβάλλεται σε διεξοδικούς ελέγχους,

ε) Οι ανενεργές συνεδρίες πρέπει να τερματίζονται μετά από 30 λεπτά αδράνειας το ανώτερο,

στ) Πρέπει να εφαρμόζονται περιορισμοί στους χρόνους σύνδεσης για την παροχή πρόσθετης ασφάλειας στις εφαρμογές υψηλού κινδύνου,

ζ) Η πρόσβαση των χρηστών και του προσωπικού υποστήριξης στις λειτουργίες του πληροφορικού συστήματος και του συστήματος εφαρμογών πρέπει να είναι περιορισμένη, σύμφωνα με την καθορισμένη πολιτική ελέγχου πρόσβασης,

η) Τα ευαίσθητα συστήματα πρέπει να διαθέτουν αποκλειστικό (απομονωμένο) υπολογιστικό περιβάλλον,

θ) Πρέπει να ισχύει μια επίσημη πολιτική, καθώς και να υιοθετούνται κατάλληλα μέτρα ασφάλειας για την προστασία από κινδύνους χρήσης κινητών υπολογιστικών εγκαταστάσεων και εγκαταστάσεων επικοινωνίας, και

ι) Για εργασίες που γίνονται από απόσταση (telecommuting activities) πρέπει να θεσπίζονται και να εφαρμόζονται μια πολιτική, επιχειρησιακά σχέδια και διαδικασίες.

3.4.7 Κρυπτογραφικοί έλεγχοι

Πρέπει να θεσπίζεται και να εφαρμόζεται μια πολιτική περί της χρήσης κρυπτογραφικών ελέγχων για την προστασία των πληροφοριών.

α) Τα ευαίσθητα δεδομένα που μεταφέρονται μέσω των γραμμών επικοινωνίας πρέπει να κρυπτογραφούνται. Παραδείγματα δεδομένων που ενδέχεται να χρειάζονται κρυπτογράφηση είναι τα PIN και οι κωδικοί πρόσβασης, οι αριθμοί λογαριασμού (συμπεριλαμβανομένων των αριθμών καρτών) και τα στοιχεία τους, τα κλειδιά κρυπτογράφησης, τα στοιχεία ταυτότητας των παικτών, οι μεταφορές κεφαλαίων από και προς τους λογαριασμούς παικτών, οι αλλαγές των στοιχείων λογαριασμού (π.χ. αλλαγή διεύθυνσης, αλλαγή πιστωτικής κάρτας, αλλαγής ονόματος κ.λπ.) και δεδομένα

διεξαγωγής του παιγνίου (π.χ. παρτίδες που διεξήχθησαν, ποσά που στοιχηματίστηκαν, ποσά που κερδήθηκαν, Jackpot που κερδήθηκαν κ.λπ.),

β) Τα δεδομένα για τα οποία δεν απαιτείται απόκρυψη, αλλά πρέπει να υποβληθούν σε επιβεβαίωση ταυτότητας, πρέπει να χρησιμοποιούν κάποια μέθοδο επιβεβαίωσης ταυτότητας μηνύματος,

γ) Τα ευαίσθητα δεδομένα πρέπει να κρυπτογραφούνται από άκρη σε άκρη (end-to-end basis) (δηλαδή τα δεδομένα δεν πρέπει ποτέ να εμφανίζονται σε οποιοδήποτε LAN ή WAN σε μη κρυπτογραφημένη μορφή). Αυτό αφορά και τα ευαίσθητα δεδομένα που μεταδίδονται μεταξύ υπολογιστών του πληροφορικού συστήματος εποπτείας και ελέγχου εντός των εγκαταστάσεων της Ε.Ε.Ε.Π.,

δ) Για τα ευαίσθητα δεδομένα που μεταδίδονται μεταξύ υπολογιστών του πληροφορικού συστήματος εποπτείας και ελέγχου ενός δικτύου μεταγωγής (switched network) στα πλαίσια ενός μόνο ασφαλούς κέντρου δεδομένων, δεν απαιτείται κρυπτογράφηση,

ε) Για τα ευαίσθητα δεδομένα που μεταδίδονται μεταξύ υπολογιστών του πληροφορικού συστήματος εποπτείας και ελέγχου που βρίσκονται σε ξεχωριστά ασφαλή κέντρα δεδομένων, δεν απαιτείται κρυπτογράφηση, εφόσον η διαδρομή επικοινωνιών είναι ασφαλής από φυσικής απόψεως και αποκλείει την πρόσβαση μη εξουσιοδοτημένων ατόμων,

