EBA/GL/2017/17

12/01/2018

Κατευθυντήριες γραμμές

σχετικά με τα μέτρα ασφάλειας για τους λειτουργικούς κινδύνους και τους κινδύνους ασφάλειας των υπηρεσιών πληρωμών σύμφωνα με την οδηγία (ΕΕ) 2015/2366 (δεύτερη οδηγία για τις υπηρεσίες πληρωμών)

1. Συμμόρφωση και υποχρεώσεις υποβολής στοιχείων και αναφορών

Καθεστώς των κατευθυντήριων γραμμών

1. Το παρόν έγγραφο περιέχει κατευθυντήριες γραμμές οι οποίες εκδίδονται βάσει του άρθρου 16 του κανονισμού (ΕΕ) αριθ. 1093/2010[1]. Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 1093/2010, οι αρμόδιες αρχές και τα χρηματοοικονομικά ιδρύματα καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις κατευθυντήριες γραμμές.

2. Οι κατευθυντήριες γραμμές παρουσιάζουν την άποψη της ΕΑΤ σχετικά με τις ενδεδειγμένες εποπτικές πρακτικές στο πλαίσιο του Ευρωπαϊκού Συστήματος Χρηματοοικονομικής Εποπτείας ή σχετικά με τον τρόπο ορθής εφαρμογής της ενωσιακής νομοθεσίας στον συγκεκριμένο τομέα. Οι αρμόδιες αρχές, όπως ορίζονται στο άρθρο 4 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 1093/2010, προς τις οποίες απευθύνονται οι κατευθυντήριες γραμμές, πρέπει να συμμορφωθούν ενσωματώνοντάς τες δεόντως στις πρακτικές τους (π.χ. τροποποιώντας το νομικό τους πλαίσιο ή τις εποπτικές διαδικασίες τους), συμπεριλαμβανομένων των σημείων στα οποία οι κατευθυντήριες γραμμές απευθύνονται κυρίως στα ιδρύματα.

Απαιτήσεις υποβολής στοιχείων και αναφορών

3. Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 1093/2010, οι αρμόδιες αρχές πρέπει να γνωστοποιήσουν στην ΕΑΤ εάν συμμορφώνονται ή προτίθενται να συμμορφωθούν προς τις παρούσες κατευθυντήριες γραμμές, ή άλλως να εκθέσουν τους λόγους μη συμμόρφωσης, έως τις 12.03.2018. Εάν η προθεσμία γνωστοποίησης παρέλθει άπρακτη, η ΕΑΤ θεωρεί ότι οι αρμόδιες αρχές δεν συμμορφώνονται. Οι γνωστοποιήσεις πρέπει να αποστέλλονται, με την υποβολή του εντύπου που παρέχεται στον δικτυακό τόπο της ΕΑΤ, στην ηλεκτρονική διεύθυνση compliance@eba.europa.eu με την επισήμανση «EBA/GL/2017/17». Οι γνωστοποιήσεις πρέπει να υποβάλλονται από πρόσωπα δεόντως εξουσιοδοτημένα να γνωστοποιούν τη συμμόρφωση εκ μέρους των αρμόδιων αρχών τους. Οποιαδήποτε μεταβολή στην κατάσταση συμμόρφωσης πρέπει επίσης να αναφέρεται στην ΕΑΤ.

4. Οι γνωστοποιήσεις δημοσιεύονται στον δικτυακό τόπο της ΕΑΤ, σύμφωνα με το άρθρο 16 παράγραφος 3.

[1] Κανονισμός (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ.12).

2. Αντικείμενο, πεδίο εφαρμογής και ορισμοί

Αντικείμενο και πεδίο εφαρμογής

5. Οι παρούσες κατευθυντήριες γραμμές απορρέουν από την εντολή που έχει δοθεί στην ΕΑΤ σύμφωνα με το άρθρο 95 παράγραφος 3 της οδηγίας (ΕΕ) 2015/2366[2] (δεύτερη οδηγία για τις υπηρεσίες πληρωμών).

6. Στις παρούσες κατευθυντήριες γραμμές προσδιορίζονται οι απαιτήσεις για τη θέσπιση, την εφαρμογή και την παρακολούθηση των μέτρων ασφάλειας τα οποία πρέπει να λαμβάνουν οι πάροχοι υπηρεσιών πληρωμών (ΠΥΠ), σύμφωνα με το άρθρο 95 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, για τη διαχείριση των λειτουργικών κινδύνων και των κινδύνων ασφάλειας που σχετίζονται με τις υπηρεσίες πληρωμών τις οποίες παρέχουν.

Αποδέκτες

7. Οι παρούσες κατευθυντήριες γραμμές απευθύνονται στους ΠΥΠ όπως ορίζονται στο άρθρο 4 σημείο 11 της οδηγίας (ΕΕ) 2015/2366 και όπως αναφέρονται στον ορισμό των «χρηματοοικονομικών ιδρυμάτων» στο άρθρο 4 σημείο 1 του κανονισμού (ΕΕ) αριθ. 1093/2010, καθώς και στις αρμόδιες αρχές όπως ορίζονται στο άρθρο 4 σημείο 2 σημείο i) του εν λόγω κανονισμού μέσω παραπομπής στην καταργηθείσα οδηγία 2007/64/ΕΚ [3] (νυν οδηγία (ΕΕ) 2015/2366[4]).

Ορισμοί

8. Εκτός εάν προβλέπεται διαφορετικά, οι όροι που χρησιμοποιούνται και ορίζονται στην οδηγία (ΕΕ) 2015/2366 έχουν την ίδια έννοια και στις παρούσες κατευθυντήριες γραμμές. Επιπλέον, για τους σκοπούς του παρόντος εγγράφου ισχύουν οι ακόλουθοι ορισμοί:

[2] Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35).

[3] Οδηγία 2007/64/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Νοεμβρίου 2007, για τις υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 97/7/ΕΚ, 2002/65/ΕΚ, 2005/60/ΕΚ και 2006/48/ΕΚ, και την κατάργηση της οδηγίας 97/5/ΕΚ (ΕΕ L 319 της 5.12.2007, σ. 1).

[4] Σύμφωνα με το άρθρο 114 δεύτερο εδάφιο της οδηγίας (ΕΕ) 2015/2366, οποιαδήποτε παραπομπή στην καταργηθείσα οδηγία 2007/64/ΕΚ νοείται ως παραπομπή στην οδηγία (ΕΕ) 2015/2366 και διαβάζεται σύμφωνα με τον πίνακα αντιστοιχίας του παραρτήματος ΙΙ της οδηγίας (ΕΕ) 2015/2366.

