EIOPA-BoS-20/600

Κατευθυντήριες γραμμές σχετικά με την ασφάλεια και τη διακυβέρνηση των τεχνολογιών των πληροφοριών και των επικοινωνιών

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Germany - Tel. + 49 69-951119-20;
Φαξ + 49 69-951119-19; email: info@eiopa.europa.eu site: www.eiopa.europa.eu

Πίνακας περιεχομένων

Πλαίσιο

1. Σύμφωνα με το άρθρο 16 του κανονισμού (ΕΕ) αριθ. 1094/2010, η ΕΙΟΡΑ μπορεί να εκδίδει κατευθυντήριες γραμμές και συστάσεις που απευθύνονται σε αρμόδιες αρχές ή χρηματοοικονομικά ιδρύματα με σκοπό τη θέσπιση συνεκτικών, αποδοτικών και αποτελεσματικών εποπτικών πρακτικών και τη διασφάλιση της κοινής, ενιαίας και συνεπούς εφαρμογής του ενωσιακού δικαίου.

2. Σύμφωνα με το άρθρο 16 παράγραφος 3 του εν λόγω κανονισμού, οι αρμόδιες αρχές και τα χρηματοοικονομικά ιδρύματα καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις εκάστοτε κατευθυντήριες γραμμές και συστάσεις.

3. Η ΕΙΟΡΑ διαπίστωσε την ανάγκη της κατάρτισης συγκεκριμένης καθοδήγησης όσον αφορά την ασφάλεια και τη διακυβέρνηση των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) σε σχέση με τα άρθρα 41 και 44 της οδηγίας 2009/138/ΕΚ στο πλαίσιο της ανάλυσης που πραγματοποιήθηκε ως απάντηση στο σχέδιο δράσης για τη χρηματοοικονομική τεχνολογία (FinTech) της Ευρωπαϊκής Επιτροπής (COM (2018) 0109 final), στο Σχέδιο εποπτικής σύγκλισης ΕΙΟΡΑ 2018-2019[1] και μετά από συνεργασία με πολλούς άλλους ενδιαφερόμενους.[2]

4. Όπως αναφέρεται στην κοινή γνωμοδότηση των Ευρωπαϊκών Εποπτικών Αρχών προς την Ευρωπαϊκή Επιτροπή, οι κατευθυντήριες γραμμές της ΕΙΟΡΑ σχετικά με το σύστημα διακυβέρνησης «*δεν αντικατοπτρίζουν δεόντως τη σημασία της μέριμνας για τη διαχείριση κινδύνων ΤΠΕ (συμπεριλαμβανομένων των κινδύνων στον κυβερνοχώρο)*». Δεν υπάρχει καθοδήγηση σχετικά με στοιχεία ζωτικής σημασίας που αναγνωρίζονται γενικά ως συνιστώσες της ορθής ασφάλειας και διακυβέρνησης ΤΠΕ».

5. Η ανάλυση της τρέχουσας (νομοθετικής) κατάστασης στην ΕΕ για την ανωτέρω κοινή γνωμοδότηση κατέδειξε ότι τα περισσότερα κράτη μέλη της ΕΕ έχουν ορίσει εθνικούς κανόνες για την ασφάλεια και τη διακυβέρνηση των ΤΠΕ. Αν και οι απαιτήσεις είναι παρόμοιες, το κανονιστικό πλαίσιο εξακολουθεί να είναι κατακερματισμένο. Επιπλέον, μια έρευνα σχετικά με τις τρέχουσες εποπτικές πρακτικές αποκάλυψε ένα ευρύ φάσμα πρακτικών - από «καμία συγκεκριμένη εποπτεία» έως «ισχυρή εποπτεία» (συμπεριλαμβανομένων των «μη επιτόπιων επιθεωρήσεων» και των «επιτόπιων επιθεωρήσεων»).

6. Επιπλέον, η πολυπλοκότητα των ΤΠΕ αυξάνεται, καθώς επίσης και η συχνότητα συναφών με τις ΤΠΕ συμβάντων (συμπεριλαμβανομένων των κυβερνοπεριστατικών), όπως και οι επιβλαβείς επιπτώσεις των εν λόγω συμβάντων στην επιχειρησιακή λειτουργία των επιχειρήσεων. Για τον λόγο αυτόν, η διαχείριση των ΤΠΕ και των κινδύνων κατά της ασφάλειας είναι θεμελιώδους σημασίας για μια επιχείρηση ώστε να επιτύχει τους στρατηγικούς, επιχειρησιακούς και λειτουργικούς της στόχους, καθώς και τους στόχους που αφορούν τη φήμη της.

7. Επιπλέον, σε ολόκληρο τον ασφαλιστικό κλάδο, συμπεριλαμβανομένων τόσο των παραδοσιακών όσο και των καινοτόμων επιχειρηματικών μοντέλων, υπάρχει αυξανόμενη εξάρτηση από τις ΤΠΕ στην παροχή ασφαλιστικών υπηρεσιών και στη συνήθη επιχειρησιακή λειτουργία των επιχειρήσεων, π.χ. ψηφιοποίηση του ασφαλιστικού τομέα (InsurTech, διαδίκτυο των πραγμάτων κ.λπ.) καθώς και διασυνδεσιμότητα μέσω τηλεπικοινωνιακών καναλιών (διαδίκτυο, κινητές και ασύρματες συνδέσεις και ευρυζωνικά δίκτυα). Αυτό καθιστά τις δραστηριότητες των

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Η έκθεση που δημοσιεύθηκε από την ΕΙΟΡΑ ως απάντηση στο σχέδιο δράσης της Ευρωπαϊκής Επιτροπής για τη χρηματοοικονομική τεχνολογία (FinTech) είναι διαθέσιμη εδώ.

επιχειρήσεων ευάλωτες σε συμβάντα ασφάλειας, συμπεριλαμβανομένων των κυβερνοεπιθέσεων. Είναι επομένως σημαντικό να διασφαλιστεί ότι οι επιχειρήσεις είναι επαρκώς προετοιμασμένες για τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας.

8. Επιπλέον, αναγνωρίζοντας την ανάγκη ετοιμότητας των επιχειρήσεων για τους κινδύνους στον κυβερνοχώρο[3] καθώς και την ανάγκη θέσπισης ενός υγιούς πλαισίου ασφάλειας στον κυβερνοχώρο από τις επιχειρήσεις, οι παρούσες κατευθυντήριες γραμμές καλύπτουν επίσης την ασφάλεια στον κυβερνοχώρο στο πλαίσιο των μέτρων ασφάλειας των πληροφοριών των επιχειρήσεων. Ενώ οι παρούσες κατευθυντήριες γραμμές αναγνωρίζουν ότι η ασφάλεια στον κυβερνοχώρο θα πρέπει να εξετάζεται στο πλαίσιο της συνολικής διαχείρισης των ΤΠΕ και των κινδύνων κατά της ασφάλειας μιας επιχείρησης, είναι σημαντικό να επισημανθεί ότι οι επιθέσεις στον κυβερνοχώρο έχουν κάποια ειδικά χαρακτηριστικά, τα οποία θα πρέπει να ληφθούν υπόψη για να διασφαλιστεί ότι τα μέτρα ασφάλειας των πληροφοριών μετριάζουν επαρκώς τους κινδύνους στον κυβερνοχώρο:

   a) η διαχείριση των κυβερνοεπιθέσεων (δηλαδή ο εντοπισμός, η προστασία, η ανίχνευση, η αντιμετώπιση και η πλήρης ανάκαμψη) είναι συχνά δυσκολότερη από τις υπόλοιπες πηγές κινδύνων ΤΠΕ και ασφάλειας και η έκταση της ζημιάς είναι επίσης δύσκολο να προσδιοριστεί·

   b) ορισμένες επιθέσεις στον κυβερνοχώρο μπορούν να καταστήσουν τις κοινές ρυθμίσεις διαχείρισης κινδύνων και επιχειρηματικής συνέχειας, καθώς και τις διαδικασίες ανάκαμψης μετά από καταστροφές, αναποτελεσματικές, καθώς ενδέχεται να διαδώσουν κακόβουλο λογισμικό σε συστήματα δημιουργίας αντιγράφων ασφαλείας για να τα καταστήσουν μη διαθέσιμα ή να αλλοιώσουν δεδομένα αντιγράφων ασφαλείας·

   c) πάροχοι υπηρεσιών, χρηματιστηριακοί πράκτορες, εντολοδόχοι και διαμεσολαβητές μπορούν να καταστούν δίαυλοι διάδοσης των επιθέσεων στον κυβερνοχώρο. Οι μεταδοτικές σιωπηρές απειλές ενδέχεται να χρησιμοποιούν τη διασυνδεσιμότητα μέσω τηλεπικοινωνιακών συνδέσμων τρίτων για να εισχωρήσουν στο σύστημα ΤΠΕ μιας επιχείρησης. Επομένως, μια διασυνδεδεμένη επιχείρηση που χαρακτηρίζεται από ατομική χαμηλή συνάφεια μπορεί να καταστεί ευάλωτη και να αποτελέσει πηγή διάδοσης κινδύνων, με συστημικές επιπτώσεις. Τηρώντας την αρχή του πιο αδύναμου κρίκου, η ασφάλεια στον κυβερνοχώρο δεν θα πρέπει να προκαλεί ανησυχία μόνο σε σημαντικούς συμμετέχοντες στην αγορά ή σε σημαντικούς παρόχους υπηρεσιών.

