EBA/GL/2014/12

19 Δεκεμβρίου 2014

Τελικές κατευθυντήριες γραμμές

σχετικά με την ασφάλεια των πληρωμών μέσω διαδικτύου

Περιεχόμενα

Κατευθυντήριες γραμμές σχετικά με την ασφάλεια των πληρωμών μέσω διαδικτύου

Πλαίσιο αναφοράς των κατευθυντήριων γραμμών

Το παρόν έγγραφο περιέχει κατευθυντήριες γραμμές οι οποίες ερείδονται στο άρθρο 16 του κανονισμού (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 (στο εξής ο «κανονισμός ΕΑΤ»). Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού ΕΑΤ, οι αρμόδιες αρχές και τα χρηματοοικονομικά ιδρύματα καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις εν λόγω κατευθυντήριες γραμμές.

Οι κατευθυντήριες γραμμές παρουσιάζουν την άποψη της ΕΑΤ σχετικά με τις κατάλληλες εποπτικές πρακτικές στο πλαίσιο του Ευρωπαϊκού Συστήματος Χρηματοοικονομικής Εποπτείας ή σχετικά με τους τρόπους ορθής εφαρμογής του δικαίου της ΕΕ στον συγκεκριμένο τομέα. Ως εκ τούτου, η ΕΑΤ αναμένει από τις αρμόδιες αρχές και τα χρηματοοικονομικά ιδρύματα στα οποία απευθύνονται οι κατευθυντήριες γραμμές να συμμορφωθούν προς αυτές. Οι αρμόδιες αρχές προς τις οποίες απευθύνονται οι κατευθυντήριες γραμμές πρέπει να συμμορφωθούν ενσωματώνοντας αυτές δεόντως στις εποπτικές πρακτικές τους (π.χ. τροποποιώντας το νομικό τους πλαίσιο ή τις εποπτικές διαδικασίες τους), ακόμη και όταν αυτές απευθύνονται πρωτίστως σε ιδρύματα.

Απαιτήσεις υποβολής στοιχείων

Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού ΕΑΤ, 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 5.05.2015. 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 στην ενότητα 5 του παρόντος εγγράφου, στην ηλεκτρονική διεύθυνση compliance@eba.europa.eu με την επισήμανση «EBA/GL/2014/12». Οι γνωστοποιήσεις πρέπει να υποβάλλονται από πρόσωπα δεόντως εξουσιοδοτημένα να γνωστοποιούν τη συμμόρφωση εκ μέρους των αρμόδιων αρχών τους.

Η γνωστοποίηση δημοσιεύεται στον δικτυακό τόπο της ΕΑΤ, σύμφωνα με το άρθρο 16 παράγραφος 3.

Τίτλος I – Πεδίο εφαρμογής και ορισμοί

Πεδίο εφαρμογής

1. Στις παρούσες κατευθυντήριες γραμμές ορίζεται ένα σύνολο ελάχιστων απαιτήσεων στον τομέα της ασφάλειας των πληρωμών μέσω διαδικτύου. Οι κατευθυντήριες γραμμές βασίζονται στους κανόνες της οδηγίας 2007/64/ΕΚ[1] («οδηγία για τις υπηρεσίες πληρωμών») σχετικά με τις απαιτήσεις ενημέρωσης για τις υπηρεσίες πληρωμών και τις υποχρεώσεις των παρόχων υπηρεσιών πληρωμών (ΠΥΠ) όσον αφορά την παροχή υπηρεσιών πληρωμών. Επιπλέον, σύμφωνα με το άρθρο 10 παράγραφος 4 της οδηγίας τα ιδρύματα πληρωμών υποχρεούνται να διαθέτουν άρτιο οργανωτικό πλαίσιο και επαρκείς μηχανισμούς εσωτερικού ελέγχου.

2. Οι κατευθυντήριες γραμμές αφορούν την παροχή υπηρεσιών πληρωμών που προσφέρονται μέσω του διαδικτύου από ΠΥΠ, όπως ορίζονται στο άρθρο 1 της οδηγίας.

3. Οι κατευθυντήριες γραμμές απευθύνονται στα χρηματοοικονομικά ιδρύματα όπως ορίζονται στο άρθρο 4 σημείο 1 του κανονισμού (ΕΕ) αριθ. 1093/2010 και στις αρμόδιες αρχές όπως ορίζονται στο άρθρο 4 σημείο 2 του κανονισμού (ΕΕ) αριθ. 1093/2010. Οι αρμόδιες αρχές των 28 κρατών μελών της Ευρωπαϊκής Ένωσης πρέπει να διασφαλίζουν την εφαρμογή αυτών των κατευθυντήριων γραμμών από τους ΠΥΠ, όπως ορίζονται στο άρθρο 1 της οδηγίας για τις υπηρεσίες πληρωμών, που τελούν υπό την εποπτεία τους.

4. Επιπλέον, οι αρμόδιες αρχές δύνανται να αποφασίσουν να απαιτήσουν από τους παρόχους υπηρεσιών πληρωμών να αναφέρουν στην αρμόδια αρχή ότι συμμορφώνονται με τις κατευθυντήριες γραμμές.

5. Οι παρούσες κατευθυντήριες γραμμές δεν επηρεάζουν την ισχύ των συστάσεων της Ευρωπαϊκής Κεντρικής Τράπεζας για την ασφάλεια των πληρωμών μέσω διαδικτύου (Recommendations for the security of internet payments) (η «έκθεση»).[2] Συγκεκριμένα, η έκθεση εξακολουθεί να αποτελεί το έγγραφο βάσει του οποίου οι κεντρικές τράπεζες στο πλαίσιο της εποπτικής λειτουργίας τους επί των συστημάτων και των μέσων πληρωμών πρέπει να αξιολογούν τη συμμόρφωση όσον αφορά την ασφάλεια των πληρωμών μέσω του διαδικτύου.

6. Οι κατευθυντήριες γραμμές αποτελούν τις ελάχιστες προσδοκίες. Εφαρμόζονται με την επιφύλαξη της ευθύνης των ΠΥΠ να παρακολουθούν και να αξιολογούν τους κινδύνους που συνεπάγονται οι δραστηριότητές τους που αφορούν πληρωμές, να αναπτύσσουν εσωτερικές λεπτομερείς πολιτικές ασφάλειας και να εφαρμόζουν επαρκή μέτρα ασφάλειας,

[1] 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.

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

έκτακτης ανάγκης, διαχείρισης περιστατικών και αδιάλειπτης λειτουργίας που είναι αναλογικά προς τους εγγενείς κινδύνους των παρεχόμενων υπηρεσιών πληρωμών.

7. Σκοπός των κατευθυντήριων γραμμών είναι να οριστούν ελάχιστες κοινές απαιτήσεις για τις υπηρεσίες πληρωμών μέσω διαδικτύου που απαριθμούνται κατωτέρω, ανεξαρτήτως της συσκευής πρόσβασης που χρησιμοποιείται:

   - [κάρτες] η εκτέλεση πληρωμών με κάρτα στο διαδίκτυο, συμπεριλαμβανομένων των πληρωμών με άυλη κάρτα, καθώς και η καταχώριση των στοιχείων για πληρωμή με κάρτα για χρήση σε «λύσεις πορτοφολιού»·

   - [μεταφορές πίστωσης] η εκτέλεση μεταφορών πίστωσης στο διαδίκτυο·

   - [ηλεκτρονική εξουσιοδότηση] η έκδοση και τροποποίηση ηλεκτρονικών εξουσιοδοτήσεων άμεσης χρέωσης·

   - [ηλεκτρονικό χρήμα] μεταφορές ηλεκτρονικού χρήματος μεταξύ δύο λογαριασμών ηλεκτρονικού χρήματος μέσω του διαδικτύου.

8. Στις περιπτώσεις όπου οι κατευθυντήριες γραμμές αναφέρονται σε ένα αποτέλεσμα, το αποτέλεσμα αυτό μπορεί να επιτευχθεί με διάφορους τρόπους. Οι παρούσες κατευθυντήριες γραμμές, πέραν των απαιτήσεων που καθορίζονται κατωτέρω, παρέχουν επίσης παραδείγματα βέλτιστων πρακτικών (στο παράρτημα 1), τις οποίες οι ΠΥΠ ενθαρρύνονται, αλλά δεν υποχρεούνται, να υιοθετήσουν.

9. Στην περίπτωση όπου η παροχή υπηρεσιών και μέσων πληρωμών προσφέρεται μέσω συστήματος πληρωμών (π.χ. συστήματα πληρωμών με κάρτα, συστήματα μεταφοράς πίστωσης, συστήματα άμεσης χρέωσης κ.λπ.), οι αρμόδιες αρχές και οι αντίστοιχες κεντρικές τράπεζες που ασκούν επίβλεψη επί των μέσων πληρωμής πρέπει να βρίσκονται σε επαφή ώστε να διασφαλίζεται η συνεπής εφαρμογή των κατευθυντήριων γραμμών από τους παράγοντες που είναι υπεύθυνοι για τη λειτουργία του συστήματος.

10. Οι πάροχοι ολοκληρωμένων λύσεων πληρωμών[3] που προσφέρουν υπηρεσίες έναρξης πληρωμής θεωρούνται είτε αποδέκτες υπηρεσιών πληρωμών μέσω του διαδικτύου (και, κατ' επέκταση, ΠΥΠ) είτε εξωτερικοί πάροχοι τεχνικών υπηρεσιών των σχετικών σχημάτων ή ΠΥΠ. Στη δεύτερη περίπτωση, οι πάροχοι ολοκληρωμένων λύσεων πληρωμών πρέπει να υποχρεούνται βάσει σύμβασης να συμμορφώνονται με τις κατευθυντήριες γραμμές.