Διοικητικό όργανο	– Για τους ΠΥΠ που είναι πιστωτικά ιδρύματα, ο όρος αυτός έχει την ίδια έννοια με τον ορισμό που παρατίθεται στο άρθρο 3 παράγραφος 1 σημείο 7 της οδηγίας 2013/36/ΕΕ[5]. – Για τους ΠΥΠ που είναι ιδρύματα πληρωμών ή ιδρύματα ηλεκτρονικού χρήματος, με τον όρο αυτό νοούνται τα διευθυντικά στελέχη ή οι υπεύθυνοι για τη διαχείριση του ΠΥΠ και, κατά περίπτωση, οι υπεύθυνοι για τη διαχείριση των δραστηριοτήτων υπηρεσιών πληρωμών του ΠΥΠ. – Για τους ΠΥΠ που αναφέρονται στο άρθρο 1 παράγραφος 1 στοιχεία γ), ε) και στ) της οδηγίας (ΕΕ) 2015/2366, ο όρος αυτός έχει την έννοια που του αποδίδεται από την ισχύουσα ενωσιακή ή εθνική νομοθεσία.
Περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας	Ένα μεμονωμένο συμβάν ή μια σειρά συνδεόμενων μη προγραμματισμένων από τον ΠΥΠ συμβάντων, τα οποία έχουν ή ενδέχεται να έχουν δυσμενείς επιπτώσεις στην ακεραιότητα, τη διαθεσιμότητα, την εμπιστευτικότητα, την αυθεντικότητα και/ή τη συνέχεια των υπηρεσιών που σχετίζονται με πληρωμές.
Ανώτερα διοικητικά στελέχη	α) Για τους ΠΥΠ που είναι πιστωτικά ιδρύματα, ο όρος αυτός έχει την ίδια έννοια με τον ορισμό που παρατίθεται στο άρθρο 3 παράγραφος 1 σημείο 9 της οδηγίας 2013/36/ΕΕ. β) Για τους ΠΥΠ που είναι ιδρύματα πληρωμών και ιδρύματα ηλεκτρονικού χρήματος, με τον όρο αυτό νοούνται τα φυσικά πρόσωπα που ασκούν εκτελεστικά καθήκοντα σε ίδρυμα και τα οποία είναι υπεύθυνα και λογοδοτούν στο διοικητικό όργανο για την καθημερινή διοίκηση του ΠΥΠ. γ) Για τους ΠΥΠ που αναφέρονται στο άρθρο 1 παράγραφος 1 στοιχεία γ), ε) και στ) της οδηγίας (ΕΕ) 2015/2366, ο όρος αυτός έχει την έννοια που του αποδίδεται από την ισχύουσα ενωσιακή ή εθνική νομοθεσία.
Κίνδυνος ασφάλειας	Ο κίνδυνος που οφείλεται στην ανεπάρκεια ή την αποτυχία εσωτερικών διεργασιών ή σε εξωτερικά γεγονότα που έχουν ή ενδέχεται να έχουν δυσμενείς επιπτώσεις στη διαθεσιμότητα, την ακεραιότητα, την εμπιστευτικότητα των συστημάτων τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) και/ή των πληροφοριών που χρησιμοποιούνται για την παροχή υπηρεσιών πληρωμών. Στο πλαίσιο αυτό περιλαμβάνεται και ο κίνδυνος που προκαλείται από επιθέσεις στον κυβερνοχώρο ή λόγω ανεπαρκούς υλικής ασφάλειας.
Διάθεση ανάληψης κινδύνου	Το συγκεντρωτικό επίπεδο και τα είδη των κινδύνων που είναι πρόθυμο να αναλάβει ένα ίδρυμα στο πλαίσιο της ικανότητάς του για ανάληψη κινδύνων, και σύμφωνα με το

[5] Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα πιστωτικών ιδρυμάτων και την προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, για την τροποποίηση της οδηγίας 2002/87/ΕΚ και για την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

επιχειρηματικό του μοντέλο, προκειμένου να επιτύχει τους στρατηγικούς στόχους του.

3. Εφαρμογή

Ημερομηνία εφαρμογής

9. Οι παρούσες κατευθυντήριες γραμμές ισχύουν από τις 13 Ιανουαρίου 2018.

4. Κατευθυντήριες γραμμές

Κατευθυντήρια γραμμή 1: Γενική αρχή

1.1 Όλοι οι ΠΥΠ θα πρέπει να συμμορφώνονται με όλες τις διατάξεις που προβλέπονται στις παρούσες κατευθυντήριες γραμμές. Το επίπεδο λεπτομέρειας θα πρέπει να είναι ανάλογο με το μέγεθος του ΠΥΠ, καθώς και με τη φύση, την κλίμακα, την πολυπλοκότητα και τον βαθμό επικινδυνότητας των συγκεκριμένων υπηρεσιών τις οποίες παρέχει ή προτίθεται να παρέχει ο ΠΥΠ.

Κατευθυντήρια γραμμή 2: Διακυβέρνηση

Πλαίσιο διαχείρισης λειτουργικών κινδύνων και κινδύνων ασφάλειας

2.1 Οι ΠΥΠ θα πρέπει να θεσπίζουν αποτελεσματικό πλαίσιο διαχείρισης λειτουργικών κινδύνων και κινδύνων ασφάλειας (εφεξής «πλαίσιο διαχείρισης κινδύνων»), το οποίο θα πρέπει να εγκρίνεται και να επανεξετάζεται, τουλάχιστον άπαξ ετησίως, από το διοικητικό όργανο και, κατά περίπτωση, από τα ανώτερα διοικητικά στελέχη. Το εν λόγω πλαίσιο θα πρέπει να εστιάζει σε μέτρα ασφάλειας για τη μείωση των λειτουργικών κινδύνων και των κινδύνων ασφάλειας και θα πρέπει να εντάσσεται πλήρως στις συνολικές διεργασίες διαχείρισης κινδύνων του ΠΥΠ.

2.2 Το πλαίσιο διαχείρισης κινδύνων θα πρέπει:

α) να περιλαμβάνει περιεκτικό έγγραφο που περιγράφει την πολιτική ασφάλειας όπως αναφέρεται στο άρθρο 5 παράγραφος 1 στοιχείο ι) της οδηγίας (ΕΕ) 2015/2366.

β) να συνάδει με τη διάθεση ανάληψης κινδύνου του ΠΥΠ·

γ) να ορίζει και να αναθέτει τους κύριους ρόλους και αρμοδιότητες, καθώς και τους σχετικούς διαύλους αναφοράς που απαιτούνται για την επιβολή των μέτρων ασφάλειας και για τη διαχείριση των κινδύνων ασφάλειας και των λειτουργικών κινδύνων·

δ) να ορίζει τις απαραίτητες διαδικασίες και συστήματα για τον προσδιορισμό, τη μέτρηση, την παρακολούθηση και τη διαχείριση του φάσματος των κινδύνων οι οποίοι απορρέουν από τις δραστηριότητες του ΠΥΠ που σχετίζονται με πληρωμές και στους οποίους εκτίθεται ο ΠΥΠ, συμπεριλαμβανομένων των ρυθμίσεων επιχειρησιακής συνέχειας.