στ) Το σύνολο των επικοινωνιών μεταξύ των τερματικών της Ε.Ε.Ε.Π. και του πληροφορικού συστήματος εποπτείας και ελέγχου πρέπει να υποβάλλεται σε αυστηρή επιβεβαίωση ταυτότητας και να κρυπτογραφείται με ιδιαίτερα ασφαλείς μεθόδους κατά τη μετάδοση εκτός των αντίστοιχων ασφαλών κέντρων δεδομένων,

ζ) Η επιβεβαίωση ταυτότητας πρέπει να διατίθεται μέσω πρωτοκόλλου Secure Socket Link (SSL) και πιστοποιητικού ασφάλειας που προέρχεται από εγκεκριμένο οργανισμό,

η) Οι αλγόριθμοι κρυπτογράφησης πρέπει να είναι αποδεδειγμένα ασφαλείς έναντι κρυπταναλυτικών επιθέσεων, και

θ) Η Ε.Ε.Ε.Π. πρέπει να διαθέτει εγκεκριμένες διαδικασίες που πρέπει να ακολουθηθούν μετά από αναφορές αδυναμιών των αλγόριθμων κρυπτογράφησης που χρησιμοποιούνται σε οποιοδήποτε μέρος του πληροφορικού συστήματος εποπτείας και ελέγχου (συμπεριλαμβανομένων ενδεικτικά, αλλά όχι περιοριστικά, των ΓΤΑ, των τειχών

προστασίας, των συστημάτων επιβεβαίωσης ταυτότητας και του λειτουργικού πληροφορικού συστήματος εποπτείας και ελέγχου). Οι αλλαγές στους αλγόριθμους κρυπτογράφησης για την αντιμετώπιση των αδυναμιών πρέπει να εφαρμόζονται το συντομότερο δυνατόν. Σε περίπτωση αδυναμίας πραγματοποίησης αλλαγών, πρέπει να γίνεται αντικατάσταση του αλγόριθμου.

3.4.8 *Διαχείριση κλειδιών κρυπτογράφησης*

α) Το ελάχιστο εύρος (μέγεθος) των κλειδιών κρυπτογράφησης ισοδυναμεί με 112 bit για τους συμμετρικούς αλγόριθμους (symmetric algorithms) και με 1024 bit για τα δημόσια κλειδιά (public keys),

β) Πρέπει να εφαρμόζεται μια ασφαλής μέθοδος για την αλλαγή του υπάρχοντος συνόλου κλειδιών κρυπτογράφησης. Δεν επιτρέπεται η χρήση μόνο του υπάρχοντος συνόλου κλειδιών για την κρυπτογράφηση του επόμενου συνόλου. Ένα παράδειγμα αποδεκτής μεθόδου αλλαγής των κλειδιών αποτελεί η χρήση τεχνικών κρυπτογράφησης δημόσιων κλειδιών για τη μεταφορά νέων συνόλων κλειδιών, και

γ) Πρέπει να εφαρμόζεται μια ασφαλής μέθοδος αποθήκευσης των κλειδιών κρυπτογράφησης. Τα κλειδιά κρυπτογράφησης δεν πρέπει να αποθηκεύονται χωρίς να έχει γίνει εκ των προτέρων κρυπτογράφησή τους μέσω διαφορετικής μεθόδου κρυπτογράφησης και/ή μέσω διαφορετικού κλειδιού κρυπτογράφησης.

3.4.9 *Κακόβουλος (malicious) και κινητός (mobile) κώδικας*

α) Πρέπει να εφαρμόζονται έλεγχοι ανίχνευσης, πρόληψης και επαναφοράς για την προστασία από τυχόν κακόβουλο κώδικα, καθώς και κατάλληλες διαδικασίες για τη σχετική ενημέρωση και ευαισθητοποίηση των χρηστών, και

β) Εάν επιτρέπεται η χρήση κινητού κώδικα, πρέπει να διασφαλίζεται μέσω της παραμετροποίησης ότι ο εξουσιοδοτημένος κινητός κώδικας λειτουργεί σύμφωνα με μια σαφώς προσδιορισμένη πολιτική ασφάλειας, ενώ πρέπει να απαγορεύεται η εκτέλεση οποιουδήποτε μη εξουσιοδοτημένου κινητού κώδικα.

