Κατευθυντήριες γραμμές 01/2021

σχετικά με παραδείγματα γνωστοποίησης παραβιάσεων δεδομένων προσωπικού χαρακτήρα

Εκδόθηκαν στις 14 Δεκεμβρίου 2021

Έκδοση 2.0

Translations proofread by EDPB Members. This language version has not yet been proofread.

Ιστορικό έκδοσης

Έκδοση 2.0	14 Δεκεμβρίου 2021	Έκδοση των κατευθυντήριων γραμμών μετά από δημόσια διαβούλευση
Έκδοση 1.0	14 Ιανουαρίου 2021	Έκδοση των κατευθυντήριων γραμμών για δημόσια διαβούλευση

Πίνακας περιεχομένων

ΤΟ ΕΥΡΩΠΑΪΚΟ ΣΥΜΒΟΥΛΙΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (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 (στο εξής: ΓΚΠΔ),

Έχοντας υπόψη τη Συμφωνία ΕΟΧ, και ιδίως το παράρτημα XI και το πρωτόκολλο 37 αυτής, όπως τροποποιήθηκαν με την απόφαση αριθ. 154/2018 της Μεικτής Επιτροπής του ΕΟΧ της 6ης Ιουλίου 2018[1],

Έχοντας υπόψη τα άρθρα 12 και 22 του εσωτερικού κανονισμού του,

Έχοντας υπόψη την ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο με τίτλο «Η προστασία των δεδομένων ως πυλώνας της ενδυνάμωσης των πολιτών και της προσέγγισης της ΕΕ στην ψηφιακή μετάβαση – δύο έτη εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων»[2],

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ

1 ΕΙΣΑΓΩΓΗ

1. Σε ορισμένες περιπτώσεις, ο ΓΚΠΔ απαιτεί τη γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα στην αρμόδια εθνική εποπτική αρχή (στο εξής: ΕΑ) και την ανακοίνωση της παραβίασης στα πρόσωπα των οποίων τα δεδομένα προσωπικού χαρακτήρα επηρεάζονται από την παραβίαση (άρθρα 33 και 34).

2. Η ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (στο εξής: ΟΕ29) εκπόνησε *γενική* καθοδήγηση σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων τον Οκτώβριο του 2017, στην οποία ανέλυσε τα σχετικά τμήματα του ΓΚΠΔ (κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP250) (στο εξής: κατευθυντήριες γραμμές WP250)[3]. Ωστόσο, λόγω της φύσης και του χρόνου έκδοσής τους, στις εν λόγω κατευθυντήριες γραμμές δεν εξετάστηκαν όλα τα πρακτικά ζητήματα με επαρκή βαθμό λεπτομέρειας. Επομένως, κρίθηκε αναγκαία η παροχή *πρακτικής και περιπτωσιολογικής* καθοδήγησης, βασισμένης στην πείρα που έχουν αποκτήσει οι ΕΑ από την έναρξη εφαρμογής του ΓΚΠΔ.

3. Το παρόν έγγραφο συμπληρώνει τις κατευθυντήριες γραμμές WP250 και αντικατοπτρίζει την κοινή πείρα των ΕΑ του ΕΟΧ από την έναρξη εφαρμογής του ΓΚΠΔ. Στόχος του είναι να παράσχει συνδρομή στους υπευθύνους επεξεργασίας δεδομένων κατά τη λήψη αποφάσεων για τον τρόπο χειρισμού των

[1] Οι αναφορές στα «κράτη μέλη» στο παρόν έγγραφο θα πρέπει να νοούνται ως αναφορές στα «κράτη μέλη του ΕΟΧ».

[2] COM(2020) 264 final της 24ης Ιουνίου 2020.

[3] ΟΕ29, WP250 rev.1, 6 Φεβρουαρίου 2018, Κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679 – εγκρίθηκαν από το ΕΣΠΔ, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

παραβιάσεων δεδομένων και τους παράγοντες που πρέπει να λαμβάνουν υπόψη κατά την αξιολόγηση κινδύνου.

4. Στο πλαίσιο κάθε προσπάθειας αντιμετώπισης παραβίασης, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία θα πρέπει καταρχάς να είναι σε θέση να την αναγνωρίσουν. Κατά το άρθρο 4 σημείο 12 του ΓΚΠΔ, ως «παραβίαση δεδομένων προσωπικού χαρακτήρα» νοείται «η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία».

5. Στη γνωμοδότηση 03/2014 σχετικά με τη γνωστοποίηση παραβίασης προσωπικών δεδομένων[4] και στις κατευθυντήριες γραμμές WP250, η ΟΕ29 εξήγησε ότι οι παραβιάσεις μπορούν να κατηγοριοποιηθούν σύμφωνα με τις ακόλουθες τρεις ευρέως γνωστές αρχές ασφάλειας πληροφοριών:

- «Παραβίαση απορρήτου» – όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αποκάλυψη δεδομένων προσωπικού χαρακτήρα ή μη εξουσιοδοτημένη ή τυχαία πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.
- «Παραβίαση ακεραιότητας» – όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αλλοίωση δεδομένων προσωπικού χαρακτήρα.
- «Παραβίαση διαθεσιμότητας» – όταν υπάρχει τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης σε δεδομένα προσωπικού χαρακτήρα ή τυχαία ή μη εξουσιοδοτημένη καταστροφή δεδομένων προσωπικού χαρακτήρα[5].

6. Η παραβίαση μπορεί δυνητικά να έχει διάφορες σημαντικές δυσμενείς συνέπειες στα πρόσωπα, οι οποίες μπορεί να έχουν ως αποτέλεσμα σωματική, υλική ή ηθική βλάβη. Στον ΓΚΠΔ επεξηγείται ότι η εν λόγω βλάβη μπορεί να περιλαμβάνει απώλεια του ελέγχου των προσώπων επί των δεδομένων τους προσωπικού χαρακτήρα, περιορισμό των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, βλάβη της φήμης και απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο. Μπορεί επίσης να περιλαμβάνει οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα για τα εν λόγω πρόσωπα. Μια από τις σημαντικότερες υποχρεώσεις του υπευθύνου επεξεργασίας δεδομένων είναι να αξιολογεί τους εν λόγω κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για την αντιμετώπισή τους.

7. Ως εκ τούτου, ο ΓΚΠΔ απαιτεί από τον υπεύθυνο επεξεργασίας:

---

[4] ΟΕ29, WP213, 25 Μαρτίου 2014, Γνωμοδότηση 03/2014 σχετικά με τη γνωστοποίηση παραβίασης προσωπικών δεδομένων, σ. 6, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Βλ. κατευθυντήριες γραμμές WP250, σ. 8. Επισημαίνεται ότι η παραβίαση δεδομένων μπορεί να αφορά μία ή πλείονες κατηγορίες συγχρόνως ή συνδυασμό κατηγοριών.

- να τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίσταται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα[6]·
- να γνωστοποιεί την παραβίαση δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[7]·
- να ανακοινώνει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[8].

8. Οι παραβιάσεις δεδομένων συνιστούν πρόβλημα αφ' εαυτών, αλλά ενδέχεται να είναι επίσης ενδεικτικές ενός ευάλωτου, ενδεχομένως παρωχημένου, καθεστώτος ασφάλειας των δεδομένων, καθώς και να καταδεικνύουν αδυναμίες του συστήματος οι οποίες πρέπει να αντιμετωπιστούν. Κατά κανόνα, είναι πάντοτε προτιμότερο να προλαμβάνονται οι παραβιάσεις των δεδομένων μέσω προηγούμενης προετοιμασίας, δεδομένου ότι αρκετές συνέπειές τους είναι εκ φύσεως μη αναστρέψιμες. Προκειμένου ο υπεύθυνος επεξεργασίας να μπορέσει να αξιολογήσει *πλήρως* τον κίνδυνο που ανακύπτει από παραβίαση οφειλόμενη σε κάποιου είδους επίθεση, θα πρέπει να προσδιοριστεί η βαθύτερη αιτία του ζητήματος, ώστε να εξακριβωθεί αν υφίστανται ακόμη οι ευπάθειες που προκάλεσαν το περιστατικό και αν είναι, επομένως, ακόμη εκμεταλλεύσιμες. Σε πολλές περιπτώσεις, ο υπεύθυνος επεξεργασίας είναι σε θέση να διαπιστώσει ότι το περιστατικό ενδέχεται να προκαλέσει κίνδυνο και πρέπει, επομένως, να γνωστοποιηθεί. Σε άλλες περιπτώσεις, δεν είναι απαραίτητο να αναβληθεί η γνωστοποίηση έως ότου αξιολογηθούν πλήρως ο κίνδυνος και οι συνέπειες που συνδέονται με την παραβίαση, καθώς η πλήρης αξιολόγηση κινδύνου μπορεί να πραγματοποιηθεί παράλληλα με τη γνωστοποίηση, οι δε πληροφορίες που αποκτώνται με τον τρόπο αυτό μπορούν να παρέχονται στην ΕΑ σταδιακά χωρίς αδικαιολόγητη καθυστέρηση[9].

9. Η παραβίαση θα πρέπει να γνωστοποιείται όταν ο υπεύθυνος επεξεργασίας θεωρεί ότι ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Ο υπεύθυνος επεξεργασίας θα πρέπει να διενεργεί την αξιολόγηση αυτή μόλις αποκτά γνώση της παραβίασης. Ο υπεύθυνος επεξεργασίας δεν θα πρέπει να αναμένει τη διενέργεια λεπτομερούς εγκληματολογικής έρευνας και τη λήψη (έγκαιρων) μέτρων μετριασμού προκειμένου να αξιολογήσει αν η παραβίαση των δεδομένων ενδέχεται να προκαλέσει κίνδυνο και θα πρέπει, επομένως, να γνωστοποιηθεί.

10. Εάν βάσει της αυτοαξιολόγησης του υπευθύνου επεξεργασίας, η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο, πλην όμως ο κίνδυνος επέλθει, η αρμόδια ΕΑ μπορεί να κάνει χρήση των διορθωτικών εξουσιών της και μπορεί να επιβάλει κυρώσεις.

11. Κάθε υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία θα πρέπει να διαθέτει σχέδια και διαδικασίες για τον χειρισμό ενδεχόμενων παραβιάσεων δεδομένων. Οι οργανισμοί θα πρέπει να διαθέτουν σαφείς διαύλους αναφοράς και να ορίζουν πρόσωπα υπεύθυνα για ορισμένες πτυχές της διαδικασίας ανάκτησης.

---

[6] Άρθρο 33 παράγραφος 5 του ΓΚΠΔ.

[7] Άρθρο 33 παράγραφος 1 του ΓΚΠΔ.

[8] Άρθρο 34 παράγραφος 1 του ΓΚΠΔ.

[9] Άρθρο 33 παράγραφος 4 του ΓΚΠΔ.

12. Η κατάρτιση και η ευαισθητοποίηση σε ζητήματα προστασίας δεδομένων για το προσωπικό του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, με έμφαση στη διαχείριση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα (προσδιορισμός περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα και περαιτέρω μέτρα τα οποία πρέπει να ληφθούν κ.λπ.), είναι επίσης σημαντικές για τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Η εν λόγω κατάρτιση θα πρέπει να επαναλαμβάνεται τακτικά, ανάλογα με το είδος της δραστηριότητας επεξεργασίας και το μέγεθος του υπευθύνου επεξεργασίας, με αναφορά στις πιο πρόσφατες τάσεις και προειδοποιήσεις που αντλούνται από κυβερνοεπιθέσεις ή άλλα περιστατικά ασφάλειας.

13. Η αρχή της λογοδοσίας και η έννοια της προστασίας των δεδομένων ήδη από τον σχεδιασμό θα μπορούσαν να περιλαμβάνουν ανάλυση η οποία θα χρησιμοποιηθεί σε «εγχειρίδιο χειρισμού παραβιάσεων δεδομένων προσωπικού χαρακτήρα» του υπευθύνου επεξεργασίας δεδομένων και του εκτελούντος την επεξεργασία δεδομένων, με στόχο την εξακρίβωση πραγματικών γεγονότων για κάθε πτυχή της επεξεργασίας σε κάθε σημαντικό στάδιο της διαδικασίας. Ένα τέτοιο εγχειρίδιο, καταρτισμένο εκ των προτέρων, θα αποτελεί πηγή πληροφοριών για άμεση χρήση, η οποία θα παρέχει στους υπευθύνους επεξεργασίας δεδομένων και στους εκτελούντες την επεξεργασία δεδομένων τη δυνατότητα να μετριάζουν τους κινδύνους και να εκπληρώνουν τις υποχρεώσεις τους χωρίς αδικαιολόγητη καθυστέρηση. Με τον τρόπο αυτό θα διασφαλίζεται ότι, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, τα άτομα στον οργανισμό θα γνωρίζουν τι πρέπει να πράξουν, θα είναι δε πιθανότερο να αντιμετωπιστεί το περιστατικό ταχύτερα από ό,τι θα αντιμετωπιζόταν ελλείψει μέτρων μετριασμού ή σχεδίου.

14. Μολονότι είναι εικονικές, οι περιπτώσεις που παρουσιάζονται κατωτέρω βασίζονται σε χαρακτηριστικές περιπτώσεις της συλλογικής πείρας που απέκτησαν οι ΕΑ από γνωστοποιήσεις παραβιάσεων δεδομένων. Οι παρεχόμενες αναλύσεις σχετίζονται σαφώς με τις εξεταζόμενες περιπτώσεις, με σκοπό, όμως, να παράσχουν συνδρομή στους υπεύθυνους επεξεργασίας κατά την αξιολόγηση των παραβιάσεων δεδομένων που εκείνοι αντιμετωπίζουν. Κάθε μεταβολή των περιστάσεων στις περιπτώσεις που περιγράφονται κατωτέρω μπορεί να έχει ως αποτέλεσμα διαφορετικά ή υψηλότερα επίπεδα κινδύνου και να απαιτεί, επομένως, διαφορετικά ή πρόσθετα μέτρα. Στις παρούσες κατευθυντήριες γραμμές, οι περιπτώσεις παρουσιάζονται βάσει ορισμένων κατηγοριών παραβιάσεων (π.χ. επιθέσεις λυτρισμικού). Σε κάθε περίπτωση, όταν αντιμετωπίζεται ορισμένη κατηγορία παραβιάσεων, επιβάλλεται η λήψη ορισμένων μέτρων μετριασμού. Τα εν λόγω μέτρα δεν επαναλαμβάνονται κατ' ανάγκη σε κάθε ανάλυση περίπτωσης που εμπίπτει στην ίδια κατηγορία παραβιάσεων. Στις περιπτώσεις που εμπίπτουν στην ίδια κατηγορία, επισημαίνονται μόνον οι διαφορές. Επομένως, ο αναγνώστης θα πρέπει να διαβάσει όλες τις περιπτώσεις που αφορούν συγκεκριμένη κατηγορία παραβιάσεων, ώστε να προσδιορίσει και να διακρίνει όλα τα ορθά μέτρα που πρέπει να ληφθούν.

15. Η εσωτερική τεκμηρίωση της παραβίασης είναι υποχρέωση ανεξάρτητη των κινδύνων που συνδέονται με την παραβίαση και πρέπει να διενεργείται σε κάθε περίπτωση. Σκοπός των περιπτώσεων που παρουσιάζονται κατωτέρω είναι να αποσαφηνιστεί σε κάποιον βαθμό η παραβίαση πρέπει να γνωστοποιηθεί στην ΕΑ και να ανακοινωθεί στα επηρεαζόμενα υποκείμενα των δεδομένων.

2 ΛΥΤΡΙΣΜΙΚΟ

16. Συχνή αιτία γνωστοποίησης παραβίασης δεδομένων είναι η επίθεση λυτρισμικού την οποία υπέστη ο υπεύθυνος επεξεργασίας δεδομένων. Στις περιπτώσεις αυτές, κακόβουλος κώδικας κρυπτογραφεί τα δεδομένα προσωπικού χαρακτήρα και, στη συνέχεια, ο δράστης της επίθεσης ζητεί από τον υπεύθυνο επεξεργασίας λύτρα ως αντάλλαγμα για την παροχή του κώδικα αποκρυπτογράφησης. Το συγκεκριμένο

είδος επίθεσης μπορεί συνήθως να ταξινομηθεί ως παραβίαση διαθεσιμότητας, αλλά συχνά μπορεί να υπάρξει επίσης παραβίαση απορρήτου.

2.1 ΠΕΡΙΠΤΩΣΗ αριθ. 01: Λυτρισμικό με κατάλληλα εφεδρικά αντίγραφα χωρίς απόσπαση δεδομένων

Τα συστήματα πληροφορικής μικρής κατασκευαστικής εταιρείας δέχθηκαν επίθεση λυτρισμικού και τα αποθηκευμένα στα εν λόγω συστήματα δεδομένα κρυπτογραφήθηκαν. Ο υπεύθυνος επεξεργασίας δεδομένων χρησιμοποίησε κρυπτογράφηση των αδρανών δεδομένων και, επομένως, όλα τα δεδομένα στα οποία το λυτρισμικό απέκτησε πρόσβαση αποθηκεύτηκαν σε κρυπτογραφημένη μορφή με τη χρήση προηγμένου αλγορίθμου κρυπτογράφησης. Το κλειδί αποκρυπτογράφησης δεν επηρεάστηκε κατά την επίθεση, δηλ. ο δράστης της επίθεσης δεν μπόρεσε ούτε να αποκτήσει πρόσβαση σε αυτό ούτε να το χρησιμοποιήσει έμμεσα. Επομένως, ο δράστης της επίθεσης απέκτησε πρόσβαση μόνο σε κρυπτογραφημένα δεδομένα προσωπικού χαρακτήρα. Συγκεκριμένα, δεν επηρεάστηκαν ούτε το σύστημα ηλεκτρονικού ταχυδρομείου της εταιρείας ούτε οποιαδήποτε συστήματα-πελάτες που χρησιμοποιούνται για την πρόσβαση σε αυτό. Η εταιρεία χρησιμοποιεί την εμπειρογνωσία εξωτερικής εταιρείας κυβερνοασφάλειας για τη διερεύνηση του περιστατικού. Υπάρχουν διαθέσιμα αρχεία καταγραφής για τον εντοπισμό όλων των ροών δεδομένων που εξέρχονται από την εταιρεία (συμπεριλαμβανομένων των εξερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου). Μετά την ανάλυση των αρχείων καταγραφής και των στοιχείων που συνέλεξαν τα συστήματα ανίχνευσης που διαθέτει η εταιρεία, η εσωτερική έρευνα, με τη στήριξη της εξωτερικής εταιρείας κυβερνοασφάλειας, κατέληξε *μετά βεβαιότητας* στο συμπέρασμα ότι ο δράστης κατάφερε μόνο να κρυπτογραφήσει δεδομένα, χωρίς να τα αποσπάσει. Τα αρχεία καταγραφής δείχνουν ότι δεν υπήρξε ροή εξερχόμενων δεδομένων κατά το χρονικό πλαίσιο της επίθεσης. Τα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση αφορούν πελάτες και υπαλλήλους της εταιρείας, συνολικά μερικές δεκάδες φυσικά πρόσωπα. Υπήρχε άμεσα διαθέσιμο εφεδρικό αντίγραφο και, λίγες ώρες μετά την επίθεση, τα δεδομένα είχαν επαναφερθεί. Η παραβίαση δεν είχε οποιαδήποτε συνέπεια στην καθημερινή λειτουργία του υπευθύνου επεξεργασίας. Δεν υπήρξαν καθυστερήσεις στις πληρωμές υπαλλήλων ή στον χειρισμό αιτημάτων πελατών.

17. Στην παρούσα περίπτωση, συντρέχουν τα ακόλουθα στοιχεία του ορισμού της «παραβίασης δεδομένων προσωπικού χαρακτήρα»: παραβίαση της ασφάλειας οδήγησε σε παράνομη μεταβολή και άνευ άδειας πρόσβαση σε αποθηκευμένα δεδομένα προσωπικού χαρακτήρα.