9. Οι στόχοι των παρουσών κατευθυντήριων γραμμών είναι οι εξής:

   a) η παροχή διευκρινίσεων και διαφάνειας στους συμμετέχοντες στην αγορά, όσον αφορά τις ελάχιστες αναμενόμενες δυνατότητες ασφάλειας των πληροφοριών και ασφάλειας στον κυβερνοχώρο, δηλαδή γραμμή βάσης ασφάλειας·

   b) η αποφυγή ενδεχόμενου ρυθμιστικού αρμπιτράζ·

   c) η προώθηση της εποπτικής σύγκλισης όσον αφορά τις προσδοκίες και τις διαδικασίες που εφαρμόζονται σε σχέση με την ασφάλεια και τη διακυβέρνηση των ΤΠΕ καθώς και τη διαχείριση των κινδύνων κατά της ασφάλειας.

[3] Για έναν ορισμό των κινδύνων στον κυβερνοχώρο, ανατρέξτε στο Λεξικό Κυβερνοχώρου του ΣΧΣ (FSB Cyber Lexicon), της 12ης Νοεμβρίου 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Κατευθυντήριες γραμμές για την ασφάλεια και τη διακυβέρνηση των τεχνολογιών πληροφοριών και επικοινωνιών

Εισαγωγή

1. Σύμφωνα με το άρθρο 16 του κανονισμού (ΕΕ) αριθ. 1094/2010[4] η ΕΙΟΡΑ εκδίδει τις παρούσες κατευθυντήριες γραμμές με αποδέκτες αρμόδιες αρχές για την παροχή καθοδήγησης σχετικά με το πώς οι επιχειρήσεις ασφάλισης ή αντασφάλισης (συλλογικά οι «επιχειρήσεις») θα πρέπει να εφαρμόζουν τις απαιτήσεις διακυβέρνησης που προβλέπονται στην οδηγία 2009/138/ΕΚ[5] («οδηγία Φερεγγυότητα ΙΙ») και στον κατ' εξουσιοδότηση κανονισμό (ΕΕ) αριθ. 2015/35 της Επιτροπής[6] («κατ' εξουσιοδότηση κανονισμός») στο πλαίσιο της ασφάλειας και διακυβέρνησης των τεχνολογιών των πληροφοριών και των επικοινωνιών («ΤΠΕ»). Για τον σκοπό αυτόν, οι παρούσες κατευθυντήριες γραμμές βασίζονται στις διατάξεις σχετικά με τη διακυβέρνηση που προβλέπονται στα άρθρα 41, 44, 46, 47, 132 και 246 της οδηγίας Φερεγγυότητα ΙΙ και στα άρθρα 258 έως 260, 266, 268 έως 271 και 274 του κατ' εξουσιοδότηση κανονισμού. Επιπλέον, οι παρούσες κατευθυντήριες γραμμές βασίζονται επίσης στην καθοδήγηση που παρέχεται στις κατευθυντήριες γραμμές της ΕΙΟΡΑ σχετικά με το σύστημα διακυβέρνησης (ΕΙΟΡΑ-BoS-14/253)[7] και στις κατευθυντήριες γραμμές της ΕΙΟΡΑ σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους (ΕΙΟΡΑ-BoS-19/270)[8].

2. Οι κατευθυντήριες γραμμές ισχύουν τόσο για μεμονωμένες επιχειρήσεις όσο και, τηρουμένων των αναλογιών, σε επίπεδο ομίλου[9]

3. Οι αρμόδιες αρχές θα πρέπει, κατά τη συμμόρφωση ή την εποπτεία της συμμόρφωσης με τις παρούσες κατευθυντήριες γραμμές, να λαμβάνουν υπόψη την αρχή της αναλογικότητας[10], η οποία θα πρέπει να διασφαλίζει ότι το οργανωτικό πλαίσιο διακυβέρνησης, μεταξύ άλλων εκείνο που αφορά την ασφάλεια και τη διακυβέρνηση των ΤΠΕ είναι ανάλογο με τη φύση, την κλίμακα και την πολυπλοκότητα των αντίστοιχων κινδύνων που αντιμετωπίζουν ή μπορεί να αντιμετωπίσουν οι επιχειρήσεις.

4. Οι παρούσες κατευθυντήριες γραμμές θα πρέπει να ερμηνεύονται σε συνδυασμό με και με την επιφύλαξη της οδηγίας Φερεγγυότητα ΙΙ, του κατ' εξουσιοδότηση κανονισμού, των κατευθυντήριων γραμμών της ΕΙΟΡΑ σχετικά με το σύστημα διακυβέρνησης και των κατευθυντήριων γραμμών της ΕΙΟΡΑ σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους. Οι παρούσες κατευθυντήριες γραμμές πρόκειται να είναι τεχνολογικά και μεθοδολογικά ουδέτερες.

---

[4] Κανονισμός (ΕΕ) αριθ. 1094/2010 Κανονισμός (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, για τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/79/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ. 48).

[5] Οδηγία 2009/138/ΕΚ Οδηγία 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2019, σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 335 της 17.12.2009, σ. 1).

[6] Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2015/35 της Επιτροπής, της 10ης Οκτωβρίου 2014, για τη συμπλήρωση της οδηγίας 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 12 της 17.1.2015, σ. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] Άρθρο 212 παράγραφος 1 της οδηγίας 2009/138/ΕΚ.

[10] Άρθρο 29 παράγραφος 3 της οδηγίας 2009/138/ΕΚ.

Ορισμοί

5. Εάν δεν παρέχεται ορισμός στις παρούσες κατευθυντήριες γραμμές, οι όροι έχουν την έννοια που τους αποδίδεται στην οδηγία Φερεγγυότητα ΙΙ.

6. Για τους σκοπούς των παρουσών κατευθυντήριων γραμμών, ισχύουν οι ακόλουθοι ορισμοί:

Κάτοχος πόρου	Πρόσωπο ή φορέας με υποχρέωση λογοδοσίας και εξουσία επί πληροφοριακού πόρου ή πόρου ΤΠΕ.
Διαθεσιμότητα	Η ιδιότητα του να είναι κάτι διαθέσιμο και έτοιμο προς χρήση κατόπιν παραγγελίας (επικαιρότητα) από εξουσιοδοτημένο φορέα.
Εμπιστευτικότητα	Η ιδιότητα της μη δημοσιοποίησης ή γνωστοποίησης πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα, φορείς, διαδικασίες ή συστήματα.
Επίθεση στον κυβερνοχώρο	Οποιοδήποτε είδος δικτυοπαραβίασης που οδηγεί σε επιθετική / κακόβουλη απόπειρα καταστροφής, έκθεσης, τροποποίησης, απενεργοποίησης, κλοπής ή απόκτησης μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης ενός πληροφοριακού πόρου, που στοχεύει τα συστήματα ΤΠΕ.
Ασφάλεια στον κυβερνοχώρο	Προστασία του εμπιστευτικού χαρακτήρα, της ακεραιότητας και της διαθεσιμότητας πληροφοριών ή/και συστημάτων πληροφοριών μέσω του κυβερνοχώρου.
Πόρος ΤΠΕ	Πόρος είτε λογισμικού είτε υλισμικού που απαντά στο επιχειρηματικό περιβάλλον.
Έργα ΤΠΕ	Κάθε έργο, ή μέρος έργου, στο πλαίσιο του οποίου αλλάζουν, αντικαθίστανται ή εφαρμόζονται συστήματα ΤΠΕ.

Κίνδυνος ΤΠΕ και ασφάλειας	Ως «επιμέρους στοιχείο λειτουργικού κινδύνου» νοείται ο κίνδυνος ζημίας λόγω παραβίασης της εμπιστευτικότητας, αστοχίας της ακεραιότητας συστημάτων και δεδομένων, ακαταλληλότητας ή μη διαθεσιμότητας συστημάτων και δεδομένων, ή αδυναμίας αλλαγής ΤΠ εντός εύλογου χρονικού διαστήματος και του κόστους όταν οι απαιτήσεις του περιβάλλοντος ή των επιχειρηματικών δραστηριοτήτων μεταβάλλονται (δηλ. ευελιξία).» Στο πλαίσιο αυτό περιλαμβάνονται κίνδυνοι στον κυβερνοχώρο καθώς και κίνδυνοι ασφάλειας των πληροφοριών που προκύπτουν λόγω ανεπάρκειας ή αστοχίας εσωτερικών διεργασιών ή εξωτερικών συμβάντων, μεταξύ των οποίων περιλαμβάνονται και οι επιθέσεις στον κυβερνοχώρο ή η ανεπαρκής υλική ασφάλεια.
Ασφάλεια πληροφοριών	Προστασία του εμπιστευτικού χαρακτήρα, της ακεραιότητας και της διαθεσιμότητας πληροφοριών ή/και συστημάτων πληροφοριών. Επιπλέον, το ίδιο μπορεί επίσης να ισχύει για άλλες ιδιότητες, όπως η αυθεντικότητα, η λογοδοσία, η μη άρνηση αναγνώρισης και η αξιοπιστία.
Υπηρεσίες ΤΠΕ	Υπηρεσίες παρεχόμενες μέσω συστημάτων ΤΠΕ παρόχων υπηρεσιών σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες.
Συστήματα ΤΠΕ	Σύνολο εφαρμογών, υπηρεσιών, πόρων τεχνολογίας πληροφοριών, πόρων ΤΠΕ ή άλλων στοιχείων χειρισμού πληροφοριών, στο οποίο περιλαμβάνεται το λειτουργικό περιβάλλον.
Πληροφοριακός πόρος	Συλλογή πληροφοριών, είτε υλικών είτε άυλων, που αξίζει να προστατεύονται.
Ακεραιότητα	Η ιδιότητα ακρίβειας και πληρότητας.
Συμβάν λειτουργικού κινδύνου ή συμβάν ασφάλειας	Ένα μεμονωμένο γεγονός ή μια σειρά συνδεόμενων μη προγραμματισμένων συμβάντων, τα οποία έχουν ή ενδέχεται να έχουν δυσμενείς επιπτώσεις στην ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των συστημάτων και υπηρεσιών ΤΠΕ.
Πάροχος υπηρεσιών	Νοείται τρίτη οντότητα που αναλαμβάνει μια διαδικασία, παρέχει μια υπηρεσία ή εκτελεί μια δραστηριότητα, ή μέρος της, στο πλαίσιο συμφωνίας εξωτερικής ανάθεσης.