3.4.10 *Παρακολούθηση (monitoring)*

α) Πρέπει να δημιουργούνται αρχεία καταγραφής των ενεργειών χρήστη, των εξαιρέσεων και των συμβάντων ασφάλειας πληροφοριών, τα οποία πρέπει να διατηρούνται για ένα συμφωνημένο χρονικό διάστημα, με σκοπό τη διευκόλυνση μελλοντικών διερευνήσεων και

την παρακολούθηση του ελέγχου πρόσβασης,

β) Κάθε τροποποίηση, προσπάθεια τροποποίησης, πρόσβαση ανάγνωσης ή άλλου είδους αλλαγή ή πρόσβαση σε οποιαδήποτε εγγραφή, αρχείο ελέγχου ή αρχείο καταγραφής του πληροφορικού συστήματος εποπτείας και ελέγχου, πρέπει να γίνεται αντιληπτή από εγκεκριμένο πληροφορικό σύστημα εποπτείας και ελέγχου μέσω ελέγχου της έκδοσης ή χρονικής σήμανσης του αρχείου. Πρέπει να διατίθεται η δυνατότητα προβολής των στοιχείων του ατόμου που προέβαλε ή άλλαξε κάποιο αρχείο καταγραφής, καθώς και η χρονική στιγμή τέλεσης της ενέργειας,

γ) Πρέπει να καθιερώνονται διαδικασίες παρακολούθησης της χρήσης των εγκαταστάσεων επεξεργασίας πληροφοριών, ενώ τα αποτελέσματα των ενεργειών παρακολούθησης πρέπει να υποβάλλονται σε αναθεώρηση σε τριμηνιαία βάση ή σύμφωνα με τις απαιτήσεις της Ε.Ε.Ε.Π.,

δ) Οι πληροφορίες καταγραφής και οι εγκαταστάσεις τους πρέπει να προστατεύονται έναντι παραποίησης και τυχόν μη εξουσιοδοτημένης πρόσβασης,

ε) Οι ενέργειες του διαχειριστή συστήματος (system administrator) και του χειριστή (system operator) συστήματος πρέπει να καταγράφονται,

στ) Τυχόν σφάλματα πρέπει να καταγράφονται, να αναλύονται και να διευθετούνται μέσω κατάλληλων ενεργειών, και

ζ) Τα ρολόγια όλων των σχετικών συστημάτων επεξεργασίας πληροφοριών του Φορέα Εκμετάλλευσης ή ενός τομέα ασφάλειας πρέπει να συγχρονίζονται με κάποια καθορισμένη πηγή της ακριβούς ώρας.

3.4.11 <u>Διαχείριση ασφάλειας επικοινωνιών</u>

Αυτή η παράγραφος αφορά τις επικοινωνίες μεταξύ του κεντρικού πληροφορικού συστήματος εποπτείας και ελέγχου και των λοιπών στοιχείων ή εξοπλισμού του πληροφορικού συστήματος εποπτείας και ελέγχου:

α) Πρέπει να εφαρμόζεται επιβεβαίωση ταυτότητας μηνύματος για τους σημαντικούς τύπους μηνυμάτων, όπως π.χ. η μετάδοση κωδικών πρόσβασης/PIN, με σκοπό την επαλήθευση της σωστής λήψης του μηνύματος από το κεντρικό σύστημα ή το σχετικό εξοπλισμό. Επιτρέπεται η χρήση πρωτοκόλλων που δεν διορθώνουν τα σφάλματα ή δεν αποστέλλουν εκ νέου τα εσφαλμένα πακέτα (π.χ. UDP), υπό την προϋπόθεση ότι δεν αποστέλλονται

σημαντικά δεδομένα ή πληροφορίες κατ' αυτόν τον τρόπο,

β) Σε περίπτωση που ανιχνεύεται ότι έχει γίνει ακούσια επισύναψη πρόσθετων δεδομένων (όπως π.χ. κάποιος ιός τύπου worm) στα ληφθέντα δεδομένα, πρέπει να απαγορεύεται η εισχώρηση του εξωγενούς κώδικα χαρακτήρων (byte code) στο πληροφορικό σύστημα εποπτείας και ελέγχου,

γ) Όλα τα πρωτόκολλα πρέπει να χρησιμοποιούν τεχνικές επικοινωνίας, οι οποίες διαθέτουν τους κατάλληλους μηχανισμούς ανίχνευσης σφαλμάτων και/ή επαναφοράς και συμμορφώνονται με τους ακόλουθους κανόνες:

i. Το πρωτόκολλο υψηλού επιπέδου πρέπει να εφαρμόζει τεχνικές (π.χ. αναγνώριση από άκρη σε άκρη – end to end) που θα αποτρέπουν την απώλεια μηνυμάτων, ακόμη και σε περίπτωση επανεκκίνησης κάποιου εκ των τερματικών/άκρων, και

ii. Οι εν λόγω τεχνικές δεν πρέπει να οδηγούν σε πλήρη διακοπή όλων των διαδικασιών του πληροφορικού συστήματος εποπτείας και ελέγχου ή οποιουδήποτε παιγνιομηχανήματος κατά το διάστημα αναμονής της εν λόγω αναγνώρισης,