2.1.1 ΠΕΡΙΠΤΩΣΗ αριθ. 01 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

18. Όπως συμβαίνει με κάθε κίνδυνο που θέτουν εξωτερικοί παράγοντες, η πιθανότητα επιτυχίας επίθεσης λυτρισμικού μπορεί να μειωθεί σημαντικά με την αύξηση της ασφάλειας του περιβάλλοντος ελέγχου των δεδομένων. Η πλειονότητα των σχετικών παραβιάσεων μπορούν να αποφευχθούν μέσω διασφάλισης της λήψης κατάλληλων οργανωτικών, υλικών και τεχνολογικών μέτρων ασφάλειας. Παραδείγματα τέτοιων μέτρων είναι η κατάλληλη διαχείριση διορθωτικών προγραμμάτων και η χρήση κατάλληλου συστήματος ανίχνευσης κακόβουλου λογισμικού. Η ύπαρξη κατάλληλων και χωριστών εφεδρικών αντιγράφων θα συμβάλει στον μετριασμό των συνεπειών τυχόν επιτυχημένης επίθεσης. Επιπλέον, η ύπαρξη προγράμματος εκπαίδευσης, κατάρτισης και ευαισθητοποίησης σε θέματα ασφάλειας, για τους υπαλλήλους, θα συμβάλει στην πρόληψη και την αναγνώριση του συγκεκριμένου είδους επίθεσης. (Κατάλογος συνιστώμενων μέτρων παρέχεται στο σημείο 2.5.) Ιδιαίτερα σημαντικό μέτρο είναι η κατάλληλη διαχείριση διορθωτικών προγραμμάτων, η οποία διασφαλίζει ότι όλα τα συστήματα είναι επικαιροποιημένα και ότι όλες οι γνωστές ευπάθειες των χρησιμοποιούμενων συστημάτων αντιμετωπίζονται, καθώς οι περισσότερες επιθέσεις λυτρισμικού εκμεταλλεύονται γνωστές ευπάθειες.

19. Κατά την αξιολόγηση των κινδύνων, ο υπεύθυνος επεξεργασίας θα πρέπει να διερευνήσει την παραβίαση και να προσδιορίσει το είδος του κακόβουλου κώδικα προκειμένου να κατανοήσει τις ενδεχόμενες συνέπειες της επίθεσης. Ένας από τους κινδύνους που πρέπει να τα εξεταστούν είναι ο κίνδυνος απόσπασης δεδομένων χωρίς να αφεθούν ίχνη στα αρχεία καταγραφής των συστημάτων.

20. Στο παρόν παράδειγμα, ο δράστης της επίθεσης απέκτησε πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, το δε απόρρητο του κρυπτογραφημένου κειμένου που περιέχει δεδομένα προσωπικού χαρακτήρα σε κρυπτογραφημένη μορφή επηρεάστηκε. Ωστόσο, ο δράστης δεν μπορεί να διαβάσει ούτε να χρησιμοποιήσει, τουλάχιστον προς το παρόν, δεδομένα που ενδεχομένως αποσπάστηκαν. Η τεχνική κρυπτογράφησης που χρησιμοποιεί ο υπεύθυνος επεξεργασίας δεδομένων ανταποκρίνεται στην τεχνολογία αιχμής. Το κλειδί αποκρυπτογράφησης δεν επηρεάστηκε και θεωρείται ότι δεν μπορεί να προσδιοριστεί με άλλο τρόπο. Ως εκ τούτου, οι κίνδυνοι για το απόρρητο των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων μειώνονται στον ελάχιστο βαθμό, εφόσον η πρόοδος της κρυπτανάλυσης δεν καταστήσει καταληπτά στο μέλλον τα κρυπτογραφημένα δεδομένα.

21. Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να εξετάσει τους κινδύνους που συνεπάγεται η παραβίαση για τα φυσικά πρόσωπα[10]. Στην προκειμένη περίπτωση, φαίνεται ότι οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων είναι αποτέλεσμα της μη διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα και ότι το απόρρητο των δεδομένων προσωπικού χαρακτήρα δεν επηρεάστηκε[11]. Στο παρόν παράδειγμα, οι δυσμενείς συνέπειες της παραβίασης μετριάστηκαν αρκετά γρήγορα μετά την παραβίαση. Η ύπαρξη κατάλληλου συστήματος εφεδρικών αντιγράφων[12] καθιστά τις συνέπειες της παραβίασης λιγότερο σοβαρές και, στην προκειμένη περίπτωση, ο υπεύθυνος επεξεργασίας μπόρεσε να κάνει αποτελεσματική χρήση του εν λόγω συστήματος.

22. Όσον αφορά τη σοβαρότητα των συνεπειών για τα υποκείμενα των δεδομένων, προσδιορίστηκαν μόνο ήσσονος σημασίας συνέπειες, δεδομένου ότι τα επηρεαζόμενα δεδομένα επαναφέρθηκαν εντός λίγων

---

[10] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. ΟΕ29 «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία "ενδέχεται να επιφέρει υψηλό κίνδυνο" για τους σκοπούς του κανονισμού 2016/679», WP248 rev. 01, οι οποίες εγκρίθηκαν από το ΕΣΠΔ, https://ec.europa.eu/newsroom/article29/items/611236, σ. 10.

[11] Από τεχνικής απόψεως, η κρυπτογράφηση δεδομένων θα περιλαμβάνει την «πρόσβαση» στα αρχικά δεδομένα και, στην περίπτωση λυτρισμικού, τη διαγραφή των αρχικών δεδομένων – για την κρυπτογράφηση και την αφαίρεση των αρχικών δεδομένων απαιτείται πρόσβαση στα δεδομένα μέσω κώδικα λυτρισμικού. Ο δράστης της επίθεσης ενδέχεται να λάβει αντίγραφο των πρωτότυπων αρχείων πριν από τη διαγραφή, αλλά τα δεδομένα προσωπικού χαρακτήρα δεν εξάγονται πάντοτε. Καθώς προχωρά η έρευνα του υπευθύνου επεξεργασίας δεδομένων, ενδέχεται να ανακύψουν νέες πληροφορίες που θα μεταβάλουν την αξιολόγηση αυτή. Πρόσβαση η οποία έχει ως αποτέλεσμα παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση δεδομένων προσωπικού χαρακτήρα ή κίνδυνο ασφάλειας για το υποκείμενο των δεδομένων, ακόμη και χωρίς ερμηνεία των δεδομένων, μπορεί να είναι εξίσου σοβαρή με την πρόσβαση με ερμηνεία στα δεδομένα προσωπικού χαρακτήρα.

[12] Οι διαδικασίες εφεδρικών αντιγράφων θα πρέπει να είναι δομημένες, συνεκτικές και επαναλήψιμες. Παραδείγματα διαδικασιών εφεδρικών αντιγράφων είναι η μέθοδος 3-2-1 και η μέθοδος διαδοχικών γενεών. Κάθε μέθοδος θα πρέπει να ελέγχεται πάντοτε όσον αφορά την αποτελεσματικότητά της για την κάλυψη και τον χρόνο επαναφοράς των δεδομένων. Οι έλεγχοι θα πρέπει επίσης να επαναλαμβάνονται σε τακτά χρονικά διαστήματα, ιδίως δε όταν επέρχονται αλλαγές στη διαδικασία επεξεργασίας ή στις περιστάσεις της, προκειμένου να διασφαλίζεται η ακεραιότητα του συστήματος.

ωρών, η δε παραβίαση δεν είχε οποιαδήποτε συνέπεια στην καθημερινή λειτουργία του υπευθύνου επεξεργασίας και δεν είχε σημαντικές συνέπειες στα υποκείμενα των δεδομένων (π.χ. πληρωμές υπαλλήλων ή χειρισμός αιτημάτων πελατών).

2.1.2 ΠΕΡΙΠΤΩΣΗ αριθ. 01 – Μετριασμός και υποχρεώσεις

23. Χωρίς εφεδρικά αντίγραφα, ο υπεύθυνος επεξεργασίας μπορεί να λάβει λιγοστά μόνο μέτρα για τη θεραπεία της απώλειας δεδομένων προσωπικού χαρακτήρα, τα δε δεδομένα πρέπει να συλλεχθούν εκ νέου. Ωστόσο, στην προκειμένη περίπτωση, οι συνέπειες της επίθεσης περιορίστηκαν αποτελεσματικά μέσω της επαναφοράς όλων των συστημάτων που επηρεάστηκαν σε αρχική κατάσταση απαλλαγμένη από κακόβουλο κώδικα, της αντιμετώπισης των ευπαθειών και της επαναφοράς των δεδομένων που επηρεάστηκαν εντός σύντομου χρονικού διαστήματος μετά την επίθεση. Χωρίς εφεδρικά αντίγραφα, τα δεδομένα χάνονται, η δε σοβαρότητα μπορεί να αυξηθεί λόγω ενδεχόμενων κινδύνων ή συνεπειών για τα φυσικά πρόσωπα.

24. Ο έγκαιρος χαρακτήρας της πραγματικής επαναφοράς δεδομένων από τα άμεσα διαθέσιμα εφεδρικά αρχεία είναι κρίσιμος παράγοντας για την ανάλυση της παραβίασης. Ο προσδιορισμός κατάλληλου χρονικού πλαισίου για την επαναφορά των δεδομένων που επηρεάστηκαν εξαρτάται από τις μοναδικές περιστάσεις της εξεταζόμενης παραβίασης. Κατά τον ΓΚΠΔ, η παραβίαση δεδομένων προσωπικού χαρακτήρα γνωστοποιείται αμελλητί και, αν είναι δυνατό, εντός 72 ωρών. Επομένως, μπορεί να διαπιστωθεί ότι η υπέρβαση του ορίου των 72 ωρών δεν συνιστάται σε καμία περίπτωση, πλην όμως, σε περιπτώσεις υψηλού κινδύνου, ακόμη και η τήρηση της εν λόγω προθεσμίας μπορεί να θεωρείται μη ικανοποιητική.

25. Στην προκειμένη περίπτωση, κατόπιν διεξαγωγής λεπτομερούς διαδικασίας εκτίμησης αντικτύπου και αντιμετώπισης περιστατικού, ο υπεύθυνος επεξεργασίας διαπίστωσε ότι η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ότι, επομένως, δεν απαιτείται ανακοίνωση στα υποκείμενα των δεδομένων, καθώς και ότι η παραβίαση δεν απαιτεί γνωστοποίηση στην ΕΑ. Ωστόσο, όπως κάθε παραβίαση δεδομένων, θα πρέπει να τεκμηριωθεί σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ. Ο οργανισμός ενδέχεται να πρέπει (ή να υποχρεωθεί μεταγενέστερα από την ΕΑ) να επικαιροποιήσει και να επανορθώσει τα οργανωτικά και τεχνικά μέτρα και τις διαδικασίες για τον χειρισμό της ασφάλειας των δεδομένων προσωπικού χαρακτήρα και τον μετριασμό των κινδύνων. Στο πλαίσιο της εν λόγω επικαιροποίησης και επανόρθωσης, ο οργανισμός θα πρέπει να διερευνήσει διεξοδικά την παραβίαση και να προσδιορίσει τα αίτια και τις μεθόδους που χρησιμοποίησε ο δράστης για την πρόληψη παρόμοιων συμβάντων στο μέλλον.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	X	X

2.2 ΠΕΡΙΠΤΩΣΗ αριθ. 02: Λυτρισμικό χωρίς κατάλληλα εφεδρικά αντίγραφα

Ένας από τους υπολογιστές που χρησιμοποιεί γεωργική εταιρεία δέχθηκε επίθεση λυτρισμικού στην οποία ο δράστης της επίθεσης κρυπτογράφησε τα δεδομένα της. Η εταιρεία χρησιμοποιεί την εμπειρογνωσία εξωτερικής εταιρείας κυβερνοασφάλειας για την παρακολούθηση του δικτύου της. Υπάρχουν διαθέσιμα αρχεία καταγραφής για τον εντοπισμό όλων των ροών δεδομένων που εξέρχονται από την εταιρεία (συμπεριλαμβανομένων των εξερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου). Μετά την ανάλυση των αρχείων καταγραφής και των στοιχείων που συνέλεξαν τα άλλα συστήματα ανίχνευσης, η εσωτερική έρευνα, με τη βοήθεια της εταιρείας κυβερνοασφάλειας, κατέληξε στο συμπέρασμα ότι ο δράστης κατάφερε μόνο να κρυπτογραφήσει τα δεδομένα, χωρίς να τα αποσπάσει. Τα αρχεία καταγραφής δείχνουν ότι δεν υπήρξε ροή εξερχόμενων δεδομένων κατά το χρονικό πλαίσιο της επίθεσης. Τα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση αφορούν τους υπαλλήλους και τους πελάτες της εταιρείας, συνολικά μερικές δεκάδες φυσικά πρόσωπα. Δεν επηρεάστηκαν ειδικές κατηγορίες δεδομένων. Δεν υπήρχαν διαθέσιμα εφεδρικά αρχεία σε ηλεκτρονική μορφή. Η πλειονότητα των δεδομένων επαναφέρθηκαν από έγχαρτα εφεδρικά αρχεία. Για την επαναφορά των δεδομένων απαιτήθηκαν 5 εργάσιμες ημέρες, με αποτέλεσμα μικρές καθυστερήσεις στην παράδοση παραγγελιών σε πελάτες.

2.2.1 ΠΕΡΙΠΤΩΣΗ αριθ. 02 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

26. Ο υπεύθυνος επεξεργασίας δεδομένων θα έπρεπε να έχει λάβει τα ίδια προηγούμενα μέτρα με εκείνα που αναφέρονται στο τμήμα 2.1 και στην ενότητα 2.9. Η σημαντικότερη διαφορά σε σχέση με την προηγούμενη περίπτωση είναι η έλλειψη ηλεκτρονικών εφεδρικών αντιγράφων και η μη κρυπτογράφηση των αδρανών δεδομένων. Η διαφορά αυτή συνεπάγεται κρίσιμες διαφοροποιήσεις στα επακόλουθα βήματα.

27. Κατά την αξιολόγηση των κινδύνων, ο υπεύθυνος επεξεργασίας θα πρέπει να διερευνήσει τη μέθοδο διείσδυσης και να προσδιορίσει το είδος του κακόβουλου κώδικα προκειμένου να κατανοήσει τις ενδεχόμενες συνέπειες της επίθεσης. Στο παρόν παράδειγμα, το λυτρισμικό κρυπτογράφησε τα δεδομένα προσωπικού χαρακτήρα χωρίς να τα αποσπάσει. Ως εκ τούτου, φαίνεται ότι οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων είναι αποτέλεσμα της μη διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα και ότι το απόρρητο των δεδομένων προσωπικού χαρακτήρα δεν επηρεάστηκε. Η διεξοδική εξέταση των αρχείων καταγραφής του τείχους προστασίας και των συνεπειών της είναι απαραίτητη για την εξακρίβωση του κινδύνου. Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να παρουσιάσει τα πραγματικά ευρήματα των εν λόγω ερευνών, κατόπιν αιτήματος.

28. Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να έχει υπόψη ότι, εάν η επίθεση έχει πιο προηγμένο χαρακτήρα, το κακόβουλο λογισμικό διαθέτει λειτουργικότητα επεξεργασίας των αρχείων καταγραφής και αφαίρεσης του ίχνους. Επομένως, δεδομένου ότι τα αρχεία καταγραφής δεν διαβιβάζονται ούτε αναπαράγονται σε κεντρικό διακομιστή αρχείων καταγραφής, ακόμη και μετά τη διεξοδική έρευνα στο πλαίσιο της οποίας διαπιστώθηκε ότι ο δράστης της επίθεσης δεν απέσπασε τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας δεδομένων δεν μπορεί να ισχυριστεί ότι η απουσία καταχώρισης αποδεικνύει τη μη απόσπαση δεδομένων και, ως εκ τούτου, το ενδεχόμενο παραβίασης απορρήτου δεν μπορεί να αποκλειστεί παντελώς.

29. Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να αξιολογήσει τους κινδύνους της εν λόγω παραβίασης[13], εάν ο δράστης της επίθεσης απέκτησε πρόσβαση στα δεδομένα. Κατά την αξιολόγηση κινδύνου, ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει επίσης να λάβει υπόψη τη φύση, την ευαισθησία, τον όγκο και το πλαίσιο των δεδομένων προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση. Στην προκειμένη περίπτωση, δεν επηρεάστηκαν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, η δε ποσότητα των δεδομένων που παραβιάστηκαν και ο αριθμός υποκειμένων δεδομένων που επηρεάστηκαν είναι μικροί.

30. Η συλλογή ακριβών πληροφοριών σχετικά με την άνευ άδειας πρόσβαση είναι καθοριστική για τη διαπίστωση του επιπέδου κινδύνου και την πρόληψη νέας ή συνεχιζόμενης επίθεσης. Σε περίπτωση αντιγραφής των δεδομένων από τη βάση δεδομένων, αυτό θα συνιστούσε προφανώς παράγοντα αύξησης του κινδύνου. Όταν υπάρχουν αμφιβολίες σχετικά με τις λεπτομέρειες της παράνομης πρόσβασης, θα πρέπει να εξετάζεται το χειρότερο σενάριο και ο κίνδυνος θα πρέπει να αξιολογείται ανάλογα.

31. Η έλλειψη εφεδρικής βάσης δεδομένων μπορεί να θεωρηθεί παράγοντας αύξησης του κινδύνου, ανάλογα με τη σοβαρότητα των συνεπειών που συνεπάγεται για τα υποκείμενα των δεδομένων η μη διαθεσιμότητα των δεδομένων.

2.2.2 ΠΕΡΙΠΤΩΣΗ αριθ. 02 – Μετριασμός και υποχρεώσεις

32. Χωρίς εφεδρικά αντίγραφα, ο υπεύθυνος επεξεργασίας μπορεί να λάβει λιγοστά μόνο μέτρα για την επανόρθωση της απώλειας δεδομένων προσωπικού χαρακτήρα, τα δε δεδομένα πρέπει να συλλεχθούν εκ νέου, εκτός εάν υπάρχει διαθέσιμη κάποια άλλη πηγή (π.χ. ηλεκτρονικά μηνύματα επιβεβαίωσης παραγγελιών). Χωρίς εφεδρικά αντίγραφα, τα δεδομένα μπορεί να χαθούν και η σοβαρότητα θα εξαρτάται από τον αντίκτυπο για τα φυσικά πρόσωπα.

33. Η επαναφορά των δεδομένων δεν αναμένεται ότι θα είναι υπερβολικά προβληματική[14], εάν τα δεδομένα είναι ακόμη διαθέσιμα σε έγχαρτη μορφή, πλην όμως, λόγω της έλλειψης ηλεκτρονικής εφεδρικής βάσης δεδομένων, η γνωστοποίηση στην ΕΑ θεωρείται αναγκαία, καθώς η επαναφορά των δεδομένων απαίτησε κάποιο χρόνο και μπορεί να προκαλέσει κάποιες καθυστερήσεις στην παράδοση παραγγελιών σε πελάτες και μεγάλη ποσότητα μεταδεδομένων (π.χ. αρχεία καταγραφής, χρονοσφραγίδες) ενδέχεται να μην είναι ανακτήσιμα.

34. Η ενημέρωση των υποκειμένων των δεδομένων σχετικά με την παραβίαση μπορεί επίσης να εξαρτάται από το χρονικό διάστημα κατά το οποίο τα δεδομένα προσωπικού χαρακτήρα δεν ήταν διαθέσιμα και τις δυσχέρειες που το γεγονός αυτό μπορεί να συνεπάγεται για τη λειτουργία του υπευθύνου επεξεργασίας (π.χ. καθυστερήσεις στην πραγματοποίηση πληρωμών υπαλλήλων). Δεδομένου ότι οι εν λόγω καθυστερήσεις σε πληρωμές και παραδόσεις μπορεί να συνεπάγονται οικονομική ζημία για τα φυσικά πρόσωπα των οποίων τα δεδομένα παραβιάστηκαν, μπορεί επίσης να υποστηριχθεί ότι η παραβίαση ενδέχεται να επιφέρει υψηλό κίνδυνο. Ενδέχεται επίσης να είναι αναπόφευκτη η ενημέρωση των

[13] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

[14] Αυτό θα εξαρτηθεί από την πολυπλοκότητα και τη δομή των δεδομένων προσωπικού χαρακτήρα. Στα πιο πολύπλοκα σενάρια, η αποκατάσταση της ακεραιότητας των δεδομένων και της συνέπειας με τα μεταδεδομένα, η διασφάλιση ορθών σχέσεων εντός των δομών των δεδομένων και ο έλεγχος της ακρίβειας των δεδομένων μπορεί να απαιτούν σημαντικούς πόρους και προσπάθειες.

υποκειμένων των δεδομένων, εάν απαιτείται η συμβολή τους για την επαναφορά των κρυπτογραφημένων δεδομένων.