11. Από το πεδίο εφαρμογής των κατευθυντήριων γραμμών εξαιρούνται:

[3] Οι πάροχοι ολοκληρωμένων λύσεων πληρωμών παρέχουν στον δικαιούχο της πληρωμής (δηλαδή στην επιχείρηση ηλεκτρονικού εμπορίου) μια τυποποιημένη διεπαφή για τις υπηρεσίες έναρξης πληρωμής που παρέχονται από τους ΠΥΠ.

- άλλες υπηρεσίες διαδικτύου που παρέχονται από έναν ΠΥΠ μέσω του διαδικτυακού τόπου πληρωμών του (π.χ. ηλεκτρονικές χρηματιστηριακές υπηρεσίες, ηλεκτρονικές συμβάσεις)·

- πληρωμές για τις οποίες η εντολή δίνεται μέσω ταχυδρομείου, τηλεφώνου, φωνητικού μηνύματος ή με χρήση τεχνολογίας που βασίζεται σε υπηρεσία σύντομων γραπτών μηνυμάτων (SMS)·

- πληρωμές μέσω κινητής συσκευής, εκτός των πληρωμών που βασίζονται σε πρόγραμμα περιήγησης·

- μεταφορές πίστωσης στις περιπτώσεις όπου τρίτο μέρος αποκτά πρόσβαση στον λογαριασμό πληρωμών του πελάτη·

- πράξεις πληρωμών που πραγματοποιούνται από επιχείρηση μέσω δικτύων ειδικού σκοπού·

- πληρωμές με κάρτα με χρήση ανώνυμων και μη επαναφορτιζόμενων φυσικών ή άυλων προπληρωμένων καρτών στις περιπτώσεις όπου δεν υφίσταται συνεχής σχέση μεταξύ του εκδότη και του κατόχου της κάρτας·

- η εκκαθάριση και ο διακανονισμός πράξεων πληρωμής.

Ορισμοί

12. Για τους σκοπούς αυτών των κατευθυντήριων γραμμών, και συμπληρωματικά προς τους ορισμούς που παρέχονται στην οδηγία για τις υπηρεσίες πληρωμών, ισχύουν οι ακόλουθοι ορισμοί:

- Με τον όρο *ταυτοποίηση* νοείται η διαδικασία που επιτρέπει στον ΠΥΠ να επαληθεύει την ταυτότητα ενός πελάτη.

- Με τον όρο *ισχυρή ταυτοποίηση πελάτη* νοείται, για τους σκοπούς των κατευθυντήριων γραμμών, διαδικασία που βασίζεται στη χρήση δύο ή περισσότερων από τα ακόλουθα στοιχεία – τα οποία κατηγοριοποιούνται ως γνώση, κυριότητα και εγγενές χαρακτηριστικό: i) κάτι το οποίο γνωρίζει μόνο ο χρήστης, π.χ. στατικό συνθηματικό, κωδικό, προσωπικό αριθμό αναγνώρισης (PIN)· ii) κάτι το οποίο μόνο ο χρήστης έχει στην κυριότητά του, π.χ. συσκευή παραγωγής πρόσθετου κωδικού ασφάλειας, έξυπνη κάρτα, κινητό τηλέφωνο· iii) ένα μοναδικό σύμφυτο χαρακτηριστικό του χρήστη, π.χ. βιομετρικό χαρακτηριστικό, όπως δακτυλικό αποτύπωμα. Επιπλέον, τα στοιχεία που επιλέγονται πρέπει να είναι ανεξάρτητα μεταξύ τους, δηλαδή η παραβίαση του ενός να μην θέτει σε κίνδυνο τα άλλα. Τουλάχιστον ένα από τα στοιχεία πρέπει να μην μπορεί να επαναχρησιμοποιηθεί ή να αναπαραχθεί (εξαιρουμένου των σύμφυτων χαρακτηριστικών) και να μην είναι δυνατόν να υποκλαπεί μέσω του διαδικτύου χωρίς να το αντιληφθεί ο χρήστης. Η διαδικασία ισχυρής ταυτοποίησης πρέπει να είναι

σχεδιασμένη κατά τέτοιο τρόπο ώστε να προστατεύεται η εμπιστευτικότητα των δεδομένων ταυτοποίησης.

- Με τον όρο *έγκριση* νοείται η διαδικασία με την οποία ελέγχεται κατά πόσον ο πελάτης ή ο ΠΥΠ έχει το δικαίωμα να προβεί σε μια συγκεκριμένη ενέργεια, π.χ. το δικαίωμα μεταφοράς κεφαλαίων, ή το δικαίωμα πρόσβασης σε ευαίσθητα δεδομένα.

- Με τον όρο *διαπιστευτήρια* νοούνται οι πληροφορίες –γενικά εμπιστευτικές– που παρέχει ένας πελάτης ή ένας ΠΥΠ για σκοπούς ταυτοποίησης. Ως «διαπιστευτήριο» νοείται επίσης η κατοχή φυσικού εργαλείου που περιέχει τις πληροφορίες (π.χ. συσκευή παραγωγής κωδικών μίας χρήσης, έξυπνη κάρτα) ή κάτι που ο χρήστης απομνημονεύει ή κάποιο στοιχείο που τον αντιπροσωπεύει (όπως τα βιομετρικά χαρακτηριστικά).

- Με τον όρο *σημαντικό περιστατικό ασφάλειας πληρωμών* νοείται περιστατικό το οποίο έχει ή ενδέχεται να έχει σημαντική επίπτωση στην ασφάλεια, την ακεραιότητα ή τη συνέχεια των συστημάτων του ΠΥΠ που συνδέονται με πληρωμές και/ή στην ασφάλεια των ευαίσθητων δεδομένων πληρωμής ή των κεφαλαίων. Για την αξιολόγηση της σημαντικότητας του περιστατικού πρέπει να λαμβάνεται υπόψη ο αριθμός των πελατών που ενδέχεται να θιγούν, το διακυβευόμενο ποσό και η επίπτωση σε άλλους ΠΥΠ ή σε άλλες υποδομές πληρωμών.

- Με τον όρο *ανάλυση του κινδύνου της συναλλαγής* νοείται η αξιολόγηση του κινδύνου που αφορά συγκεκριμένη συναλλαγή, στο πλαίσιο της οποίας λαμβάνονται υπόψη κριτήρια όπως, για παράδειγμα, τα συναλλακτικά πρότυπα (συμπεριφορά) του πελάτη όσον αφορά τις πληρωμές, η αξία της σχετικής συναλλαγής, το είδος του προϊόντος και το προφίλ του δικαιούχου.

- Με τον όρο *άυλες κάρτες* νοείται λύση πληρωμής που βασίζεται σε κάρτα, στο πλαίσιο της οποίας δημιουργείται ένας εναλλακτικός, προσωρινός αριθμός κάρτας με περιορισμένη περίοδο ισχύος, περιορισμένη χρήση και προκαθορισμένο όριο δαπανών, που μπορεί να χρησιμοποιηθεί για την πραγματοποίηση αγορών στο διαδίκτυο.

- Με τον όρο *λύσεις πορτοφολιού* νοούνται λύσεις που παρέχουν τη δυνατότητα σε έναν πελάτη να καταχωρίζει δεδομένα που αφορούν ένα ή περισσότερα μέσα πληρωμών προκειμένου να προβαίνει σε πληρωμές προς διάφορες επιχειρήσεις ηλεκτρονικού εμπορίου.

Τίτλος ΙΙ – Κατευθυντήριες γραμμές σχετικά με την ασφάλεια των πληρωμών μέσω διαδικτύου

Γενικό περιβάλλον ελέγχου και ασφάλειας

Διακυβέρνηση

1. Οι ΠΥΠ πρέπει να εφαρμόζουν και να επανεξετάζουν τακτικά μια επίσημη πολιτική ασφάλειας για τις υπηρεσίες πληρωμών μέσω διαδικτύου.

1.1 Η πολιτική ασφάλειας πρέπει να είναι δεόντως καταγεγραμμένη και να επανεξετάζεται ανά τακτά χρονικά διαστήματα (σύμφωνα με την κατευθυντήρια γραμμή 2.4) και να εγκρίνεται από τα ανώτατα στελέχη της διοίκησης. Πρέπει να θέτει στόχους ασφάλειας και να καθορίζει τη διάθεση ανάληψης κινδύνων.

1.2 Η πολιτική ασφάλειας πρέπει να προσδιορίζει ρόλους και αρμοδιότητες, συμπεριλαμβανομένης της λειτουργίας διαχείρισης του κινδύνου με απευθείας αναφορά στο Διοικητικό Συμβούλιο, καθώς και τις γραμμές αναφοράς για τις παρεχόμενες υπηρεσίες πληρωμών μέσω του διαδικτύου, συμπεριλαμβανομένης της διαχείρισης ευαίσθητων δεδομένων πληρωμής όσον αφορά την αξιολόγηση, τον έλεγχο και τον μετριασμό των κινδύνων.

Αξιολόγηση του κινδύνου

2. Οι ΠΥΠ πρέπει να διενεργούν και να τεκμηριώνουν αναλυτικές αξιολογήσεις κινδύνου όσον αφορά την ασφάλεια των πληρωμών μέσω του διαδικτύου και των συναφών υπηρεσιών, τόσο πριν από τη δημιουργία της υπηρεσίας (ή των υπηρεσιών) όσο και ανά τακτά χρονικά διαστήματα στη συνέχεια.