δ) Το πρωτόκολλο ανώτερου επιπέδου πρέπει να εφαρμόζει τεχνικές (π.χ. αριθμοί μετάδοσης) αναγνώρισης και απόρριψης των επαναλαμβανόμενων μηνυμάτων, ακόμη και σε περίπτωση επανεκκίνησης κάποιου εκ των τερματικών/άκρων,

ε) Αυτές οι απαιτήσεις δεν ισχύουν για τα μη ασφαλή μηνύματα, όπως τα μηνύματα ευρυεκπομπής (broadcast messages),

στ) Όλες οι λειτουργίες του πρωτοκόλλου πρέπει να ορίζονται σαφώς στην τεκμηρίωσή του,

ζ) Οι ακόλουθοι κανόνες ισχύουν για τις χρονικές σημάνσεις (timestamps) στα πρωτόκολλα υψηλού επιπέδου:

i. Πρέπει να περιλαμβάνει πρόβλεψη εισαγωγής τοπικής χρονικής σήμανσης από το σύστημα μετάδοσης (δηλαδή το πληροφορικό σύστημα εποπτείας και ελέγχου ή το παιγνιομηχάνημα) σε όλα τα μηνύματα που αποστέλλει. Αυτή η χρονική σήμανση θα συμβάλλει στην αναγνώριση περιπτώσεων δυσλειτουργίας του εξοπλισμού, που αφορά διαφυγή υλισμικού ή λογισμικού, και

ii. Πρέπει να περιλαμβάνει πρόβλεψη εισαγωγής τοπικής χρονικής σήμανσης από το σύστημα μετάδοσης (δηλαδή το πληροφορικό σύστημα εποπτείας και ελέγχου ή το παιγνιομηχάνημα) τη στιγμή λήψης του τελευταίου έγκυρου μηνύματος υψηλού

επιπέδου, και

η) Οι ακόλουθες απαιτήσεις ισχύουν για τη διεπαφή πρωτοκόλλων υψηλού επιπέδου με πρωτόκολλα κατώτερου επιπέδου:

i. Δεν πρέπει να ισχύουν περιορισμοί ως προς τον αριθμό των χαρακτήρων που μπορούν να περιλαμβάνουν τα μηνύματα, τα οποία ανταλλάσσονται μεταξύ των ανώτερων και των κατώτερων επιπέδων,

ii. Οι διεπαφές μεταξύ των πρωτοκόλλων υψηλού επιπέδου και των πρωτοκόλλων χαμηλού επιπέδου πρέπει να εξυπηρετούν μηνύματα ποικίλου μεγέθους, συμπεριλαμβανομένων όσων υπερβαίνουν το τυπικό μέγεθος προσωρινής αποθήκευσης (standard buffer size) του κατώτατου επιπέδου, και

iii. Πρέπει να εφαρμόζεται μια μέθοδος ελέγχου ροής για την αποφυγή πιθανής απώλειας εξαιρετικά σημαντικών μηνυμάτων.

3.4.12 <u>Τείχη προστασίας (Firewalls)</u>

Οι ακόλουθες απαιτήσεις ισχύουν για τα τείχη προστασίας:

α) Όλες οι συνδέσεις με τους κεντρικούς υπολογιστές του πληροφορικού συστήματος εποπτείας και ελέγχου στο ασφαλές κέντρο δεδομένων πρέπει να διέρχονται από ένα τουλάχιστον εγκεκριμένο τείχος προστασίας σε επίπεδο εφαρμογής. Το ίδιο ισχύει και για τις συνδέσεις με τους κεντρικούς υπολογιστές που δεν αφορούν το πληροφορικό σύστημα εποπτείας και ελέγχου (π.χ. πληροφορικά συστήματα εποπτείας και ελέγχου υπολογιστών MIS – Management Information Systems) και χρησιμοποιούνται από την Ε.Ε.Ε.Π.. Ο όρος «συνδέσεις» χρησιμοποιείται υπό ευρεία έννοια και περιλαμβάνει τους τύπους μεταφοράς δεδομένων UDP και TCP,