35. Η παρούσα περίπτωση αποτελεί παράδειγμα επίθεσης λυτρισμικού η οποία ενέχει κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ο οποίος δεν είναι ωστόσο υψηλός κίνδυνος. Η παραβίαση θα πρέπει να τεκμηριωθεί σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ και να γνωστοποιηθεί στην ΕΑ σύμφωνα με το άρθρο 33 παράγραφος 1 του ΓΚΠΔ. Ο οργανισμός ενδέχεται να πρέπει (ή να υποχρεωθεί από την ΕΑ) να επικαιροποιήσει και να επανορθώσει τα οργανωτικά και τεχνικά μέτρα και τις διαδικασίες για τον χειρισμό της ασφάλειας των δεδομένων προσωπικού χαρακτήρα και τον μετριασμό των κινδύνων.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	X

2.3 ΠΕΡΙΠΤΩΣΗ αριθ. 03: Λυτρισμικό με εφεδρικά αρχεία χωρίς απόσπαση δεδομένων σε νοσοκομείο

Το σύστημα πληροφοριών νοσοκομείου / κέντρου υγειονομικής περίθαλψης δέχθηκε επίθεση λυτρισμικού, στην οποία ο δράστης κρυπτογράφησε σημαντικό μέρος των δεδομένων του. Η εταιρεία χρησιμοποιεί την εμπειρογνωσία εξωτερικής εταιρείας κυβερνοασφάλειας για την παρακολούθηση του δικτύου της. Υπάρχουν διαθέσιμα αρχεία καταγραφής για τον εντοπισμό όλων των ροών δεδομένων που εξέρχονται από την εταιρεία (συμπεριλαμβανομένων των εξερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου). Μετά την ανάλυση των αρχείων καταγραφής και των στοιχείων που συνέλεξαν τα άλλα συστήματα ανίχνευσης, η εσωτερική έρευνα, με τη βοήθεια της εταιρείας κυβερνοασφάλειας, κατέληξε στο συμπέρασμα ότι ο δράστης κατάφερε μόνο να κρυπτογραφήσει τα δεδομένα χωρίς να τα αποσπάσει. Τα αρχεία καταγραφής δείχνουν ότι δεν υπήρξε ροή εξερχόμενων δεδομένων κατά το χρονικό πλαίσιο της επίθεσης. Τα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση αφορούν τους υπαλλήλους και τους ασθενείς, δηλ. χιλιάδες φυσικά πρόσωπα. Υπήρχαν διαθέσιμα εφεδρικά αρχεία σε ηλεκτρονική μορφή. Η πλειονότητα των δεδομένων επαναφέρθηκε, αλλά η σχετική διαδικασία διήρκεσε 2 εργάσιμες ημέρες και είχε ως αποτέλεσμα σημαντικές καθυστερήσεις στη θεραπεία των ασθενών, με ματαίωση/αναβολή χειρουργικών επεμβάσεων, και τη μείωση του επιπέδου εξυπηρέτησης λόγω της μη διαθεσιμότητας των συστημάτων.

2.3.1 ΠΕΡΙΠΤΩΣΗ αριθ. 03 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

36. Ο υπεύθυνος επεξεργασίας δεδομένων θα έπρεπε να έχει λάβει τα ίδια προηγούμενα μέτρα με εκείνα που αναφέρονται στο τμήμα 2.1 και στην ενότητα 2.5. Η σημαντική διαφορά σε σχέση με την προηγούμενη περίπτωση είναι η υψηλή σοβαρότητα των συνεπειών για σημαντικό τμήμα των υποκειμένων των δεδομένων[15].

37. Η ποσότητα των δεδομένων που παραβιάστηκαν και ο αριθμός των επηρεαζόμενων υποκειμένων των δεδομένων είναι υψηλοί, καθώς τα νοσοκομεία επεξεργάζονται συνήθως μεγάλες ποσότητες δεδομένων.

[15] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

Η μη διαθεσιμότητα των δεδομένων έχει μεγάλο αντίκτυπο σε σημαντικό τμήμα των υποκειμένων των δεδομένων. Επιπλέον, υπάρχει υπολειπόμενος κίνδυνος υψηλής σοβαρότητας για το απόρρητο των δεδομένων των ασθενών.

38. Το είδος της παραβίασης, η φύση, η ευαισθησία και ο όγκος των επηρεαζόμενων δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της παραβίασης είναι σημαντικά. Μολονότι υπήρχαν εφεδρικά αρχεία των δεδομένων και τα δεδομένα μπορούν να επαναφερθούν σε μερικές ημέρες, εξακολουθεί να υφίσταται υψηλός κίνδυνος λόγω της σοβαρότητας των συνεπειών για τα υποκείμενα των δεδομένων, ως αποτέλεσμα της μη διαθεσιμότητας των δεδομένων κατά τον χρόνο της επίθεσης και τις επόμενες ημέρες.

2.3.2 ΠΕΡΙΠΤΩΣΗ αριθ. 03 – Μετριασμός και υποχρεώσεις

39. Η γνωστοποίηση στην ΕΑ θεωρείται αναγκαία, καθώς η παραβίαση αφορά ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα και η επαναφορά των δεδομένων μπορεί να απαιτήσει μεγάλο χρονικό διάστημα, με αποτέλεσμα σημαντικές καθυστερήσεις στην περίθαλψη των ασθενών. Η ενημέρωση των υποκειμένων των δεδομένων σχετικά με την παραβίαση είναι αναγκαία λόγω του αντικτύπου για τους ασθενείς, ακόμη και μετά την επαναφορά των κρυπτογραφημένων δεδομένων. Παρότι κρυπτογραφήθηκαν δεδομένα που αφορούν όλους τους ασθενείς που νοσηλεύθηκαν στο νοσοκομείο κατά τα τελευταία έτη, επηρεάστηκαν μόνο οι ασθενείς οι οποίοι επρόκειτο να νοσηλευθούν στο νοσοκομείο στο διάστημα κατά το οποίο το σύστημα πληροφορικής δεν ήταν διαθέσιμο. Ο υπεύθυνος επεξεργασίας θα πρέπει να ανακοινώσει απευθείας στους εν λόγω ασθενείς την παραβίαση των δεδομένων. Η απευθείας ανακοίνωση στους λοιπούς ασθενείς, εκ των οποίων ορισμένοι μπορεί να μην νοσηλεύθηκαν στο νοσοκομείο επί περισσότερα από είκοσι έτη, ενδέχεται να μην απαιτείται βάσει της εξαίρεσης που προβλέπεται στο άρθρο 34 παράγραφος 3 στοιχείο γ) του ΓΚΠΔ. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση[16] ή λαμβάνεται παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο. Εν προκειμένω, το νοσοκομείο θα πρέπει να δημοσιοποιήσει την επίθεση λυτρισμικού και τις συνέπειές της.

40. Η παρούσα περίπτωση αποτελεί παράδειγμα επίθεσης λυτρισμικού η οποία ενέχει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Η παραβίαση θα πρέπει να τεκμηριωθεί σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ, να γνωστοποιηθεί στην ΕΑ σύμφωνα με το άρθρο 33 παράγραφος 1 του ΓΚΠΔ και να ανακοινωθεί στα υποκείμενα των δεδομένων σύμφωνα με το άρθρο 34 παράγραφος 1 του ΓΚΠΔ. Ο οργανισμός πρέπει επίσης να επικαιροποιήσει και να επανορθώσει τα οργανωτικά και τεχνικά μέτρα και τις διαδικασίες για τον χειρισμό της ασφάλειας των δεδομένων προσωπικού χαρακτήρα και τον μετριασμό των κινδύνων.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

[16] Κατά την αιτιολογική σκέψη 86 του ΓΚΠΔ, «*[ο]ι ανακοινώσεις αυτές στα υποκείμενα των δεδομένων θα πρέπει να πραγματοποιούνται το συντομότερο δυνατόν, σε στενή συνεργασία με την ελεγκτική αρχή, τηρώντας την καθοδήγηση που παρέχεται από αυτήν ή άλλες σχετικές αρχές, όπως αρχές επιβολής του νόμου. Για παράδειγμα, η ανάγκη να μετριαστεί άμεσος κίνδυνος ζημίας θα απαιτούσε την άμεση ανακοίνωση στα υποκείμενα των δεδομένων, ενώ η αναγκαιότητα εφαρμογής κατάλληλων μέτρων κατά συνεχών ή παρόμοιων παραβιάσεων δεδομένων προσωπικού χαρακτήρα μπορεί να δικαιολογεί περισσότερο χρόνο για την ανακοίνωση*».

2.4 ΠΕΡΙΠΤΩΣΗ αριθ. 04: Λυτρισμικό χωρίς εφεδρικά αρχεία με απόσπαση δεδομένων

Ο διακομιστής εταιρείας δημόσιων μεταφορών δέχθηκε επίθεση λυτρισμικού στην οποία ο δράστης της επίθεσης κρυπτογράφησε τα δεδομένα του. Σύμφωνα με τα ευρήματα της εσωτερικής έρευνας, ο δράστης όχι μόνο κρυπτογράφησε τα δεδομένα αλλά επίσης τα απέσπασε. Τα δεδομένα που παραβιάστηκαν ήταν τα δεδομένα προσωπικού χαρακτήρα πελατών και υπαλλήλων καθώς και αρκετών χιλιάδων ατόμων που κάνουν χρήση των υπηρεσιών της εταιρείας (π.χ. μέσω της ηλεκτρονικής αγοράς εισιτηρίων). Πέραν των βασικών δεδομένων ταυτότητας, η παραβίαση αφορά αριθμούς δελτίων ταυτότητας και οικονομικά στοιχεία, όπως στοιχεία πιστωτικών καρτών. Υπήρχε εφεδρική βάση δεδομένων, αλλά ο δράστης της επίθεσης κατάφερε επίσης να την κρυπτογραφήσει.

2.4.1 ΠΕΡΙΠΤΩΣΗ αριθ. 04 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

41. Ο υπεύθυνος επεξεργασίας δεδομένων θα έπρεπε να έχει λάβει τα ίδια προηγούμενα μέτρα με εκείνα που αναφέρονται στο τμήμα 2.1 και στην ενότητα 2.5. Μολονότι υπήρχαν εφεδρικά αντίγραφα, επηρεάστηκαν και αυτά από την επίθεση. Η κατάσταση αυτή δημιουργεί αφ' εαυτής ερωτήματα σχετικά με την ποιότητα των προηγούμενων μέτρων ασφάλειας των πληροφοριακών συστημάτων που έλαβε ο υπεύθυνος επεξεργασίας και θα πρέπει να διερευνηθεί περαιτέρω, δεδομένου ότι, σε ένα καλά σχεδιασμένο εφεδρικό σύστημα, πολλαπλά εφεδρικά αντίγραφα πρέπει να αποθηκεύονται με ασφαλή τρόπο, χωρίς πρόσβαση από το βασικό σύστημα, διαφορετικά μπορεί να επηρεαστούν στο πλαίσιο της ίδιας επίθεσης. Επιπλέον, οι επιθέσεις λυτρισμικού μπορεί να μην γίνουν αντιληπτές για περισσότερες ημέρες, με αποτέλεσμα να συνεχίζεται η αργή κρυπτογράφηση δεδομένων που χρησιμοποιούνται σπάνια. Αυτό μπορεί να καταστήσει περιττά τα πολλαπλά αντίγραφα ασφάλειας και, επομένως, θα πρέπει επίσης να λαμβάνονται περιοδικά αντίγραφα ασφάλειας τα οποία θα απομονώνονται. Αυτό θα αυξήσει την πιθανότητα ανάκτησης, μολονότι με αυξημένη απώλεια δεδομένων.

42. Η παρούσα παραβίαση αφορά όχι μόνο τη διαθεσιμότητα δεδομένων, αλλά και το απόρρητο, καθώς ο δράστης της επίθεσης μπορεί να μετέβαλε και/ή να αντέγραψε δεδομένα από τον διακομιστή. Ως εκ τούτου, το είδος της παραβίασης επιφέρει υψηλό κίνδυνο[17].

43. Η φύση, η ευαισθησία και ο όγκος των δεδομένων προσωπικού χαρακτήρα αυξάνουν περαιτέρω τους κινδύνους, καθώς ο αριθμός των επηρεαζόμενων φυσικών προσώπων είναι υψηλός, όπως και η συνολική ποσότητα των επηρεαζόμενων δεδομένων προσωπικού χαρακτήρα. Πέραν των βασικών δεδομένων ταυτότητας, η παραβίαση αφορά επίσης έγγραφα ταυτότητας και οικονομικά στοιχεία, όπως στοιχεία πιστωτικών καρτών. Παραβίαση δεδομένων η οποία αφορά τα συγκεκριμένα είδη δεδομένων ενέχει υψηλό κίνδυνο και, εφόσον υποβληθούν σε επεξεργασία από κοινού, τα δεδομένα μπορούν να χρησιμοποιηθούν, μεταξύ άλλων, για υποκλοπή ταυτότητας ή απάτη.

44. Λόγω ελαττωματικής λογικής του διακομιστή ή ελαττωματικών οργανωτικών ελέγχων, τα εφεδρικά αρχεία επηρεάστηκαν από το λυτρισμικό, με αποτέλεσμα να εμποδιστεί η επαναφορά των δεδομένων και να αυξηθεί ο κίνδυνος.

45. Η παρούσα παραβίαση δεδομένων ενέχει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, καθώς θα μπορούσε να προκαλέσει τόσο υλική (π.χ. οικονομική ζημία, καθώς επηρεάστηκαν

[17] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

στοιχεία πιστωτικών καρτών) όσο και ηθική βλάβη (π.χ. υποκλοπή ταυτότητας ή απάτη, καθώς επηρεάστηκαν στοιχεία δελτίων ταυτότητας).

2.4.2 ΠΕΡΙΠΤΩΣΗ αριθ. 04 – Μετριασμός και υποχρεώσεις

46. Η ανακοίνωση της παραβίασης στα υποκείμενα των δεδομένων είναι απαραίτητη, ώστε να μπορέσουν να λάβουν τα αναγκαία μέτρα για την αποφυγή υλικής βλάβης (π.χ. απενεργοποίηση των πιστωτικών καρτών τους).

47. Πέραν της τεκμηρίωσης της παραβίασης σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ, στην προκειμένη περίπτωση είναι επίσης υποχρεωτική η γνωστοποίηση στην ΕΑ (άρθρο 33 παράγραφος 1 του ΓΚΠΔ), ο δε υπεύθυνος επεξεργασίας υποχρεούται επίσης να ανακοινώσει την παραβίαση στα υποκείμενα των δεδομένων (άρθρο 34 παράγραφος 1 του ΓΚΠΔ). Η ανακοίνωση στα υποκείμενα των δεδομένων μπορεί να πραγματοποιηθεί σε ατομική βάση, αλλά, για τα φυσικά πρόσωπα για τα οποία δεν διαθέτει στοιχεία επικοινωνίας, ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί σε δημόσια ανακοίνωση, υπό τον όρο ότι τέτοια ανακοίνωση δεν θα προκαλέσει περαιτέρω αρνητικές συνέπειες για τα δεδομένα των υποκειμένων, π.χ. μέσω γνωστοποίησης στον δικτυακό τόπο του οργανισμού. Στην τελευταία αυτή περίπτωση απαιτείται ακριβής και σαφής ανακοίνωση, σε περίοπτη θέση στην ιστοσελίδα του υπευθύνου επεξεργασίας, με ακριβή παραπομπή στις σχετικές διατάξεις του ΓΚΠΔ. Ο οργανισμός ενδέχεται να πρέπει επίσης να επικαιροποιήσει και να επανορθώσει τα οργανωτικά και τεχνικά μέτρα και τις διαδικασίες για τον χειρισμό της ασφάλειας των δεδομένων προσωπικού χαρακτήρα και τον μετριασμό των κινδύνων.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

2.5 Οργανωτικά και τεχνικά μέτρα για την πρόληψη / τον μετριασμό του αντικτύπου των επιθέσεων λυτρισμικού

48. Το γεγονός ότι πραγματοποιήθηκε επίθεση λυτρισμικού είναι συνήθως ένδειξη για την ύπαρξη μίας ή περισσότερων ευπαθειών στο σύστημα του υπευθύνου επεξεργασίας. Αυτό ισχύει επίσης σε περιπτώσεις λυτρισμικού στις οποίες τα δεδομένα προσωπικού χαρακτήρα κρυπτογραφήθηκαν μεν, πλην όμως δεν αποσπάστηκαν. Ανεξάρτητα από το αποτέλεσμα και τις συνέπειες της επίθεσης, τονίζεται ιδιαίτερα η σημασία της συνολικής αξιολόγησης του συστήματος ασφάλειας των δεδομένων, με ιδιαίτερη έμφαση στην ασφάλεια των πληροφοριακών συστημάτων. Οι αδυναμίες και τα κενά ασφάλειας που εντοπίζονται πρέπει να τεκμηριωθούν και να αντιμετωπιστούν αμελλητί.

49. Συνιστώμενα μέτρα:

(Ο κατάλογος των μέτρων που ακολουθούν δεν έχει σε καμία περίπτωση αποκλειστικό ή πλήρη χαρακτήρα. Αντιθέτως, στόχος είναι η παροχή ιδεών με σκοπό την πρόληψη και ενδεχόμενων λύσεων. Κάθε διαδικασία επεξεργασίας είναι διαφορετική και, επομένως, ο υπεύθυνος επεξεργασίας θα πρέπει να αποφασίσει ποια μέτρα ανταποκρίνονται καλύτερα στη δεδομένη κατάσταση.)

- Συνεχής επικαιροποίηση του υλικολογισμικού, του λειτουργικού συστήματος και του λογισμικού εφαρμογών στους διακομιστές, τα μηχανήματα-πελάτες, τις συνιστώσες ενεργού δικτύου και κάθε άλλο μηχάνημα στο ίδιο τοπικό δίκτυο (συμπεριλαμβανομένων των συσκευών ασύρματης πρόσβασης στο διαδίκτυο). Διασφάλιση της ύπαρξης κατάλληλων μέτρων ασφάλειας των πληροφοριακών συστημάτων, της αποτελεσματικότητας και της τακτικής επικαιροποίησής τους όταν η επεξεργασία ή οι περιστάσεις μεταβάλλονται ή εξελίσσονται. Αυτό περιλαμβάνει την τήρηση λεπτομερών αρχείων καταγραφής των διορθωτικών προγραμμάτων που εφαρμόζονται και της σχετικής χρονοσφραγίδας.

- Σχεδιασμός και οργάνωση συστημάτων και υποδομών επεξεργασίας για την κατάτμηση ή την απομόνωση συστημάτων δεδομένων και δικτύων, με σκοπό την αποφυγή της διάδοσης κακόβουλου λογισμικού εντός του οργανισμού και σε εξωτερικά συστήματα.
- Ύπαρξη επικαιροποιημένης, ασφαλούς και δοκιμασμένης διαδικασίας εφεδρικών αρχείων. Τα μέσα μεσοπρόθεσμης και μακροπρόθεσμης αποθήκευσης εφεδρικών αρχείων πρέπει να τηρούνται χωριστά από την αποθήκευση επιχειρησιακών δεδομένων και να μην είναι προσβάσιμα σε τρίτους, ακόμη και σε περίπτωση επιτυχημένης επίθεσης (όπως ημερήσια σταδιακά δημιουργούμενα εφεδρικά αρχεία και εβδομαδιαία πλήρη εφεδρικά αρχεία).
- Ύπαρξη/απόκτηση κατάλληλου, επικαιροποιημένου, αποτελεσματικού και ολοκληρωμένου λογισμικού κατά των κακόβουλων λογισμικών.
- Ύπαρξη κατάλληλου, επικαιροποιημένου, αποτελεσματικού και ολοκληρωμένου τείχους προστασίας και συστήματος ανίχνευσης και πρόληψης παρεισδύσεων. Κατεύθυνση της κίνησης του δικτύου μέσω του τείχους προστασίας / του συστήματος ανίχνευσης παρεισδύσεων, ακόμη και σε περίπτωση τηλεργασίας κατ' οίκον ή κινητής εργασίας (π.χ. μέσω της χρήσης συνδέσεων VPN σε οργανωτικούς μηχανισμούς ασφάλειας κατά την πρόσβαση στο διαδίκτυο).
- Κατάρτιση των υπαλλήλων στις μεθόδους αναγνώρισης και πρόληψης επιθέσεων κατά των πληροφοριακών συστημάτων. Ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει τρόπους εξακρίβωσης της γνησιότητας και της αξιοπιστίας των ηλεκτρονικών και άλλων μηνυμάτων που λαμβάνονται με άλλα μέσα επικοινωνίας. Οι υπάλληλοι θα πρέπει να εκπαιδεύονται ώστε να αναγνωρίζουν πότε πραγματοποιήθηκε τέτοια επίθεση, να γνωρίζουν τον τρόπο αφαίρεσης του τελικού σημείου από το δίκτυο και να εκπληρώνουν την υποχρέωσή τους άμεσης αναφοράς της επίθεσης στον υπεύθυνο ασφάλειας.
- Υπογράμμιση της αναγκαιότητας προσδιορισμού του είδους του κακόβουλου κώδικα προκειμένου να διαπιστωθούν οι συνέπειες της επίθεσης και να αναζητηθούν τα κατάλληλα μέτρα για τον μετριασμό του κινδύνου. Εάν η επίθεση λυτρισμικού υπήρξε επιτυχημένη και δεν υπάρχουν εφεδρικά αρχεία, μπορεί να χρησιμοποιηθούν διαθέσιμα εργαλεία όπως αυτά του έργου «no more ransom» (όχι άλλα λύτρα) (nomoreransom.org) για την ανάκτηση δεδομένων. Ωστόσο, εάν υπάρχουν διαθέσιμα ασφαλή εφεδρικά αρχεία, συνιστάται η επαναφορά των δεδομένων από αυτά.
- Διαβίβαση ή αναπαραγωγή όλων των αρχείων καταγραφής σε κεντρικό διακομιστή αρχείων καταγραφής (συμπεριλαμβανομένης ενδεχομένως της υπογραφής ή κρυπτογραφικής χρονοσήμανσης καταγραφών).
- Ισχυρή κρυπτογράφηση και επαλήθευση ταυτότητας πολλαπλών παραγόντων, ειδικότερα για τη διοικητική πρόσβαση σε πληροφοριακά συστήματα, κατάλληλη διαχείριση κλειδιών και κωδικών πρόσβασης.
- Δοκιμές ευπάθειας και διείσδυσης σε τακτική βάση.
- Σύσταση ομάδας αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT) ή ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) εντός του οργανισμού ή συμμετοχή σε συλλογική CSIRT/CERT. Κατάρτιση σχεδίου αντιμετώπισης περιστατικών, σχεδίου αποκατάστασης της λειτουργίας έπειτα από καταστροφή και σχεδίου επιχειρησιακής συνέχειας και διασφάλιση των διεξοδικής δοκιμής τους.
- Κατά την αξιολόγηση αντιμέτρων, η ανάλυση κινδύνων θα πρέπει να επανεξετάζεται, να ελέγχεται και να επικαιροποιείται.