2.1 Οι ΠΥΠ, μέσω της λειτουργίας τους για τη διαχείριση του κινδύνου, πρέπει να διενεργούν και να τεκμηριώνουν λεπτομερείς αξιολογήσεις κινδύνου για τις πληρωμές μέσω διαδικτύου και τις συναφείς υπηρεσίες. Οι ΠΥΠ πρέπει να εξετάζουν τα αποτελέσματα της συνεχούς παρακολούθησης των απειλών κατά της ασφάλειας των υπηρεσιών πληρωμών μέσω διαδικτύου που προσφέρουν ή σχεδιάζουν να προσφέρουν, λαμβάνοντας υπόψη i) τις τεχνολογικές λύσεις που χρησιμοποιούν, ii) τις υπηρεσίες που αναθέτουν σε εξωτερικούς παρόχους και iii) το τεχνικό περιβάλλον των πελατών. Οι ΠΥΠ πρέπει να εξετάζουν τους κινδύνους που συνδέονται με τις επιλεγμένες τεχνολογικές πλατφόρμες, με την αρχιτεκτονική των εφαρμογών, με τις τεχνικές και τις ρουτίνες προγραμματισμού τόσο από τη δική τους πλευρά[4] όσο και

[4] Όπως η ευαισθησία του συστήματος σε επιθέσεις υφαρπαγής συνόδου (session hijacking), προσθήκη κακόβουλου κώδικα SQL (SQL injection), επίθεση μέσω δέσμης ενεργειών από άλλη τοποθεσία (cross-site scripting), υπερχείλιση προσωρινής μνήμης (buffer overflow) κ.λπ.

από την πλευρά των πελατών τους,[5] καθώς και τα αποτελέσματα της διαδικασίας παρακολούθησης περιστατικών ασφάλειας (βλέπε κατευθυντήρια γραμμή 3).

2.2 Βάσει των ανωτέρω, οι ΠΥΠ πρέπει να καθορίζουν κατά πόσον και σε ποιον βαθμό ενδέχεται να απαιτούνται αλλαγές στα υπάρχοντα μέτρα ασφάλειας, στις τεχνολογίες που χρησιμοποιούνται και στις διαδικασίες ή τις υπηρεσίες που προσφέρονται. Οι ΠΥΠ πρέπει να λαμβάνουν υπόψη τον χρόνο που απαιτείται για την εφαρμογή των αλλαγών (περιλαμβανομένου του χρόνου της υιοθέτησής τους από τους πελάτες) και να λαμβάνουν τα κατάλληλα προσωρινά μέτρα για την ελαχιστοποίηση των περιστατικών ασφάλειας και απάτης, καθώς και των ενδεχόμενων δυσλειτουργιών.

2.3 Η αξιολόγηση των κινδύνων πρέπει να καλύπτει την ανάγκη προστασίας και διασφάλισης των ευαίσθητων δεδομένων των πληρωμών.

2.4 Οι ΠΥΠ πρέπει να προβαίνουν σε επανεξέταση των σεναρίων κινδύνου και των υφιστάμενων μέτρων ασφάλειας ύστερα από σημαντικά περιστατικά που επηρεάζουν τις υπηρεσίες τους, πριν από την πραγματοποίηση σημαντικών αλλαγών στην υποδομή ή στις διαδικασίες και μετά τον εντοπισμό νέων απειλών μέσω διαδικασιών παρακολούθησης του κινδύνου. Επιπλέον, πρέπει να διενεργείται τουλάχιστον μία φορά ετησίως γενική επανεξέταση της αξιολόγησης του κινδύνου. Τα αποτελέσματα των αξιολογήσεων κινδύνου και των επανεξετάσεων πρέπει να υποβάλλονται προς έγκριση στα ανώτατα διοικητικά στελέχη.

Παρακολούθηση και αναφορά περιστατικών

3. Οι ΠΥΠ πρέπει να διασφαλίζουν τη συνεπή και ολοκληρωμένη παρακολούθηση και διαχείριση των συμβάντων ασφάλειας, συμπεριλαμβανομένων των καταγγελιών των πελατών σχετικά με την ασφάλεια. Οι ΠΥΠ πρέπει να δημιουργήσουν διαδικασία για την αναφορά τέτοιων περιστατικών στη διοίκηση και, στην περίπτωση σημαντικών περιστατικών ασφάλειας πληρωμών, στις αρμόδιες αρχές.

3.1 Οι ΠΥΠ πρέπει να εφαρμόζουν διαδικασία για τον έλεγχο, τον χειρισμό και την παρακολούθηση των περιστατικών ασφάλειας και των καταγγελιών πελατών που αφορούν θέματα ασφάλειας και να αναφέρουν τα περιστατικά αυτά στη διοίκηση.

3.2 Οι ΠΥΠ πρέπει να εφαρμόζουν διαδικασία για την άμεση ενημέρωση των αρμόδιων αρχών (δηλαδή των εποπτικών αρχών και των αρχών προστασίας δεδομένων), όπου υπάρχουν, σε περίπτωση σημαντικών περιστατικών ασφάλειας πληρωμών που σχετίζονται με τις παρεχόμενες υπηρεσίες πληρωμών.

[5] Όπως κίνδυνοι που συνδέονται με τη χρήση εφαρμογών πολυμέσων, προσθηκών για προγράμματα περιήγησης, πλαισίων, εξωτερικών συνδέσμων κ.λπ.

3.3 Οι ΠΥΠ πρέπει να εφαρμόζουν διαδικασία για τη συνεργασία με τις αρμόδιες διωκτικές αρχές όσον αφορά σημαντικά περιστατικά ασφάλειας πληρωμών, συμπεριλαμβανομένων των παραβιάσεων των δεδομένων.

3.4 Οι ΠΥΠ που αποδέχονται συναλλαγές με κάρτα πρέπει, βάσει σύμβασης, να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν ευαίσθητα δεδομένα πληρωμών να συνεργάζονται σε περιπτώσεις σημαντικών περιστατικών ασφάλειας πληρωμών, συμπεριλαμβανομένων παραβιάσεων δεδομένων, τόσο με τους ίδιους όσο και με τις αντίστοιχες διωκτικές αρχές. Εάν ένας ΠΥΠ διαπιστώσει ότι μια επιχείρηση ηλεκτρονικού εμπορίου δεν συνεργάζεται σύμφωνα με τα απαιτούμενα βάσει της σύμβασης, πρέπει να λάβει μέτρα για να επιβάλει τη συμβατική αυτή υποχρέωση, ή να καταγγείλει τη σύμβαση.

Έλεγχος και μετριασμός των κινδύνων

4. Οι ΠΥΠ πρέπει να εφαρμόζουν μέτρα ασφάλειας σύμφωνα με την αντίστοιχη πολιτική ασφάλειας που ακολουθούν προκειμένου να μετριάζουν τους κινδύνους που εντοπίζονται. Τα μέτρα αυτά πρέπει να ενσωματώνουν πολλαπλά επίπεδα ασφάλειας, στο πλαίσιο των οποίων η αποτυχία μίας γραμμής άμυνας αντιμετωπίζεται από την επόμενη γραμμή άμυνας («εις βάθος άμυνα»).

4.1 Κατά τον σχεδιασμό, την ανάπτυξη και τη συντήρηση υπηρεσιών πληρωμών μέσω διαδικτύου, οι ΠΥΠ πρέπει να δίνουν ιδιαίτερη προσοχή στον επαρκή διαχωρισμό των καθηκόντων στα περιβάλλοντα τεχνολογίας της πληροφορίας (ΤΠ) (π.χ. τα περιβάλλοντα ανάπτυξης, δοκιμής και παραγωγής) και στην ορθή εφαρμογή της αρχής των «ελάχιστων προνομίων» ως βάση για τη χρηστή διαχείριση της ταυτότητας και της πρόσβασης[6].

4.2 Οι ΠΥΠ πρέπει να διαθέτουν κατάλληλες λύσεις ασφάλειας για την προστασία των δικτύων, των δικτυακών τόπων, των εξυπηρετητών και των ζεύξεων επικοινωνίας από περιστατικά κατάχρησης ή από επιθέσεις. Οι ΠΥΠ πρέπει να αφαιρούν από τους εξυπηρετητές όλες τις περιττές λειτουργίες προκειμένου να τους προστατεύουν (να τους καθιστούν περισσότερο ανθεκτικούς) και να εξαλείφουν ή να μειώνουν τα τρωτά σημεία των εφαρμογών που κινδυνεύουν. Η πρόσβαση μέσω των διαφόρων εφαρμογών στα απαραίτητα δεδομένα και πηγές πρέπει να διατηρείται στο απολύτως αναγκαίο επίπεδο, με βάση την «αρχή των ελάχιστων προνομίων». Προκειμένου να περιοριστεί η χρήση «πλαστών» δικτυακών τόπων (που μιμούνται νόμιμους δικτυακούς τόπους ΠΥΠ), οι δικτυακοί τόποι συναλλαγών που προσφέρουν υπηρεσίες πληρωμών μέσω διαδικτύου πρέπει να διαθέτουν, για την ταυτοποίησή τους, πιστοποιητικά εκτεταμένης επικύρωσης που εκδίδονται στο όνομα του ΠΥΠ ή να εφαρμόζουν άλλες παρόμοιες μεθόδους ταυτοποίησης.

[6] Κάθε πρόγραμμα και κάθε προνομιούχος χρήστης του συστήματος πρέπει να λειτουργεί χρησιμοποιώντας τα ελάχιστα απαραίτητα προνόμια για την ολοκλήρωση του έργου του. Βλέπε Saltzer, J.H. (1974), «Protection and the Control of Information Sharing in Multics», Communications of the ACM, τεύχος 17, αριθ. 7, σ. 388.

4.3 Οι ΠΥΠ πρέπει να εφαρμόζουν κατάλληλες διαδικασίες παρακολούθησης, ιχνηλασίας και περιορισμού της πρόσβασης σε: i) ευαίσθητα δεδομένα πληρωμών, και ii) κρίσιμους λογικούς και φυσικούς πόρους, όπως δίκτυα, συστήματα, βάσεις δεδομένων, υποσυστήματα ασφάλειας κ.λπ. Οι ΠΥΠ πρέπει να δημιουργούν, να αποθηκεύουν και να αναλύουν κατάλληλα αρχεία καταγραφής και ίχνη ελέγχου.