Δοκιμή διείσδυσης βάσει πληροφοριών σχετικά με απειλές	Μια ελεγχόμενη απόπειρα να τεθεί σε κίνδυνο η ανθεκτικότητα ενός φορέα όσον αφορά την ασφάλεια στον κυβερνοχώρο, μέσω της προσομοίωσης τακτικών, τεχνικών και διαδικασιών πραγματικών παραγόντων απειλών. Βασίζεται σε στοχευμένες πληροφορίες απειλών και εστιάζει στα άτομα, τις διαδικασίες και την τεχνολογία ενός φορέα, με ελάχιστη πρόγνωση και επιπτώσεις στις επιχειρησιακές λειτουργίες.
Τρωτότητα	Αδυναμία, ευαισθησία ή ελάττωμα ενός πόρου ή ελέγχου, που μπορεί να αξιοποιηθεί από μία ή περισσότερες απειλές.

7. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται από την 1η Ιουλίου 2021.

Κατευθυντήρια γραμμή 1 – Αναλογικότητα

8. Οι επιχειρήσεις θα πρέπει να εφαρμόζουν τις παρούσες κατευθυντήριες γραμμές με τρόπο ανάλογο προς τη φύση, την κλίμακα και την πολυπλοκότητα των κινδύνων που ενέχουν οι δραστηριότητές τους.

Κατευθυντήρια γραμμή 2 – ΤΠΕ εντός του συστήματος διακυβέρνησης

9. Το διοικητικό, διαχειριστικό ή εποπτικό όργανο θα πρέπει να διασφαλίζει ότι το σύστημα διακυβέρνησης των επιχειρήσεων, ιδίως το σύστημα διαχείρισης κινδύνων και εσωτερικού ελέγχου, διαχειρίζεται επαρκώς τους κινδύνους ΤΠΕ και ασφάλειας των επιχειρήσεων.

10. Το διοικητικό, διαχειριστικό ή εποπτικό όργανο θα πρέπει να μεριμνά ώστε ο αριθμός και οι δεξιότητες των μελών του προσωπικού των επιχειρήσεων να επαρκούν για την υποστήριξη σε διαρκή βάση των λειτουργικών τους αναγκών στον τομέα των ΤΠΕ και των διεργασιών όσον αφορά τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας, καθώς και για τη διασφάλιση της εφαρμογής της οικείας στρατηγικής ΤΠΕ. Επιπλέον, το προσωπικό θα πρέπει να λαμβάνει επαρκή κατάρτιση σχετικά με τους κινδύνους ΤΠΕ και ασφάλειας, συμπεριλαμβανομένης της ασφάλειας των πληροφοριών, σε τακτική βάση, όπως ορίζεται στην κατευθυντήρια γραμμή 13.

11. Το διοικητικό, διαχειριστικό ή εποπτικό όργανο θα πρέπει να διασφαλίζει ότι οι κατανεμημένοι πόροι είναι κατάλληλοι για την εκπλήρωση των ανωτέρω απαιτήσεων.

Κατευθυντήρια γραμμή 3 – Στρατηγική ΤΠΕ

12. Το διοικητικό, διαχειριστικό ή εποπτικό όργανο έχει τη συνολική ευθύνη για τον καθορισμό και την έγκριση της γραπτής στρατηγικής ΤΠΕ των επιχειρήσεων στο πλαίσιο και σύμφωνα με τη συνολική επιχειρηματική στρατηγική τους, καθώς και για την εποπτεία της κοινοποίησης και της υλοποίησής της.

13. Η στρατηγική ΤΠΕ θα πρέπει να καθορίζει τουλάχιστον τα εξής:

    a) τον τρόπο με τον οποίο θα πρέπει να εξελίσσονται οι ΤΠΕ των επιχειρήσεων ώστε να υποστηρίζει και να εφαρμόζει αποτελεσματικά την επιχειρηματική τους στρατηγική, συμπεριλαμβανομένης της εξέλιξης της οργανωτικής δομής, των

επιχειρηματικών μοντέλων, των συστημάτων ΤΠΕ και των κύριων αλληλεξαρτήσεων με παρόχους υπηρεσιών·

b) την εξέλιξη της αρχιτεκτονικής ΤΠΕ, συμπεριλαμβανομένων των εξαρτήσεων των παρόχων υπηρεσιών· και

c) σαφείς στόχους ασφάλειας των πληροφοριών, με ιδιαίτερη έμφαση στα συστήματα ΤΠΕ και στις υπηρεσίες, στο προσωπικό και στις διεργασίες.

14. Οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι η στρατηγική ΤΠΕ υλοποιείται, υιοθετείται και κοινοποιείται εγκαίρως στο σύνολο του αρμόδιου προσωπικού και στους παρόχους υπηρεσιών.

15. Οι επιχειρήσεις θα πρέπει να καταρτίζουν μια διεργασία για την παρακολούθηση και τη μέτρηση της αποτελεσματικότητας της εφαρμογής της στρατηγικής ΤΠΕ. Η εν λόγω διεργασία θα πρέπει να εξετάζεται και να επικαιροποιείται σε τακτική βάση.

Κατευθυντήρια γραμμή 4 – Κίνδυνοι ΤΠΕ και ασφάλειας εντός του συστήματος διαχείρισης κινδύνων

16. Το διοικητικό, διαχειριστικό ή εποπτικό όργανο έχει τη συνολική ευθύνη να θεσπίσει ένα αποτελεσματικό σύστημα για τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας στο πλαίσιο του συνολικού συστήματος διαχείρισης κινδύνων της επιχείρησης. Αυτό περιλαμβάνει τον προσδιορισμό της ανοχής κινδύνου για τους εν λόγω κινδύνους, σύμφωνα με τη στρατηγική κινδύνων της επιχείρησης, καθώς και μια τακτική γραπτή έκθεση σχετικά με το αποτέλεσμα της διαδικασίας διαχείρισης κινδύνων που απευθύνεται στο διοικητικό, διαχειριστικό ή εποπτικό όργανο.

17. Στο πλαίσιο του συνολικού οικείου συστήματος διαχείρισης κινδύνων, οι επιχειρήσεις θα πρέπει, όσον αφορά τους κινδύνους ΤΠΕ και ασφάλειας (και ενώ καθορίζουν τις απαιτήσεις προστασίας ΤΠΕ όπως περιγράφονται κατωτέρω), να λαμβάνουν υπόψη τουλάχιστον τα ακόλουθα:

a) οι επιχειρήσεις θα πρέπει να καταρτίζουν και να επικαιροποιούν τακτικά μια χαρτογράφηση των επιχειρηματικών διεργασιών και δραστηριοτήτων τους, των επιχειρησιακών λειτουργιών, των ρόλων και των πόρων (π.χ. πληροφοριακών πόρων και πόρων ΤΠΕ) προκειμένου να προσδιορίζουν τη σημασία τους και τις αλληλεξαρτήσεις τους με τους κινδύνους ΤΠΕ και ασφάλειας·

b) οι επιχειρήσεις θα πρέπει να προσδιορίζουν και να μετρούν όλους τους συναφείς κινδύνους ΤΠΕ και ασφάλειας στους οποίους εκτίθενται και να ταξινομούν τις προσδιοριζόμενες επιχειρηματικές διεργασίες και δραστηριότητες, επιχειρησιακές λειτουργίες, ρόλους και πόρους (π.χ. πληροφοριακούς πόρους και πόρους ΤΠΕ) ως προς το επίπεδο σοβαρότητας. Οι επιχειρήσεις θα πρέπει επίσης να αξιολογούν τουλάχιστον τις απαιτήσεις προστασίας, εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των εν λόγω επιχειρηματικών διεργασιών και δραστηριοτήτων, των επιχειρηματικών λειτουργιών, των ρόλων και των πόρων (π.χ. των πληροφοριακών πόρων και των πόρων ΤΠΕ). Οι κάτοχοι πόρων, οι οποίοι φέρουν ευθύνη για την ταξινόμηση των πόρων, θα πρέπει να προσδιορίζονται·

c) οι μέθοδοι που χρησιμοποιούνται για τον καθορισμό του επιπέδου κρισιμότητας, καθώς και του απαιτούμενου επιπέδου προστασίας, ιδίως όσον αφορά τους στόχους προστασίας της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας, θα πρέπει να διασφαλίζουν ότι οι προκύπτουσες απαιτήσεις προστασίας είναι συνεκτικές και ολοκληρωμένες·

d) η μέτρηση των κινδύνων ΤΠΕ και ασφάλειας θα πρέπει να διενεργείται βάσει των καθορισμένων κριτηρίων κινδύνων ΤΠΕ και ασφάλειας, λαμβάνοντας υπόψη το επίπεδο σοβαρότητας των επιχειρηματικών διεργασιών και δραστηριοτήτων τους, των επιχειρησιακών λειτουργιών, των ρόλων και των πόρων (π.χ. πληροφοριακοί πόροι και πόροι ΤΠΕ), την έκταση των γνωστών τρωτών σημείων και προηγούμενων συμβάντων που επηρέασαν την επιχείρηση·

e) η αξιολόγηση των κινδύνων ΤΠΕ και ασφάλειας θα πρέπει να πραγματοποιείται και να τεκμηριώνεται τακτικά. Η εν λόγω αξιολόγηση θα πρέπει επίσης να πραγματοποιείται πριν από οποιαδήποτε σημαντική αλλαγή στην υποδομή, τις διεργασίες ή τις διαδικασίες που επηρεάζουν τις επιχειρηματικές διεργασίες και δραστηριότητες, τις επιχειρησιακές λειτουργίες, τους ρόλους και τους πόρους (π.χ. πληροφοριακούς πόρους και πόρους ΤΠΕ)·

f) βάσει της αξιολόγησης κινδύνου που διενεργούν, οι επιχειρήσεις θα πρέπει, τουλάχιστον, να καθορίζουν και να εφαρμόζουν μέτρα για τη διαχείριση των προσδιοριζόμενων κινδύνων ΤΠΕ και ασφάλειας και για την προστασία των πληροφοριακών πόρων βάσει της κατηγοριοποίησής τους. Αυτό θα πρέπει να περιλαμβάνει τον ορισμό μέτρων για τη διαχείριση των κινδύνων που εξακολουθούν να υπάρχουν.