3 ΕΠΙΘΕΣΕΙΣ ΑΠΟΣΠΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

50. Επιθέσεις οι οποίες εκμεταλλεύονται ευπάθειες σε υπηρεσίες που παρέχει ο υπεύθυνος επεξεργασίας σε τρίτους μέσω του διαδικτύου, π.χ. τελούνται μέσω επιθέσεων έγχυσης (έγχυση SQL, διάσχιση διαδρομής),

υπονόμευσης δικτυακών τόπων και παρόμοιων μεθόδων, μπορεί να προσομοιάζουν σε επιθέσεις λυτρισμικού υπό την έννοια ότι ο κίνδυνος απορρέει από την πράξη μη εξουσιοδοτημένου τρίτου, πλην όμως οι εν λόγω επιθέσεις έχουν συνήθως ως στόχο την αντιγραφή, την απόσπαση και την κατάχρηση δεδομένων προσωπικού χαρακτήρα με κακόβουλο σκοπό. Επομένως, πρόκειται κυρίως για παραβιάσεις του απορρήτου των δεδομένων και, ενδεχομένως, επίσης της ακεραιότητας των δεδομένων. Παράλληλα, εάν ο υπεύθυνος επεξεργασίας γνωρίζει τα χαρακτηριστικά του συγκεκριμένου είδους παραβιάσεων, οι υπεύθυνοι επεξεργασίας έχουν στη διάθεσή τους πολλά μέτρα τα οποία μπορούν να μειώσουν σημαντικά τον κίνδυνο επιτυχημένης εκτέλεσης της επίθεσης.

3.1 ΠΕΡΙΠΤΩΣΗ αριθ. 05: Απόσπαση δεδομένων αιτήσεων για θέσεις εργασίας από δικτυακό τόπο

Υπηρεσία απασχόλησης δέχθηκε κυβερνοεπίθεση, μέσω της οποίας τοποθετήθηκε στον δικτυακό τόπο της κακόβουλος κώδικας. Μέσω του κακόβουλου κώδικα, προσωπικές πληροφορίες οι οποίες υποβλήθηκαν μέσω ηλεκτρονικών εντύπων αιτήσεων για θέσεις εργασίας και αποθηκεύτηκαν στον διακομιστή στο διαδίκτυο κατέστησαν προσβάσιμες σε μη εξουσιοδοτημένο/-α πρόσωπο/-α. 213 τέτοια έντυπα έχουν ενδεχομένως επηρεαστεί, η δε ανάλυση των επηρεαζόμενων δεδομένων κατέδειξε ότι η παραβίαση δεν επηρέασε ειδικές κατηγορίες δεδομένων. Η συγκεκριμένη εργαλειοθήκη κακόβουλου λογισμικού που εγκαταστάθηκε στον δικτυακό τόπο διέθετε λειτουργικότητες χάρη στις οποίες ο δράστης της επίθεσης κατάφερε να αφαιρέσει κάθε ιστορικό απόσπασης δεδομένων καθώς και να παρακολουθεί την επεξεργασία στον διακομιστή και να συλλέγει δεδομένα προσωπικού χαρακτήρα. Η εργαλειοθήκη ανακαλύφθηκε έναν μήνα μετά την εγκατάστασή της.

3.1.1 ΠΕΡΙΠΤΩΣΗ αριθ. 05 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

51. Η ασφάλεια του περιβάλλοντος του υπευθύνου επεξεργασίας δεδομένων έχει μεγάλη σημασία, καθώς η πλειονότητα των εν λόγω παραβιάσεων μπορούν να αποφευχθούν μέσω διασφάλισης της συνεχούς επικαιροποίησης όλων των συστημάτων, της κρυπτογράφησης ευαίσθητων δεδομένων και της ανάπτυξης εφαρμογών βάσει προτύπων υψηλής ασφάλειας, όπως ισχυρής επαλήθευσης ταυτότητας, μέτρων κατά της ωμής βίας, επιθέσεων, της «διαφυγής» ή της «εξυγίανσης»[18] των εισαγόμενων από τον χρήστη δεδομένων κ.λπ. Απαιτούνται επίσης περιοδικοί έλεγχοι της ασφάλειας των πληροφοριακών συστημάτων, αξιολογήσεις ευπάθειας και δοκιμές διείσδυσης, προκειμένου τα συγκεκριμένα είδη ευπαθειών να εντοπίζονται εκ των προτέρων και να αντιμετωπίζονται. Στην προκειμένη περίπτωση, η χρήση εργαλείων παρακολούθησης της ακεραιότητας των αρχείων σε περιβάλλον παραγωγής μπορούσε να είχε συμβάλει στον εντοπισμό της έγχυσης κώδικα. (Κατάλογος συνιστώμενων μέτρων παρέχεται στο σημείο 3.7.)

52. Ο υπεύθυνος επεξεργασίας θα πρέπει να ξεκινά πάντοτε τη διερεύνηση της παραβίασης προσδιορίζοντας το είδος της επίθεσης και τις μεθόδους της, προκειμένου να αξιολογήσει τα μέτρα τα οποία πρέπει να ληφθούν. Για λόγους ταχύτητας και αποτελεσματικότητας, ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να διαθέτει σχέδιο αντιμετώπισης περιστατικών, στο οποίο προσδιορίζονται τα άμεσα και αναγκαία μέτρα για τη θέση του περιστατικού υπό έλεγχο. Στην προκειμένη περίπτωση, το είδος της παραβίασης ήταν παράγοντας αύξησης του κινδύνου, καθώς όχι μόνον παραβιάστηκε το απόρρητο των δεδομένων, αλλά ο

[18] Η διαφυγή ή η εξυγίανση των εισαγόμενων από τον χρήστη δεδομένων είναι μορφή επικύρωσης των εισαγόμενων δεδομένων, με την οποία διασφαλίζεται ότι στο πληροφοριακό σύστημα εισάγονται μόνο δεδομένα με κατάλληλο μορφότυπο.

παράγοντας διείσδυσης διέθετε επίσης μέσα πραγματοποίησης αλλαγών στο σύστημα με αποτέλεσμα να τεθεί επίσης υπό αμφισβήτηση η ακεραιότητα των δεδομένων.

53. Η φύση, η ευαισθησία και ο όγκος των επηρεαζόμενων από την παραβίαση δεδομένων προσωπικού χαρακτήρα θα πρέπει να αξιολογηθούν προκειμένου να εξακριβωθεί ο βαθμός στον οποίο η παραβίαση επηρέασε τα υποκείμενα των δεδομένων. Μολονότι δεν επηρεάστηκαν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, τα δεδομένα στα οποία αποκτήθηκε πρόσβαση περιέχουν πολλές πληροφορίες σχετικά με τα φυσικά πρόσωπα προερχόμενες από τα ηλεκτρονικά έντυπα, τα δε εν λόγω δεδομένα μπορούν να χρησιμοποιηθούν καταχρηστικά με πλείονες τρόπους (στόχευση μέσω αυτόκλητου μάρκετινγκ, υποκλοπή ταυτότητας κ.λπ.) και, επομένως, η σοβαρότητα των συνεπειών αυξάνει τον κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων[19].

3.1.2 ΠΕΡΙΠΤΩΣΗ αριθ. 05 – Μετριασμός και υποχρεώσεις

54. Εφόσον είναι δυνατό, μετά την επίλυση του προβλήματος, η βάση δεδομένων θα πρέπει να συγκριθεί με την αποθηκευμένη σε ασφαλές εφεδρικό αρχείο βάση. Η πείρα που αποκτήθηκε από την παραβίαση θα πρέπει να χρησιμοποιηθεί κατά την επικαιροποίηση των υποδομών ΤΠ. Ο υπεύθυνος επεξεργασίας θα πρέπει να επαναφέρει όλα τα επηρεαζόμενα πληροφοριακά συστήματα σε γνωστή αρχική κατάσταση, να θεραπεύσει την ευπάθεια και να εφαρμόσει νέα μέτρα ασφάλειας για την αποφυγή παρόμοιων παραβιάσεων στο μέλλον, π.χ. ελέγχους ακεραιότητας αρχείων και ελέγχους ασφάλειας. Εάν τα δεδομένα προσωπικού χαρακτήρα όχι μόνον αποσπάστηκαν αλλά και διαγράφηκαν, ο υπεύθυνος επεξεργασίας πρέπει να λάβει συστηματικά μέτρα για την ανάκτηση των δεδομένων προσωπικού χαρακτήρα στην κατάσταση στην οποία ήταν πριν από την παραβίαση. Ενδέχεται να πρέπει να εφαρμοστεί η δημιουργία πλήρων εφεδρικών αρχείων, σταδιακών αλλαγών και, στη συνέχεια, ενδεχομένως, να πρέπει να επαναληφθεί η επεξεργασία από το τελευταίο σταδιακά δημιουργηθέν εφεδρικό αντίγραφο – κάτι το οποίο απαιτεί να είναι ο υπεύθυνος επεξεργασίας σε θέση να επαναλάβει τις αλλαγές που πραγματοποιήθηκαν από το τελευταίο δημιουργηθέν εφεδρικό αντίγραφο. Αυτό μπορεί να απαιτεί τον σχεδιασμό του συστήματος, από τον υπεύθυνο επεξεργασίας, κατά τρόπο ώστε να διατηρεί τα ημερήσια εισαγόμενα αρχεία, για την περίπτωση που θα πρέπει να υποβληθούν εκ νέου σε επεξεργασία, και προϋποθέτει εύρωστη μέθοδο αποθήκευσης και κατάλληλη πολιτική διατήρησης.

55. Υπό το πρίσμα των ανωτέρω παρατηρήσεων, καθώς η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, τα υποκείμενα των δεδομένων θα πρέπει οπωσδήποτε να ενημερωθούν σχετικά (άρθρο 34 παράγραφος 1 του ΓΚΠΔ) και τούτο σημαίνει, βεβαίως, ότι η/οι αρμόδια/-ες ΕΑ θα πρέπει επίσης να εμπλακεί/-ούν στη διαδικασία μέσω γνωστοποίησης της παραβίασης δεδομένων. Η τεκμηρίωση της παραβίασης είναι υποχρεωτική, σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ και διευκολύνει την αξιολόγηση της κατάστασης.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

[19] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

3.2 ΠΕΡΙΠΤΩΣΗ αριθ. 06: Απόσπαση κατακερματισμένου κωδικού πρόσβασης από δικτυακό τόπο

Ευπάθεια συνιστάμενη στην έγχυση SQL χρησιμοποιήθηκε για την απόκτηση πρόσβασης σε βάση δεδομένων διακομιστή δικτυακού τόπου μαγειρικής. Οι χρήστες δικαιούνταν να επιλέγουν ως ονόματα χρήστη μόνο αυθαίρετα ψευδώνυμα. Αποθαρρυνόταν η χρήση διευθύνσεων ηλεκτρονικού ταχυδρομείου για τον σκοπό αυτό. Οι κωδικοί πρόσβασης που αποθηκεύονταν στη βάση δεδομένων κατακερματίζονταν με ισχυρό αλγόριθμο, το δε αλάτι δεν επηρεάστηκε. Επηρεαζόμενα δεδομένα: κατακερματισμένοι κωδικοί πρόσβασης 1 200 χρηστών. Για λόγους ασφάλειας, ο υπεύθυνος επεξεργασίας ενημέρωσε τα υποκείμενα των δεδομένων σχετικά με την παραβίαση μέσω ηλεκτρονικού ταχυδρομείου και ζήτησε να αλλάξουν τους κωδικούς πρόσβασής τους, ιδίως εάν χρησιμοποιούσαν τον ίδιο κωδικό πρόσβασης για άλλες υπηρεσίες.

3.2.1 ΠΕΡΙΠΤΩΣΗ αριθ. 06 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

56. Στην προκειμένη περίπτωση, επηρεάζεται το απόρρητο των δεδομένων, αλλά οι κωδικοί πρόσβασης στη βάση δεδομένων ήταν κατακερματισμένοι με επικαιροποιημένη μέθοδο, γεγονός που μείωνε τον κίνδυνο όσον αφορά τη φύση, την ευαισθησία και τον όγκο των δεδομένων προσωπικού χαρακτήρα. Η παρούσα περίπτωση δεν ενέχει κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

57. Επιπλέον, δεν επηρεάστηκαν τα στοιχεία επικοινωνίας (π.χ. διευθύνσεις ηλεκτρονικού ταχυδρομείου ή αριθμοί τηλεφώνου) των υποκειμένων των δεδομένων και τούτο σημαίνει ότι δεν υπάρχει σημαντικός κίνδυνος να γίνουν τα υποκείμενα των δεδομένων στόχος αποπειρών απάτης (π.χ. μέσω της λήψης μηνυμάτων ηλεκτρονικού ψαρέματος ή δόλιων γραπτών μηνυμάτων και τηλεφωνικών κλήσεων). Η παραβίαση δεν αφορούσε ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.

58. Ορισμένα ονόματα χρήστη θα μπορούσαν να θεωρηθούν δεδομένα προσωπικού χαρακτήρα, αλλά το αντικείμενο του δικτυακού τόπου δεν αφήνει περιθώριο για αρνητικούς συσχετισμούς. Επισημαίνεται, ωστόσο, ότι η αξιολόγηση κινδύνου μπορεί να μεταβληθεί[20], εάν το είδος του δικτυακού τόπου και τα δεδομένα στα οποία αποκτήθηκε πρόσβαση μπορεί να αποκαλύπτουν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (π.χ. δικτυακός τόπος πολιτικού κόμματος ή συνδικαλιστικής οργάνωσης). Η χρήση προηγμένης κρυπτογράφησης θα μπορούσε να μετριάσει τις αρνητικές συνέπειες της παραβίασης. Εάν επιτρέπεται περιορισμένος αριθμός αποπειρών σύνδεσης, οι επιθέσεις σύνδεσης ωμής βίας δεν θα ευδοκιμήσουν και, με τον τρόπο αυτό, θα μειωθούν σε μεγάλο βαθμό οι κίνδυνοι που συνεπάγονται οι δράστες επιθέσεων που γνωρίζουν ήδη τα ονόματα χρήστη.

3.2.2 ΠΕΡΙΠΤΩΣΗ αριθ. 06 – Μετριασμός και υποχρεώσεις

59. Η ανακοίνωση της παραβίασης στα υποκείμενα των δεδομένων θα μπορούσε να θεωρηθεί, σε ορισμένες περιπτώσεις, παράγοντας μετριασμού, δεδομένου ότι τα υποκείμενα των δεδομένων είναι επίσης σε θέση να λάβουν τα αναγκαία μέτρα για την αποφυγή περαιτέρω βλαβών λόγω της παραβίασης, για παράδειγμα μέσω της αλλαγής των κωδικών πρόσβασής τους στον δικτυακό τόπο. Στην προκειμένη περίπτωση, η γνωστοποίηση δεν ήταν υποχρεωτική, αλλά σε πολλές περιπτώσεις μπορεί να θεωρηθεί ορθή πρακτική.

[20] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

60. Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να επανορθώσει την ευπάθεια και να εφαρμόσει νέα μέτρα ασφάλειας για την αποφυγή παρόμοιων παραβιάσεων δεδομένων στο μέλλον, όπως, για παράδειγμα, συστηματικούς ελέγχους ασφάλειας στον δικτυακό τόπο.

61. Η παραβίαση θα πρέπει να τεκμηριωθεί σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ, αλλά δεν απαιτείται ούτε γνωστοποίηση ούτε ανακοίνωση.

62. Επίσης, συνιστάται με έμφαση η ανακοίνωση στα υποκείμενα των δεδομένων παραβίασης που αφορά κωδικούς πρόσβασης σε κάθε περίπτωση, ακόμη και όταν οι κωδικοί πρόσβασης αποθηκεύονταν κατακερματισμένοι με τη χρήση αλατιού και προηγμένου αλγορίθμου. Είναι προτιμότερη η χρήση μεθόδων επαλήθευσης ταυτότητας που καθιστά περιττή την επεξεργασία κωδικών πρόσβασης από τον διακομιστή. Θα πρέπει να δοθεί στα υποκείμενα των δεδομένων η δυνατότητα να λάβουν κατάλληλα μέτρα σχετικά με τους κωδικούς πρόσβασής τους στον δικτυακό τόπο.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	X	X

3.3 ΠΕΡΙΠΤΩΣΗ αριθ. 07: Επίθεση μέσω παραβιασμένων διαπιστευτηρίων σε δικτυακό τόπο τράπεζας

Τράπεζα δέχθηκε κυβερνοεπίθεση σε έναν από τους ιστοτόπους ηλεκτρονικής τραπεζικής της. Στόχος της επίθεσης ήταν η απαρίθμηση όλων των ενδεχόμενων αναγνωριστικών χρήστη για τη σύνδεση στον ιστότοπο με τη χρήση σταθερού κοινού κωδικού πρόσβασης. Οι κωδικοί πρόσβασης αποτελούνται από 8 ψηφία. Λόγω ευπάθειας του ιστοτόπου, σε ορισμένες περιπτώσεις πληροφορίες που αφορούσαν τα υποκείμενα των δεδομένων (όνομα, επώνυμο, φύλο, ημερομηνία και τόπος γέννησης, αριθμός φορολογικού μητρώου, αναγνωριστικοί κωδικοί χρήστη) διέρρευσαν στον δράστη της επίθεσης, ακόμη και αν ο χρησιμοποιηθείς κωδικός πρόσβασης δεν ήταν ορθός ή ο τραπεζικός λογαριασμός δεν ήταν πλέον ενεργός. Αυτό επηρέασε περίπου 100 000 υποκείμενα των δεδομένων. Ο δράστης της επίθεσης κατάφερε να συνδεθεί σε περίπου 2 000 λογαριασμούς, στους οποίους χρησιμοποιούνταν ο κοινός κωδικός πρόσβασης που δοκίμασε ο δράστης της επίθεσης. Εκ των υστέρων, ο υπεύθυνος επεξεργασίας κατάφερε να εντοπίσει όλες τις παράνομες απόπειρες σύνδεσης. Ο υπεύθυνος επεξεργασίας μπόρεσε να επιβεβαιώσει ότι, σύμφωνα με τους ελέγχους καταπολέμησης της απάτης, δεν πραγματοποιήθηκε καμία συναλλαγή στους εν λόγω λογαριασμούς κατά τη διάρκεια της επίθεσης. Η τράπεζα γνώριζε την παραβίαση δεδομένων, καθώς το κέντρο λειτουργιών ασφάλειας της τράπεζας εντόπισε υψηλό αριθμό αιτημάτων σύνδεσης προς τον δικτυακό τόπο. Για την αντιμετώπιση του περιστατικού, ο υπεύθυνος επεξεργασίας απενεργοποίησε τη δυνατότητα σύνδεσης στον δικτυακό τόπο και επέβαλε την εκ νέου ρύθμιση κωδικών πρόσβασης για τους παραβιασθέντες λογαριασμούς. Ο υπεύθυνος επεξεργασίας ανακοίνωσε την παραβίαση μόνο στους χρήστες των οποίων οι λογαριασμοί παραβιάστηκαν, δηλ. στους χρήστες των οποίων οι κωδικοί πρόσβασης παραβιάστηκαν ή των οποίων τα δεδομένα αποκαλύφθηκαν.