4.4 Κατά τον σχεδιασμό[7], την ανάπτυξη και τη συντήρηση υπηρεσιών πληρωμών μέσω διαδικτύου, οι ΠΥΠ πρέπει να διασφαλίζουν ότι η ελαχιστοποίηση των δεδομένων[8] συνιστά ουσιώδες στοιχείο της βασικής λειτουργικότητας: η συλλογή, η δρομολόγηση, η επεξεργασία, η αποθήκευση και/ή η αρχειοθέτηση, καθώς και η απεικόνιση ευαίσθητων δεδομένων πληρωμών πρέπει να διατηρούνται στα απολύτως αναγκαία επίπεδα.

4.5 Τα μέτρα ασφάλειας για τις υπηρεσίες πληρωμών μέσω διαδικτύου πρέπει να υποβάλλονται σε δοκιμές υπό την επίβλεψη της λειτουργίας διαχείρισης του κινδύνου προκειμένου να διασφαλίζεται η ανθεκτικότητα και η αποτελεσματικότητά τους. Όλες οι αλλαγές πρέπει να υπόκεινται σε επίσημη διαδικασία διαχείρισης των αλλαγών που να διασφαλίζει ότι οι αλλαγές προγραμματίζονται, υποβάλλονται σε δοκιμές, τεκμηριώνονται και εγκρίνονται δεόντως. Βάσει των αλλαγών που πραγματοποιούνται και των απειλών για την ασφάλεια που παρατηρούνται, οι δοκιμές πρέπει να επαναλαμβάνονται ανά τακτά χρονικά διαστήματα και να περιλαμβάνουν σενάρια συναφών και γνωστών πιθανών επιθέσεων.

4.6 Τα μέτρα ασφάλειας του ΠΥΠ για τις υπηρεσίες πληρωμών μέσω διαδικτύου πρέπει να ελέγχονται περιοδικά για να διασφαλίζεται η ανθεκτικότητα και η αποτελεσματικότητά τους. Η υλοποίηση και η λειτουργία των υπηρεσιών διαδικτυακών πληρωμών πρέπει επίσης να ελέγχονται. Η συχνότητα και η εστίαση των ελέγχων αυτών πρέπει να καθορίζονται λαμβανομένων υπόψη των σχετικών κινδύνων για την ασφάλεια, και να είναι αναλογικές προς αυτούς. Οι έλεγχοι πρέπει να διενεργούνται από αξιόπιστους και ανεξάρτητους εμπειρογνώμονες (εσωτερικούς ή εξωτερικούς), οι οποίοι δεν πρέπει να συμμετέχουν κατά κανένα τρόπο στην ανάπτυξη, την εφαρμογή ή την λειτουργική διαχείριση των παρεχόμενων υπηρεσιών πληρωμών μέσω διαδικτύου.

4.7 Σε κάθε περίπτωση όπου οι ΠΥΠ προβαίνουν σε εξωτερική ανάθεση καθηκόντων που αφορούν την ασφάλεια των υπηρεσιών πληρωμών μέσω διαδικτύου, η σχετική σύμβαση πρέπει να περιλαμβάνει διατάξεις που να απαιτούν τη συμμόρφωση με τις αρχές και τις κατευθυντήριες γραμμές που ορίζονται στις παρούσες κατευθυντήριες γραμμές.

[7] Προστασία της ιδιωτικότητας εκ του σχεδιασμού.

[8] Η ελαχιστοποίηση των δεδομένων παραπέμπει στην πολιτική που συνίσταται στη συλλογή των ελάχιστων αναγκαίων προσωπικών στοιχείων τα οποία απαιτούνται για την εκτέλεση μιας δεδομένης λειτουργίας.

4.8 Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα πρέπει βάσει σύμβασης να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου που χειρίζονται (δηλαδή αποθηκεύουν, επεξεργάζονται και διαβιβάζουν) ευαίσθητα δεδομένα πληρωμών να εφαρμόζουν μέτρα ασφάλειας στις υποδομές πληροφορικής τους, σύμφωνα με τις κατευθυντήριες γραμμές 4.1 έως 4.7, προκειμένου να αποτρέπεται η κλοπή των ευαίσθητων αυτών δεδομένων πληρωμών μέσω των συστημάτων τους. Εάν ένας ΠΥΠ διαπιστώσει ότι μια επιχείρηση ηλεκτρονικού εμπορίου δεν εφαρμόζει τα απαραίτητα μέτρα ασφάλειας, πρέπει να λάβει μέτρα για να επιβάλει τη συμβατική αυτή υποχρέωση, ή να καταγγείλει τη σύμβαση.

Ιχνηλασιμότητα

5. Οι ΠΥΠ πρέπει να εφαρμόζουν διαδικασίες με τις οποίες να διασφαλίζεται ότι όλες οι συναλλαγές, καθώς και η ροή επεξεργασίας της ηλεκτρονικής εξουσιοδότησης, ιχνηλατούνται δεόντως.

5.1 Οι ΠΥΠ πρέπει να διασφαλίζουν ότι η υπηρεσία τους ενσωματώνει μηχανισμούς ασφάλειας για τη λεπτομερή καταγραφή των δεδομένων των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων, συμπεριλαμβανομένων του αύξοντος αριθμού των συναλλαγών, χρονοσφραγίδων για τα δεδομένα των συναλλαγών, αλλαγών παραμετροποίησης, καθώς και της πρόσβασης στα δεδομένα των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων.

5.2 Οι ΠΥΠ πρέπει να διατηρούν αρχεία καταγραφής με τα οποία να καθίσταται δυνατή η ιχνηλασία οποιασδήποτε προσθήκης, αλλαγής ή διαγραφής των δεδομένων των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων.

5.3 Οι ΠΥΠ πρέπει να αντλούν και να αναλύουν τα δεδομένα των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων και να διασφαλίζουν ότι έχουν στη διάθεσή τους εργαλεία για την αξιολόγηση των αρχείων καταγραφής. Οι αντίστοιχες εφαρμογές πρέπει να είναι διαθέσιμες μόνο σε εξουσιοδοτημένο προσωπικό.

Ειδικά μέτρα ελέγχου και ασφάλειας για τις πληρωμές μέσω διαδικτύου

Αρχική εξακρίβωση ταυτότητας πελάτη, ενημέρωση

6. Η ταυτότητα των πελατών πρέπει να εξακριβώνεται δεόντως σύμφωνα με την ευρωπαϊκή νομοθεσία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες[9] και να επιβεβαιώνεται η βούληση των πελατών να προβούν σε πληρωμές

[9] Παραδείγματος χάριν, οδηγία 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2005, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας. ΕΕ L 309 της 25.11.2005, σ. 15-36. Βλέπε επίσης την οδηγία 2006/70/ΕΚ της Επιτροπής, της 1ης Αυγούστου 2006, για τη θέσπιση μέτρων εφαρμογής της οδηγίας 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τον ορισμό του «πολιτικώς εκτεθειμένου προσώπου» και τα τεχνικά κριτήρια για την εφαρμογή της απλουστευμένης δέουσας επιμέλειας ως προς

μέσω διαδικτύου με χρήση των υπηρεσιών πριν από την παροχή πρόσβασης στις υπηρεσίες αυτές. Οι ΠΥΠ πρέπει να παρέχουν επαρκή προηγούμενη, τακτική ή, κατά περίπτωση ειδική ενημέρωση στον πελάτη σχετικά με τις αναγκαίες προϋποθέσεις (π.χ. εξοπλισμός, διαδικασίες) για την εκτέλεση ασφαλών πράξεων πληρωμής μέσω του διαδικτύου καθώς και σχετικά με τους εγγενείς κινδύνους.

6.1 Οι ΠΥΠ πρέπει να διασφαλίζουν ότι έχουν εφαρμοστεί όλες οι διαδικασίες δέουσας επιμέλειας ως προς τον πελάτη και ότι ο πελάτης έχει παράσχει επαρκή έγγραφα ταυτότητας[10] και σχετικές πληροφορίες προτού χορηγηθεί σε αυτόν πρόσβαση στις υπηρεσίες πληρωμών μέσω διαδικτύου[11].

6.2 Οι ΠΥΠ πρέπει να διασφαλίζουν ότι η προηγούμενη ενημέρωση[12] που παρέχεται στον πελάτη περιλαμβάνει λεπτομέρειες που αφορούν ειδικά τις υπηρεσίες πληρωμών μέσω διαδικτύου. Στις πληροφορίες αυτές πρέπει να περιλαμβάνονται, κατά περίπτωση:

- σαφείς πληροφορίες σχετικά με τυχόν απαιτήσεις όσον αφορά τον εξοπλισμό, το λογισμικό ή άλλα απαραίτητα εργαλεία που πρέπει να διαθέτει ο πελάτης (π.χ. λογισμικό προστασίας από ιούς, τείχη προστασίας)·

- κατευθυντήριες γραμμές για την ορθή και ασφαλή χρήση εξατομικευμένων διαπιστευτηρίων ασφάλειας·

- αναλυτική περιγραφή κάθε σταδίου της διαδικασίας για την υποβολή και την έγκριση πράξης πληρωμής από τον πελάτη και/ή τη λήψη πληροφοριών, συμπεριλαμβανομένων των συνεπειών κάθε ενέργειας·

- κατευθυντήριες γραμμές για την ορθή και ασφαλή χρήση κάθε υλισμικού και λογισμικού που παρέχεται στον πελάτη·

- οι διαδικασίες που πρέπει να ακολουθούνται σε περίπτωση απώλειας ή κλοπής των εξατομικευμένων διαπιστευτηρίων ασφάλειας ή του υλισμικού ή του λογισμικού του πελάτη για την είσοδο στον δικτυακό τόπο ή για την εκτέλεση πράξεων πληρωμής·

τον πελάτη και την εφαρμογή της εξαίρεσης σε περιπτώσεις άσκησης χρηματοπιστωτικής δραστηριότητας σε περιστασιακή ή πολύ περιορισμένη βάση. ΕΕ L 214 της 4.8.2006, σ. 29-34.

[10] Παραδείγματος χάριν, διαβατήριο, εθνικό δελτίο ταυτότητας ή προηγμένη ηλεκτρονική υπογραφή.