18. Τα αποτελέσματα της διαδικασίας διαχείρισης κινδύνων ΤΠΕ και ασφάλειας θα πρέπει να εγκρίνονται από το διοικητικό, διαχειριστικό ή εποπτικό όργανο και να συμπεριλαμβάνονται στη διαδικασία διαχείρισης λειτουργικού κινδύνου στο πλαίσιο της συνολικής διαχείρισης κινδύνων των επιχειρήσεων.

Κατευθυντήρια γραμμή 5 - Έλεγχος

19. Η διακυβέρνηση, τα συστήματα και οι διεργασίες των επιχειρήσεων για τους κινδύνους ΤΠΕ και ασφάλειας θα πρέπει να ελέγχονται σε τακτική βάση σύμφωνα με το πρόγραμμα ελέγχου[11] των επιχειρήσεων από ελεγκτές με επαρκείς γνώσεις, δεξιότητες και εμπειρογνωμοσύνη σε θέματα κινδύνων ΤΠΕ και ασφάλειας, ώστε να παρέχουν ανεξάρτητη διασφάλιση της αποτελεσματικότητάς τους στο διοικητικό, διαχειριστικό ή εποπτικό όργανο. Για τον προσδιορισμό της συχνότητας και του σημείου εστίασης των εν λόγω ελέγχων θα πρέπει να συνεκτιμώνται οι αντίστοιχοι κίνδυνοι ΤΠΕ και ασφάλειας.

Κατευθυντήρια γραμμή 6 – Πολιτική και μέτρα ασφάλειας των πληροφοριών

20. Οι επιχειρήσεις πρέπει να καταρτίσουν μια γραπτή πολιτική ασφάλειας πληροφοριών που θα εγκρίνεται από το διοικητικό, διαχειριστικό ή εποπτικό όργανο και η οποία θα πρέπει να καθορίζει τις αρχές και τους κανόνες υψηλού επιπέδου για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών των επιχειρήσεων για την υποστήριξη της υλοποίησης της στρατηγικής ΤΠΕ.

21. Η πολιτική θα πρέπει να περιλαμβάνει περιγραφή των κύριων ρόλων και αρμοδιοτήτων για τη διαχείριση ασφάλειας πληροφοριών και θα πρέπει να καθορίζει τις απαιτήσεις για το προσωπικό, τις διεργασίες και την τεχνολογία σε σχέση με την ασφάλεια πληροφοριών, αναγνωρίζοντας ότι το προσωπικό σε όλα τα επίπεδα έχει ευθύνες όσον αφορά τη διασφάλιση της ασφάλειας πληροφοριών των επιχειρήσεων.

[11] Άρθρο 271 του κατ' εξουσιοδότηση κανονισμού.

22. Η πολιτική θα πρέπει να κοινοποιείται εντός της επιχείρησης και να ισχύει για όλο το προσωπικό. Η πολιτική ασφάλειας των πληροφοριών ή τμήματα αυτής θα πρέπει, κατά περίπτωση, να κοινοποιούνται και να ισχύουν για τους παρόχους υπηρεσιών.

23. Με βάση την πολιτική, οι επιχειρήσεις θα πρέπει να θεσπίζουν και να εφαρμόζουν πιο συγκεκριμένες διαδικασίες ασφάλειας πληροφοριών καθώς και μέτρα ασφάλειας πληροφοριών, μεταξύ άλλων για τον μετριασμό των κινδύνων ΤΠΕ και ασφάλειας στους οποίους εκτίθενται. Οι εν λόγω διαδικασίες και τα μέτρα ασφάλειας πληροφοριών θα πρέπει να περιλαμβάνουν κάθε διαδικασία που περιγράφεται στις παρούσες κατευθυντήριες γραμμές, κατά περίπτωση.

Κατευθυντήρια γραμμή 7 - Λειτουργία ασφάλειας πληροφοριών

24. Οι επιχειρήσεις θα πρέπει να θεσπίζουν, στο σύστημα διακυβέρνησής τους και σύμφωνα με την αρχή της αναλογικότητας, μια υπηρεσία ασφάλειας πληροφοριών, με ανάθεση σχετικών αρμοδιοτήτων σε καθοριζόμενο άτομο. Η επιχείρηση θα πρέπει να διασφαλίζει την ανεξαρτησία και την αντικειμενικότητα της λειτουργίας ασφάλειας πληροφοριών, διαχωρίζοντάς την δεόντως από τις διεργασίες ανάπτυξης και λειτουργιών των ΤΠΕ. Η υπηρεσία θα πρέπει να λογοδοτεί στο διοικητικό, διαχειριστικό ή εποπτικό όργανο.

25. Τα καθήκοντα της υπηρεσίας ασφάλειας πληροφοριών είναι συνήθως τα ακόλουθα:

    a) υποστήριξη του διοικητικού, διαχειριστικού ή εποπτικού οργάνου κατά τον καθορισμό και τη διατήρηση της πολιτικής ασφάλειας πληροφοριών για επιχειρήσεις και έλεγχο της ανάπτυξής της·

    b) ενημέρωση και παροχή συμβουλών στο διοικητικό, διαχειριστικό ή εποπτικό όργανο σε τακτική και ad hoc βάση όσον αφορά την κατάσταση της ασφάλειας πληροφοριών καθώς και τις εξελίξεις στον τομέα αυτό·

    c) παρακολούθηση και έλεγχο των μέτρων για την ασφάλεια των πληροφοριών·

    d) διασφάλιση της τήρησης των απαιτήσεων ασφάλειας των πληροφοριών κατά τη χρήση παρόχων υπηρεσιών·

    e) διασφάλιση ότι όλοι οι υπάλληλοι και οι πάροχοι υπηρεσιών που έχουν πρόσβαση σε πληροφορίες και συστήματα είναι επαρκώς ενημερωμένοι για την πολιτική ασφάλειας πληροφοριών, για παράδειγμα μέσω συνεδριών κατάρτισης και ενημέρωσης σχετικά με την ασφάλεια πληροφοριών·

    f) συντονισμός του λειτουργικού ελέγχου ή του ελέγχου συμβάντων ασφαλείας και σχετική υποβολή αναφορών στο διοικητικό, διαχειριστικό ή εποπτικό όργανο.

Κατευθυντήρια γραμμή 8 – Λογική ασφάλεια

26. Οι επιχειρήσεις θα πρέπει να ορίζουν, να τεκμηριώνουν και να εφαρμόζουν διαδικασίες για τον λογικό έλεγχο πρόσβασης ή τη λογική ασφάλεια (διαχείριση ταυτότητας και πρόσβασης) σύμφωνα με τις απαιτήσεις προστασίας, όπως ορίζονται στην κατευθυντήρια γραμμή 4. Οι εν λόγω διαδικασίες θα πρέπει να εφαρμόζονται, να επιβάλλονται, να παρακολουθούνται και να ελέγχονται τακτικά, και θα πρέπει επίσης να περιλαμβάνουν ελέγχους για την παρακολούθηση ανωμαλιών. Σε περίπτωση που ο όρος «χρήστης» περιλαμβάνει επίσης τεχνικούς χρήστες, στο πλαίσιο των εν λόγω διαδικασιών θα πρέπει να εφαρμόζονται, κατ' ελάχιστον, τα ακόλουθα στοιχεία:

    a) ανάγκη για γνώση, ελάχιστα προνόμια και διαχωρισμός καθηκόντων: οι επιχειρήσεις θα πρέπει να διαχειρίζονται τα δικαιώματα πρόσβασης,

συμπεριλαμβανομένης της απομακρυσμένης πρόσβασης σε πληροφοριακούς πόρους και των υποστηρικτικών συστημάτων τους βάσει της αρχής της «ανάγκης για γνώση». Στους χρήστες θα πρέπει να χορηγούνται τα ελάχιστα δικαιώματα πρόσβασης τα οποία είναι απολύτως απαραίτητα για την εκτέλεση των καθηκόντων τους (αρχή των «ελάχιστων προνομίων»), δηλαδή θα πρέπει να αποτρέπεται η αδικαιολόγητη πρόσβαση σε δεδομένα ή το να μπορεί να χρησιμοποιηθεί για την παράκαμψη ελέγχων η χορήγηση συνδυασμένων δικαιωμάτων πρόσβασης (αρχή του «διαχωρισμού των καθηκόντων»)·

b) ευθύνη χρηστών: οι επιχειρήσεις θα πρέπει να περιορίζουν, στον μέγιστο δυνατό βαθμό, τη χρήση γενικών και κοινόχρηστων λογαριασμών χρηστών και να διασφαλίζουν ότι οι χρήστες μπορούν να προσδιορίζονται και να εντοπίζονται από αρμόδιο φυσικό πρόσωπο ή μια εξουσιοδοτημένη εργασία για τις ενέργειες που εκτελούνται στα συστήματα ΤΠΕ ανά πάσα στιγμή·

c) δικαιώματα διαβαθμισμένης πρόσβασης: οι επιχειρήσεις θα πρέπει να εφαρμόζουν ισχυρούς μηχανισμούς ελέγχου για τη διαβαθμισμένη πρόσβαση στα συστήματά τους, περιορίζοντας αυστηρά την πρόσβαση και παρακολουθώντας επισταμένως τους λογαριασμούς με αυξημένη πρόσβαση στα συστήματα (π.χ. λογαριασμούς διαχειριστών).