3.3.1 ΠΕΡΙΠΤΩΣΗ αριθ. 07 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

63. Είναι σημαντικό να επισημανθεί ότι οι υπεύθυνοι επεξεργασίας που χειρίζονται δεδομένα εξαιρετικά προσωπικού χαρακτήρα[21] έχουν μεγαλύτερη ευθύνη όσον αφορά την παροχή κατάλληλης ασφάλειας των δεδομένων, π.χ. μέσω της πρόβλεψης επιχειρησιακού κέντρου για την ασφάλεια και άλλων μέτρων πρόληψης, εντοπισμού και αντιμετώπισης περιστατικών. Η μη πλήρωση των υψηλότερων αυτών προτύπων θα συνεπάγεται αναμφίβολα τη λήψη σοβαρότερων μέτρων κατά τη διάρκεια έρευνας εκ μέρους της ΕΑ.

64. Η παραβίαση αφορά οικονομικά στοιχεία πέραν της ταυτότητας και των αναγνωριστικών χρήστη, με αποτέλεσμα να καθίσταται ιδιαίτερα σοβαρή. Ο αριθμός των επηρεαζόμενων φυσικών προσώπων είναι υψηλός.

65. Το γεγονός ότι η παραβίαση έλαβε χώρα σε ένα τόσο ευαίσθητο περιβάλλον υποδεικνύει την ύπαρξη σημαντικών κενών όσον αφορά την ασφάλεια των δεδομένων στο σύστημα του υπευθύνου επεξεργασίας, μπορεί δε να αποτελεί ένδειξη ότι η επανεξέταση και η επικαιροποίηση των επηρεαζόμενων μέτρων είναι «απαραίτητη» σύμφωνα με το άρθρο 24 παράγραφος 1, το άρθρο 25 παράγραφος 1 και το άρθρο 32 παράγραφος 1 του ΓΚΠΔ. Τα δεδομένα που παραβιάστηκαν καθιστούν δυνατή τη μοναδική ταυτοποίηση υποκειμένων των δεδομένων και περιέχουν και άλλες πληροφορίες σχετικά με αυτά (συμπεριλαμβανομένων του φύλου, της ημερομηνίας και του τόπου γέννησης), μπορούν δε να χρησιμοποιηθούν από τον δράστη της επίθεσης για να μαντέψει τους κωδικούς πρόσβασης των πελατών ή για να δρομολογήσει εκστρατεία στοχευμένου ηλεκτρονικού ψαρέματος προς τους πελάτες της τράπεζας.

66. Για τους λόγους αυτούς, θεωρήθηκε ότι η παραβίαση των δεδομένων ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις υποχρεώσεις όλων των ενδιαφερόμενων υποκειμένων των δεδομένων[22]. Επομένως, η επέλευση υλικής (π.χ. οικονομική ζημία) και ηθικής βλάβης (π.χ. υποκλοπή ταυτότητας ή απάτη) αποτελεί ενδεχόμενο αποτέλεσμα.

3.3.2 ΠΕΡΙΠΤΩΣΗ αριθ. 07 – Μετριασμός και υποχρεώσεις

67. Τα μέτρα του υπευθύνου επεξεργασίας, που αναφέρθηκαν στην περιγραφή της περίπτωσης, είναι κατάλληλα. Μετά την παραβίαση, ο υπεύθυνος επεξεργασίας επανόρθωσε επίσης την ευπάθεια του ιστοτόπου και έλαβε άλλα μέτρα για την πρόληψη παρόμοιων παραβιάσεων δεδομένων στο μέλλον, όπως προσθήκη επαλήθευσης ταυτότητας δύο παραγόντων στον οικείο ιστότοπο και ισχυροποίηση της επαλήθευσης ταυτότητας του πελάτη.

68. Η τεκμηρίωση της παραβίασης σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ και η γνωστοποίηση της παραβίασης στην ΕΑ δεν είναι προαιρετικές στο παρόν σενάριο. Επιπλέον, ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώσει το σύνολο των 100 000 υποκειμένων των δεδομένων (συμπεριλαμβανομένων εκείνων των οποίων οι λογαριασμοί δεν παραβιάστηκαν) σύμφωνα με το άρθρο 34 του ΓΚΠΔ.

---

[21] Όπως πληροφορίες για τα υποκείμενα των δεδομένων, οι οποίες αφορούν μεθόδους πληρωμής, π.χ. αριθμούς καρτών, τραπεζικούς λογαριασμούς, ηλεκτρονικές πληρωμές, μισθοδοσία, αντίγραφα κίνησης τραπεζικών λογαριασμών, οικονομικές μελέτες ή κάθε άλλο στοιχείο το οποίο μπορεί να αποκαλύπτει οικονομικές πληροφορίες που αφορούν τα υποκείμενα των δεδομένων.

[22] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

3.4 Οργανωτικά και τεχνικά μέτρα για την πρόληψη / τον μετριασμό του αντικτύπου των επιθέσεων χάκερ

69. Όπως και στην περίπτωση των επιθέσεων λυτρισμικού, ανεξάρτητα από το αποτέλεσμα και τις συνέπειες της επίθεσης, η εκ νέου αξιολόγηση της ασφάλειας των πληροφοριακών συστημάτων είναι υποχρεωτική για τους υπευθύνους επεξεργασίας σε τέτοιες περιπτώσεις.

70. Συνιστώμενα μέτρα[23]:

(*Ο κατάλογος των μέτρων που ακολουθούν δεν έχει σε καμία περίπτωση αποκλειστικό ή πλήρη χαρακτήρα. Αντιθέτως, στόχος είναι η παροχή ιδεών με σκοπό την πρόληψη και ενδεχόμενων λύσεων. Κάθε διαδικασία επεξεργασίας είναι διαφορετική και, επομένως, ο υπεύθυνος επεξεργασίας θα πρέπει να αποφασίσει ποια μέτρα ανταποκρίνονται καλύτερα στη δεδομένη κατάσταση*.)

- Προηγμένη κρυπτογράφηση και διαχείριση κλειδιών, ιδίως όταν υποβάλλονται σε επεξεργασία κωδικοί πρόσβασης και ευαίσθητα ή οικονομικά στοιχεία. Ο κρυπτογραφικός κατακερματισμός και ο εμπλουτισμός των απόρρητων πληροφοριών (κωδικών πρόσβασης) είναι πάντοτε προτιμότερος από την κρυπτογράφηση των κωδικών πρόσβασης. Είναι προτιμότερη η χρήση μεθόδων επαλήθευσης ταυτότητας που καθιστά περιττή την επεξεργασία κωδικών πρόσβασης από τον διακομιστή.
- Συνεχής επικαιροποίηση του συστήματος (λογισμικό και υλικολογισμικό). Διασφάλιση της ύπαρξης μέτρων ασφάλειας των πληροφοριακών συστημάτων, της αποτελεσματικότητας και της τακτικής επικαιροποίησής τους όταν η επεξεργασία ή οι περιστάσεις μεταβάλλονται ή εξελίσσονται. Προκειμένου να μπορεί να αποδείξει τη συμμόρφωση με το άρθρο 5 παράγραφος 1 στοιχείο στ) του ΓΚΠΔ, σύμφωνα με το άρθρο 5 παράγραφος 2 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας θα πρέπει να τηρεί αρχείο όλων των επικαιροποιήσεων που πραγματοποιούνται, συμπεριλαμβανομένου επίσης του χρόνου εφαρμογής τους.
- Χρήση ισχυρών μεθόδων επαλήθευσης ταυτότητας, όπως επαλήθευση ταυτότητας δύο παραγόντων και διακομιστές επαλήθευσης ταυτότητας, την οποία συμπληρώνει επικαιροποιημένη πολιτική για τους κωδικούς πρόσβασης.
- Τα ασφαλή πρότυπα ανάπτυξης περιλαμβάνουν το φιλτράρισμα των εισαγόμενων από τον χρήστη δεδομένων (με τη χρήση λευκής λίστας, στο μέτρο του δυνατού), τη διαφυγή των εισαγόμενων από τον χρήστη δεδομένων και μέτρα πρόληψης ωμής βίας (όπως τον περιορισμό του μέγιστου αριθμού επαναπροσπαθειών). Τα τείχη προστασίας διαδικτυακών εφαρμογών μπορούν να συμβάλλουν στην αποτελεσματική χρήση της εν λόγω τεχνικής.
- Θέσπιση ισχυρών προνομίων χρήστη και πολιτικής διαχείρισης του ελέγχου πρόσβασης.
- Χρήση κατάλληλου, επικαιροποιημένου, αποτελεσματικού και ολοκληρωμένου τείχους προστασίας, συστήματος ανίχνευσης παρεισδύσεων και άλλων συστημάτων περιμετρικής προστασίας.
- Συστηματικοί έλεγχοι ασφάλειας πληροφοριακών συστημάτων και αξιολογήσεις ευπάθειας (δοκιμές διείσδυσης).

[23] Για την ανάπτυξη ασφαλών διαδικτυακών εφαρμογών, βλ. επίσης: https://www.owasp.org/index.php/Main_Page.

- Τακτικές επανεξετάσεις και δοκιμές προκειμένου να διασφαλίζεται ότι τα εφεδρικά αρχεία μπορούν να χρησιμοποιηθούν για την επαναφορά τυχόν δεδομένων των οποίων η ακεραιότητα ή η διαθεσιμότητα επηρεάστηκε.
- Κανένα αναγνωριστικό ταυτότητας συνόδου στη διεύθυνση URL σε μορφή απλού κειμένου.

4 ΕΣΩΤΕΡΙΚΗ ΠΗΓΗ ΑΝΘΡΩΠΙΝΟΥ ΚΙΝΔΥΝΟΥ

71. Ο ρόλος του ανθρώπινου σφάλματος στις παραβιάσεις δεδομένων προσωπικού χαρακτήρα πρέπει να τονιστεί, καθώς η παρουσία του δεν είναι ασυνήθιστη. Δεδομένου ότι τα εν λόγω είδη παραβιάσεων μπορούν να τελεστούν τόσο με πρόθεση όσο και χωρίς πρόθεση, είναι πολύ δύσκολο για τους υπευθύνους επεξεργασίας δεδομένων να προσδιορίσουν τις ευπάθειες και να λάβουν μέτρα για την αποφυγή τους. Η διεθνής διάσκεψη των επιτρόπων για την προστασία των δεδομένων και την ιδιωτική ζωή αναγνώρισε τη σημασία της αντιμετώπισης των εν λόγω ανθρώπινων παραγόντων και εξέδωσε το ψήφισμα για την αντιμετώπιση του ρόλου του ανθρώπινου σφάλματος στις παραβιάσεις δεδομένων προσωπικού χαρακτήρα τον Οκτώβριο του 2019[24]. Στο εν λόγω ψήφισμα τονίζεται ότι θα πρέπει να ληφθούν κατάλληλα μέτρα ασφάλειας για την πρόληψη ανθρώπινων σφαλμάτων και παρέχεται μη εξαντλητικός κατάλογος των εν λόγω μέτρων ασφάλειας και προσεγγίσεων.

4.1 ΠΕΡΙΠΤΩΣΗ αριθ. 08: Απόσπαση επιχειρηματικών δεδομένων από υπάλληλο

Κατά τη διάρκεια της προθεσμίας ειδοποίησης καταγγελίας της σύμβασής του, υπάλληλος εταιρείας αντιγράφει επιχειρηματικά δεδομένα από τη βάση δεδομένων της εταιρείας. Ο υπάλληλος διαθέτει άδεια πρόσβασης στα δεδομένα μόνο για την άσκηση των εργασιακών καθηκόντων του. Μήνες αργότερα, αφού παραιτήθηκε από την εργασία του, ο υπάλληλος χρησιμοποιεί τα δεδομένα που απέκτησε με τον τρόπο αυτό (βασικά στοιχεία επικοινωνίας) σε νέα επεξεργασία δεδομένων, στην οποία είναι ο υπεύθυνος επεξεργασίας, με σκοπό να επικοινωνήσει με τους πελάτες της εταιρείας και να τους προσελκύσει στη νέα επιχείρησή του.

4.1.1 ΠΕΡΙΠΤΩΣΗ αριθ. 08 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

72. Στην προκειμένη περίπτωση, δεν λήφθηκαν προηγούμενα μέτρα για να εμποδιστεί ο υπάλληλος να αντιγράψει στοιχεία επικοινωνίας των πελατών της εταιρείας, καθώς χρειαζόταν –και διέθετε– νόμιμη πρόσβαση στις εν λόγω πληροφορίες για την άσκηση των εργασιακών καθηκόντων του. Δεδομένου ότι η εκτέλεση των περισσότερων καθηκόντων που αφορούν τις σχέσεις με τους πελάτες απαιτεί κάποιου είδους πρόσβαση του υπαλλήλου σε δεδομένα προσωπικού χαρακτήρα, η αποφυγή των εν λόγω παραβιάσεων δεδομένων είναι εξαιρετική δυσχερής. Η επιβολή περιορισμών στην έκταση της πρόσβασης μπορεί να περιορίσει τις εργασίες που είναι σε θέση να εκτελεί ο συγκεκριμένος υπάλληλος. Ωστόσο, η ύπαρξη ειδικών πολιτικών πρόσβασης και ο συνεχής έλεγχος μπορούν να συμβάλουν στην αποφυγή των εν λόγω παραβιάσεων.

73. Ως συνήθως, κατά την αξιολόγηση κινδύνου, πρέπει να ληφθούν υπόψη το είδος της παραβίασης καθώς και η φύση, η ευαισθησία και ο όγκος των επηρεαζόμενων δεδομένων προσωπικού χαρακτήρα. Αυτό το είδος παραβιάσεων είναι συνήθως παραβιάσεις απορρήτου, δεδομένου ότι η βάση δεδομένων παραμένει συνήθως άθικτη, καθώς το περιεχόμενό της αντιγράφεται «απλώς» για περαιτέρω χρήση. Εξάλλου, η ποσότητα των επηρεαζόμενων δεδομένων είναι συνήθως μικρή ή μέτρια. Στην προκειμένη περίπτωση, δεν

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

επηρεάστηκαν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, καθώς ο υπάλληλος χρειαζόταν μόνο τα στοιχεία επικοινωνίας πελατών ώστε να μπορέσει να επικοινωνήσει μαζί τους μετά την αναχώρησή του από την εταιρεία. Επομένως, τα επηρεαζόμενα δεδομένα δεν είναι ευαίσθητα.

74. Παρότι ο μοναδικός σκοπός του πρώην υπαλλήλου που αντέγραψε δολίως τα δεδομένα μπορεί να περιορίζεται στην απόκτηση των στοιχείων επικοινωνίας των πελατών της εταιρείας για δικούς του εμπορικούς σκοπούς, ο υπεύθυνος επεξεργασίας δεν μπορεί να θεωρήσει ότι ο κίνδυνος για τα επηρεαζόμενα υποκείμενα των δεδομένων είναι χαμηλός, καθώς ο υπεύθυνος επεξεργασίας δεν έχει οποιοδήποτε είδος διαβεβαίωσης όσον αφορά τις προθέσεις του υπαλλήλου. Επομένως, παρότι οι συνέπειες της παραβίασης ενδέχεται να περιορίζονται στην έκθεση σε αυτόκλητο μάρκετινγκ για ίδιο λογαριασμό εκ μέρους του πρώην υπαλλήλου, δεν αποκλείεται περαιτέρω και σοβαρότερη κατάχρηση των κλαπέντων δεδομένων, ανάλογα με τον σκοπό της επεξεργασίας που προβλέπει ο πρώην υπάλληλος[25].

4.1.2 ΠΕΡΙΠΤΩΣΗ αριθ. 08 – Μετριασμός και υποχρεώσεις

75. Ο μετριασμός των δυσμενών συνεπειών της παραβίασης στην ανωτέρω περίπτωση είναι δυσχερής. Ενδέχεται να απαιτεί τη λήψη άμεσων νομικών μέτρων για την πρόληψη της περαιτέρω κατάχρησης και διάδοσης των δεδομένων από τον πρώην υπάλληλο. Επόμενος στόχος θα πρέπει να είναι η αποφυγή παρόμοιων καταστάσεων στο μέλλον. Ο υπεύθυνος επεξεργασίας μπορεί να επιχειρήσει να διατάξει τον πρώην υπάλληλο να παύσει να χρησιμοποιεί τα δεδομένα, αλλά η επιτυχία μιας τέτοιας ενέργειας είναι, στην καλύτερη περίπτωση, αμφίβολη. Κατάλληλα τεχνικά μέτρα, όπως η αδυναμία αντιγραφής ή καταφόρτωσης δεδομένων σε κινητές συσκευές, μπορεί να είναι χρήσιμα.

76. Δεν υπάρχει ενιαία λύση για το συγκεκριμένο είδος περιπτώσεων, πλην όμως η εφαρμογή συστηματικής προσέγγισης μπορεί να συμβάλει στην πρόληψή τους. Για παράδειγμα, η εταιρεία μπορεί να εξετάσει –όταν είναι δυνατό– την ανάκληση ορισμένων μορφών πρόσβασης από υπαλλήλους που δήλωσαν τη βούλησή τους να παραιτηθούν ή να εφαρμόσει αρχεία καταγραφής πρόσβασης ώστε οι περιπτώσεις ανεπιθύμητης πρόσβασης να καταγράφονται και να επισημαίνονται. Η σύμβαση που υπογράφεται με τους υπαλλήλους θα πρέπει να περιλαμβάνει ρήτρες που απαγορεύουν τέτοιες ενέργειες.

77. Συνολικά, καθώς η συγκεκριμένη παραβίαση δεν θα επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, αρκεί η γνωστοποίηση στην ΕΑ. Ωστόσο, η ενημέρωση των υποκειμένων των δεδομένων μπορεί να είναι επωφελής και για τον υπεύθυνο επεξεργασίας δεδομένων, καθώς θα είναι μάλλον προτιμότερο να πληροφορηθούν τη διαρροή δεδομένων από την εταιρεία παρά από τον πρώην υπάλληλο που επιχειρεί να επικοινωνήσει μαζί τους. Η τεκμηρίωση της παραβίασης δεδομένων, σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ, είναι υποχρέωση επιβαλλόμενη εκ του νόμου.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	X

[25] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

4.2 ΠΕΡΙΠΤΩΣΗ αριθ. 09: Τυχαία διαβίβαση δεδομένων σε έμπιστο τρίτο

Ασφαλιστικός πράκτορας παρατήρησε ότι –λόγω εσφαλμένων ρυθμίσεων σε αρχείο Excel που έλαβε μέσω ηλεκτρονικού ταχυδρομείου– είχε πρόσβαση σε πληροφορίες που αφορούσαν 24 φυσικά πρόσωπα που δεν ήταν δικοί του πελάτες. Ο ασφαλιστικός πράκτορας δεσμεύεται από το επαγγελματικό απόρρητο και ήταν ο μοναδικός παραλήπτης του ηλεκτρονικού μηνύματος. Βάσει της συμφωνίας μεταξύ του υπευθύνου επεξεργασίας δεδομένων και του ασφαλιστικού πράκτορα, ο δεύτερος υποχρεούται να αναφέρει στον πρώτο αμελλητί κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα. Ως εκ τούτου, ο ασφαλιστικός πράκτορας ανέφερε το σφάλμα στον υπεύθυνο επεξεργασίας, ο οποίος διόρθωσε το αρχείο και το απέστειλε εκ νέου, ζητώντας από τον πράκτορα να διαγράψει το προηγούμενο μήνυμα. Σύμφωνα με την προαναφερθείσα συμφωνία, ο πράκτορας οφείλει να επιβεβαιώσει με γραπτή δήλωση τη διαγραφή, κάτι το οποίο έπραξε. Οι πληροφορίες που αποκτήθηκαν δεν περιλαμβάνουν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, αλλά μόνο στοιχεία επικοινωνίας και στοιχεία σχετικά με την ασφάλιση (είδος ασφάλισης, ποσό). Κατόπιν ανάλυσης των δεδομένων προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση, ο υπεύθυνος επεξεργασίας δεδομένων δεν εντόπισε ιδιαίτερα χαρακτηριστικά είτε στα φυσικά πρόσωπα είτε στον υπεύθυνο επεξεργασίας δεδομένων τα οποία μπορούν να επηρεάσουν το επίπεδο του αντικτύπου της παραβίασης.