[11] Η διαδικασία εξακρίβωσης της ταυτότητας του πελάτη εφαρμόζεται με την επιφύλαξη τυχόν εξαιρέσεων που προβλέπονται στην ισχύουσα νομοθεσία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Οι ΠΥΠ δεν υποχρεούνται να διενεργούν χωριστή διαδικασία εξακρίβωσης της ταυτότητας του πελάτη για τις υπηρεσίες πληρωμών μέσω διαδικτύου, υπό την προϋπόθεση ότι η ταυτότητα του εν λόγω πελάτη έχει ήδη εξακριβωθεί, π.χ. στο πλαίσιο άλλων υφιστάμενων υπηρεσιών που σχετίζονται με πληρωμές ή για το άνοιγμα λογαριασμού.

[12] Η εν λόγω ενημέρωση συμπληρώνει το άρθρο 42 της οδηγίας για τις υπηρεσίες πληρωμών στο οποίο προσδιορίζονται οι πληροφορίες που ο ΠΥΠ πρέπει να παρέχει στον χρήστη της υπηρεσίας πληρωμών πριν από τη σύναψη σύμβασης για την παροχή υπηρεσιών πληρωμών.

- οι διαδικασίες που πρέπει να ακολουθούνται εάν εντοπιστεί ή εγερθεί υπόνοια για κατάχρηση·

- περιγραφή των αρμοδιοτήτων και των ευθυνών του ΠΥΠ και του πελάτη αντιστοίχως όσον αφορά τη χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου.

6.3 Οι ΠΥΠ πρέπει να διασφαλίζουν ότι στη σύμβαση-πλαίσιο που συνάπτεται με τον πελάτη διευκρινίζεται ότι ο ΠΥΠ μπορεί να αναστείλει την εκτέλεση συγκεκριμένης πράξης ή τη χρήση του μέσου πληρωμής[13] για λόγους ασφάλειας. Στη σύμβαση πρέπει να προσδιορίζονται η μέθοδος και οι όροι ειδοποίησης του πελάτη καθώς και ο τρόπος με τον οποίο ο πελάτης μπορεί να επικοινωνεί με τον ΠΥΠ προκειμένου ο τελευταίος να άρει την αναστολή εκτέλεσης της πράξης ή της υπηρεσίας πληρωμής μέσω διαδικτύου, σύμφωνα με την οδηγία για τις υπηρεσίες πληρωμών.

Ισχυρή ταυτοποίηση του πελάτη

7. Η έναρξη πληρωμών μέσω διαδικτύου, καθώς και η πρόσβαση σε ευαίσθητα δεδομένα πληρωμών, πρέπει να προστατεύεται μέσω της ισχυρής ταυτοποίησης των πελατών. Οι ΠΥΠ πρέπει να εφαρμόζουν διαδικασία ισχυρής ταυτοποίησης των πελατών σύμφωνα με τον ορισμό που παρέχεται στις παρούσες κατευθυντήριες γραμμές.

7.1 [μεταφορά πίστωσης/ηλεκτρονική εξουσιοδότηση /ηλεκτρονικό χρήμα] Οι ΠΥΠ πρέπει να προβαίνουν σε ισχυρή ταυτοποίηση του πελάτη για την έγκριση των πράξεων πληρωμής μέσω διαδικτύου του πελάτη (συμπεριλαμβανομένων ομαδοποιημένων μεταφορών πίστωσης) και για την έκδοση ή την τροποποίηση ηλεκτρονικών εξουσιοδοτήσεων άμεσης χρέωσης. Ωστόσο, οι ΠΥΠ θα μπορούσαν να εξετάσουν το ενδεχόμενο θέσπισης εναλλακτικών μέτρων ταυτοποίησης των πελατών για:

- εξερχόμενες πληρωμές σε έμπιστους δικαιούχους που περιλαμβάνονται σε προϋπάρχουσες λευκές λίστες για τον συγκεκριμένο πελάτη·

- πράξεις μεταξύ δύο λογαριασμών του ίδιου πελάτη που τηρούνται στον ίδιο ΠΥΠ·

- μεταφορές εντός του ίδιου ΠΥΠ που δικαιολογούνται βάσει ανάλυσης του κινδύνου της συναλλαγής·

- πληρωμές μικρής αξίας, όπως αναφέρονται στην οδηγία για τις υπηρεσίες πληρωμών[14].

[13] Βλέπε άρθρο 55 της οδηγίας για τις υπηρεσίες πληρωμών, σχετικά με τους περιορισμούς της χρήσης του μέσου πληρωμών.

[14] Βλέπε τον ορισμό των μέσων πληρωμών μικρής αξίας στο άρθρο 34 παράγραφος 1 και στο άρθρο 53 παράγραφος 1 της οδηγίας για τις υπηρεσίες πληρωμών.

7.2 Για την απόκτηση πρόσβασης σε ευαίσθητα δεδομένα πληρωμών ή την τροποποίησή τους (συμπεριλαμβανομένης της δημιουργίας και της τροποποίησης λευκών λιστών) απαιτείται ισχυρή ταυτοποίηση του πελάτη. Στις περιπτώσεις όπου ένας ΠΥΠ προσφέρει αμιγώς συμβουλευτικές υπηρεσίες, χωρίς να εμφανίζονται ευαίσθητες πληροφορίες σχετικά με τον πελάτη ή τις πληρωμές, όπως δεδομένα καρτών πληρωμών, που θα μπορούσαν εύκολα να χρησιμοποιηθούν για να διαπραχθεί απάτη, ο ΠΥΠ μπορεί να προσαρμόζει τις απαιτήσεις ταυτοποίησης με βάση την αξιολόγηση του κινδύνου που διενεργεί.

7.3 [κάρτες] Για τις πράξεις πληρωμών με κάρτα, όλοι οι ΠΥΠ που εκδίδουν κάρτες πρέπει να υποστηρίζουν συστήματα ισχυρής ταυτοποίησης του κατόχου της κάρτας. Όλες οι κάρτες που εκδίδονται πρέπει να είναι τεχνικά έτοιμες (καταχωρισμένες) για χρήση με διαδικασία ισχυρής ταυτοποίησης.

7.4 [κάρτες] Οι ΠΥΠ που παρέχουν υπηρεσίες αποδοχής συναλλαγών με κάρτα πρέπει να υποστηρίζουν τεχνολογίες που επιτρέπουν στον εκδότη να εφαρμόζει διαδικασία ισχυρής ταυτοποίησης του κατόχου της κάρτας για τα σχήματα καρτών στα οποία συμμετέχει ο αποδέκτης.

7.5 [κάρτες] Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα πρέπει να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου να υποστηρίζουν λύσεις που επιτρέπουν στον εκδότη να διενεργεί ισχυρή ταυτοποίηση του κατόχου της κάρτας για συναλλαγές με κάρτα μέσω του διαδικτύου. Το ενδεχόμενο χρήσης εναλλακτικών μέτρων ταυτοποίησης θα μπορούσε να εξεταστεί για προκαθορισμένες κατηγορίες συναλλαγών χαμηλού κινδύνου, π.χ. βάσει ανάλυσης του κινδύνου της συναλλαγής, ή για πράξεις που αφορούν πληρωμές μικρής αξίας, όπως αναφέρεται στην οδηγία για τις υπηρεσίες πληρωμών.

7.6 [κάρτες] Για τα σχήματα καρτών πληρωμών που δέχεται η υπηρεσία, οι πάροχοι «λύσεων πορτοφολιού» πρέπει να απαιτούν ισχυρή ταυτοποίηση του πελάτη από τον εκδότη όταν ο νόμιμος κάτοχος καταχωρίζει για πρώτη φορά τα στοιχεία της κάρτας.

7.7 Οι πάροχοι «λύσεων πορτοφολιού» πρέπει να υποστηρίζουν τις διαδικασίες ισχυρής ταυτοποίησης του πελάτη όταν οι πελάτες εισέρχονται στους δικτυακούς τόπους των υπηρεσιών πληρωμών μέσω λύσεων πορτοφολιού ή προβαίνουν σε συναλλαγές με κάρτα μέσω του διαδικτύου. Το ενδεχόμενο χρήσης εναλλακτικών μέτρων ταυτοποίησης θα μπορούσε να εξεταστεί για προκαθορισμένες κατηγορίες συναλλαγών χαμηλού κινδύνου, π.χ. βάσει ανάλυσης του κινδύνου της συναλλαγής, ή για πράξεις που αφορούν πληρωμές μικρής αξίας, όπως αναφέρεται στην οδηγία για τις υπηρεσίες πληρωμών.

7.8 [κάρτες] Για τις άυλες κάρτες, η αρχική καταχώριση πρέπει να πραγματοποιείται σε ασφαλές και αξιόπιστο περιβάλλον[15]. Η ισχυρή ταυτοποίηση του πελάτη πρέπει να είναι υποχρεωτική για τη διαδικασία δημιουργίας των στοιχείων της άυλης κάρτας εάν η κάρτα εκδίδεται σε διαδικτυακό περιβάλλον.

7.9 Οι ΠΥΠ πρέπει να διασφαλίζουν τη δέουσα διμερή ταυτοποίηση κατά την επικοινωνία τους με επιχειρήσεις ηλεκτρονικού εμπορίου για τους σκοπούς της έναρξης πληρωμών μέσω διαδικτύου και της πρόσβασης σε ευαίσθητα δεδομένα πληρωμών.

Εγγραφή σε εργαλεία και/ή λογισμικό ταυτοποίησης που παραδίδονται στον πελάτη και παροχή αυτών

8. Οι ΠΥΠ πρέπει να διασφαλίζουν ότι η εγγραφή του πελάτη σε εργαλεία ταυτοποίησης, και η αρχική παροχή των εργαλείων αυτών, τα οποία απαιτούνται για τη χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου και/ή η παράδοση λογισμικού σχετικού με τις πληρωμές στους πελάτες διεξάγεται με ασφαλή τρόπο.