d) απομακρυσμένη πρόσβαση: για την εξασφάλιση ασφαλούς επικοινωνίας και τη μείωση του κινδύνου, η απομακρυσμένη διοικητική πρόσβαση σε κρίσιμα συστήματα ΤΠΕ θα πρέπει να επιτρέπεται μόνο με βάση την αρχή της ανάγκης για γνώση και εφόσον χρησιμοποιούνται διαδικασίες αυστηρής ηλεκτρονικής επαλήθευσης ταυτότητας·

e) καταχώριση δραστηριοτήτων χρηστών: οι δραστηριότητες των χρηστών θα πρέπει να καταγράφονται και να παρακολουθούνται με τρόπο ανάλογο του κινδύνου, περιλαμβάνοντας, τουλάχιστον, δραστηριότητες προνομιακών χρηστών. Τα αρχεία καταγραφής πρόσβασης θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη τροποποίηση ή διαγραφή και να διατηρούνται για χρονικό διάστημα ανάλογο της κρισιμότητας των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων, με την επιφύλαξη των απαιτήσεων διατήρησης που προβλέπονται στο ενωσιακό και στο εθνικό δίκαιο. Οι επιχειρήσεις θα πρέπει να χρησιμοποιούν τις εν λόγω πληροφορίες για να διευκολύνουν την αναγνώριση και τη διερεύνηση μη φυσιολογικών δραστηριοτήτων που έχουν εντοπιστεί κατά την παροχή υπηρεσιών·

f) διαχείριση πρόσβασης: τα δικαιώματα πρόσβασης θα πρέπει να παραχωρούνται, να καταργούνται και να τροποποιούνται εγκαίρως, σύμφωνα με προκαθορισμένες συνήθεις πράξεις έγκρισης όταν εμπλέκεται ο σχετικός κάτοχος πόρων. Σε περίπτωση που δεν απαιτείται πλέον πρόσβαση, τα δικαιώματα πρόσβασης πρέπει να ανακαλούνται αμέσως.

g) αξιολόγηση πρόσβασης: τα δικαιώματα πρόσβασης θα πρέπει να επανεξετάζονται σε περιοδική βάση ώστε να διασφαλίζεται ότι οι χρήστες δεν διαθέτουν υπερβολικά προνόμια και ότι τα δικαιώματα πρόσβασης θα ανακαλούνται/αποσύρονται όταν δεν είναι πλέον απαραίτητα·

h) η χορήγηση, τροποποίηση, ανάκληση δικαιωμάτων πρόσβασης θα πρέπει να τεκμηριώνονται κατά τρόπο που να διευκολύνει την κατανόηση και την ανάλυση· και

i) Μέθοδοι ηλεκτρονικής επαλήθευσης ταυτότητας: οι επιχειρήσεις θα πρέπει να επιβάλλουν μεθόδους ηλεκτρονικής επαλήθευσης ταυτότητας οι οποίες χαρακτηρίζονται από επαρκές επίπεδο αξιοπιστίας ώστε να διασφαλίζεται με

κατάλληλο και αποτελεσματικό τρόπο η συμμόρφωση προς τις πολιτικές και τις διαδικασίες ελέγχου της πρόσβασης. Οι μέθοδοι ηλεκτρονικής επαλήθευσης ταυτότητας θα πρέπει να είναι ανάλογες προς τον βαθμό κρισιμότητας των συστημάτων ΤΠΕ, των πληροφοριών ή διεργασιών που αποτελούν αντικείμενο πρόσβασης. Στο πλαίσιο αυτό θα πρέπει να περιλαμβάνονται, κατ' ελάχιστον, ισχυροί κωδικοί πρόσβασης ή ισχυρότερες μέθοδοι ηλεκτρονικής επαλήθευσης ταυτότητας (όπως η ηλεκτρονική επαλήθευση ταυτότητας δύο παραγόντων), βάσει του αντίστοιχου κινδύνου.

27. Η ηλεκτρονική πρόσβαση από εφαρμογές σε δεδομένα και συστήματα ΤΠΕ θα πρέπει να περιορίζεται στο ελάχιστο επίπεδο που απαιτείται για την παροχή της αντίστοιχης υπηρεσίας.

Κατευθυντήρια γραμμή 9 – Φυσική ασφάλεια

28. Τα μέτρα φυσικής ασφάλειας των επιχειρήσεων (π.χ. προστασία έναντι διακοπής ρεύματος, πυρκαγιάς, πλημμύρας και μη εξουσιοδοτημένης φυσικής πρόσβασης) πρέπει να καθορίζονται, να τεκμηριώνονται και να εφαρμόζονται για την προστασία των χώρων, των κέντρων δεδομένων και των ευαίσθητων περιοχών από μη εξουσιοδοτημένη πρόσβαση και από περιβαλλοντικούς κινδύνους.

29. Η φυσική πρόσβαση σε συστήματα ΤΠΕ θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα. Η εξουσιοδότηση θα πρέπει να παρέχεται ανάλογα με τα καθήκοντα και τις αρμοδιότητες του ατόμου, και να περιορίζεται σε άτομα που υποβάλλονται σε κατάλληλη κατάρτιση και παρακολούθηση. Η φυσική πρόσβαση θα πρέπει να επανεξετάζεται σε περιοδική βάση ώστε να διασφαλίζεται η άμεση ανάκληση/απόσυρση δικαιωμάτων πρόσβασης όταν αυτά δεν είναι απαραίτητα.

30. Τα ενδεδειγμένα μέτρα για την προστασία από περιβαλλοντικούς κινδύνους θα πρέπει να είναι ανάλογα προς τη σημασία των κτιρίων και την κρισιμότητα των λειτουργιών ή των συστημάτων ΤΠΕ που βρίσκονται στα εν λόγω κτίρια.

Κατευθυντήρια γραμμή 10 – Ασφάλεια λειτουργιών ΤΠΕ

31. Οι επιχειρήσεις θα πρέπει να εφαρμόζουν διαδικασίες για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των συστημάτων ΤΠΕ και των υπηρεσιών ΤΠΕ, προκειμένου να ελαχιστοποιούνται αντίστοιχα οι επιπτώσεις των ζητημάτων ασφάλειας στην παροχή υπηρεσιών ΤΠΕ. Στις διαδικασίες αυτές θα πρέπει να περιλαμβάνονται δεόντως τα ακόλουθα μέτρα:

    a) εντοπισμός πιθανών ευπαθειών, οι οποίες θα πρέπει να αξιολογούνται και να αποκαθίστανται διασφαλίζοντας ότι τα συστήματα ΤΠΕ είναι ενημερωμένα, συμπεριλαμβανομένου του λογισμικού που παρέχουν οι επιχειρήσεις στους εσωτερικούς και τους εξωτερικούς χρήστες, εγκαθιστώντας κρίσιμες ενημερώσεις ασφάλειας, συμπεριλαμβάνοντας ενημερώσεις ορισμών λογισμικού προστασίας από ιούς ή εφαρμόζοντας αντισταθμιστικούς ελέγχους·

    b) εφαρμογή γραμμών βάσης ασφαλούς διαμόρφωσης για όλα τα κρίσιμα στοιχεία όπως λειτουργικά συστήματα, βάσεις δεδομένων, δρομολογητές ή διακόπτες·

    c) εφαρμογή συστημάτων κατάτμησης του δικτύου (network segmentation), πρόληψης απώλειας δεδομένων και κρυπτογράφηση της κίνησης του δικτύου (σύμφωνα με την κατηγοριοποίηση των πληροφοριακών πόρων)·

    d) εφαρμογή προστασίας τελικών σημείων, συμπεριλαμβανομένων δρομολογητών, σταθμών εργασίας και κινητών συσκευών. Οι επιχειρήσεις θα πρέπει να αξιολογούν εάν ένα τελικό σημείο πληροί τα πρότυπα ασφαλείας που καθορίζονται από αυτές πριν αυτό αποκτήσει πρόσβαση στο εταιρικό δίκτυο·

e) διασφάλιση ότι εφαρμόζονται μηχανισμοί ελέγχου της ακεραιότητας για την επαλήθευση της ακεραιότητας των συστημάτων ΤΠΕ·

f) κρυπτογράφηση των δεδομένων όταν τελούν σε κατάσταση αποθήκευσης και διαβίβασης (σύμφωνα με την κατηγοριοποίηση των πληροφοριακών πόρων).

Κατευθυντήρια γραμμή 11 - Παρακολούθηση ασφάλειας

32. Οι επιχειρήσεις θα πρέπει να θεσπίζουν και να εφαρμόζουν διεργασίες και διαδικασίες για τη συνεχή παρακολούθηση δραστηριοτήτων που επηρεάζουν την ασφάλεια των πληροφοριών των επιχειρήσεων. Η παρακολούθηση θα πρέπει να καλύπτει τουλάχιστον τα εξής:

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

b) συναλλαγές από παρόχους υπηρεσιών, άλλες οντότητες και εσωτερικούς χρήστες· και

c) πιθανές εσωτερικές και εξωτερικές απειλές.