2.3 Οι ΠΥΠ θα πρέπει να διασφαλίζουν ότι το πλαίσιο διαχείρισης κινδύνων είναι δεόντως τεκμηριωμένο και ότι επικαιροποιείται με βάση τα καταγεγραμμένα «διδάγματα που αντλούνται» κατά την εφαρμογή και την παρακολούθησή του.

2.4 Οι ΠΥΠ θα πρέπει να μεριμνούν ώστε, πριν από κάποια σημαντική αλλαγή σε υποδομές, διεργασίες ή διαδικασίες και έπειτα από κάθε περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας το οποίο επηρεάζει την ασφάλεια των υπηρεσιών πληρωμών που παρέχουν, να επανεξετάζουν χωρίς αδικαιολόγητη καθυστέρηση αν απαιτούνται αλλαγές ή βελτιώσεις στο πλαίσιο διαχείρισης κινδύνων.

Υποδείγματα διαχείρισης κινδύνων και εσωτερικού ελέγχου

2.5 Οι ΠΥΠ θα πρέπει να δημιουργούν τρεις αποτελεσματικές γραμμές άμυνας, ή ισοδύναμο εσωτερικό υπόδειγμα διαχείρισης κινδύνων και ελέγχου, για τον προσδιορισμό και τη διαχείριση των λειτουργικών κινδύνων και των κινδύνων ασφάλειας. Οι ΠΥΠ θα πρέπει να διασφαλίζουν ότι το προαναφερθέν εσωτερικό υπόδειγμα ελέγχου διαθέτει επαρκή εξουσία, ανεξαρτησία, πόρους και απευθείας διαύλους αναφοράς προς το διοικητικό όργανο και, κατά περίπτωση, προς τα ανώτερα διοικητικά στελέχη.

2.6 Τα μέτρα ασφάλειας που προβλέπονται στις παρούσες κατευθυντήριες γραμμές θα πρέπει να ελέγχονται από λειτουργικά ανεξάρτητους από το ΠΥΠ εσωτερικούς ή εξωτερικούς ελεγκτές με εμπειρογνωσία σε θέματα ασφάλειας πληροφοριακών συστημάτων και πληρωμών. Για τον προσδιορισμό της συχνότητας και του σημείου εστίασης των εν λόγω ελέγχων θα πρέπει να συνεκτιμώνται οι αντίστοιχοι κίνδυνοι ασφάλειας.

Εξωτερική ανάθεση

2.7 Οι ΠΥΠ θα πρέπει να διασφαλίζουν την αποτελεσματικότητα των μέτρων ασφάλειας που προβλέπονται στις παρούσες κατευθυντήριες γραμμές σε περιπτώσεις εξωτερικής ανάθεσης λειτουργικών δραστηριοτήτων των υπηρεσιών πληρωμών, οι οποίες περιλαμβάνουν και τα πληροφοριακά συστήματα.

2.8 Οι ΠΥΠ θα πρέπει να διασφαλίζουν την ενσωμάτωση κατάλληλων και αναλογικών σκοπών, μέτρων και στόχων επιδόσεων όσον αφορά την ασφάλεια τόσο στις συμβάσεις όσο και στα Συμβόλαια Διασφάλισης Επιπέδου Ποιότητας με τους προμηθευτές στους οποίους αναθέτουν εξωτερικά τις εν λόγω λειτουργίες. Οι ΠΥΠ θα πρέπει να παρακολουθούν και να ζητούν διαβεβαίωση σχετικά με το επίπεδο συμμόρφωσης των εν λόγω προμηθευτών με τους αντικειμενικούς σκοπούς, τα μέτρα και τους στόχους επιδόσεων όσον αφορά την ασφάλεια.

Κατευθυντήρια γραμμή 3: Αξιολόγηση κινδύνων

Προσδιορισμός λειτουργιών, διεργασιών και πόρων

3.1 Οι ΠΥΠ θα πρέπει να προβαίνουν στον προσδιορισμό, καθώς και στην κατάρτιση και τακτική επικαιροποίηση του καταλόγου των επιχειρηματικών τους λειτουργιών, των κύριων ρόλων και των υποστηρικτικών διεργασιών για την καταγραφή της σημασίας κάθε επιμέρους λειτουργίας, ρόλου και υποστηρικτικής διεργασίας, καθώς και των αλληλεξαρτήσεών τους σε σχέση με τους λειτουργικούς κινδύνους και τους κινδύνους ασφάλειας.

3.2 Οι ΠΥΠ θα πρέπει να προβαίνουν στον προσδιορισμό, καθώς και στην κατάρτιση και τακτική επικαιροποίηση του καταλόγου των πληροφοριακών πόρων, όπως των συστημάτων ΤΠΕ, των παραμέτρων τους, άλλων υποδομών, καθώς και των διασυνδέσεων με άλλα εσωτερικά και εξωτερικά συστήματα προκειμένου να είναι σε θέση να διαχειρίζονται τα αγαθά που υποστηρίζουν τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες τους.

Κατηγοριοποίηση λειτουργιών, διεργασιών και πόρων

3.3 Οι ΠΥΠ θα πρέπει να κατηγοριοποιούν τις επιχειρηματικές λειτουργίες, τις υποστηρικτικές διεργασίες και τους πληροφοριακούς πόρους βάσει της κρισιμότητάς τους.

Αξιολογήσεις κινδύνων των λειτουργιών, των διεργασιών και των πόρων

3.4 Οι ΠΥΠ θα πρέπει να διασφαλίζουν τη συνεχή παρακολούθηση των απειλών και ευπαθειών και την τακτική επανεξέταση των σεναρίων κινδύνων που επηρεάζουν τις επιχειρηματικές λειτουργίες, τις κρίσιμες διαδικασίες και τους πληροφοριακούς τους πόρους. Στο πλαίσιο της υποχρέωσης των ΠΥΠ να διεξάγουν και να παρέχουν στις αρμόδιες αρχές επικαιροποιημένη και ολοκληρωμένη αξιολόγηση κινδύνων όσον αφορά τους λειτουργικούς κινδύνους και τους κινδύνους ασφάλειας που σχετίζονται με τις υπηρεσίες πληρωμών τις οποίες παρέχουν, καθώς και σχετικά με την επάρκεια των μέτρων μείωσης των κινδύνων και των μηχανισμών ελέγχου που εφαρμόζονται για την αντιμετώπιση των εν λόγω κινδύνων, όπως ορίζεται στο άρθρο 95 παράγραφος 2 της οδηγίας (ΕΕ) 2015/2366, οι ΠΥΠ θα πρέπει να διενεργούν και να τεκμηριώνουν, τουλάχιστον σε ετήσια βάση ή σε βραχύτερα χρονικά διαστήματα οριζόμενα από την αρμόδια αρχή, αξιολογήσεις κινδύνων των λειτουργιών, των διεργασιών και των πληροφοριακών πόρων που έχουν προσδιορίσει και κατηγοριοποιήσει, με στόχο τον προσδιορισμό και την αξιολόγηση των κυριότερων λειτουργικών κινδύνων και κινδύνων ασφάλειας. Οι εν λόγω αξιολογήσεις κινδύνων θα πρέπει επίσης να πραγματοποιούνται προτού επέλθει οποιαδήποτε σημαντική αλλαγή σε υποδομές, διεργασίες ή διαδικασίες η οποία επηρεάζει την ασφάλεια των υπηρεσιών πληρωμών.