4.2.1 ΠΕΡΙΠΤΩΣΗ αριθ. 09 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

78. Στην προκειμένη περίπτωση, η παραβίαση δεν απορρέει από εκ προθέσεως ενέργεια υπαλλήλου, αλλά από εκ παραδρομής μη εσκεμμένο ανθρώπινο σφάλμα. Τέτοιου είδους παραβιάσεις μπορούν να αποφεύγονται ή να περιορίζονται όσον αφορά τη συχνότητά τους μέσω α) της υποχρεωτικής συμμετοχής σε προγράμματα κατάρτισης, εκπαίδευσης και ευαισθητοποίησης, στο πλαίσιο των οποίων οι υπάλληλοι αποκτούν καλύτερη κατανόηση της σημασίας της προστασίας των δεδομένων προσωπικού χαρακτήρα, β) της μείωσης της ανταλλαγής αρχείων μέσω ηλεκτρονικού ταχυδρομείου, για παράδειγμα, χρησιμοποιώντας αντ' αυτού ειδικά συστήματα για την επεξεργασία δεδομένων πελατών, γ) του διπλού ελέγχου των αρχείων πριν από την αποστολή τους, δ) του διαχωρισμού της δημιουργίας και της αποστολής αρχείων.

79. Η παρούσα παραβίαση δεδομένων αφορά μόνο το απόρρητο των δεδομένων, καθώς η ακεραιότητα και η δυνατότητα πρόσβασης σε αυτά δεν επηρεάστηκαν. Η παραβίαση των δεδομένων αφορούσε μόνο 24 περίπου πελάτες και, επομένως, η ποσότητα των επηρεαζόμενων δεδομένων μπορεί να θεωρηθεί μικρή. Επιπλέον, τα επηρεαζόμενα δεδομένα προσωπικού χαρακτήρα δεν περιλαμβάνουν ευαίσθητα δεδομένα. Το γεγονός ότι ο εκτελών την επεξεργασία δεδομένων επικοινώνησε αμελλητί με τον υπεύθυνο επεξεργασίας δεδομένων, μόλις αντιλήφθηκε την παραβίαση των δεδομένων, μπορεί να θεωρηθεί παράγοντας μετριασμού του κινδύνου. (Το ενδεχόμενο να εστάλησαν δεδομένα και σε άλλους ασφαλιστικούς πράκτορες θα πρέπει επίσης να αξιολογηθεί και, εάν επιβεβαιωθεί, θα πρέπει να ληφθούν κατάλληλα μέτρα.) Χάρη στα κατάλληλα μέτρα που λήφθηκαν μετά την παραβίαση των δεδομένων, θεωρείται πιθανό ότι η παραβίαση δεν θα έχει αντίκτυπο στο δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

80. Ο συνδυασμός του μικρού αριθμού επηρεαζόμενων φυσικών προσώπων, του άμεσου εντοπισμού της παραβίασης και των μέτρων που λήφθηκαν για την ελαχιστοποίηση των συνεπειών της συνεπάγεται ότι η παρούσα περίπτωση δεν ενέχει κίνδυνο.

4.2.2 ΠΕΡΙΠΤΩΣΗ αριθ. 09 – Μετριασμός και υποχρεώσεις

81. Συντρέχουν, επιπλέον, και άλλες περιστάσεις οι οποίες μετριάζουν τον κίνδυνο: ο πράκτορας δεσμεύεται από το επαγγελματικό απόρρητο· ανέφερε ο ίδιος το πρόβλημα στον υπεύθυνο επεξεργασίας· και διέγραψε το αρχείο μόλις του ζητήθηκε. Η ευαισθητοποίηση και ενδεχομένως η συμπερίληψη πρόσθετων μέτρων

ελέγχου των εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα θα συμβάλει πιθανώς στην αποφυγή παρόμοιων καταστάσεων στο μέλλον.

82. Πέραν της τεκμηρίωσης της παραβίασης, σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ, δεν απαιτείται η λήψη άλλου μέτρου.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	X	X

4.3 Οργανωτικά και τεχνικά μέτρα για την πρόληψη / τον μετριασμό του αντικτύπου των εσωτερικών πηγών ανθρώπινου κινδύνου

83. Ο συνδυασμός των κατωτέρω αναφερόμενων μέτρων –τα οποία εφαρμόζονται ανάλογα με τα μοναδικά χαρακτηριστικά κάθε περίπτωσης– αναμένεται να συμβάλει στη μείωση της πιθανότητας επανάληψης παρόμοιας παραβίασης στο μέλλον.

84. Συνιστώμενα μέτρα:

(*Ο κατάλογος των μέτρων που ακολουθούν δεν έχει σε καμία περίπτωση αποκλειστικό ή πλήρη χαρακτήρα. Αντιθέτως, στόχος είναι η παροχή ιδεών με σκοπό την πρόληψη και ενδεχόμενων λύσεων. Κάθε διαδικασία επεξεργασίας είναι διαφορετική και, επομένως, ο υπεύθυνος επεξεργασίας θα πρέπει να αποφασίσει ποια μέτρα ανταποκρίνονται καλύτερα στη δεδομένη κατάσταση.*)

- Περιοδική πραγματοποίηση προγραμμάτων κατάρτισης, εκπαίδευσης και ευαισθητοποίησης για τους υπαλλήλους, σχετικά με τις υποχρεώσεις τους όσον αφορά την ιδιωτική ζωή και την ασφάλεια καθώς και τον εντοπισμό και την αναφορά απειλών για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα[26]. Κατάρτιση προγράμματος ευαισθητοποίησης με σκοπό την υπόμνηση στους υπαλλήλους των συνηθέστερων σφαλμάτων που οδηγούν σε παραβιάσεις δεδομένων προσωπικού χαρακτήρα και των τρόπων αποφυγής τους.
- Θέσπιση εύρωστων και αποτελεσματικών πρακτικών, διαδικασιών και συστημάτων για την προστασία των δεδομένων και την ιδιωτική ζωή[27].
- Αξιολόγηση πρακτικών, διαδικασιών και συστημάτων για τη ιδιωτική ζωή προκειμένου να διασφαλίζεται συνεχής αποτελεσματικότητα[28].
- Κατάρτιση κατάλληλων πολιτικών ελέγχου πρόσβασης και επιβολή της τήρησης των κανόνων από τους χρήστες.
- Εφαρμογή τεχνικών για την επιβολή της επαλήθευσης ταυτότητας χρήστη κατά την πρόσβαση σε ευαίσθητα δεδομένα προσωπικού χαρακτήρα.
- Απενεργοποίηση του λογαριασμού του χρήστη στην εταιρεία, μόλις το πρόσωπο αναχωρήσει από την εταιρεία.

[26] Τμήμα 2) υποτμήμα i) του ψηφίσματος για την αντιμετώπιση του ρόλου του ανθρώπινου σφάλματος στις παραβιάσεις δεδομένων προσωπικού χαρακτήρα.

[27] Τμήμα 2) υποτμήμα ii) του ψηφίσματος για την αντιμετώπιση του ρόλου του ανθρώπινου σφάλματος στις παραβιάσεις δεδομένων προσωπικού χαρακτήρα.

[28] Τμήμα 2) υποτμήμα iii) του ψηφίσματος για την αντιμετώπιση του ρόλου του ανθρώπινου σφάλματος στις παραβιάσεις δεδομένων προσωπικού χαρακτήρα.

- Έλεγχος ασυνήθιστων ροών δεδομένων μεταξύ του διακομιστή αρχείων και των σταθμών εργασίας υπαλλήλων.
- Ρύθμιση ασφάλειας διεπαφής εισόδου-εξόδου στο BIOS ή μέσω της χρήσης λογισμικού που ελέγχει τη χρήση διεπαφών υπολογιστή (κλείδωμα ή ξεκλείδωμα, π.χ. USB/CD/DVD κ.λπ.).
- Επανεξέταση της πολιτικής πρόσβασης των υπαλλήλων (π.χ. πρόσβαση σε ευαίσθητα δεδομένα και απαίτηση καταχώρισης επιχειρηματικού λόγου από τον χρήστη, ώστε το στοιχείο αυτό να είναι διαθέσιμο για τους ελέγχους).
- Απενεργοποίηση υπηρεσιών ανοικτού υπολογιστικού νέφους.
- Απαγόρευση και αποφυγή πρόσβασης σε γνωστές υπηρεσίες ανοικτού ταχυδρομείου.
- Απενεργοποίηση της λειτουργίας λήψης αντιγράφου οθόνης στο λειτουργικό σύστημα.
- Επιβολή πολιτικής καθαρού γραφείου.
- Αυτόματο κλείδωμα όλων των υπολογιστών ύστερα από ορισμένο χρόνο αδράνειας.
- Χρήση μηχανισμών [π.χ. (ασύρματου) αδειοδοτικού για τη σύνδεση σε κλειδωμένους λογαριασμούς / το άνοιγμα κλειδωμένων λογαριασμών] για ταχεία μετάβαση από τον ένα χρήστη στον άλλο σε καταμερισμένα περιβάλλοντα.
- Χρήση ειδικών συστημάτων για τη διαχείριση δεδομένων προσωπικού χαρακτήρα τα οποία εφαρμόζουν κατάλληλους μηχανισμούς ελέγχου πρόσβασης και προλαμβάνουν το ανθρώπινο σφάλμα, όπως την αποστολή επικοινωνιών σε εσφαλμένο παραλήπτη. Η χρήση λογιστικών φύλλων και άλλων εγγράφων γραφείου δεν είναι κατάλληλος τρόπος διαχείρισης των δεδομένων των πελατών.

5 ΑΠΩΛΕΙΑ Ή ΚΛΟΠΗ ΣΥΣΚΕΥΩΝ ΚΑΙ ΕΓΓΡΑΦΩΝ ΣΕ ΕΓΧΑΡΤΗ ΜΟΡΦΗ

85. Περίπτωση η οποία απαντά συχνά είναι η απώλεια ή η κλοπή κινητών συσκευών. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας πρέπει να λάβει υπόψη τις περιστάσεις της πράξης επεξεργασίας, όπως το είδος των δεδομένων που αποθηκεύτηκαν στη συσκευή και τα υποστηρικτικά μέσα, καθώς και τα μέτρα που λήφθηκαν πριν από την παραβίαση προκειμένου να διασφαλιστεί κατάλληλο επίπεδο ασφάλειας. Όλα τα προαναφερθέντα στοιχεία επηρεάζουν τον δυνητικό αντίκτυπο της παραβίασης δεδομένων. Η αξιολόγηση κινδύνου μπορεί να είναι δυσχερής, δεδομένου ότι η συσκευή δεν είναι πλέον διαθέσιμη.

86. Τέτοιου είδους παραβιάσεις μπορούν πάντοτε να ταξινομηθούν ως παραβιάσεις απορρήτου. Ωστόσο, εάν δεν υπάρχει εφεδρικό αντίγραφο της κλαπείσας βάσης δεδομένων, η παραβίαση μπορεί επίσης να είναι παραβίαση διαθεσιμότητας και παραβίαση ακεραιότητας.

87. Τα σενάρια που ακολουθούν καταδεικνύουν τον τρόπο με τον οποίο οι προαναφερθείσες περιστάσεις επηρεάζουν το ενδεχόμενο και τη σοβαρότητα της παραβίασης δεδομένων.

5.1 ΠΕΡΙΠΤΩΣΗ αριθ. 10: Κλαπέν υλικό αποθήκευσης κρυπτογραφημένων δεδομένων προσωπικού χαρακτήρα

Στο πλαίσιο διάρρηξης σε παιδικό σταθμό, εκλάπησαν δύο ταμπλέτες. Οι ταμπλέτες περιείχαν εφαρμογή στην οποία τηρούνταν δεδομένα προσωπικού χαρακτήρα για τα παιδιά που πηγαίνουν στον παιδικό σταθμό. Τα δεδομένα περιλάμβαναν το όνομα, την ημερομηνία γέννησης και δεδομένα προσωπικού χαρακτήρα σχετικά με την εκπαίδευση των παιδιών. Τόσο οι κρυπτογραφημένες ταμπλέτες, οι οποίες δεν ήταν σε λειτουργία κατά τον χρόνο της διάρρηξης, όσο και η εφαρμογή προστατεύονταν από ισχυρό κωδικό πρόσβασης. Ο υπεύθυνος επεξεργασίας είχε πραγματικά και άμεσα στη διάθεσή του δεδομένα εφεδρικών αρχείων. Σύντομα μετά την ενημέρωση για τη διάρρηξη, ο παιδικός σταθμός έδωσε εξ αποστάσεως εντολή καταστροφής των δεδομένων των ταμπλετών.

5.1.1 ΠΕΡΙΠΤΩΣΗ αριθ. 10 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

88. Στη συγκεκριμένη περίπτωση, ο υπεύθυνος επεξεργασίας έλαβε κατάλληλα μέτρα για την πρόληψη και τον μετριασμό του αντικτύπου δυνητικής παραβίασης δεδομένων μέσω κρυπτογράφησης της συσκευής, θέσπισης κατάλληλης προστασίας των κωδικών πρόσβασης και εξασφάλισης εφεδρικών αρχείων των αποθηκευμένων στις ταμπλέτες δεδομένων. (Κατάλογος συνιστώμενων μέτρων παρέχεται στο σημείο 5.7.)

89. Μόλις ενημερωθεί για την παραβίαση, ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να αξιολογήσει την πηγή κινδύνου, τα συστήματα που υποστηρίζουν την επεξεργασία δεδομένων, το είδος των επηρεαζόμενων δεδομένων προσωπικού χαρακτήρα και τον δυνητικό αντίκτυπο της παραβίασης των δεδομένων για τα επηρεαζόμενα φυσικά πρόσωπα. Η παραβίαση δεδομένων που περιγράφηκε ανωτέρω θα μπορούσε να επηρεάσει το απόρρητο, τη διαθεσιμότητα και την ακεραιότητα των δεδομένων, αλλά, χάρη στην κατάλληλη διαδικασία που εφάρμοσε ο υπεύθυνος επεξεργασίας δεδομένων πριν από και μετά την παραβίαση, τα δεδομένα δεν επηρεάστηκαν με κανέναν από τους τρόπους αυτούς.

5.1.2 ΠΕΡΙΠΤΩΣΗ αριθ. 10 – Μετριασμός και υποχρεώσεις

90. Το απόρρητο των δεδομένων προσωπικού χαρακτήρα στις συσκευές δεν επηρεάστηκε χάρη στην ισχυρή προστασία των κωδικών πρόσβασης τόσο στις ταμπλέτες όσο και στις εφαρμογές. Οι ταμπλέτες ήταν ρυθμισμένες κατά τρόπο ώστε η ρύθμιση κωδικού πρόσβασης να συνεπάγεται επίσης την κρυπτογράφηση των δεδομένων στη συσκευή. Η πρόβλεψη αυτή ενισχύθηκε περαιτέρω από την ενέργεια του υπευθύνου επεξεργασίας να επιχειρήσει να καταστρέψει εξ αποστάσεως όλα τα δεδομένα στις κλαπείσες συσκευές.

91. Χάρη στα ληφθέντα μέτρα, το απόρρητο των δεδομένων διατηρήθηκε επίσης στο ακέραιο. Επιπλέον, τα εφεδρικά αρχεία διασφάλισαν τη συνεχή διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα και, επομένως, δεν μπορούσε να υπάρξει δυνητικός αρνητικός αντίκτυπος.

92. Για τους προαναφερθέντες λόγους, η παραβίαση δεδομένων που περιγράφηκε ανωτέρω δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, δεν είναι αναγκαία η γνωστοποίηση στην ΕΑ ή η ανακοίνωση στα ενδιαφερόμενα υποκείμενα των δεδομένων. Ωστόσο, και αυτή η παραβίαση δεδομένων πρέπει να τεκμηριωθεί σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	X	X

5.2 ΠΕΡΙΠΤΩΣΗ αριθ. 11: Κλαπέν υλικό αποθήκευσης μη κρυπτογραφημένων δεδομένων προσωπικού χαρακτήρα

Ο φορητός υπολογιστής υπαλλήλου εταιρείας παροχής υπηρεσιών εκλάπη. Ο κλαπείς φορητός υπολογιστής περιείχε το ονοματεπώνυμο, το φύλο, τη διεύθυνση και την ημερομηνία γέννησης 100 000 και πλέον πελατών. Λόγω της μη διαθεσιμότητας της κλαπείσας συσκευής, δεν είναι δυνατόν να προσδιοριστεί αν επηρεάστηκαν και άλλες κατηγορίες δεδομένων προσωπικού χαρακτήρα. Η πρόσβαση στον σκληρό δίσκο του φορητού υπολογιστή δεν προστατευόταν με οποιονδήποτε κωδικό πρόσβασης. Η επαναφορά των δεδομένων προσωπικού χαρακτήρα κατέστη δυνατή από τα διαθέσιμα εφεδρικά αρχεία που δημιουργούνται σε καθημερινή βάση.

5.2.1 ΠΕΡΙΠΤΩΣΗ αριθ. 11 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

93. Ο υπεύθυνος επεξεργασίας δεν έλαβε προηγούμενα μέτρα ασφάλειας και, επομένως, ο δράστης της κλοπής ή οποιοδήποτε άλλο πρόσωπο στην κατοχή του οποίου περιήλθε στη συνέχεια η συσκευή είχε ευχερή

πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που ήταν αποθηκευμένα στον κλαπέντα φορητό υπολογιστή.

94. Η συγκεκριμένη παραβίαση δεδομένων αφορά το απόρρητο των δεδομένων που ήταν αποθηκευμένα στην κλαπείσα συσκευή.

95. Ο φορητός υπολογιστής που περιείχε τα δεδομένα προσωπικού χαρακτήρα ήταν ευάλωτος στην προκειμένη περίπτωση, καθώς δεν διέθετε οποιαδήποτε προστασία των κωδικών πρόσβασης ή κρυπτογράφηση. Η έλλειψη βασικών μέτρων ασφάλειας αυξάνει το επίπεδο κινδύνου για τα επηρεαζόμενα υποκείμενα των δεδομένων. Επιπλέον, ο προσδιορισμός των ενδιαφερόμενων υποκειμένων των δεδομένων είναι επίσης προβληματικός, στοιχείο το οποίο αυξάνει επίσης τη σοβαρότητα της παραβίασης. Ο μεγάλος αριθμός ενδιαφερόμενων φυσικών προσώπων αυξάνει τον κίνδυνο, αλλά η παραβίαση δεδομένων δεν αφορά ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.

96. Κατά την αξιολόγηση κινδύνου[29], ο υπεύθυνος επεξεργασίας θα πρέπει να λάβει υπόψη τις δυνητικές συνέπειες και αρνητικές συνέπειες της παραβίασης του απορρήτου. Λόγω της παραβίασης, τα ενδιαφερόμενα υποκείμενα των δεδομένων μπορεί να γίνουν θύματα υποκλοπής ταυτότητας βασισμένης στα διαθέσιμα στην κλαπείσα συσκευή δεδομένα και, επομένως, ο κίνδυνος θεωρείται υψηλός.

5.2.2 ΠΕΡΙΠΤΩΣΗ αριθ. 11 – Μετριασμός και υποχρεώσεις

97. Η ενεργοποίηση της κρυπτογράφησης της συσκευής και η χρήση ισχυρής προστασίας των κωδικών πρόσβασης της αποθηκευμένης βάσης δεδομένων μπορούσαν να αποτρέψουν το ενδεχόμενο να επιφέρει η παραβίαση δεδομένων κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

98. Λόγω των ανωτέρω περιστάσεων, απαιτείται γνωστοποίηση στην ΕΑ, η δε ανακοίνωση στα ενδιαφερόμενα υποκείμενα των δεδομένων είναι επίσης απαραίτητη.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

5.3 ΠΕΡΙΠΤΩΣΗ αριθ. 12: Κλαπέντα αρχεία σε έγχαρτη μορφή τα οποία περιέχουν ευαίσθητα δεδομένα

Ημερολόγιο σε έγχαρτη μορφή εκλάπη από κέντρο απεξάρτησης τοξικομανών. Το ημερολόγιο περιείχε βασικά δεδομένα σχετικά με την ταυτότητα και την υγεία των ασθενών που νοσηλεύονταν στο κέντρο απεξάρτησης. Τα δεδομένα αποθηκεύονταν μόνο στο ημερολόγιο σε έγχαρτη μορφή και δεν υπήρχαν εφεδρικά αρχεία για τους ιατρούς που περιθάλπουν τους ασθενείς. Το ημερολόγιο δεν ήταν αποθηκευμένο σε κλειδωμένο συρτάρι ή αίθουσα, ο υπεύθυνος επεξεργασίας δεδομένων δεν είχε θεσπίσει ούτε σύστημα ελέγχου πρόσβασης ούτε οποιοδήποτε άλλο μέτρο ασφάλειας για τα έγγραφα σε έγχαρτη μορφή.

5.3.1 ΠΕΡΙΠΤΩΣΗ αριθ. 12 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

99. Ο υπεύθυνος επεξεργασίας δεν έλαβε προηγούμενα μέτρα ασφάλειας και, επομένως, το πρόσωπο που απέκτησε το ημερολόγιο είχε ευχερή πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που ήταν

[29] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

αποθηκευμένα σε αυτό. Επιπλέον, η φύση των δεδομένων προσωπικού χαρακτήρα που ήταν αποθηκευμένα στο ημερολόγιο καθιστά την έλλειψη εφεδρικών αρχείων με τα εν λόγω δεδομένα πολύ σοβαρό παράγοντα κινδύνου.