33. Βάσει της παρακολούθησης, οι επιχειρήσεις θα πρέπει να εφαρμόζουν κατάλληλες και αποτελεσματικές δυνατότητες για τον εντοπισμό, την αναφορά και την ανταπόκριση σε μη φυσιολογικές δραστηριότητες και απειλές, όπως φυσική ή λογική εισβολή, παραβιάσεις της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας στοιχείων πληροφοριών, κακόβουλο κώδικα και ευρέως γνωστές ευπάθειες λογισμικού και υλικού.

34. Η υποβολή αναφορών από την παρακολούθηση της ασφάλειας θα πρέπει να βοηθάει τις επιχειρήσεις να κατανοούν τη φύση των επιχειρησιακών συμβάντων και των συμβάντων ασφαλείας, να εντοπίζουν τις τάσεις και να υποστηρίζουν τις εσωτερικές έρευνες των επιχειρήσεων και να τους επιτρέπει να λαμβάνουν τις κατάλληλες αποφάσεις.

Κατευθυντήρια γραμμή 12 - Έλεγχοι ασφάλειας πληροφοριών, αξιολόγηση και δοκιμές

35. Οι επιχειρήσεις θα πρέπει να διενεργούν ποικίλους διαφορετικούς ελέγχους ασφάλειας των πληροφοριών, αξιολογήσεις και δοκιμές, ώστε να διασφαλίζεται ο αποτελεσματικός εντοπισμός των τρωτών σημείων στα συστήματα και τις υπηρεσίες ΤΠΕ τους. Για παράδειγμα, οι επιχειρήσεις μπορούν να προβαίνουν σε ανάλυση ελλείψεων με βάση τα πρότυπα ασφάλειας πληροφοριών, ελέγχους συμμόρφωσης, εσωτερικούς και εξωτερικούς ελέγχους των συστημάτων πληροφοριών ή ελέγχους φυσικής ασφάλειας.

36. Οι επιχειρήσεις θα πρέπει να θεσπίζουν και να εφαρμόζουν πλαίσιο δοκιμών ασφάλειας πληροφοριών το οποίο θα επικυρώνει την αξιοπιστία και την αποτελεσματικότητα των μέτρων ασφάλειας πληροφοριών, καθώς και να διασφαλίζουν ότι στο εν λόγω πλαίσιο λαμβάνονται υπόψη απειλές και ευπάθειες, οι οποίες προσδιορίζονται μέσω της παρακολούθησης απειλών και της διαδικασίας αξιολόγησης των κινδύνων ΤΠΕ και ασφάλειας.

37. Οι δοκιμές θα πρέπει να διενεργούνται με ασφαλή τρόπο και από ανεξάρτητους υπεύθυνους εκτέλεσης δοκιμών με επαρκείς γνώσεις, δεξιότητες και εμπειρογνωμοσύνη στον τομέα δοκιμών των μέτρων ασφάλειας πληροφοριών.

38. Οι επιχειρήσεις θα πρέπει να πραγματοποιούν δοκιμές σε τακτική βάση. Το εύρος, η συχνότητα και η μέθοδος δοκιμών (όπως η δοκιμή διείσδυσης,

συμπεριλαμβανομένων των ελεγχόμενων δοκιμών διείσδυσης με τη χρήση στοχευμένων πληροφοριών απειλών) θα πρέπει να είναι ανάλογα με το επίπεδο του εντοπιζόμενου κινδύνου. Οι δοκιμές κρίσιμων συστημάτων ΤΠΕ και οι σαρώσεις ευπάθειας θα πρέπει να πραγματοποιούνται σε ετήσια βάση.

39. Οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι οι δοκιμές των μέτρων ασφάλειας διενεργούνται σε περίπτωση αλλαγών στην υποδομή, στις διεργασίες ή στις διαδικασίες, καθώς και σε περίπτωση αλλαγών λόγω μειζόνων περιστατικών λειτουργικού κινδύνου ή μειζόνων περιστατικών ασφάλειας ή λόγω της έκδοσης νέων ή σημαντικά τροποποιημένων κρίσιμων εφαρμογών. Οι επιχειρήσεις θα πρέπει να παρακολουθούν και να αξιολογούν τα αποτελέσματα των δοκιμών ασφάλειας και να επικαιροποιούν αναλόγως και χωρίς αδικαιολόγητες καθυστερήσεις τα μέτρα ασφάλειάς τους στην περίπτωση των κρίσιμων συστημάτων ΤΠΕ.

Κατευθυντήρια γραμμή 13 – Κατάρτιση και ευαισθητοποίηση σε θέματα ασφάλειας των πληροφοριών

40. Οι επιχειρήσεις θα πρέπει να εκπονούν προγράμματα κατάρτισης για την ασφάλεια των πληροφοριών για όλο το προσωπικό, συμπεριλαμβανομένου του διοικητικού, διαχειριστικού ή εποπτικού οργάνου, ώστε να διασφαλίζεται ότι έχουν εκπαιδευτεί για την εκτέλεση των καθηκόντων και των αρμοδιοτήτων τους για τη μείωση των ανθρώπινων σφαλμάτων, της κλοπής, της απάτης, της αθέμιτης χρήσης ή των απωλειών. Οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι το πρόγραμμα κατάρτισης παρέχει εκπαίδευση σε όλο το προσωπικό σε τακτική βάση.

41. Οι επιχειρήσεις θα πρέπει να καταρτίζουν και να υλοποιούν περιοδικά προγράμματα ευαισθητοποίησης σχετικά με την ασφάλεια για την εκπαίδευση του προσωπικού τους, συμπεριλαμβανομένου του διοικητικού, διαχειριστικού ή εποπτικού οργάνου, σχετικά με τον τρόπο αντιμετώπισης κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριών.

Κατευθυντήρια γραμμή 14 – Διαχείριση λειτουργιών ΤΠΕ

42. Οι επιχειρήσεις θα πρέπει να διαχειρίζονται τις σχετικές με τις ΤΠΕ δραστηριότητές τους βάσει της στρατηγικής ΤΠΕ. Ο τρόπος λειτουργίας των επιχειρήσεων, η παρακολούθηση και ο έλεγχος των συστημάτων και των υπηρεσιών ΤΠΕ, συμπεριλαμβανομένης της τεκμηρίωσης κρίσιμων διεργασιών, διαδικασιών και λειτουργιών ΤΠΕ, θα πρέπει να προσδιορίζονται σε σχετικά έγγραφα.

43. Οι επιχειρήσεις θα πρέπει να εφαρμόζουν διαδικασίες καταγραφής και παρακολούθησης για τις κρίσιμες λειτουργίες ΤΠΕ, ώστε να είναι εφικτή η ανίχνευση, η ανάλυση και η διόρθωση σφαλμάτων.

44. Οι επιχειρήσεις θα πρέπει να τηρούν ενημερωμένο κατάλογο των πόρων ΤΠΕ που διαθέτουν. Ο κατάλογος πόρων ΤΠΕ θα πρέπει να χαρακτηρίζεται από επαρκή βαθμό λεπτομέρειας ώστε να παρέχεται η δυνατότητα άμεσου προσδιορισμού του πόρου ΤΠΕ, της θέσης του, της κατηγοριοποίησης ασφάλειας και του καθεστώτος ιδιοκτησίας του.

45. Οι επιχειρήσεις θα πρέπει να παρακολουθούν και να διαχειρίζονται τον κύκλο ζωής των πόρων ΤΠΕ ώστε να διασφαλίζεται ότι εξακολουθούν να πληρούν και να υποστηρίζουν τις απαιτήσεις διαχείρισης των επιχειρησιακών δραστηριοτήτων και των κινδύνων. Οι επιχειρήσεις θα πρέπει να παρακολουθούν αν οι πόροι ΤΠΕ υποστηρίζονται από τους προμηθευτές τους ή εσωτερικούς σχεδιαστές εφαρμογών, καθώς και αν όλες οι σχετικές ενημερώσεις και αναβαθμίσεις εφαρμόζονται βάσει τεκμηριωμένης διεργασίας. Οι κίνδυνοι που απορρέουν από παρωχημένους ή μη

υποστηριζόμενους πόρους ΤΠΕ θα πρέπει να αξιολογούνται και να περιορίζονται. Οι αποσυρθέντες πόροι ΤΠΕ θα πρέπει να υποβάλλονται σε ασφαλή επεξεργασία και διαγραφή.

46. Οι επιχειρήσεις θα πρέπει να εφαρμόζουν διεργασίες σχεδιασμού και παρακολούθησης των επιδόσεων και των ικανοτήτων με σκοπό την έγκαιρη πρόληψη, ανίχνευση και αντιμετώπιση σημαντικών ζητημάτων όσον αφορά τις επιδόσεις των συστημάτων και τις ελλείψεις ικανοτήτων ΤΠΕ.

47. Οι επιχειρήσεις θα πρέπει να καθορίζουν και να εφαρμόζουν διαδικασίες δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης δεδομένων και συστημάτων ΤΠΕ, ώστε να διασφαλίζεται η δυνατότητα ανάκτησής τους όπως απαιτείται. Το πεδίο εφαρμογής και η συχνότητα της δημιουργίας εφεδρικών αντιγράφων θα πρέπει να καθορίζονται σύμφωνα με τις απαιτήσεις επιχειρησιακής ανάκτησης και την κρισιμότητα των δεδομένων και των συστημάτων ΤΠΕ και να αξιολογούνται με βάση τη διενεργηθείσα αξιολόγηση κινδύνων. Οι δοκιμές των διαδικασιών δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης θα πρέπει να εκτελούνται σε τακτική βάση.

48. Οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι τα αντίγραφα ασφαλείας των δεδομένων και των συστημάτων ΤΠΕ αποθηκεύονται σε μία ή περισσότερες τοποθεσίες εκτός της κύριας τοποθεσίας, οι οποίες είναι ασφαλείς και επαρκώς απομακρυσμένες από την κύρια τοποθεσία ώστε να αποφεύγεται η έκθεσή τους στους ίδιους κινδύνους.