3.5 Βάσει των αξιολογήσεων κινδύνων, οι ΠΥΠ θα πρέπει να καθορίζουν αν –και σε ποιον βαθμό– απαιτούνται αλλαγές στα υφιστάμενα μέτρα ασφάλειας, στις τεχνολογίες που χρησιμοποιούνται και στις διαδικασίες ή στις προσφερόμενες υπηρεσίες πληρωμών. Οι ΠΥΠ θα πρέπει να λαμβάνουν υπόψη τον χρόνο που απαιτείται για την εφαρμογή των αλλαγών και τον χρόνο λήψης κατάλληλων προσωρινών μέτρων ασφάλειας για την ελαχιστοποίηση των λειτουργικών συμβάντων ή των συμβάντων που συνδέονται με την ασφάλεια, όπως επίσης και για την ελαχιστοποίηση της απάτης και ενδεχόμενων διαταραχών λειτουργίας στην παροχή υπηρεσιών πληρωμών.

Κατευθυντήρια γραμμή 4: Προστασία

4.1 Οι ΠΥΠ θα πρέπει να θεσπίζουν και να εφαρμόζουν προληπτικά μέτρα ασφάλειας έναντι των προσδιορισθέντων λειτουργικών κινδύνων και κινδύνων ασφάλειας. Τα εν λόγω μέτρα θα πρέπει να εξασφαλίζουν επαρκές επίπεδο ασφάλειας σύμφωνα με τους προσδιορισθέντες κινδύνους.

4.2 Οι ΠΥΠ θα πρέπει να καθιερώνουν και να εφαρμόζουν μια προσέγγιση «άμυνας εις βάθος» εγκαθιστώντας πολλαπλά επίπεδα ελέγχων που καλύπτουν τα πρόσωπα, τις διεργασίες και την τεχνολογία, όπου κάθε επίπεδο θα χρησιμεύει ως δίχτυ ασφαλείας για τα προηγούμενα επίπεδα. Η άμυνα εις βάθος θα πρέπει να γίνεται αντιληπτή με την έννοια του καθορισμού περισσότερων του ενός ελέγχων για την κάλυψη του ίδιου κινδύνου, όπως η αρχή της επαλήθευσης από δεύτερο πρόσωπο (four-eyes principle), η αυθεντικοποίηση δύο παραγόντων (two-factor authentication), ο η κατάτμηση του δικτύου (network segmentation) και η εγκατάσταση πολλαπλών τειχών προστασίας (multiple firewalls).

4.3 Οι ΠΥΠ θα πρέπει να διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των κρίσιμων λογικών και υλικών πόρων, των μέσων τους, καθώς και των ευαίσθητων δεδομένων πληρωμών των χρηστών των υπηρεσιών πληρωμών τους τόσο όταν τα στοιχεία αυτά τελούν σε κατάσταση αποθήκευσης όσο και όταν βρίσκονται σε κατάσταση διαβίβασης ή χρήσης. Εάν τα δεδομένα περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα, τα εν λόγω μέτρα θα πρέπει να εφαρμόζονται σύμφωνα με τον κανονισμό (ΕΕ) 2016/679[6] ή, κατά περίπτωση, τον κανονισμό (ΕΚ) αριθ. 45/2001.[7]

4.4 Οι ΠΥΠ θα πρέπει, σε συνεχή βάση, να προσδιορίζουν αν οι αλλαγές στο υφιστάμενο λειτουργικό περιβάλλον επηρεάζουν τα ισχύοντα μέτρα ασφάλειας ή απαιτούν τη θέσπιση περαιτέρω μέτρων για τη μείωση του αντίστοιχου κινδύνου. Οι αλλαγές αυτές θα πρέπει να υπόκεινται σε επίσημη διαδικασία διαχείρισης των αλλαγών του ΠΥΠ, η οποία θα πρέπει να διασφαλίζει ότι οι αλλαγές προγραμματίζονται, υποβάλλονται σε δοκιμές, τεκμηριώνονται και εγκρίνονται δεόντως. Βάσει των απειλών για την ασφάλεια που παρατηρούνται και των αλλαγών που επέρχονται, θα πρέπει να διενεργούνται δοκιμές σύμφωνα με σενάρια συναφών και γνωστών δυνητικών επιθέσεων.

4.5 Κατά τον σχεδιασμό, την ανάπτυξη και την παροχή υπηρεσιών πληρωμών, οι ΠΥΠ θα πρέπει να διασφαλίζουν την εφαρμογή των αρχών του διαχωρισμού των καθηκόντων και των «ελάχιστων προνομίων». Οι ΠΥΠ θα πρέπει να αποδίδουν ιδιαίτερη προσοχή στον διαχωρισμό των περιβαλλόντων ΤΠ, ιδίως μεταξύ των περιβαλλόντων ανάπτυξης, δοκιμής και παραγωγής.

[6] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

[7] Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

Ακεραιότητα και εμπιστευτικότητα των δεδομένων και των συστημάτων

4.6 Κατά τον σχεδιασμό, την ανάπτυξη και την παροχή υπηρεσιών πληρωμών, οι ΠΥΠ θα πρέπει να διασφαλίζουν ότι η συλλογή, δρομολόγηση, επεξεργασία, αποθήκευση και/ή αρχειοθέτηση και απεικόνιση ευαίσθητων δεδομένων πληρωμών των χρηστών υπηρεσιών πληρωμών είναι επαρκείς και σχετικές και περιορίζονται στο αναγκαίο επίπεδο για την παροχή των υπηρεσιών πληρωμών τους.

4.7 Οι ΠΥΠ θα πρέπει να ελέγχουν τακτικά αν είναι ενημερωμένο το λογισμικό που χρησιμοποιείται για την παροχή υπηρεσιών πληρωμών, συμπεριλαμβανομένου του λογισμικού των χρηστών που σχετίζεται με πληρωμές καθώς και αν εγκαθίστανται κρίσιμες ενημερώσεις ασφάλειας. Οι ΠΥΠ θα πρέπει να διασφαλίζουν ότι εφαρμόζονται μηχανισμοί ελέγχου για την επαλήθευση της ακεραιότητας του λογισμικού, του υλικολογισμικού και των πληροφοριών σχετικά με τις υπηρεσίες πληρωμών τους.