100. Η παρούσα περίπτωση αποτελεί παράδειγμα παραβίασης δεδομένων υψηλού κινδύνου. Λόγω της μη λήψης κατάλληλων προφυλάξεων ασφάλειας, απωλέσθηκαν ευαίσθητα δεδομένα που αφορούν την υγεία, κατά το άρθρο 9 παράγραφος 1 του ΓΚΠΔ. Δεδομένου ότι η παρούσα περίπτωση αφορά ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα, οι δυνητικοί κίνδυνοι για τα ενδιαφερόμενα υποκείμενα των δεδομένων αυξήθηκαν, στοιχείο το οποίο θα πρέπει επίσης να λάβει υπόψη ο υπεύθυνος επεξεργασίας κατά την αξιολόγηση του κινδύνου[30].

101. Η παρούσα παραβίαση αφορά την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα των επηρεαζόμενων δεδομένων προσωπικού χαρακτήρα. Λόγω της παραβίασης, θίγεται το ιατρικό απόρρητο και μη εξουσιοδοτημένοι τρίτοι μπορεί να αποκτήσουν πρόσβαση στις ιδιωτικές ιατρικές πληροφορίες των ασθενών, στοιχείο το οποίο μπορεί να έχει σοβαρό αντίκτυπο στην προσωπική ζωή των ασθενών. Η παραβίαση της διαθεσιμότητας μπορεί επίσης να διαταράξει τη συνέχεια της θεραπείας των ασθενών. Δεδομένου ότι δεν μπορεί να αποκλειστεί η μεταβολή/διαγραφή τμημάτων του περιεχομένου του ημερολογίου, επηρεάζεται επίσης η ακεραιότητα των δεδομένων προσωπικού χαρακτήρα.

5.3.2 ΠΕΡΙΠΤΩΣΗ αριθ. 12 – Μετριασμός και υποχρεώσεις

102. Κατά την αξιολόγηση των μέτρων ασφάλειας θα πρέπει να εξεταστεί επίσης το είδος του υποστηρικτικού μέσου. Δεδομένου ότι το ημερολόγιο ασθενών ήταν υλικό έγγραφο, η προστασία του έπρεπε να είχε οργανωθεί διαφορετικά από την προστασία ηλεκτρονικής συσκευής. Η ψευδωνυμοποίηση των ονομάτων των ασθενών, η αποθήκευση του ημερολογίου σε ασφαλή χώρο και σε κλειδωμένο συρτάρι ή αίθουσα και ο κατάλληλος έλεγχος της πρόσβασης με επαλήθευση ταυτότητας κατά την πρόσβαση μπορούσε να είχε αποτρέψει την παραβίαση δεδομένων.

103. Η ανωτέρω παραβίαση δεδομένων μπορεί να έχει σημαντικό αντίκτυπο για τα ενδιαφερόμενα υποκείμενα δεδομένων· Επομένως, η γνωστοποίηση στην ΕΑ και η ανακοίνωση της παραβίασης στα ενδιαφερόμενα υποκείμενα των δεδομένων είναι υποχρεωτική.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

5.4 Οργανωτικά και τεχνικά μέτρα για την πρόληψη / τον μετριασμό του αντικτύπου της απώλειας ή της κλοπής συσκευών

104. Ο συνδυασμός των κατωτέρω αναφερόμενων μέτρων —τα οποία εφαρμόζονται ανάλογα με τα μοναδικά χαρακτηριστικά κάθε περίπτωσης— αναμένεται να συμβάλει στη μείωση της πιθανότητας επανάληψης παρόμοιας παραβίασης στο μέλλον.

105. Συνιστώμενα μέτρα:

(*Ο κατάλογος των μέτρων που ακολουθούν δεν έχει σε καμία περίπτωση αποκλειστικό ή πλήρη χαρακτήρα. Αντιθέτως, στόχος είναι η παροχή ιδεών με σκοπό την πρόληψη και ενδεχόμενων λύσεων.*

[30] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

Κάθε διαδικασία επεξεργασίας είναι διαφορετική και, επομένως, ο υπεύθυνος επεξεργασίας θα πρέπει να αποφασίσει ποια μέτρα ανταποκρίνονται καλύτερα στη δεδομένη κατάσταση.)

- Ενεργοποίηση της κρυπτογράφησης της συσκευής (π.χ. Bitlocker, Veracrypt ή DM-Crypt).
- Χρήση κωδικού εισόδου / κωδικού πρόσβασης σε όλες τις συσκευές. Κρυπτογράφηση όλων των κινητών ηλεκτρονικών συσκευών κατά τρόπο που απαιτεί την εισαγωγή σύνθετου κωδικού πρόσβασης για την αποκρυπτογράφηση.
- Χρήση επαλήθευσης ταυτότητας πολλαπλών παραγόντων.
- Ενεργοποίηση των λειτουργικοτήτων σε εξαιρετικά κινητές συσκευές ώστε να είναι δυνατός ο εντοπισμός τους σε περίπτωση απώλειας ή εσφαλμένης τοποθέτησης.
- Χρήση λογισμικού/εφαρμογής MDM (διαχείριση κινητών συσκευών) και εντοπισμού. Χρήση αντιθαμβωτικών φίλτρων. Κλείσιμο συσκευών κατά την απουσία του χρήστη.
- Εφόσον είναι δυνατό και ενδείκνυται για τη συγκεκριμένη επεξεργασία δεδομένων, αποθήκευση των δεδομένων προσωπικού χαρακτήρα όχι σε κινητή συσκευή, αλλά σε κεντρικό νωτιαίο διακομιστή.
- Εάν ο σταθμός εργασίας είναι συνδεδεμένος με το εταιρικό τοπικό δίκτυο, αυτόματη δημιουργία εφεδρικών αρχείων από τους φακέλους εργασίας, εκτός εάν η αποθήκευση δεδομένων προσωπικού χαρακτήρα εκεί είναι αναπόφευκτη.
- Χρήση ασφαλούς VPN (π.χ. που απαιτεί χωριστό κλειδί επαλήθευσης ταυτότητας δύο παραγόντων για την εγκαθίδρυση ασφαλούς σύνδεσης) για τη σύνδεση κινητών συσκευών σε νωτιαίους διακομιστές.
- Παροχή υλικών κλειδαριών στους υπαλλήλους ώστε να μπορούν να ασφαλίζουν υλικά τις κινητές συσκευές που χρησιμοποιούν κατά την απουσία τους.
- Κατάλληλη ρύθμιση της χρήσης συσκευών εκτός της εταιρείας.
- Κατάλληλη ρύθμιση της χρήσης συσκευών εντός της εταιρείας.
- Χρήση λογισμικού/εφαρμογής MDM (διαχείριση κινητών συσκευών) και ενεργοποίηση της λειτουργίας εξ αποστάσεως καταστροφής των δεδομένων.
- Χρήση κεντρικής διαχείρισης συσκευών με ελάχιστα δικαιώματα όσον αφορά την εγκατάσταση λογισμικού από τους τελικούς χρήστες.
- Εγκατάσταση υλικών μέσων ελέγχου πρόσβασης.
- Αποφυγή αποθήκευσης ευαίσθητων πληροφοριών σε κινητές συσκευές ή σκληρούς δίσκους. Εάν απαιτείται πρόσβαση στο εσωτερικό σύστημα της εταιρείας, θα πρέπει να χρησιμοποιούνται ασφαλείς δίαυλοι, όπως προαναφέρθηκε.

6 ΣΦΑΛΜΑ ΑΠΟΣΤΟΛΗΣ

106. Η πηγή κινδύνου είναι και στην προκειμένη περίπτωση εσωτερικό ανθρώπινο σφάλμα, πλην όμως δεν υπάρχει κακόβουλη ενέργεια η οποία οδηγεί στην παραβίαση. Η παραβίαση προκαλείται εκ παραδρομής. Ο υπεύθυνος επεξεργασίας δεν έχει πολλές δυνατότητες μετά την επέλευση τέτοιας παραβίασης και, επομένως, η πρόληψη είναι ακόμη πιο σημαντική στις περιπτώσεις αυτές από ό,τι σε άλλου είδους παραβιάσεις.

6.1 ΠΕΡΙΠΤΩΣΗ αριθ. 13: Σφάλμα ταχυδρομικής αποστολής

Εταιρεία λιανικής πώλησης συσκεύασε δύο παραγγελίες υποδημάτων. Λόγω ανθρώπινου σφάλματος, τα προϊόντα και τα αντίστοιχα δελτία αποστολής εστάλησαν σε εσφαλμένους παραλήπτες. Τούτο σημαίνει ότι κάθε πελάτης παρέλαβε την παραγγελία του άλλου, καθώς και τα δελτία αποστολής που περιείχαν τα δεδομένα προσωπικού χαρακτήρα του άλλου πελάτη. Μόλις αντιλήφθηκε την παραβίαση, ο υπεύθυνος επεξεργασίας ανακάλεσε τις παραγγελίες και τις απέστειλε στους ορθούς παραλήπτες.

6.1.1 ΠΕΡΙΠΤΩΣΗ αριθ. 13 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

107. Τα δελτία αποστολής περιείχαν τα δεδομένα προσωπικού χαρακτήρα που απαιτούνται για την κατάλληλη παράδοση (όνομα, διεύθυνση, καθώς και το αγορασθέν προϊόν και την τιμή του). Είναι σημαντικό να προσδιοριστεί αρχικά ο τρόπος επέλευσης του ανθρώπινου σφάλματος και αν μπορούσε να έχει αποφευχθεί με κάποιον τρόπο. Στην προκειμένη περίπτωση, ο κίνδυνος είναι χαμηλός, καθώς η παραβίαση δεν αφορά ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα ή άλλα δεδομένα των οποίων η κατάχρηση θα μπορούσε να συνεπάγεται σημαντικές αρνητικές συνέπειες, η παραβίαση δεν είναι αποτέλεσμα συστημικού σφάλματος του υπευθύνου επεξεργασίας, αφορά δε μόνο δύο φυσικά πρόσωπα. Δεν εντοπίστηκε καμία αρνητική συνέπεια για τα φυσικά πρόσωπα.

6.1.2 ΠΕΡΙΠΤΩΣΗ αριθ. 13 – Μετριασμός και υποχρεώσεις

108. Ο υπεύθυνος επεξεργασίας θα πρέπει να προβλέψει τη δωρεάν επιστροφή των προϊόντων και των συνοδευτικών δελτίων αποστολής και θα πρέπει να ζητήσει επίσης από τους εσφαλμένους παραλήπτες να καταστρέψουν/διαγράψουν όλα τα ενδεχόμενα αντίγραφα των δελτίων αποστολής που περιέχουν τα δεδομένα προσωπικού χαρακτήρα του άλλου προσώπου.

109. Ακόμη και αν η ίδια η παραβίαση δεν ενέχει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των επηρεαζόμενων φυσικών προσώπων και, επομένως, η ανακοίνωση στα υποκείμενα των δεδομένων δεν είναι υποχρεωτική βάσει του άρθρου 34 του ΓΚΠΔ, η ανακοίνωση της παραβίασης σε αυτά είναι αναπόφευκτη, καθώς απαιτείται η συνεργασία τους για τον μετριασμό του κινδύνου.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	X	X

6.2 ΠΕΡΙΠΤΩΣΗ αριθ. 14: Εκ παραδρομής αποστολή εξαιρετικά εμπιστευτικών δεδομένων προσωπικού χαρακτήρα μέσω ηλεκτρονικού ταχυδρομείου

Η υπηρεσία απασχόλησης δημόσιου οργανισμού απέστειλε ηλεκτρονικό μήνυμα –σχετικά με προσεχή σεμινάρια κατάρτισης– στα φυσικά πρόσωπα που είναι καταχωρισμένα στο σύστημά της ως άτομα που αναζητούν εργασία. Εκ παραδρομής, προσαρτήθηκε στο εν λόγω ηλεκτρονικό μήνυμα έγγραφο το οποίο περιείχε τα δεδομένα προσωπικού χαρακτήρα όλων των εν λόγω ατόμων (όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, ταχυδρομική διεύθυνση, αριθμός μητρώου κοινωνικής ασφάλισης). Ο αριθμός των επηρεαζόμενων φυσικών προσώπων υπερβαίνει τα 60 000. Κατά συνέπεια, η υπηρεσία επικοινώνησε με όλους τους παραλήπτες του μηνύματος και τους ζήτησε να διαγράψουν το προηγούμενο μήνυμα που έλαβαν και να μην χρησιμοποιήσουν τις πληροφορίες που περιέχονται σε αυτό.

6.2.1 ΠΕΡΙΠΤΩΣΗ αριθ. 14 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

110. Για την αποστολή τέτοιων μηνυμάτων θα έπρεπε να εφαρμόζονται αυστηρότεροι κανόνες. Πρέπει να εξεταστεί η θέσπιση πρόσθετων μηχανισμών ελέγχου.

111. Ο αριθμός των επηρεαζόμενων φυσικών προσώπων είναι μεγάλος, το δε γεγονός ότι η παραβίαση αφορά τον αριθμό μητρώου κοινωνικής ασφάλισης, σε συνδυασμό με άλλα, πιο βασικά, δεδομένα προσωπικού

χαρακτήρα, αυξάνει περαιτέρω τον κίνδυνο, ο οποίος μπορεί να προσδιοριστεί ως υψηλός[31]. Ο υπεύθυνος επεξεργασίας δεν μπορεί να εμποδίσει την ενδεχόμενη διανομή των δεδομένων από οποιονδήποτε εκ των παραληπτών του μηνύματος.

6.2.2 ΠΕΡΙΠΤΩΣΗ αριθ. 14 – Μετριασμός και υποχρεώσεις

112. Όπως προαναφέρθηκε, τα μέσα για τον αποτελεσματικό μετριασμό των κινδύνων παρόμοιας παραβίασης είναι περιορισμένα. Μολονότι ζήτησε τη διαγραφή του μηνύματος, ο υπεύθυνος επεξεργασίας δεν μπορεί να υποχρεώσει τους παραλήπτες να πράξουν κάτι τέτοιο και, κατά συνέπεια, δεν μπορεί επίσης να είναι βέβαιος ότι θα συμμορφωθούν με το αίτημά του.

113. Η εκτέλεση και των τριών ενεργειών που αναφέρονται κατωτέρω θα πρέπει να είναι αυτονόητη σε τέτοιες περιπτώσεις.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

6.3 ΠΕΡΙΠΤΩΣΗ αριθ. 15: Εκ παραδρομής αποστολή δεδομένων προσωπικού χαρακτήρα μέσω ηλεκτρονικού ταχυδρομείου

> Κατάλογος των συμμετεχόντων σε σεμινάριο νομικών αγγλικών, το οποίο πραγματοποιείται σε ξενοδοχείο επί 5 ημέρες, αποστέλλεται εκ παραδρομής σε 15 πρώην συμμετέχοντες στο σεμινάριο αντί του ξενοδοχείου. Ο κατάλογος περιέχει ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου και διατροφικές προτιμήσεις των 15 συμμετεχόντων. Μόνο δύο συμμετέχοντες έχουν συμπληρώσει τις διατροφικές προτιμήσεις τους, αναφέροντας ότι έχουν δυσανεξία στη λακτόζη. Κανένας εκ των συμμετεχόντων δεν διαθέτει προστατευμένη ταυτότητα. Ο υπεύθυνος επεξεργασίας εντοπίζει το σφάλμα αμέσως μετά την αποστολή του καταλόγου, ενημερώνει τους παραλήπτες για το σφάλμα και τους ζητεί να διαγράψουν τον κατάλογο.

6.3.1 ΠΕΡΙΠΤΩΣΗ αριθ. 15 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

114. Για την αποστολή μηνυμάτων που περιέχουν δεδομένα προσωπικού χαρακτήρα θα έπρεπε να έχουν εφαρμοστεί αυστηροί κανόνες. Πρέπει να εξεταστεί η θέσπιση πρόσθετων μηχανισμών ελέγχου.

115. Οι κίνδυνοι που απορρέουν από τη φύση, την ευαισθησία, τον όγκο και το πλαίσιο των δεδομένων προσωπικού χαρακτήρα είναι χαμηλοί. Τα δεδομένα προσωπικού χαρακτήρα περιλαμβάνουν ευαίσθητα δεδομένα σχετικά με διατροφικές προτιμήσεις δύο εκ των συμμετεχόντων. Μολονότι η πληροφορία ότι ένα πρόσωπο έχει δυσανεξία στη λακτόζη είναι δεδομένο που αφορά την υγεία, ο κίνδυνος να χρησιμοποιηθεί το εν λόγω δεδομένο με επιζήμιο τρόπο θα πρέπει να θεωρηθεί σχετικά χαμηλός. Παρότι, όταν πρόκειται για δεδομένα που αφορούν την υγεία, θεωρείται συνήθως ότι η παραβίαση ενδέχεται να επιφέρει υψηλό κίνδυνο για το υποκείμενο των δεδομένων[32], ωστόσο, στην προκειμένη περίπτωση, δεν εντοπίζεται κανένας κίνδυνος ότι η παραβίαση θα έχει ως αποτέλεσμα σωματική, υλική ή ηθική βλάβη για το υποκείμενο των δεδομένων, λόγω της γνωστοποίησης άνευ άδειας πληροφοριών σχετικών με τη δυσανεξία στη λακτόζη. Αντίθετα με ό,τι ισχύει για ορισμένες άλλες διατροφικές προτιμήσεις, η δυσανεξία στη λακτόζη δεν μπορεί

[31] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

[32] Βλ. κατευθυντήριες γραμμές WP250, σ. 29.

κανονικά να συνδεθεί με τυχόν θρησκευτικές ή φιλοσοφικές πεποιθήσεις. Η ποσότητα των δεδομένων που παραβιάστηκαν και ο αριθμός των επηρεαζόμενων υποκειμένων των δεδομένων είναι επίσης πολύ μικροί.

6.3.2 ΠΕΡΙΠΤΩΣΗ αριθ. 15 – Μετριασμός και υποχρεώσεις

116. Εν ολίγοις, μπορεί να θεωρηθεί ότι η παραβίαση δεν είχε σημαντικές συνέπειες για τα υποκείμενα των δεδομένων. Το γεγονός ότι ο υπεύθυνος επεξεργασίας επικοινώνησε αμελλητί με τους παραλήπτες, μόλις αντιλήφθηκε το σφάλμα, μπορεί να θεωρηθεί παράγοντας μετριασμού.

117. Εάν ηλεκτρονικό μήνυμα αποσταλεί σε εσφαλμένο / μη εξουσιοδοτημένο παραλήπτη, συνιστάται στον υπεύθυνο επεξεργασίας δεδομένων να αποστείλει ηλεκτρονικό μήνυμα συνέχειας σε κάθε παραλήπτη που έλαβε το αρχικό μήνυμα που δεν προοριζόταν για αυτόν, με απόκρυψη των στοιχείων των λοιπών παραληπτών, με το οποίο θα ζητεί συγγνώμη για το συμβάν και τη διαγραφή του μηνύματος που τον θίγει και θα ενημερώνει τους παραλήπτες ότι δεν έχουν το δικαίωμα να κάνουν περαιτέρω χρήση των διευθύνσεων ηλεκτρονικού ταχυδρομείου που περιήλθαν σε γνώση τους.

118. Για τους προαναφερθέντες λόγους, η παρούσα παραβίαση δεδομένων δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, δεν είναι αναγκαία η γνωστοποίηση στην ΕΑ ή η ανακοίνωση στα ενδιαφερόμενα υποκείμενα των δεδομένων. Ωστόσο, και αυτή η παραβίαση δεδομένων πρέπει να τεκμηριωθεί σύμφωνα με το άρθρο 33 παράγραφος 5 του ΓΚΠΔ.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	X	X

6.4 ΠΕΡΙΠΤΩΣΗ αριθ. 16: Σφάλμα ταχυδρομικής αποστολής

Ασφαλιστικός όμιλος παρέχει ασφάλιση αυτοκινήτων. Στο πλαίσιο αυτό, αποστέλλει τακτικά ταχυδρομικώς ασφαλιστήρια συμβόλαια προσαρμοσμένων εισφορών. Επιπλέον του ονόματος και της διεύθυνσης του λήπτη της ασφάλισης, η επιστολή περιέχει τον αριθμό κυκλοφορίας του οχήματος, με εμφανή τα ψηφία, τις τιμές των ασφαλίστρων του τρέχοντος και του επόμενου έτους ασφάλισης, την κατά προσέγγιση ετήσια διανυθείσα απόσταση και την ημερομηνία γέννησης του λήπτη της ασφάλισης. Στην επιστολή δεν περιέχονται δεδομένα που αφορούν την υγεία κατά το άρθρο 9 του ΓΚΠΔ, στοιχεία πληρωμής (τραπεζικά στοιχεία), οικονομικά και χρηματοοικονομικά δεδομένα.