Κατευθυντήρια γραμμή 15 - Διαχείριση συμβάντων και προβλημάτων ΤΠΕ

49. Οι επιχειρήσεις θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασία διαχείρισης περιστατικών και προβλημάτων για την παρακολούθηση και την καταγραφή περιστατικών λειτουργικού κινδύνου ή περιστατικών ασφάλειας, καθώς και για να εξασφαλίζεται η δυνατότητα των επιχειρήσεων να συνεχίζουν ή να επανεκκινούν τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες σε περίπτωση εμφάνισης διαταραχών.

50. Οι επιχειρήσεις θα πρέπει να καθορίζουν κατάλληλα κριτήρια και κατώτατα όρια για την ταξινόμηση ενός γεγονότος ως λειτουργικού συμβάντος ή συμβάντος που αφορά την ασφάλεια, καθώς και δείκτες έγκαιρης προειδοποίησης που θα πρέπει να χρησιμεύουν ως συναγερμός, ώστε να καθίσταται δυνατός ο έγκαιρος εντοπισμός των εν λόγω συμβάντων.

51. Για την ελαχιστοποίηση των επιπτώσεων δυσμενών συμβάντων και την εξασφάλιση της δυνατότητας έγκαιρης ανάκτησης, οι επιχειρήσεις θα πρέπει να δημιουργούν κατάλληλες διεργασίες και οργανωτικές δομές για τη διασφάλιση συνεκτικής και ολοκληρωμένης παρακολούθησης, χειρισμού και μεταγενέστερης παρακολούθησης των περιστατικών λειτουργικού κινδύνου και των περιστατικών ασφάλειας, για τη διασφάλιση του προσδιορισμού και της αντιμετώπισης των βασικών αιτιών, και λαμβάνονται διορθωτικά μέτρα με σκοπό την αποφυγή παρόμοιων συμβάντων στο μέλλον. Στη διεργασία διαχείρισης περιστατικών και προβλημάτων θα πρέπει, τουλάχιστον, να καθορίζονται:

    a) οι διαδικασίες για τον προσδιορισμό, την ανίχνευση, την καταγραφή, την κατηγοριοποίηση και την ταξινόμηση των συμβάντων βάσει κατά προτεραιότητα ιεράρχησης που καθορίζεται από την επιχείρηση και ανάλογα με την κρισιμότητα των επιχειρησιακών λειτουργιών και των συμβάσεων υπηρεσιών·

b) οι ρόλοι και οι αρμοδιότητες για τα διάφορα σενάρια περιστατικών (π.χ. σφάλματα, δυσλειτουργίες, επιθέσεις στον κυβερνοχώρο)·

c) διαδικασία διαχείρισης προβλημάτων για τον προσδιορισμό, την ανάλυση και την επίλυση των βασικών αιτιών ενός ή περισσότερων περιστατικών: οι επιχειρήσεις θα πρέπει να αναλύουν τα περιστατικά λειτουργικού κινδύνου ή τα περιστατικά ασφάλειας που έχουν προσδιοριστεί ή έχουν εμφανιστεί εντός και/ή εκτός του οργανισμού, ενώ επίσης θα πρέπει να λαμβάνουν υπόψη τα κύρια διδάγματα που αντλούνται από τις εν λόγω αναλύσεις και να επικαιροποιούν αναλόγως τα μέτρα ασφάλειας·

d) αποτελεσματικά σχέδια εσωτερικής επικοινωνίας, συμπεριλαμβανομένων διαδικασιών γνωστοποίησης περιστατικών και παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας —οι οποίες καλύπτουν επίσης καταγγελίες πελατών σχετικά με θέματα ασφάλειας— ώστε να διασφαλίζεται ότι:

   i. τα περιστατικά με δυνητικά σοβαρές δυσμενείς επιπτώσεις σε συστήματα ΤΠΕ και υπηρεσίες ΤΠΕ κρίσιμης σημασίας αναφέρονται στα αρμόδια ανώτερα διοικητικά στελέχη·

   ii. το διοικητικό, διαχειριστικό ή εποπτικό όργανο ενημερώνεται σε ad hoc βάση σε περίπτωση σημαντικών περιστατικών και ενημερώνεται, τουλάχιστον, για τις επιπτώσεις, την αντίδραση και τους πρόσθετους ελέγχους που πρέπει να καθοριστούν λόγω των περιστατικών·

e) διαδικασίες αντιμετώπισης περιστατικών για τη μείωση των επιπτώσεων που συνδέονται με τα περιστατικά και για την εξασφάλιση της δυνατότητας έγκαιρης και ασφαλούς επιχειρησιακής λειτουργίας της υπηρεσίας·

f) ειδικά σχέδια εξωτερικής επικοινωνίας για τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες, με στόχο:

   i. τη συνεργασία με τους σχετικούς ενδιαφερομένους για την αποτελεσματική αντιμετώπιση και ανάκτηση μετά το περιστατικό,

   ii. την έγκαιρη παροχή πληροφοριών, συμπεριλαμβανομένης της αναφοράς περιστατικών, σε εξωτερικά μέρη [π.χ. πελάτες, άλλους συμμετέχοντες στην αγορά, αρμόδιες (εποπτικές) αρχές, κατά περίπτωση και σύμφωνα με τον ισχύοντα κανονισμό].

Κατευθυντήρια γραμμή 16 – Διαχείριση έργου ΤΠΕ

52. Οι επιχειρήσεις θα πρέπει να εφαρμόζουν μια μεθοδολογία έργου ΤΠΕ (συμπεριλαμβανομένων ανεξάρτητων θεμάτων απαιτήσεων ασφάλειας) με κατάλληλη διαδικασία διακυβέρνησης και ηγετικές ικανότητες στην υλοποίηση έργων για την αποτελεσματική υποστήριξη της εφαρμογής της στρατηγικής ΤΠΕ μέσω έργων ΤΠΕ.

53. Οι επιχειρήσεις θα πρέπει να μεριμνούν δεόντως για την παρακολούθηση και τη μείωση των κινδύνων που απορρέουν από το χαρτοφυλάκιο έργων ΤΠΕ, λαμβάνοντας επίσης υπόψη τους κινδύνους που ενδέχεται να προκύπτουν από αλληλεξαρτήσεις μεταξύ διαφόρων έργων και από την εξάρτηση πολλαπλών έργων από τους ίδιους πόρους και/ή την ίδια εμπειρογνωσία.

Κατευθυντήρια γραμμή 17 - Απόκτηση και ανάπτυξη συστημάτων ΤΠΕ

54. Οι επιχειρήσεις θα πρέπει να αναπτύσσουν και να εφαρμόζουν μια διαδικασία που θα διέπει την απόκτηση, την ανάπτυξη και τη συντήρηση των συστημάτων ΤΠΕ προκειμένου να διασφαλίζεται ότι η εμπιστευτικότητα, η ακεραιότητα, η

διαθεσιμότητα των προς επεξεργασία δεδομένων διασφαλίζονται με κατανοητό τρόπο και ότι πληρούνται οι καθορισμένες απαιτήσεις προστασίας. Η διαδικασία αυτή θα πρέπει να σχεδιάζεται με τη χρήση προσέγγισης βάσει κινδύνου.

55. Οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι πριν από την απόκτηση συστημάτων ή την εκτέλεση δραστηριοτήτων ανάπτυξης, οι λειτουργικές και μη λειτουργικές απαιτήσεις (συμπεριλαμβανομένων των απαιτήσεων ασφάλειας πληροφοριών) και οι τεχνικοί στόχοι καθορίζονται με σαφήνεια.

56. Οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι εφαρμόζονται μέτρα για την αποτροπή ακούσιας αλλοίωσης ή εκούσιας χειραγώγησης των συστημάτων ΤΠΕ κατά την ανάπτυξη.

57. Οι επιχειρήσεις θα πρέπει να διαθέτουν μεθοδολογία για τις δοκιμές και την έγκριση των συστημάτων ΤΠΕ, των υπηρεσιών ΤΠΕ και των μέτρων ασφάλειας των πληροφοριών.

58. Οι επιχειρήσεις θα πρέπει να υποβάλλουν σε δοκιμές τα συστήματα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τα μέτρα ασφάλειας πληροφοριών για τον προσδιορισμό πιθανών αδυναμιών, παραβιάσεων και περιστατικών ασφάλειας.

59. Οι επιχειρήσεις θα πρέπει να μεριμνούν για τον διαχωρισμό των περιβαλλόντων παραγωγής από τα περιβάλλοντα ανάπτυξης, δοκιμών και άλλα περιβάλλοντα εκτός της παραγωγής.

60. Οι επιχειρήσεις θα πρέπει να εφαρμόζουν μέτρα για την προστασία της ακεραιότητας του πηγαίου κώδικα (όπου υπάρχει) των συστημάτων ΤΠΕ. Θα πρέπει επίσης να τεκμηριώνουν την ανάπτυξη, την εφαρμογή, τη λειτουργία και/ή την παραμετροποίηση των συστημάτων ΤΠΕ κατά τρόπο ολοκληρωμένο, ώστε να περιορίζεται τυχόν αδικαιολόγητη εξάρτηση από ειδικούς εμπειρογνώμονες επί του αντικειμένου αυτού.