Φυσική ασφάλεια

4.8 Οι ΠΥΠ θα πρέπει να εφαρμόζουν κατάλληλα μέτρα φυσικής ασφάλειας, ειδικότερα για την προστασία των ευαίσθητων δεδομένων πληρωμών των χρηστών υπηρεσιών πληρωμών, καθώς και των συστημάτων ΤΠΕ που χρησιμοποιούνται για την παροχή υπηρεσιών πληρωμών.

Έλεγχος πρόσβασης

4.9 Η φυσική και λογική πρόσβαση σε συστήματα ΤΠΕ θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα. Σχετική εξουσιοδότηση θα πρέπει να ανατίθεται ανάλογα με τα καθήκοντα και τις αρμοδιότητες του προσωπικού, και να περιορίζεται σε πρόσωπα που υποβάλλονται σε κατάλληλη κατάρτιση και παρακολούθηση. Οι ΠΥΠ θα πρέπει να θέτουν σε εφαρμογή μηχανισμούς ελέγχου που επιτρέπουν με αξιόπιστο τρόπο την πρόσβαση στα συστήματα ΤΠΕ μόνο σε όσους έχουν θεμιτή επιχειρηματική ανάγκη. Η ηλεκτρονική πρόσβαση από εφαρμογές σε δεδομένα και συστήματα θα πρέπει να περιορίζεται στο ελάχιστο επίπεδο που απαιτείται για την παροχή της αντίστοιχης υπηρεσίας.

4.10 Οι ΠΥΠ θα πρέπει να θέτουν σε εφαρμογή ισχυρούς μηχανισμούς ελέγχου για τη διαβαθμισμένη πρόσβαση στα συστήματά τους, περιορίζοντας αυστηρά την πρόσβαση και παρακολουθώντας επισταμένως το προσωπικό με αυξημένα δικαιώματα. Θα πρέπει να εφαρμόζονται μηχανισμοί ελέγχου όπως πρόσβαση βάσει ρόλων, καταγραφή και έλεγχος της δραστηριότητας των προνομιούχων χρηστών, διαδικασίες αυστηρής αυθεντικοποίησης και παρακολούθηση ασυνήθιστων ενεργειών. Οι ΠΥΠ θα πρέπει να διαχειρίζονται τα δικαιώματα πρόσβασης σε πληροφοριακούς πόρους και στα υποστηρικτικά τους συστήματα βάσει της αρχής της ανάγκης να γνωρίζουν. Τα δικαιώματα πρόσβασης θα πρέπει να υπόκεινται σε περιοδική επανεξέταση.

4.11 Τα αρχεία καταγραφής πρόσβασης θα πρέπει να διατηρούνται για χρονικό διάστημα ανάλογο της κρισιμότητας των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων που έχουν προσδιοριστεί, σύμφωνα με τις κατευθυντήριες γραμμές 3.1 και 3.2, με την επιφύλαξη των απαιτήσεων διατήρησης που προβλέπονται στο ενωσιακό και στο εθνικό δίκαιο. Οι ΠΥΠ θα πρέπει να χρησιμοποιούν τις εν λόγω πληροφορίες για να διευκολύνουν την αναγνώριση και τη διερεύνηση ασυνήθιστων δραστηριοτήτων που έχουν εντοπιστεί κατά την παροχή υπηρεσιών πληρωμών.

4.12 Για την εξασφάλιση ασφαλούς επικοινωνίας και τη μείωση του κινδύνου, η απομακρυσμένη διοικητική πρόσβαση σε κρίσιμα συστατικά στοιχεία ΤΠΕ θα πρέπει να χορηγείται μόνον επί τη βάσει της αρχής της ανάγκης για γνώση και εφόσον χρησιμοποιούνται διαδικασίες αυστηρής αυθεντικοποίησης.

4.13 Η λειτουργία των προϊόντων, των εργαλείων και των διαδικασιών που σχετίζονται με τις διεργασίες ελέγχου πρόσβασης θα πρέπει να παρέχει τη δέουσα προστασία ώστε να μην υπονομεύονται ή παρακάμπτονται οι διεργασίες ελέγχου πρόσβασης. Στο πλαίσιο αυτό περιλαμβάνεται η εγγραφή, παράδοση, ανάκληση και απόσυρση των αντίστοιχων προϊόντων, εργαλείων και διαδικασιών.

Κατευθυντήρια γραμμή 5: Εντοπισμός

Συνεχής παρακολούθηση και εντοπισμός

5.1 Οι ΠΥΠ θα πρέπει να εγκαθιστούν και να εφαρμόζουν διεργασίες με δυνατότητες για τη συνεχή παρακολούθηση των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων προκειμένου να εντοπίζουν τυχόν μη φυσιολογικές δραστηριότητες κατά την παροχή υπηρεσιών πληρωμών. Στο πλαίσιο αυτής της συνεχούς παρακολούθησης, οι ΠΥΠ θα πρέπει να διαθέτουν κατάλληλες και αποτελεσματικές δυνατότητες για τον εντοπισμό φυσικής ή λογικής παρείσφρησης, καθώς και παραβιάσεων της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών πόρων που χρησιμοποιούνται στην παροχή υπηρεσιών πληρωμών.

5.2 Οι διεργασίες συνεχούς παρακολούθησης και εντοπισμού θα πρέπει να καλύπτουν:

α) συναφείς εσωτερικούς και εξωτερικούς παράγοντες, συμπεριλαμβανομένων διαχειριστικών λειτουργιών που καλύπτουν τόσο επιχειρηματικές ανάγκες όσο και ΤΠΕ

β) συναλλαγές, με σκοπό τον εντοπισμό κατάχρησης πρόσβασης από παρόχους υπηρεσιών ή άλλες οντότητες· και

γ) πιθανές εσωτερικές και εξωτερικές απειλές.

5.3 Οι ΠΥΠ θα πρέπει να εφαρμόζουν μέτρα ανίχνευσης, αφενός, για να εντοπίζονται πιθανές διαρροές πληροφοριών, η ύπαρξη κακόβουλου κώδικα, λοιπών απειλών για την ασφάλεια και ευρέως γνωστών ευπαθειών λογισμικού και υλικού και, αφετέρου, για να αναζητούνται αντίστοιχες ενημερώσεις ασφάλειας.

Παρακολούθηση και αναφορά περιστατικών λειτουργικού κινδύνου ή περιστατικών ασφάλειας

5.4 Οι ΠΥΠ θα πρέπει να καθορίζουν κατάλληλα κριτήρια και κατώτατα όρια για την κατηγοριοποίηση ενός συμβάντος ως περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας, όπως προβλέπεται στην ενότητα «Ορισμοί» του παρόντος εγγράφου, καθώς και δείκτες έγκαιρης προειδοποίησης που θα πρέπει να χρησιμεύουν ως συναγερμός για τον ΠΥΠ, ώστε να καθίσταται δυνατός ο έγκαιρος εντοπισμός λειτουργικών συμβάντων ή συμβάντων που αφορούν την ασφάλεια.