Οι επιστολές τοποθετούνται σε φακέλους με αυτοματοποιημένο μηχανικό τρόπο. Λόγω μηχανικής βλάβης, δύο επιστολές οι οποίες απευθύνονταν σε διαφορετικούς λήπτες ασφάλισης τοποθετήθηκαν στον ίδιο φάκελο και εστάλησαν ταχυδρομικώς σε έναν λήπτη ασφάλισης. Ο λήπτης της ασφάλισης ανοίγει την επιστολή στο σπίτι του και βλέπει την επιστολή που ορθώς εστάλη στη διεύθυνσή του καθώς και την επιστολή που προοριζόταν για άλλον λήπτη ασφάλισης και παραδόθηκε εσφαλμένως στον ίδιο.

6.4.1 ΠΕΡΙΠΤΩΣΗ αριθ. 16 – Προηγούμενα μέτρα και αξιολόγηση κινδύνου

119. Η επιστολή που παραδόθηκε εσφαλμένως περιέχει το όνομα, τη διεύθυνση, την ημερομηνία γέννησης, τον αριθμό κυκλοφορίας του οχήματος, με εμφανή τα ψηφία, και την ταξινόμηση της τιμής ασφαλίστρων για το τρέχον και το επόμενο έτος. Οι συνέπειες για το επηρεαζόμενο πρόσωπο πρέπει να θεωρηθούν μεσαίας σοβαρότητας, καθώς μη δημόσια διαθέσιμες πληροφορίες, όπως η ημερομηνία γέννησης ή ο αριθμός κυκλοφορίας οχήματος, με εμφανή τα ψηφία, και στοιχεία σχετικά με την επαύξηση της τιμής των ασφαλίστρων γνωστοποιούνται σε μη εξουσιοδοτημένο παραλήπτη. Η πιθανότητα κατάχρησης των συγκεκριμένων δεδομένων αξιολογείται από χαμηλή έως μεσαία. Ωστόσο, μολονότι πολλοί παραλήπτες θα

πετάξουν κατά πάσα πιθανότητα στα σκουπίδια την επιστολή που παρέλαβαν εσφαλμένως, σε μεμονωμένες περιπτώσεις δεν μπορεί να αποκλειστεί πλήρως το ενδεχόμενο να αναρτηθεί η επιστολή σε μέσα κοινωνικής δικτύωσης ή να επιχειρηθεί επικοινωνία με τον λήπτη της ασφάλισης.

6.4.2 ΠΕΡΙΠΤΩΣΗ αριθ. 16 – Μετριασμός και υποχρεώσεις

120. Ο υπεύθυνος επεξεργασίας θα πρέπει να μεριμνήσει για την επιστροφή του πρωτότυπου εγγράφου με δικά του έξοδα. Ο εσφαλμένος παραλήπτης θα πρέπει να ενημερωθεί επίσης ότι δεν δικαιούται να κάνει κακή χρήση των πληροφοριών που περιήλθαν σε γνώση του.

121. Είναι πιθανώς αδύνατον να αποφευχθεί πλήρως κάθε σφάλμα ταχυδρομικής αποστολής σε περίπτωση μαζικής αποστολής αλληλογραφίας μέσω πλήρως αυτοματοποιημένων μηχανών. Ωστόσο, σε περίπτωση αυξημένης συχνότητας σφαλμάτων, είναι αναγκαίο να ελεγχθεί αν οι μηχανές έχουν ρυθμιστεί και συντηρούνται καταλλήλως ή αν κάποιο άλλο συστημικό ζήτημα είχε ως αποτέλεσμα την εν λόγω παραβίαση.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	X

6.5 Οργανωτικά και τεχνικά μέτρα για την πρόληψη / τον μετριασμό του αντικτύπου των σφαλμάτων αποστολής

122. Ο συνδυασμός των κατωτέρω αναφερόμενων μέτρων –τα οποία εφαρμόζονται ανάλογα με τα μοναδικά χαρακτηριστικά κάθε περίπτωσης– αναμένεται να συμβάλει στη μείωση της πιθανότητας επανάληψης παρόμοιας παραβίασης στο μέλλον.

123. Συνιστώμενα μέτρα:

(*Ο κατάλογος των μέτρων που ακολουθούν δεν έχει σε καμία περίπτωση αποκλειστικό ή πλήρη χαρακτήρα. Αντιθέτως, στόχος είναι η παροχή ιδεών με σκοπό την πρόληψη και ενδεχόμενων λύσεων. Κάθε διαδικασία επεξεργασίας είναι διαφορετική και, επομένως, ο υπεύθυνος επεξεργασίας θα πρέπει να αποφασίσει ποια μέτρα ανταποκρίνονται καλύτερα στη δεδομένη κατάσταση.*)

- Καθορισμός επακριβών κανόνων –που δεν αφήνουν περιθώρια ερμηνείας– για την αποστολή επιστολών / ηλεκτρονικών μηνυμάτων.
- Κατάλληλη κατάρτιση του προσωπικού σχετικά με τον τρόπο αποστολής επιστολών / ηλεκτρονικών μηνυμάτων.
- Κατά την αποστολή ηλεκτρονικών μηνυμάτων σε πολλαπλούς παραλήπτες, αυτοί απαριθμούνται, από προεπιλογή, στο πεδίο «bcc».
- Απαιτείται επιπλέον επιβεβαίωση κατά την αποστολή ηλεκτρονικών μηνυμάτων σε πολλαπλούς παραλήπτες, οι οποίοι δεν απαριθμούνται στο πεδίο «bcc».
- Εφαρμογή της αρχής του ελέγχου από δεύτερο πρόσωπο.
- Αυτόματη, αντί χειροκίνητης, αναγραφής της διεύθυνσης, με δεδομένα τα οποία αντλούνται από διαθέσιμη και επικαιροποιημένη βάση δεδομένων· το αυτόματο σύστημα αναγραφής της διεύθυνσης θα πρέπει να επανεξετάζεται τακτικά για την αναζήτηση κρυφών σφαλμάτων και εσφαλμένων ρυθμίσεων.
- Εφαρμογή καθυστέρησης αποστολής μηνύματος (π.χ. το μήνυμα μπορεί να διαγραφεί / να υποβληθεί σε επεξεργασία εντός ορισμένου χρονικού διαστήματος μετά το πάτημα του σχετικού κουμπιού).
- Απενεργοποίηση της αυτόματης συμπλήρωσης κατά την αναγραφή διευθύνσεων ηλεκτρονικού ταχυδρομείου.

- Μαθήματα ευαισθητοποίησης σχετικά με τα συνηθέστερα σφάλματα που οδηγούν σε παραβίαση δεδομένων προσωπικού χαρακτήρα.
- Μαθήματα κατάρτισης και εγχειρίδια σχετικά με τον τρόπο χειρισμού περιστατικών που οδηγούν σε παραβίαση δεδομένων προσωπικού χαρακτήρα και τα πρόσωπα που πρέπει να ενημερωθούν (συμμετοχή ΥΠΔ).

7 ΆΛΛΕΣ ΠΕΡΙΠΤΩΣΕΙΣ – ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ

7.1 ΠΕΡΙΠΤΩΣΗ αριθ. 17: Υποκλοπή ταυτότητας

Το τηλεφωνικό κέντρο εταιρείας τηλεπικοινωνιών λαμβάνει τηλεφωνική κλήση από πρόσωπο που δηλώνει πελάτης. Ο φερόμενος ως πελάτης ζητεί από την εταιρεία να αλλάξει τη διεύθυνση ηλεκτρονικού ταχυδρομείου στην οποία θα πρέπει να αποστέλλονται πλέον τα στοιχεία που αφορούν την τιμολόγηση. Ο υπάλληλος του τηλεφωνικού κέντρου επικυρώνει την ταυτότητα του πελάτη ζητώντας ορισμένα δεδομένα προσωπικού χαρακτήρα όπως προβλέπεται από τις διαδικασίες της εταιρείας. Ο φερόμενος ως πελάτης αναφέρει ορθώς τον αριθμό φορολογικού μητρώου και την ταχυδρομική διεύθυνση του πελάτη (επειδή απέκτησε πρόσβαση στα εν λόγω στοιχεία). Μετά την επικύρωση, ο υπάλληλος πραγματοποιεί τη ζητηθείσα αλλαγή και, πλέον, τα στοιχεία που αφορούν την τιμολόγηση αποστέλλονται στη νέα διεύθυνση ηλεκτρονικού ταχυδρομείου. Η διαδικασία δεν προβλέπει οποιαδήποτε γνωστοποίηση στην προηγούμενη διεύθυνση ηλεκτρονικού ταχυδρομείου. Τον επόμενο μήνα ο πραγματικός πελάτης επικοινωνεί με την εταιρεία και ζητεί να πληροφορηθεί τον λόγο για τον οποίο δεν λαμβάνει τα στοιχεία που αφορούν την τιμολόγηση στη διεύθυνσή του ηλεκτρονικού ταχυδρομείου και αρνείται ότι τηλεφώνησε και ζήτησε την αλλαγή της διεύθυνσης ηλεκτρονικού ταχυδρομείου. Η εταιρεία αντιλαμβάνεται αργότερα ότι οι πληροφορίες εστάλησαν σε πρόσωπο που δεν δικαιούνταν να τις λάβει και προβαίνει εκ νέου σε αλλαγή της διεύθυνσης ηλεκτρονικού ταχυδρομείου.

7.1.1 ΠΕΡΙΠΤΩΣΗ αριθ. 17 – Αξιολόγηση κινδύνου, μετριασμός και υποχρεώσεις

124. Η παρούσα περίπτωση καταδεικνύει τη σημασία των προηγούμενων μέτρων. Όσον αφορά τον κίνδυνο, η παραβίαση ενέχει υψηλό επίπεδο κινδύνου33, καθώς τα στοιχεία τιμολόγησης μπορούν να παράσχουν πληροφορίες σχετικά με την ιδιωτική ζωή του υποκειμένου των δεδομένων (π.χ. συνήθειες, επαφές) και θα μπορούσαν να οδηγήσουν σε υλική ζημία (π.χ. επίμονη παρακολούθηση, κίνδυνος για τη σωματική ακεραιότητα). Τα δεδομένα προσωπικού χαρακτήρα που αποκτήθηκαν κατά την εν λόγω επίθεση μπορούν επίσης να χρησιμοποιηθούν για τη διευκόλυνση της υποκλοπής λογαριασμού στον εν λόγω οργανισμό ή για την εκμετάλλευση περαιτέρω μέτρων επαλήθευσης ταυτότητας σε άλλους οργανισμούς. Λαμβανομένων υπόψη των κινδύνων αυτών, το «κατάλληλο» μέτρο επαλήθευσης ταυτότητας θα πρέπει να ανταποκρίνεται σε υψηλές απαιτήσεις, ανάλογα με τα δεδομένα προσωπικού χαρακτήρα τα οποία μπορούν να υποβληθούν σε επεξεργασία κατόπιν επαλήθευσης της ταυτότητας.

125. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας οφείλει να προβεί τόσο σε γνωστοποίηση στην ΕΑ όσο και σε ανακοίνωση στο υποκείμενο των δεδομένων.

[33] Για καθοδήγηση σχετικά με πράξεις επεξεργασίας που «*ενδέχεται να επιφέρουν υψηλό κίνδυνο*» για τα δικαιώματα και τις ελευθερίες, βλ. υποσημείωση 10 ανωτέρω.

126. Είναι σαφές ότι η διαδικασία προηγούμενης επικύρωσης του πελάτη πρέπει να τελειοποιηθεί λαμβανομένης υπόψη της παρούσας περίπτωσης. Οι μέθοδοι που χρησιμοποιήθηκαν για την επαλήθευση ταυτότητας δεν ήταν επαρκείς. Ο κακόβουλος τρίτος μπόρεσε να ισχυριστεί ότι ήταν ο πραγματικός χρήστης μέσω της χρήσης δημόσια διαθέσιμων πληροφοριών και πληροφοριών στις οποίες απέκτησε πρόσβαση με άλλον τρόπο.

127. Η χρήση αυτού του είδους στατικής επαλήθευσης ταυτότητας που βασίζεται στη γνώση πληροφοριών (στην οποία η απάντηση δεν μεταβάλλεται και οι πληροφορίες δεν είναι απόρρητες όπως συμβαίνει στην περίπτωση κωδικού πρόσβασης) δεν συνιστάται.

128. Αντ' αυτής, ο οργανισμός θα πρέπει να χρησιμοποιεί μορφή επαλήθευσης της ταυτότητας η οποία θα έχει ως αποτέλεσμα υψηλό βαθμό εμπιστοσύνης ότι ο χρήστης του οποίου η ταυτότητα επαληθεύτηκε είναι ο πραγματικός χρήστης και όχι κάποιο άλλο πρόσωπο. Η εφαρμογή μεθόδου εξωζωνικής επαλήθευσης ταυτότητας πολλαπλών παραγόντων θα επέλυε το πρόβλημα, π.χ. για την επαλήθευση του αιτήματος αλλαγής, μέσω της αποστολής αιτήματος επιβεβαίωσης στην προηγούμενη διεύθυνση επικοινωνίας· ή μέσω της προσθήκης επιπλέον ερωτήσεων και αιτήματος παροχής πληροφοριών που είναι εμφανείς μόνο στους προηγούμενους λογαριασμούς. Ο υπεύθυνος επεξεργασίας πρέπει να αποφασίσει τα μέτρα τα οποία θα θεσπίσει, καθώς γνωρίζει καλύτερα τις λεπτομέρειες και τις απαιτήσεις της εσωτερικής λειτουργίας του οργανισμού του.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓

7.2 ΠΕΡΙΠΤΩΣΗ αριθ. 18: Απόσπαση δεδομένων από ηλεκτρονικό μήνυμα

Αλυσίδα υπεραγορών εντόπισε, 3 μήνες μετά τη διάρθρωση, ότι ορισμένοι λογαριασμοί είχαν αλλοιωθεί και ότι είχαν δημιουργηθεί κανόνες βάσει των οποίων κάθε ηλεκτρονικό μήνυμα που περιείχε ορισμένες φράσεις (π.χ. «τιμολόγιο», «πληρωμή», «τραπεζικό έμβασμα», «επαλήθευση στοιχείων πιστωτικής κάρτας», «στοιχεία τραπεζικού λογαριασμού») μεταφερόταν σε μη χρησιμοποιούμενο φάκελο και διαβιβαζόταν επίσης σε εξωτερική διεύθυνση ηλεκτρονικού ταχυδρομείου. Επίσης, στο διάστημα αυτό, είχε ήδη λάβει χώρα επίθεση κοινωνικής μηχανικής, στο πλαίσιο της οποίας ο δράστης της επίθεσης, εμφανιζόμενος ως προμηθευτής, αλλοίωσε τα στοιχεία του τραπεζικού λογαριασμού του συγκεκριμένου προμηθευτή και τα αντικατέστησε με τα στοιχεία του δικού του τραπεζικού λογαριασμού. Τέλος, στο ίδιο διάστημα, εστάλησαν πλείονα ψευδή τιμολόγια στα οποία αναγραφόταν τα νέα στοιχεία του τραπεζικού λογαριασμού. Το σύστημα παρακολούθησης της πλατφόρμας ηλεκτρονικού ταχυδρομείου εξέδωσε τελικά προειδοποίηση σε σχέση με τους φακέλους. Η εταιρεία δεν μπόρεσε να εξακριβώσει τον τρόπο με τον οποίο ο δράστης της επίθεσης μπόρεσε να αποκτήσει πρόσβαση στους λογαριασμούς ηλεκτρονικού ταχυδρομείου, αλλά υπέθεσε ότι κάποιο ηλεκτρονικό μήνυμα που έφερε ιό έδωσε πρόσβαση στην υπεύθυνη για τις πληρωμές ομάδα χρηστών.

Λόγω της διαβίβασης των ηλεκτρονικών μηνυμάτων βάσει λέξεων-κλειδιών, ο δράστης της επίθεσης έλαβε πληροφορίες σχετικά με 99 υπαλλήλους: όνομα και μισθός συγκεκριμένου μήνα σε σχέση με 89 υποκείμενα των δεδομένων· όνομα, οικογενειακή κατάσταση, αριθμός τέκνων, μισθός, ώρες εργασίας και άλλες πληροφορίες στο φύλλο μισθοδοσίας 10 υπαλλήλων των οποίων οι συμβάσεις καταγγέλθηκαν Ο υπεύθυνος επεξεργασίας ενημέρωσε μόνο τους 10 υπαλλήλους της δεύτερης ομάδας επηρεαζόμενων προσώπων.

7.2.1 ΠΕΡΙΠΤΩΣΗ αριθ. 18 – Αξιολόγηση κινδύνου, μετριασμός και υποχρεώσεις

129. Ακόμη και αν ο δράστης της επίθεσης δεν αποσκοπούσε πιθανώς στη συλλογή δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι η παραβίαση μπορεί να οδηγήσει τόσο σε υλική (π.χ. οικονομική ζημία) όσο και σε ηθική βλάβη (π.χ. υποκλοπή ταυτότητας ή απάτη) και τα δεδομένα μπορούν να χρησιμοποιηθούν για τη διευκόλυνση άλλων επιθέσεων (π.χ. ηλεκτρονικό ψάρεμα), η παραβίαση των δεδομένων προσωπικού χαρακτήρα ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις υποχρεώσεις φυσικών προσώπων. Ως εκ τούτου, η παραβίαση θα πρέπει να ανακοινωθεί και στους 99 υπαλλήλους και όχι μόνο στους 10 υπαλλήλους σε σχέση με τους οποίους διέρρευσαν πληροφορίες για τον μισθό τους.

130. Μόλις έλαβε γνώση της παραβίασης, ο υπεύθυνος επεξεργασίας επέβαλε την αλλαγή κωδικών πρόσβασης για τους επηρεαζόμενους λογαριασμούς, εμπόδισε την αποστολή ηλεκτρονικών μηνυμάτων στον λογαριασμό ηλεκτρονικού ταχυδρομείου του δράστη της επίθεσης, ενημέρωσε τον πάροχο υπηρεσιών σχετικά με τη διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποίησε ο δράστης της επίθεσης σε σχέση με τις πράξεις του, αφαίρεσε τους κανόνες που είχε θεσπίσει ο δράστης της επίθεσης και τελειοποίησε τις προειδοποιήσεις του συστήματος παρακολούθησης, ώστε να παρέχεται προειδοποίηση μόλις δημιουργηθεί αυτόματος κανόνας. Εναλλακτικά, ο υπεύθυνος επεξεργασίας μπορεί να αφαιρέσει το δικαίωμα των χρηστών να καθορίζουν κανόνες διαβίβασης, ώστε η ομάδα εξυπηρέτησης των πληροφοριακών συστημάτων να πράττει κάτι τέτοιο μόνο κατόπιν αιτήματος, ή μπορεί να θεσπίσει πολιτική σύμφωνα με την οποία οι χρήστες θα πρέπει να ελέγχουν και να υποβάλλουν αναφορά σχετικά με τους κανόνες που έχουν θεσπιστεί στους λογαριασμούς τους μία φορά την εβδομάδα ή συχνότερα, σε τομείς που συνεπάγονται χειρισμό οικονομικών στοιχείων.

131. Το γεγονός ότι υπήρξε παραβίαση και δεν εντοπίστηκε για τόσο μεγάλο χρονικό διάστημα και το γεγονός ότι, σε μεγαλύτερο χρονικό διάστημα, μπορούσε να έχει χρησιμοποιηθεί κοινωνική μηχανική για την αλλοίωση περισσότερων δεδομένων ανέδειξε σημαντικά προβλήματα στο σύστημα ασφάλειας συστημάτων πληροφοριών του υπευθύνου επεξεργασίας. Τα προβλήματα αυτά θα πρέπει να αντιμετωπιστούν χωρίς καθυστέρηση, με έμφαση στην επανεξέταση των αυτοματισμών και τους ελέγχους αλλαγών καθώς και σε μέτρα εντοπισμού και αντιμετώπισης περιστατικών. Οι υπεύθυνοι επεξεργασίας που χειρίζονται ευαίσθητα δεδομένα, οικονομικά στοιχεία κ.λπ. υπέχουν μεγαλύτερη ευθύνη όσον αφορά την παροχή κατάλληλης ασφάλειας δεδομένων.

Αναγκαίες ενέργειες βάσει των προσδιορισθέντων κινδύνων		
Εσωτερική τεκμηρίωση	Γνωστοποίηση στην ΕΑ	Ανακοίνωση στα υποκείμενα των δεδομένων
✓	✓	✓