8.1 Η εγγραφή σε εργαλεία ταυτοποίησης και/ή λογισμικό σχετικό με τις πληρωμές που παραδίδονται στον πελάτη και η παροχή αυτών πρέπει να πληρούν τις ακόλουθες προϋποθέσεις.

- Οι σχετικές διαδικασίες πρέπει να διενεργούνται σε ασφαλές και αξιόπιστο περιβάλλον, λαμβανομένων ταυτόχρονα υπόψη των πιθανών κινδύνων που απορρέουν από συσκευές που δεν υπόκεινται στον έλεγχο του ΠΥΠ.

- Πρέπει να εφαρμόζονται αποτελεσματικές και ασφαλείς διαδικασίες για την παράδοση εξατομικευμένων διαπιστευτηρίων ασφάλειας, του λογισμικού που σχετίζεται με τις πληρωμές και όλων των εξατομικευμένων συσκευών που σχετίζονται με τις πληρωμές μέσω διαδικτύου. Το λογισμικό που παραδίδεται μέσω του διαδικτύου πρέπει επίσης να φέρει την ψηφιακή υπογραφή του ΠΥΠ ώστε να παρέχεται η δυνατότητα στον πελάτη να εξακριβώνει τη γνησιότητα και ότι δεν έχει παραποιηθεί.

- [κάρτες] Για συναλλαγές με κάρτα, ο πελάτης πρέπει να έχει την δυνατότητα να εγγραφεί για ισχυρή ταυτοποίηση ανεξαρτήτως μιας συγκεκριμένης αγοράς μέσω διαδικτύου. Στις περιπτώσεις όπου προσφέρεται δυνατότητα ενεργοποίησης στο πλαίσιο αγορών μέσω διαδικτύου, αυτή πρέπει να

[15] Περιβάλλοντα υπό την ευθύνη του ΠΥΠ, στο πλαίσιο των οποίων εξασφαλίζονται η επαρκής ταυτοποίηση του πελάτη και του ΠΥΠ που προσφέρει την υπηρεσία και η προστασία των εμπιστευτικών/ευαίσθητων πληροφοριών, είναι τα εξής: i) οι εγκαταστάσεις του ΠΥΠ· ii) δικτυακός τόπος εκτέλεσης τραπεζικών εργασιών μέσω διαδικτύου ή άλλος ασφαλής δικτυακός τόπος, π.χ. στην περίπτωση όπου η αρχή διακυβέρνησης προσφέρει παρόμοια χαρακτηριστικά ασφάλειας, μεταξύ άλλων, όπως αυτά που ορίζονται στην κατευθυντήρια γραμμή 4· ή iii) υπηρεσίες αυτόματων ταμειολογιστικών μηχανών (ATM). (Στην περίπτωση των ATM, απαιτείται ισχυρή ταυτοποίηση του πελάτη. Αυτή συνήθως πραγματοποιείται μέσω μικροεπεξεργαστή και προσωπικού κωδικού αναγνώρισης, ή μικροεπεξεργαστή και βιομετρικών στοιχείων).

πραγματοποιείται με ανακατεύθυνση του πελάτη σε ασφαλές και αξιόπιστο περιβάλλον.

8.2 [κάρτες] Οι εκδότες πρέπει να ενθαρρύνουν ενεργά την εγγραφή του κατόχου της κάρτας για ισχυρή ταυτοποίηση και να επιτρέπουν στους κατόχους κάρτας να παρακάμπτουν την εγγραφή μόνο σε περιορισμένο αριθμό εξαιρετικών περιπτώσεων όπου αυτό δικαιολογείται από τον κίνδυνο που συνδέεται με τη συγκεκριμένη συναλλαγή με κάρτα.

Απόπειρες σύνδεσης, χρονικό όριο σύνδεσης, διάρκεια ισχύος της ταυτοποίησης

9. Οι ΠΥΠ πρέπει να περιορίζουν τον αριθμό των προσπαθειών σύνδεσης ή ταυτοποίησης, να ορίζουν κανόνες για το χρονικό όριο σύνδεσης στις υπηρεσίες πληρωμών μέσω διαδικτύου και να θέτουν χρονικά όρια για τη διάρκεια ισχύος της ταυτοποίησης.

9.1 Όταν χρησιμοποιείται κωδικός αναγνώρισης μίας χρήσης για τους σκοπούς της ταυτοποίησης, οι ΠΥΠ πρέπει να διασφαλίζουν ότι η περίοδος ισχύος των εν λόγω κωδικών αναγνώρισης περιορίζεται αυστηρά στο ελάχιστο αναγκαίο.

9.2 Οι ΠΥΠ πρέπει να ορίζουν τον μέγιστο αριθμό αποτυχημένων προσπαθειών εισόδου ή ταυτοποίησης, μετά τον οποίο η πρόσβαση στην υπηρεσία πληρωμών μέσω διαδικτύου αναστέλλεται (προσωρινά ή μόνιμα). Πρέπει να εφαρμόζουν ασφαλή διαδικασία για την εκ νέου ενεργοποίηση των υπηρεσιών πληρωμών μέσω διαδικτύου που έχουν ανασταλεί.

9.3 Οι ΠΥΠ πρέπει να ορίζουν τη μέγιστη χρονική περίοδο μετά το πέρας της οποίας οι αδρανείς συνδέσεις στις υπηρεσίες πληρωμών μέσω διαδικτύου τερματίζονται αυτομάτως.

Παρακολούθηση συναλλαγών

10. Οι μηχανισμοί παρακολούθησης των συναλλαγών που έχουν σχεδιαστεί για την πρόληψη, τον εντοπισμό και την αναστολή εκτέλεσης παράνομων πράξεων πληρωμής πρέπει να τίθενται σε λειτουργία πριν από την τελική έγκριση του ΠΥΠ· συναλλαγές που θεωρούνται ύποπτες ή υψηλού κινδύνου πρέπει να υπόκεινται σε ειδική διαδικασία ελέγχου και αξιολόγησης. Ισοδύναμοι μηχανισμοί παρακολούθησης της ασφάλειας και έγκρισης πρέπει να εφαρμόζονται και για την έκδοση ηλεκτρονικών εξουσιοδοτήσεων.

10.1 Οι ΠΥΠ πρέπει να χρησιμοποιούν συστήματα ανίχνευσης και πρόληψης της απάτης για τον εντοπισμό ύποπτων συναλλαγών πριν από την τελική έγκριση των πράξεων ή των ηλεκτρονικών εξουσιοδοτήσεων από τον ΠΥΠ. Τα συστήματα αυτά πρέπει να βασίζονται, για παράδειγμα, σε παραμετροποιημένους κανόνες (όπως μαύρες λίστες με στοιχεία καρτών που έχουν διαρρεύσει ή κλαπεί) και να παρακολουθούν ασυνήθιστα πρότυπα συμπεριφοράς του πελάτη ή της συσκευής πρόσβασης του

πελάτη (όπως αλλαγή της διεύθυνσης πρωτοκόλλου ίντερνετ (διεύθυνση IP)[16] ή περιοχής διευθύνσεων IP κατά τη διάρκεια της σύνδεσης στην υπηρεσία πληρωμών μέσω διαδικτύου, η οποία ενίοτε εντοπίζεται μέσω ελέγχων για τον εντοπισμό της γεωγραφικής θέσης της διεύθυνσης IP,[17] ασυνήθεις κατηγορίες επιχειρήσεων ηλεκτρονικού εμπορίου για έναν συγκεκριμένο πελάτη ή ασυνήθιστα δεδομένα συναλλαγών κ.λπ.). Τα συστήματα αυτά πρέπει επίσης να είναι σε θέση να εντοπίζουν ενδείξεις προσβολής από κακόβουλο λογισμικό κατά τη διάρκεια της σύνδεσης (π.χ. αναγνώριση υποβολής στοιχείων μέσω αυτόματης δέσμης εντολών (script) αντί από άνθρωπο) και γνωστών σεναρίων απάτης. Η έκταση, η πολυπλοκότητα και η δυνατότητα προσαρμογής των λύσεων παρακολούθησης πρέπει να είναι ανάλογες με το αποτέλεσμα της αξιολόγησης του κινδύνου και ταυτόχρονα να συμμορφώνονται με τη σχετική νομοθεσία για την προστασία των δεδομένων.

10.2 Οι ΠΥΠ που αποδέχονται υπηρεσίες συναλλαγών με κάρτα πρέπει να εφαρμόζουν συστήματα εντοπισμού και πρόληψης της απάτης προκειμένου να παρακολουθούν τις δραστηριότητες των επιχειρήσεων ηλεκτρονικού εμπορίου.

10.3 Οι ΠΥΠ πρέπει να διεξάγουν οποιαδήποτε διαδικασία ελέγχου και αξιολόγησης της συναλλαγής εντός εύλογου χρονικού διαστήματος, προκειμένου να μην καθυστερούν αδικαιολόγητα την έναρξη και/ή την εκτέλεση της σχετικής υπηρεσίας πληρωμής.

10.4 Στις περιπτώσεις όπου ο ΠΥΠ, σύμφωνα με την πολιτική κινδύνου που ακολουθεί, αποφασίζει την αναστολή εκτέλεσης μιας πράξης πληρωμής η οποία έχει εντοπιστεί ως πιθανώς παράνομη, ο ΠΥΠ πρέπει να διατηρήσει την αναστολή για όσο το δυνατόν συντομότερο χρονικό διάστημα μέχρις ότου επιλυθούν τα ζητήματα ασφάλειας.

Προστασία των ευαίσθητων δεδομένων πληρωμών

11. Τα ευαίσθητα δεδομένα πληρωμών πρέπει να προστατεύονται κατά την αποθήκευση, την επεξεργασία ή τη διαβίβασή τους.