β) Η επιλογή τείχους προστασίας επηρεάζεται από το πρωτόκολλο χαμηλού επιπέδου που χρησιμοποιείται από την εφαρμογή (π.χ. ορισμένα τείχη προστασίας δεν δύνανται να λαμβάνουν έξυπνες αποφάσεις ως προς τις ροές UDP). Η μείωση της αποτελεσματικότητας του τείχους προστασίας του επιπέδου εφαρμογής σε φίλτρο πακέτων (packet filter) δεν θα επιτρέπεται εξαιτίας απλώς μόνο μιας λανθασμένης επιλογής συνδυασμού τείχους προστασίας / πρωτοκόλλου χαμηλού επιπέδου,

γ) Οι συσκευές που ανήκουν στον ίδιο τομέα μετάδοσης (broadcast domain) με τους κεντρικούς υπολογιστές του πληροφορικού συστήματος εποπτείας και ελέγχου δεν πρέπει

να τοποθετούνται σε εγκαταστάσεις που επιτρέπουν τη δημιουργία εναλλακτικής διαδρομής δικτύου, η οποία παρακάμπτει το τείχος προστασίας. Ορισμένα ενδεικτικά παραδείγματα απαγορευμένων εγκαταστάσεων είναι τα εξής:

i. Η/Υ χειριστή με μόντεμ τηλεφώνου, και
ii. Η/Υ χειριστή με σύνδεση στο VLAN του πληροφορικού συστήματος εποπτείας και ελέγχου, καθώς και σύνδεση στο εταιρικό VLAN,

δ) Τα τείχος προστασίας πρέπει να αποτελεί ξεχωριστή συσκευή υλισμικού με τα ακόλουθα χαρακτηριστικά:

i. Μόνο οι εφαρμογές που σχετίζονται με το τείχος προστασίας μπορούν να είναι εγκατεστημένες στο τείχος προστασίας, και
ii. Μόνο ένας περιορισμένος αριθμός λογαριασμών μπορεί να υπάρχει στο τείχος προστασίας (π.χ. μόνο οι διαχειριστές του πληροφορικού συστήματος εποπτείας και ελέγχου),

ε) Όλα τα πακέτα δεδομένων που κατευθύνονται προς το τείχος προστασίας πρέπει να απορρίπτονται σε περίπτωση που φτάσουν σε διεπαφές με δίκτυα τα οποία βρίσκονται εκτός της περιβάλλουσας γραμμής βάσης (baseline envelope). Στόχος είναι ο περιορισμός της πρόσβασης στο τείχος προστασίας μόνο σε εξουσιοδοτημένους σταθμούς εργασίας εντός της περιβάλλουσας γραμμής βάσης,

στ) Το τείχος προστασίας πρέπει να απορρίπτει όλες τις συνδέσεις, εκτός από εκείνες που εγκρίνονται ρητώς από την Ε.Ε.Ε.Π.,

ζ) Το τείχος προστασίας πρέπει να τηρεί ένα αρχείο καταγραφής ελέγχου όλων των αλλαγών των παραμέτρων, οι οποίες επηρεάζουν το είδος των συνδέσεων που επιτρέπονται μέσω του τείχους προστασίας,

η) Το τείχος προστασίας πρέπει να τηρεί ένα αρχείο καταγραφής ελέγχου όλων των επιτυχημένων και αποτυχημένων προσπαθειών σύνδεσης μέσω αυτού,

θ) Το τείχος προστασίας πρέπει να διακόπτει το σύνολο των επικοινωνιών σε περίπτωση πλήρωσης του αρχείου καταγραφής ελέγχου,

ι) Το τείχος προστασίας πρέπει να απορρίπτει όλα τα μηνύματα που λαμβάνονται σε κάποια διεπαφή, εάν το επίμαχο μήνυμα προορίζεται για συσκευή η οποία είναι συνδεδεμένη σε άλλη διεπαφή,

ια) Η Ε.Ε.Ε.Π. πρέπει να εφαρμόζει εγκεκριμένες διαδικασίες που πρέπει να ακολουθηθούν μετά από αναφορές περιστατικών ασφάλειας και για τη διασφάλιση ενημέρωσης των τειχών προστασίας σύμφωνα με τις συμβουλευτικές συστάσεις που εκδίδονται κατόπιν τέτοιων περιστατικών, και

ιβ) Τα δίκτυα της ασφαλούς πλευράς του τείχους προστασίας πρέπει να χρησιμοποιούν αριθμούς ιδιωτικού δικτύου RFC1918. Οι εν λόγω αριθμοί πρέπει να μεταφράζονται σε αριθμούς δημόσιου δικτύου για μετάδοση μέσω Internet.