5.5 Οι ΠΥΠ θα πρέπει να δημιουργούν κατάλληλες διεργασίες και οργανωτικές δομές προκειμένου να διασφαλίζεται η συνεκτική και ολοκληρωμένη παρακολούθηση, ο χειρισμός και η δυνατότητα επανελέγχου σε περιπτώσεις εντοπισμού περιστατικών λειτουργικού κινδύνου και κινδύνου ασφάλειας.

5.6 Οι ΠΥΠ θα πρέπει να θεσπίζουν σχετική διαδικασία για την αναφορά αυτών των περιστατικών λειτουργικού κινδύνου ή των περιστατικών ασφάλειας, καθώς και για την αναφορά των καταγγελιών των πελατών σχετικά με την ασφάλεια προς τα ανώτερα διοικητικά τους στελέχη.

Κατευθυντήρια γραμμή 6: Επιχειρησιακή συνέχεια

6.1 Οι ΠΥΠ θα πρέπει να διατηρούν διαδικασίες διαχείρισης επιχειρησιακής συνέχειας με στόχο τη μεγιστοποίηση της ικανότητας παροχής υπηρεσιών πληρωμών σε συνεχή βάση και τον περιορισμό απωλειών σε περίπτωση σημαντικής διακοπής της επιχειρησιακής τους λειτουργίας.

6.2 Για την αναποτελεσματική διαχείριση της επιχειρησιακής συνέχειας, οι ΠΥΠ θα πρέπει να αναλύουν με προσοχή την έκθεσή τους σε κινδύνους απώλειας της επιχειρησιακής τους λειτουργίας και να αξιολογούν, τόσο ποσοτικά όσο και ποιοτικά, τις δυνητικές τους επιπτώσεις με τη χρήση εσωτερικών και/ή εξωτερικών δεδομένων και ανάλυσης σεναρίων. Επί τη βάσει των κρίσιμων λειτουργιών, διαδικασιών, συστημάτων, συναλλαγών και αλληλεξαρτήσεων που έχουν προσδιοριστεί και κατηγοριοποιηθεί σύμφωνα με τις κατευθυντήριες γραμμές 3.1 έως 3.3, οι ΠΥΠ θα πρέπει να ιεραρχούν κατά σειρά προτεραιότητας τις ενέργειες επιχειρησιακής συνέχειας χρησιμοποιώντας μια προσέγγιση η οποία βασίζεται στον κίνδυνο και μπορεί να στηρίζεται στις αξιολογήσεις κινδύνων που διενεργούνται σύμφωνα με την κατευθυντήρια γραμμή 3. Ανάλογα με το επιχειρηματικό μοντέλο του εκάστοτε ΠΥΠ, η διαδικασία αυτή μπορεί, για παράδειγμα, να διευκολύνει την περαιτέρω επεξεργασία κρίσιμων συναλλαγών ενόσω συνεχίζονται οι προσπάθειες αποκατάστασης.

6.3 Βάσει της ανάλυσης που διενεργείται σύμφωνα με την κατευθυντήρια γραμμή 6.2, ο ΠΥΠ θα πρέπει να θέτει σε εφαρμογή:

α) σχέδια επιχειρησιακής συνέχειας, προκειμένου να διασφαλίζεται η ικανότητα κατάλληλης αντίδρασης του ΠΥΠ σε καταστάσεις έκτακτης ανάγκης και η δυνατότητά του να διατηρεί τις κρίσιμες επιχειρηματικές δραστηριότητές του· και

β) μέτρα μείωσης του κινδύνου τα οποία πρέπει να λαμβάνονται σε περίπτωση τερματισμού των υπηρεσιών πληρωμών του και σε περίπτωση λήξης υφιστάμενων συμβάσεων, ούτως ώστε να αποφεύγονται δυσμενείς συνέπειες στα συστήματα πληρωμών και στους χρήστες υπηρεσιών πληρωμών, καθώς και για να διασφαλίζεται η εκτέλεση των εκκρεμών πράξεων πληρωμών.

Σχεδιασμός επιχειρησιακής συνέχειας βάσει σεναρίων

6.4 Ο ΠΥΠ θα πρέπει να εξετάζει πληθώρα διαφορετικών σεναρίων, συμπεριλαμβανομένων ακραίων αλλά εύλογων σεναρίων, στα οποία ενδέχεται να εκτεθεί, καθώς και να αξιολογεί τις πιθανές επιπτώσεις που ενδέχεται να έχουν τα εν λόγω σενάρια.

6.5 Βάσει της ανάλυσης που διενεργείται σύμφωνα με την κατευθυντήρια γραμμή 6.2 και των εύλογων σεναρίων που προσδιορίζονται σύμφωνα με την κατευθυντήρια γραμμή 6.4, ο ΠΥΠ θα πρέπει να καταρτίζει σχέδια αντιμετώπισης και ανάκτησης, τα οποία θα πρέπει:

α) να εστιάζουν στις επιπτώσεις στη λειτουργία των κρίσιμων λειτουργιών, διεργασιών, συστημάτων, συναλλαγών και αλληλεξαρτήσεων·

β) να είναι τεκμηριωμένα και να τίθενται στη διάθεση των επιχειρηματικών και υποστηρικτικών μονάδων, και να είναι εύκολα προσβάσιμα σε περίπτωση έκτακτης ανάγκης· και

γ) να είναι επικαιροποιημένα σύμφωνα με τα διδάγματα που αντλούνται από τις δοκιμές, τους νέους κινδύνους που προσδιορίζονται και τις απειλές, καθώς και τους μεταβαλλόμενους στόχους και τις προτεραιότητες ανάκτησης.

Δοκιμές σχεδίων επιχειρησιακής συνέχειας

6.6 Οι ΠΥΠ θα πρέπει να υποβάλλουν σε δοκιμή τα σχέδια επιχειρησιακής συνέχειάς τους και να διασφαλίζουν ότι διενεργείται δοκιμή της λειτουργίας των κρίσιμων λειτουργιών, διεργασιών, συστημάτων, συναλλαγών και αλληλεξαρτήσεών τους τουλάχιστον σε ετήσια βάση. Τα σχέδια θα πρέπει να υποστηρίζουν τους στόχους για την προστασία και, εφόσον απαιτείται, την αποκατάσταση της ακεραιότητας και της διαθεσιμότητας των λειτουργιών τους, καθώς και την εμπιστευτικότητα των πληροφοριακών τους πόρων.