11.1 Όλα τα δεδομένα που χρησιμοποιούνται για την αναγνώριση και την ταυτοποίηση των πελατών (π.χ. κατά την είσοδο, κατά την έναρξη πληρωμής μέσω διαδικτύου, καθώς και κατά την έκδοση, τροποποίηση ή ακύρωση ηλεκτρονικών εξουσιοδοτήσεων), όπως επίσης και η διεπαφή του πελάτη (δικτυακός τόπος ΠΥΠ ή επιχείρησης ηλεκτρονικού εμπορίου) πρέπει να προστατεύονται δεόντως από κλοπή, μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

11.2 Οι ΠΥΠ πρέπει να διασφαλίζουν ότι, όταν ανταλλάσσονται ευαίσθητα δεδομένα πληρωμών μέσω του διαδικτύου, εφαρμόζεται ασφαλής διατερματική

[16] Η διεύθυνση IP είναι ένας μοναδικός αριθμητικός κωδικός που αντιστοιχεί σε κάθε υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο.

[17] Με έναν έλεγχο γεωγραφικού εντοπισμού διεύθυνσης “Geo-IP” εξακριβώνεται κατά πόσον η χώρα έκδοσης αντιστοιχεί στη διεύθυνση IP από την οποία ο χρήστης επιχειρεί τη συναλλαγή.

κρυπτογράφηση [18] μεταξύ των μερών που επικοινωνούν καθ' όλη τη διάρκεια της σύνδεσης, προκειμένου να διασφαλίζονται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, με τη χρήση ισχυρών και ευρέως αναγνωρισμένων τεχνικών κρυπτογράφησης.

11.3 Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα πρέπει να ενθαρρύνουν τις επιχειρήσεις ηλεκτρονικού εμπορίου να μην αποθηκεύουν τυχόν ευαίσθητα δεδομένα πληρωμών. Στην περίπτωση που επιχειρήσεις ηλεκτρονικού εμπορίου διαχειρίζονται, δηλαδή αποθηκεύουν, επεξεργάζονται η διαβιβάζουν ευαίσθητα δεδομένα πληρωμών, οι εν λόγω ΠΥΠ πρέπει βάσει σύμβασης να απαιτούν από τις επιχειρήσεις αυτές να εφαρμόζουν τα απαραίτητα μέτρα προστασίας των δεδομένων αυτών. Οι ΠΥΠ πρέπει να διενεργούν τακτικούς ελέγχους και εάν ένας ΠΥΠ διαπιστώσει ότι επιχείρηση ηλεκτρονικού εμπορίου η οποία διαχειρίζεται ευαίσθητα δεδομένα πληρωμών δεν εφαρμόζει τα απαιτούμενα μέτρα ασφάλειας, πρέπει να προβεί σε ενέργειες για την επιβολή της συμβατικής αυτής υποχρέωσης ή να καταγγείλει τη σύμβαση.

[18] Ο όρος «διατερματική κρυπτογράφηση» αναφέρεται στην κρυπτογράφηση που πραγματοποιείται εντός ή στο τερματικό σύστημα προέλευσης, με την αντίστοιχη αποκρυπτογράφηση να πραγματοποιείται μόνο εντός ή στο τερματικό σύστημα προορισμού. ETSI EN 302 109 V1.1.1. (2003-06).

Ευαισθητοποίηση, εκπαίδευση και επικοινωνία με τους πελάτες

Εκπαίδευση και επικοινωνία με τους πελάτες

12. Οι ΠΥΠ πρέπει να παρέχουν βοήθεια και καθοδήγηση στους πελάτες, όπου απαιτείται, όσον αφορά την ασφαλή χρήση των υπηρεσιών πληρωμών μέσω διαδικτύου. Οι ΠΥΠ πρέπει να επικοινωνούν με τους πελάτες τους με τέτοιο τρόπο ώστε να τους διαβεβαιώνουν ως προς τη γνησιότητα των μηνυμάτων που λαμβάνουν.

12.1 Οι ΠΥΠ πρέπει να παρέχουν τουλάχιστον έναν ασφαλή δίαυλο [19] συνεχούς επικοινωνίας με τους πελάτες σχετικά με την ορθή και ασφαλή χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου. Οι ΠΥΠ πρέπει να ενημερώνουν τους πελάτες για τον δίαυλο αυτόν και να εξηγούν ότι κάθε μήνυμα που αποστέλλεται εξ ονόματος του ΠΥΠ με οποιοδήποτε άλλο μέσο, όπως με μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο αφορά την ορθή και ασφαλή χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου, δεν είναι αξιόπιστο. Ο ΠΥΠ πρέπει να εξηγεί:

- τη διαδικασία που πρέπει να ακολουθούν οι πελάτες για να αναφέρουν στον ΠΥΠ (υπόνοιες για) παράνομες πληρωμές, ύποπτα περιστατικά ή ανωμαλίες κατά τη διάρκεια της σύνδεσης στις υπηρεσίες πληρωμών μέσω του διαδικτύου και/ή πιθανές απόπειρες "κοινωνικής μηχανικής" [20].

- τα επόμενα βήματα, δηλαδή τον τρόπο με τον οποίο ο ΠΥΠ θα απαντήσει στον πελάτη·

- τον τρόπο με τον οποίο ο ΠΥΠ θα ενημερώσει τον πελάτη σχετικά με (πιθανές) παράνομες συναλλαγές ή τη αποτυχία έναρξής τους, ή θα προειδοποιήσει τον πελάτη σχετικά με την εκδήλωση επιθέσεων (π.χ. ηλεκτρονικό «ψάρεμα» με μηνύματα ηλεκτρονικού ταχυδρομείου).

12.2 Μέσω του ασφαλούς διαύλου, ο ΠΥΠ πρέπει να τηρεί τους πελάτες ενήμερους σχετικά με ενημερώσεις των διαδικασιών ασφάλειας όσον αφορά τις υπηρεσίες πληρωμών μέσω διαδικτύου. Τυχόν προειδοποιήσεις σχετικά με σημαντικούς αναδυόμενους κινδύνους (π.χ. προειδοποιήσεις σχετικά με χρήση «κοινωνικής μηχανικής») πρέπει επίσης να παρέχονται μέσω του ασφαλούς διαύλου.

12.3 Οι ΠΥΠ πρέπει να παρέχουν υπηρεσίες εξυπηρέτησης πελατών για όλα τα ερωτήματα, τα παράπονα, τα αιτήματα υποστήριξης και τις γνωστοποιήσεις για ανωμαλίες ή περιστατικά που αφορούν υπηρεσίες πληρωμών μέσω διαδικτύου και συναφείς

[19] Όπως μια ειδική ηλεκτρονική ταχυδρομική θυρίδα στον δικτυακό τόπο του ΠΥΠ ή ένας ασφαλής δικτυακός τόπος.

[20] Με τον όρο «κοινωνική μηχανική» στο πλαίσιο αυτό νοούνται τεχνικές χειραγώγησης προσώπων για την απόσπαση πληροφοριών (π.χ. μέσω μηνύματος ηλεκτρονικού ταχυδρομείου ή τηλεφωνικών κλήσεων) ή τεχνικές συγκέντρωσης πληροφοριών από μέσα κοινωνικής δικτύωσης, για σκοπούς διάπραξης απάτης ή εξασφάλισης μη εξουσιοδοτημένης πρόσβασης σε υπολογιστή ή δίκτυο.

υπηρεσίες, και οι πελάτες πρέπει να ενημερώνονται επαρκώς σχετικά με τον τρόπο με τον οποίο μπορούν να λάβουν τέτοιου είδους βοήθεια.

12.4 Οι ΠΥΠ πρέπει να διοργανώνουν προγράμματα εκπαίδευσης και ευαισθητοποίησης των πελατών προκειμένου να διασφαλίζουν ότι οι πελάτες κατανοούν, τουλάχιστον, την ανάγκη:

- προστασίας των κωδικών πρόσβασης, των συσκευών παραγωγής πρόσθετου κωδικού ασφάλειας, των προσωπικών στοιχείων και άλλων εμπιστευτικών δεδομένων·
- ορθής διαχείρισης της ασφάλειας των προσωπικών τους συσκευών (π.χ. του υπολογιστή), μέσω της εγκατάστασης και της ενημέρωσης των στοιχείων ασφάλειας (λογισμικά προστασίας από ιούς, τείχη προστασίας, ενημερώσεις ασφάλειας)·
- εξέτασης των σημαντικών απειλών και κινδύνων που συνδέονται με τη λήψη λογισμικού μέσω του διαδικτύου εάν ο πελάτης δεν μπορεί να είναι βέβαιος σε εύλογο βαθμό ότι το λογισμικό είναι γνήσιο και ότι δεν έχει παραποιηθεί·
- χρήσης του γνήσιου δικτυακού τόπου πληρωμών μέσω διαδικτύου του ΠΥΠ.

12.5 Οι ΠΥΠ που αποδέχονται συναλλαγές με κάρτα πρέπει να απαιτούν από επιχειρήσεις ηλεκτρονικού εμπορίου το σαφή διαχωρισμό της διαδικασίας πληρωμής από το περιβάλλον του ηλεκτρονικού καταστήματος προκειμένου να διευκολύνουν τους πελάτες να αναγνωρίζουν πότε επικοινωνούν με τον ΠΥΠ και όχι με τον δικαιούχο πληρωμής (π.χ. με ανακατεύθυνση του πελάτη και άνοιγμα χωριστού παραθύρου ώστε η διαδικασία πληρωμής να μην εμφανίζεται σε ένα πλαίσιο εντός της ιστοσελίδας της επιχείρησης ηλεκτρονικού εμπορίου).

Ειδοποιήσεις, καθορισμός ορίων

13. Οι ΠΥΠ πρέπει να καθορίζουν όρια για τις υπηρεσίες πληρωμών μέσω διαδικτύου και μπορούν να παρέχουν στους πελάτες τους επιλογές για περαιτέρω περιορισμό του κινδύνου εντός των ορίων αυτών. Μπορούν επίσης να παρέχουν υπηρεσίες προειδοποίησης και διαχείρισης του προφίλ πελατών.