6.7 Τα σχέδια θα πρέπει να επικαιροποιούνται τουλάχιστον ετησίως με βάση τα αποτελέσματα των δοκιμών, τις τρέχουσες πληροφορίες σχετικά με απειλές, την ανταλλαγή πληροφοριών και τα διδάγματα που αντλούνται από προηγούμενα γεγονότα, καθώς και με βάση τους μεταβαλλόμενους στόχους ανάκτησης, όπως επίσης και την ανάλυση εύλογων από λειτουργική και τεχνική άποψη σεναρίων που δεν έχουν επέλθει ακόμη και, κατά περίπτωση, μετά από αλλαγές στα συστήματα και τις διεργασίες. Οι ΠΥΠ θα πρέπει να διασφαλίζουν τη διαβούλευση και τον συντονισμό με τους σχετικούς εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς κατά την κατάρτιση των σχεδίων επιχειρησιακής συνέχειάς τους.

6.8 Η δοκιμή των σχεδίων επιχειρησιακής συνέχειας των ΠΥΠ θα πρέπει:

α) να περιλαμβάνει επαρκές σύνολο σεναρίων, όπως αναφέρεται στην κατευθυντήρια γραμμή 6.4·

β) να είναι σχεδιασμένη κατά τρόπον ώστε να θέτει υπό αμφισβήτηση τις υποθέσεις στις οποίες στηρίζονται τα σχέδια επιχειρησιακής συνέχειας, συμπεριλαμβανομένων των ρυθμίσεων διακυβέρνησης και των σχεδίων επικοινωνίας σε καταστάσεις κρίσεων· και

γ) να περιλαμβάνει διαδικασίες για την επαλήθευση της ικανότητας του προσωπικού και των διαδικασιών τους στο να ανταπεξέρχονται επαρκώς στα ανωτέρω σενάρια.

6.9 Οι ΠΥΠ θα πρέπει κατά περιόδους να παρακολουθούν την αποτελεσματικότητα των σχεδίων επιχειρησιακής τους συνέχειάς, καθώς και να καταγράφουν και να αναλύουν τυχόν δυσκολίες ή αστοχίες που προκύπτουν από τις δοκιμές.

Επικοινωνία σε καταστάσεις κρίσεων

6.10 Σε περίπτωση διακοπής λειτουργίας ή έκτακτης ανάγκης, και κατά τη διάρκεια της εφαρμογής των σχεδίων επιχειρησιακής συνέχειας, οι ΠΥΠ θα πρέπει να διασφαλίζουν την εφαρμογή αποτελεσματικών μέτρων επικοινωνίας σε καταστάσεις κρίσεων, ούτως ώστε όλοι οι σχετικοί εσωτερικοί και εξωτερικοί ενδιαφερόμενοι φορείς, συμπεριλαμβανομένων εξωτερικών παρόχων υπηρεσιών, να ενημερώνονται με έγκαιρο και κατάλληλο τρόπο.

Κατευθυντήρια γραμμή 7: Δοκιμές μέτρων ασφάλειας

7.1 Οι ΠΥΠ θα πρέπει να θεσπίζουν και να εφαρμόζουν πλαίσιο δοκιμών το οποίο επικυρώνει την ισχύ και την αποτελεσματικότητα των μέτρων ασφάλειας και να διασφαλίζουν ότι το πλαίσιο δοκιμών προσαρμόζεται ώστε να συνεκτιμώνται νέες απειλές και ευπάθειες, που προσδιορίζονται μέσω δραστηριοτήτων παρακολούθησης κινδύνων.

7.2 Οι ΠΥΠ θα πρέπει να διασφαλίζουν τη διενέργεια δοκιμών σε περίπτωση αλλαγών σε υποδομές, διεργασίες ή διαδικασίες, καθώς και σε περίπτωση που πραγματοποιούνται αλλαγές ως συνέπεια σοβαρών περιστατικών λειτουργικού κινδύνου ή περιστατικών ασφάλειας.

7.3 Το πλαίσιο δοκιμών θα πρέπει επίσης να περιλαμβάνει τα μέτρα ασφάλειας που αφορούν i) τα τερματικά πληρωμών και τις συσκευές που χρησιμοποιούνται για την παροχή υπηρεσιών πληρωμών, ii) τα τερματικά πληρωμών και τις συσκευές που χρησιμοποιούνται για την αυθεντικοποίηση του χρήστη υπηρεσιών πληρωμών και iii) τις συσκευές και το λογισμικό που παρέχει ο ΠΥΠ στον χρήστη υπηρεσιών πληρωμών για την παραγωγή/λήψη κωδικού εξακρίβωσης ταυτότητας (κλειδάριθμων).

7.4 Το πλαίσιο δοκιμών θα πρέπει να διασφαλίζει ότι οι δοκιμές:

α) διενεργούνται στο πλαίσιο της επίσημης διαδικασίας διαχείρισης αλλαγών του ΠΥΠ για τη διασφάλιση της ισχύος και της αποτελεσματικότητάς τους·

β) εκτελούνται από ανεξάρτητους φορείς διεξαγωγής δοκιμών που διαθέτουν επαρκείς γνώσεις, δεξιότητες και εμπειρογνωσία στη διενέργεια δοκιμών όσον αφορά μέτρα

ασφάλειας υπηρεσιών πληρωμών και δεν εμπλέκονται στην ανάπτυξη των μέτρων ασφάλειας των αντίστοιχων υπηρεσιών ή συστημάτων πληρωμών που πρόκειται να υποβληθούν σε δοκιμή, τουλάχιστον για τις τελικές δοκιμές που διεξάγονται προτού τεθούν τα μέτρα ασφάλειας σε λειτουργία· και

γ) περιλαμβάνουν επαρκείς ελέγχους ευπαθειών και δοκιμές παρείσδυσης ανάλογα με το επίπεδο κινδύνου που προσδιορίζεται σε σχέση με τις υπηρεσίες πληρωμών.

7.5 Οι ΠΥΠ θα πρέπει να διενεργούν συνεχείς και επαναλαμβανόμενες δοκιμές των μέτρων ασφάλειας για τις υπηρεσίες πληρωμών που παρέχουν. Για τα συστήματα που είναι κρίσιμης σημασίας για την παροχή των υπηρεσιών πληρωμών τους (όπως περιγράφονται στην κατευθυντήρια γραμμή 3.2), οι εν λόγω δοκιμές θα πρέπει να διενεργούνται τουλάχιστον σε ετήσια βάση. Τα συστήματα μη κρίσιμης σημασίας θα πρέπει να υποβάλλονται περιοδικά σε δοκιμή αναλόγως του επιπέδου επικινδυνότητάς τους, αλλά τουλάχιστον ανά τριετία.

7.6 Οι ΠΥΠ θα πρέπει να παρακολουθούν και να αξιολογούν τα αποτελέσματα των διεξαγόμενων δοκιμών, καθώς και να επικαιροποιούν αναλόγως και χωρίς αδικαιολόγητη καθυστέρηση τα μέτρα ασφάλειάς τους στην περίπτωση των κρίσιμων συστημάτων.