13.1 Πριν από την παροχή υπηρεσιών πληρωμών μέσω διαδικτύου σε πελάτες, οι ΠΥΠ πρέπει να θέτουν όρια[21] που θα ισχύουν για τις υπηρεσίες αυτές (π.χ. μέγιστο ποσό για κάθε επιμέρους πληρωμή ή συγκεντρωτικό ποσό για μια συγκεκριμένη χρονική περίοδο) και πρέπει να ενημερώνουν σχετικά τους πελάτες τους. Οι ΠΥΠ πρέπει να

[21] Τα όρια αυτά πρέπει να ισχύουν είτε καθολικά (δηλαδή για όλα τα μέσα πληρωμής που παρέχουν δυνατότητα πληρωμών μέσω διαδικτύου) είτε μεμονωμένα.

παρέχουν στους πελάτες τη δυνατότητα απενεργοποίησης της λειτουργίας πληρωμής μέσω διαδικτύου.

Πρόσβαση των πελατών σε πληροφορίες σχετικά με την κατάσταση έναρξης και εκτέλεσης της πληρωμής

14. Οι ΠΥΠ πρέπει να επιβεβαιώνουν στους πελάτες τους την έναρξη της πληρωμής και να τους παρέχουν εγκαίρως τις απαραίτητες πληροφορίες ώστε να ελέγχουν την ορθή έναρξη και/ή εκτέλεση της πράξης πληρωμής.

14.1 [μεταφορά πίστωσης/ηλεκτρονική εξουσιοδότηση] Οι ΠΥΠ πρέπει να παρέχουν στους πελάτες τη δυνατότητα να ελέγχουν την κατάσταση της εκτέλεσης των πράξεων σε σχεδόν πραγματικό χρόνο, καθώς και τα υπόλοιπα λογαριασμών ανά πάσα στιγμή[22] σε ένα ασφαλές και αξιόπιστο περιβάλλον.

14.2 Οποιοδήποτε λεπτομερές ηλεκτρονικό παραστατικό πρέπει να καθίσταται διαθέσιμο σε ασφαλές και αξιόπιστο περιβάλλον. Όταν οι ΠΥΠ ενημερώνουν τους πελάτες σχετικά με τη διαθεσιμότητα ηλεκτρονικών παραστατικών (π.χ. ανά τακτά χρονικά διαστήματα, όταν εκδίδεται περιοδικό ηλεκτρονικό αντίγραφο κίνησης λογαριασμού, ή κατά περίπτωση μετά την εκτέλεση μιας πράξης) μέσω εναλλακτικού διαύλου, όπως μέσω SMS, μηνύματος ηλεκτρονικού ταχυδρομείου ή επιστολής, τα ευαίσθητα δεδομένα πληρωμής δεν πρέπει να περιλαμβάνονται στην επικοινωνία αυτή ή, εάν περιλαμβάνονται, πρέπει να εμφανίζονται συγκαλυμμένα.

[22] Με εξαίρεση έκτακτες περιπτώσεις μη διαθεσιμότητας της υπηρεσίας αυτής για λόγους τεχνικής συντήρησης, ή λόγω σοβαρών περιστατικών.

Παράρτημα 1: Παραδείγματα βέλτιστων πρακτικών

Πέραν των απαιτήσεων που ορίζονται ανωτέρω, στις παρούσες κατευθυντήριες γραμμές περιγράφονται ορισμένες βέλτιστες πρακτικές τις οποίες οι ΠΥΠ και οι σχετικοί συμμετέχοντες της αγοράς ενθαρρύνονται, αλλά δεν υποχρεούνται, να υιοθετήσουν. Προς διευκόλυνση, τα κεφάλαια στα οποία εφαρμόζονται οι εν λόγω βέλτιστες πρακτικές αναφέρονται ρητά.

Γενικό περιβάλλον ελέγχου και ασφάλειας

Διακυβέρνηση

ΒΠ 1: Η πολιτική ασφάλειας μπορεί να καταγράφεται σε ειδικό έγγραφο.

Έλεγχος και μετριασμός των κινδύνων

ΒΠ 2: Οι ΠΥΠ μπορούν να παρέχουν εργαλεία ασφάλειας (π.χ. συσκευές και/ή ειδικά προσαρμοσμένα προγράμματα περιήγησης, που προστατεύονται δεόντως) για την προστασία της διεπαφής με τον πελάτη από παράνομη χρήση ή επιθέσεις (π.χ. επιθέσεις τύπου «man in the browser»).

Ιχνηλασιμότητα

ΒΠ 3: Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα μπορούν να απαιτούν βάσει σύμβασης από τις επιχειρήσεις ηλεκτρονικού εμπορίου που αποθηκεύουν πληροφορίες σχετικά με πληρωμές να εφαρμόζουν επαρκείς διαδικασίες για την υποστήριξη της ιχνηλασιμότητας.

Ειδικά μέτρα ελέγχου και ασφάλειας για τις πληρωμές μέσω διαδικτύου

Αρχική εξακρίβωση ταυτότητας πελάτη, ενημέρωση

ΒΠ 4: Ο πελάτης μπορεί να συνάπτει ειδική σύμβαση παροχής υπηρεσιών για την εκτέλεση πράξεων πληρωμής μέσω διαδικτύου, αντί να περιλαμβάνονται οι όροι για τις υπηρεσίες αυτές σε ευρύτερη σύμβαση παροχής γενικών υπηρεσιών που συνάπτεται με τον ΠΥΠ.

ΒΠ 5: Οι ΠΥΠ μπορούν επίσης να μεριμνούν για την παροχή στους πελάτες, σε συνεχή βάση ή, όπου εφαρμόζεται, κατά περίπτωση και με κατάλληλα μέσα (π.χ. φυλλάδια, ιστοσελίδες), σαφών και κατανοητών οδηγιών στο πλαίσιο των οποίων επεξηγούνται οι ευθύνες τους για την ασφαλή χρήση της υπηρεσίας.

Ισχυρή ταυτοποίηση πελάτη

ΒΠ 6: [κάρτες] Οι επιχειρήσεις ηλεκτρονικού εμπορίου μπορούν να υποστηρίζουν την ισχυρή ταυτοποίηση του κατόχου της κάρτας από τον εκδότη σε συναλλαγές με κάρτα μέσω του διαδικτύου.

ΒΠ 7: Για τους σκοπούς της διευκόλυνσης των πελατών, οι ΠΥΠ μπορούν να εξετάσουν το ενδεχόμενο χρήσης ενός ενιαίου εργαλείου ισχυρής ταυτοποίησης του πελάτη για όλες

τις υπηρεσίες πληρωμών μέσω διαδικτύου. Αυτό θα μπορούσε να αυξήσει την αποδοχή της λύσης από τους πελάτες και να διευκολύνει την ορθή χρήση.

ΒΠ 8: Η ισχυρή ταυτοποίηση του πελάτη μπορεί να περιλαμβάνει στοιχεία που συνδέουν την ταυτοποίηση με ένα συγκεκριμένο ποσό και έναν συγκεκριμένο δικαιούχο πληρωμής. Αυτό θα μπορούσε να παράσχει στους πελάτες αυξημένη βεβαιότητα κατά την έγκριση πληρωμών. Η τεχνολογική λύση που διευκολύνει τη σύνδεση των δεδομένων ισχυρής ταυτοποίησης με τα δεδομένα των συναλλαγών πρέπει να είναι ανθεκτική στην παραποίηση.

Προστασία των ευαίσθητων δεδομένων πληρωμών

ΒΠ 9: Είναι επιθυμητό οι επιχειρήσεις ηλεκτρονικού εμπορίου που χειρίζονται ευαίσθητα δεδομένα πληρωμών να εκπαιδεύουν καταλλήλως το προσωπικό τους που είναι αρμόδιο για τη διαχείριση περιστατικών απάτης και να επικαιροποιούν την εκπαίδευση αυτή τακτικά, ώστε να διασφαλίζεται ότι το περιεχόμενο να ανταποκρίνεται σε ένα δυναμικό περιβάλλον ασφάλειας.

Εκπαίδευση και επικοινωνία με τους πελάτες

ΒΠ 10: Είναι επιθυμητό οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα να διοργανώνουν εκπαιδευτικά προγράμματα για τις συνεργαζόμενες επιχειρήσεις ηλεκτρονικού εμπορίου σχετικά με την πρόληψη της απάτης.

Ειδοποιήσεις, καθορισμός ορίων

ΒΠ 11: Στο πλαίσιο των καθορισμένων ορίων, οι ΠΥΠ μπορούν να παρέχουν στους πελάτες τους τη δυνατότητα να διαχειρίζονται τα όρια των υπηρεσιών πληρωμών μέσω διαδικτύου σε ένα ασφαλές και αξιόπιστο περιβάλλον.

ΒΠ 12: Οι ΠΥΠ μπορούν να εφαρμόζουν διαδικασίες προειδοποίησης των πελατών, όπως μέσω τηλεφωνικής επικοινωνίας ή αποστολής γραπτού μηνύματος (SMS), για ύποπτες ή υψηλού κινδύνου πράξεις πληρωμών που βασίζονται στις εσωτερικές τους πολιτικές διαχείρισης του κινδύνου.

ΒΠ 13: Οι ΠΥΠ μπορούν να να παρέχουν στους πελάτες τη δυνατότητα να προσδιορίζουν γενικούς, εξατομικευμένους κανόνες ως παραμέτρους για τη συμπεριφορά τους όσον αφορά τις πληρωμές μέσω διαδικτύου και τις συναφείς υπηρεσίες, π.χ. ότι θα δρομολογούν πληρωμές μόνο από κάποιες συγκεκριμένες χώρες και ότι οι πληρωμές που δρομολογούνται από άλλα σημεία θα αναστέλλονται, ή ότι μπορούν να συμπεριλαμβάνουν συγκεκριμένους δικαιούχους πληρωμής σε λευκές ή μαύρες λίστες.