Κατευθυντήρια γραμμή 8: Επίγνωση καταστάσεων και συνεχής εκμάθηση

Φύση των απειλών και επίγνωση καταστάσεων

8.1 Οι ΠΥΠ θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασίες και οργανωτικές δομές για τον προσδιορισμό και τη συνεχή παρακολούθηση απειλών για την ασφάλεια και λειτουργικών απειλών που θα μπορούσαν να επηρεάσουν σημαντικά την ικανότητά τους να παρέχουν υπηρεσίες πληρωμών.

8.2 Οι ΠΥΠ θα πρέπει να αναλύουν τα περιστατικά λειτουργικού κινδύνου ή τα περιστατικά ασφάλειας τα οποία έχουν επέλθει είτε εντός είτε εκτός του οργανισμού. Οι ΠΥΠ θα πρέπει να εξετάζουν τα κύρια διδάγματα που αντλούνται από τις εν λόγω αναλύσεις και να επικαιροποιούν αναλόγως τα μέτρα ασφάλειας.

8.3 Οι ΠΥΠ θα πρέπει να παρακολουθούν ενεργά τις τεχνολογικές εξελίξεις προκειμένου να διασφαλίζουν ότι έχουν επίγνωση των κινδύνων ασφάλειας.

Προγράμματα κατάρτισης και ευαισθητοποίησης σε θέματα ασφάλειας

8.4 Οι ΠΥΠ θα πρέπει να καθιερώνουν πρόγραμμα κατάρτισης για όλα τα μέλη του προσωπικού, προκειμένου να διασφαλίζεται ότι λαμβάνουν κατάλληλη κατάρτιση για την άσκηση των καθηκόντων και των αρμοδιοτήτων τους σύμφωνα με τις σχετικές πολιτικές και διαδικασίες ασφάλειας, ούτως ώστε να μειώνονται τα φαινόμενα ανθρώπινου σφάλματος, κλοπής, απάτης, κατάχρησης ή απώλειας. Οι ΠΥΠ θα πρέπει να διασφαλίζουν ότι το πρόγραμμα κατάρτισης προβλέπει την παροχή κατάρτισης στα μέλη του προσωπικού τουλάχιστον σε ετήσια βάση ή συχνότερα, εφόσον απαιτείται.

8.5 Οι ΠΥΠ θα πρέπει να διασφαλίζουν ότι τα μέλη του προσωπικού που κατέχουν καίριους ρόλους όπως προσδιορίζονται σύμφωνα με την κατευθυντήρια γραμμή 3.1 λαμβάνουν στοχευμένη κατάρτιση σε θέματα ασφάλειας πληροφοριών σε ετήσια βάση ή συχνότερα, εφόσον απαιτείται.

8.6 Οι ΠΥΠ θα πρέπει να καθιερώνουν και να υλοποιούν περιοδικά προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας, προκειμένου να εκπαιδεύουν το προσωπικό τους και να αντιμετωπίζουν κινδύνους που σχετίζονται με την ασφάλεια πληροφοριών. Στο πλαίσιο των προγραμμάτων αυτών θα πρέπει να απαιτείται από τα μέλη του προσωπικού των ΠΥΠ να αναφέρουν οποιαδήποτε ασυνήθιστη δραστηριότητα και ασυνήθιστα συμβάντα.

Κατευθυντήρια γραμμή 9: Διαχείριση σχέσεων χρηστών υπηρεσιών πληρωμών

Ευαισθητοποίηση των χρηστών υπηρεσιών πληρωμών σχετικά με τους κινδύνους ασφάλειας και τις ενέργειες μείωσης των κινδύνων

9.1 Οι ΠΥΠ θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασίες υποστήριξης και καθοδήγησης προς τους χρήστες υπηρεσιών πληρωμών με σκοπό την ενίσχυση της ευαισθητοποίησής τους σχετικά με τους κινδύνους ασφάλειας που συνδέονται με τις υπηρεσίες πληρωμών.

9.2 Η υποστήριξη και η καθοδήγηση που παρέχονται στους χρήστες υπηρεσιών πληρωμών θα πρέπει να επικαιροποιούνται ανάλογα με τις νέες απειλές και ευπάθειες, ενώ επίσης οι αλλαγές θα πρέπει να ανακοινώνονται στους χρήστες υπηρεσιών πληρωμών.

9.3 Όπου είναι δυνατό βάσει των λειτουργικών δυνατοτήτων των προϊόντων, οι ΠΥΠ θα πρέπει να επιτρέπουν στους χρήστες υπηρεσιών πληρωμών να απενεργοποιούν συγκεκριμένες από τις παρεχόμενες λειτουργίες πληρωμών.

9.4 Εάν, σύμφωνα με το άρθρο 68 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, ένας ΠΥΠ έχει συμφωνήσει με τον πληρωτή την ύπαρξη ορίων δαπάνης όσον αφορά τις πράξεις πληρωμής που εκτελούνται μέσω συγκεκριμένων μέσων πληρωμών, ο ΠΥΠ θα πρέπει να παρέχει στον πληρωτή τη δυνατότητα να προσαρμόζει τα εν λόγω όρια μέχρι το ανώτατο συμφωνηθέν όριο.

9.5 Οι ΠΥΠ θα πρέπει να παρέχουν στους χρήστες υπηρεσιών πληρωμών τη δυνατότητα να λαμβάνουν ειδοποιήσεις σχετικά με κινηθείσες και/ή αποτυχημένες απόπειρες έναρξης πράξεων πληρωμής, οι οποίες τους παρέχουν τη δυνατότητα εντοπισμού δόλιας ή κακόβουλης χρήσης του λογαριασμού τους.

9.6 Οι ΠΥΠ θα πρέπει να τηρούν ενήμερους τους χρήστες υπηρεσιών πληρωμών σχετικά με επικαιροποιήσεις των διαδικασιών ασφάλειας οι οποίες τους επηρεάζουν, αναφορικά με τις υπηρεσίες πληρωμών που αξιοποιούν.

9.7 Οι ΠΥΠ θα πρέπει να παρέχουν στους χρήστες υπηρεσιών πληρωμών υποστήριξη σχετικά με όλες τις ερωτήσεις, τα αιτήματα για υποστήριξη και τις γνωστοποιήσεις ασυνήθιστων γεγονότων ή ζητημάτων που αφορούν θέματα ασφάλειας σε σχέση με τις υπηρεσίες πληρωμών. Οι χρήστες

υπηρεσιών πληρωμών θα πρέπει να ενημερώνονται κατάλληλα σχετικά με τον τρόπο με τον οποίο μπορούν να λαμβάνουν την εν λόγω υποστήριξη.