61. Οι διεργασίες των επιχειρήσεων για την απόκτηση και την ανάπτυξη συστημάτων ΤΠΕ θα πρέπει να εφαρμόζονται επίσης σε συστήματα ΤΠΕ των οποίων η ανάπτυξη ή η διαχείριση πραγματοποιείται από τους τελικούς χρήστες της επιχειρηματικής λειτουργίας εκτός του οργανισμού ΤΠΕ (π.χ. εφαρμογές που διαχειρίζονται επιχειρήσεις ή υπολογιστικές εφαρμογές τελικού χρήστη) με τη χρήση προσέγγισης βάσει κινδύνου. Οι επιχειρήσεις θα πρέπει να τηρούν μητρώο των εν λόγω εφαρμογών για την υποστήριξη των κρίσιμων επιχειρηματικών λειτουργιών ή διεργασιών.

Κατευθυντήρια γραμμή 18 – Διαχείριση αλλαγών ΤΠΕ

62. Οι επιχειρήσεις θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασία διαχείρισης αλλαγών ΤΠΕ ώστε να διασφαλίζεται ότι όλες οι αλλαγές στα συστήματα ΤΠΕ καταγράφονται, αξιολογούνται, υποβάλλονται σε δοκιμές, εγκρίνονται, εξουσιοδοτούνται και εφαρμόζονται με ελεγχόμενο τρόπο. Οι αλλαγές κατά τη διάρκεια έκτακτων ή επειγουσών αλλαγών ΤΠΕ θα πρέπει να είναι ανιχνεύσιμες και να κοινοποιούνται εκ των υστέρων στον σχετικό κάτοχο πόρων για εκ των υστέρων ανάλυση.

63. Οι επιχειρήσεις θα πρέπει να προσδιορίζουν αν οι αλλαγές στο υφιστάμενο λειτουργικό περιβάλλον έχουν αντίκτυπο στα ισχύοντα μέτρα ασφάλειας ή απαιτούν τη θέσπιση πρόσθετων μέτρων για τη μείωση των αντίστοιχων κινδύνων. Οι αλλαγές αυτές θα πρέπει να πραγματοποιούνται σύμφωνα με την επίσημη διαδικασία διαχείρισης αλλαγών που εφαρμόζουν οι επιχειρήσεις.

Κατευθυντήρια γραμμή 19 – Διαχείριση της επιχειρησιακής συνέχειας

64. Στο πλαίσιο της συνολικής πολιτικής επιχειρησιακής συνέχειας των επιχειρήσεων, το διοικητικό, διαχειριστικό ή εποπτικό όργανο έχει την ευθύνη για τον καθορισμό και την έγκριση της πολιτικής συνέχειας ΤΠΕ των επιχειρήσεων. Η πολιτική συνέχειας των ΤΠΕ θα πρέπει να κοινοποιείται δεόντως εντός των επιχειρήσεων και θα πρέπει να εφαρμόζεται σε όλο το αρμόδιο προσωπικό και, κατά περίπτωση, στους παρόχους υπηρεσιών.

Κατευθυντήρια γραμμή 20 – Ανάλυση επιπτώσεων για τις επιχειρήσεις

65. Στο πλαίσιο της ορθής διαχείρισης επιχειρησιακής συνέχειας, οι επιχειρήσεις θα πρέπει να διεξάγουν ανάλυση επιπτώσεων στις επιχειρήσεις για να αξιολογούν την έκθεση των επιχειρήσεων σε σοβαρές διαταραχές δραστηριότητας και τις πιθανές επιπτώσεις τους, ποσοτικά και ποιοτικά, χρησιμοποιώντας εσωτερικά ή/και εξωτερικά δεδομένα και ανάλυση σεναρίων. Η ανάλυση επιπτώσεων στις επιχειρήσεις θα πρέπει επίσης να λαμβάνει υπόψη τη σοβαρότητα των προσδιορισμένων και ταξινομημένων επιχειρηματικών διαδικασιών και δραστηριοτήτων, των επιχειρησιακών λειτουργιών, των ρόλων και των πόρων (π.χ. πληροφοριακών πόρων και πόρων ΤΠΕ) και των αλληλεξαρτήσεων τους σύμφωνα με την κατευθυντήρια γραμμή 4.

66. Οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι τα συστήματα ΤΠΕ και οι υπηρεσίες ΤΠΕ τους σχεδιάζονται και συνάδουν με την ανάλυση των επιχειρηματικών επιπτώσεων που διενεργούν, για παράδειγμα εξασφαλίζοντας την εφεδρεία ορισμένων κρίσιμων συνιστωσών για την πρόληψη διαταραχών λόγω συμβάντων που έχουν επιπτώσεις στις εν λόγω συνιστώσες.

Κατευθυντήρια γραμμή 21 – Σχεδιασμός επιχειρησιακής συνέχειας

67. Τα συνολικά Σχέδια Επιχειρησιακής Συνέχειας των επιχειρήσεων θα πρέπει να λαμβάνουν υπόψη σημαντικούς κινδύνους που θα μπορούσαν να επηρεάσουν δυσμενώς τα συστήματα ΤΠΕ και τις υπηρεσίες ΤΠΕ. Τα σχέδια θα πρέπει να υποστηρίζουν στόχους για την προστασία και, εάν είναι απαραίτητο, την αποκατάσταση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των επιχειρηματικών διαδικασιών και δραστηριοτήτων, των επιχειρηματικών λειτουργιών, ρόλων και πόρων (π.χ. πληροφοριακών πόρων και πόρων ΤΠΕ) των επιχειρήσεων. Κατά την κατάρτιση των εν λόγω σχεδίων, οι επιχειρήσεις θα πρέπει να συντονίζονται με τους σχετικούς εσωτερικούς και εξωτερικούς ενδιαφερομένους, κατά περίπτωση.

68. Οι επιχειρήσεις θα πρέπει να εφαρμόζουν Σχέδια Επιχειρησιακής Συνέχειας για να διασφαλίζουν ότι είναι σε θέση να αντιδράσουν με τον κατάλληλο τρόπο σε πιθανά σενάρια αστοχίας στο πλαίσιο ενός χρονικού στόχου ανάκτησης (ο μέγιστος χρόνος εντός του οποίου ένα σύστημα ή μια διαδικασία πρέπει να αποκατασταθεί μετά από ένα συμβάν) και ενός στόχου σημείου ανάκτησης (το μέγιστο χρονικό διάστημα κατά τη διάρκεια του οποίου δεδομένα μπορούν να χαθούν σε περίπτωση συμβάντος σε προκαθορισμένο επίπεδο υπηρεσίας).

69. Οι επιχειρήσεις θα πρέπει να εξετάζουν μια σειρά διαφορετικών σεναρίων στα οικεία Σχέδια Επιχειρησιακής Συνέχειας, συμπεριλαμβανομένων ακραίων αλλά εύλογων σεναρίων και σεναρίων επίθεσης στον κυβερνοχώρο, και να εκτιμούν τις πιθανές επιπτώσεις των εν λόγω σεναρίων. Με βάση τα σενάρια αυτά, οι επιχειρήσεις θα πρέπει να περιγράφουν τον τρόπο διασφάλισης της συνέχειας των συστημάτων και των υπηρεσιών ΤΠΕ, καθώς και της ασφάλειας πληροφοριών των επιχειρήσεων.

Κατευθυντήρια γραμμή 22 – Σχέδια αντιμετώπισης και ανάκτησης

70. Βάσει της εκτίμησης επιπτώσεων στις επιχειρήσεις και των εύλογων σεναρίων, οι επιχειρήσεις θα πρέπει να καταρτίζουν σχέδια αντιμετώπισης και ανάκτησης. Στα σχέδια αυτά θα πρέπει να προσδιορίζονται οι συνθήκες οι οποίες ενδέχεται να απαιτήσουν ενεργοποίηση των σχεδίων, καθώς και τη λήψη μέτρων για τη διασφάλιση της ακεραιότητας, της διαθεσιμότητας, της συνέχειας και της ανάκτησης, τουλάχιστον, των κρίσιμων συστημάτων ΤΠΕ, των υπηρεσιών και δεδομένων ΤΠΕ των επιχειρήσεων. Τα σχέδια αντιμετώπισης και ανάκτησης θα πρέπει να αποσκοπούν στην επίτευξη των στόχων ανάκτησης των λειτουργιών των επιχειρήσεων.

71. Στα σχέδια αντιμετώπισης και ανάκτησης θα πρέπει να λαμβάνονται υπόψη τόσο βραχυπρόθεσμες όσο και, κατά περίπτωση, μακροπρόθεσμες επιλογές ανάκτησης. Τα σχέδια θα πρέπει, τουλάχιστον:

    a) να επικεντρώνονται στην ανάκτηση των λειτουργιών σημαντικών υπηρεσιών ΤΠΕ, επιχειρησιακών λειτουργιών, υποστηρικτικών διαδικασιών, πληροφοριακών πόρων και των αλληλεξαρτήσεων τους για την αποφυγή δυσμενών επιπτώσεων στη λειτουργία της επιχείρησης·

    b) να τεκμηριώνονται και να διατίθενται στις επιχειρηματικές μονάδες και στις μονάδες υποστήριξης και να είναι εύκολα διαθέσιμες σε περίπτωση έκτακτης ανάγκης, συμπεριλαμβανομένου ενός σαφούς ορισμού ρόλων και αρμοδιοτήτων· και

    c) να επικαιροποιούνται συνεχώς με βάση τα διδάγματα που αντλούνται από τα συμβάντα, τις δοκιμές, τους νέους κινδύνους που προσδιορίζονται και τις απειλές, καθώς και τους μεταβαλλόμενους στόχους και τις προτεραιότητες ανάκτησης.

72. Στα σχέδια θα πρέπει να λαμβάνονται επίσης υπόψη εναλλακτικές επιλογές σε περίπτωση που η ανάκτηση μπορεί να μην είναι εφικτή σε βραχυπρόθεσμο ορίζοντα λόγω κόστους, κινδύνων, υλικοτεχνικής υποστήριξης ή απρόβλεπτων περιστάσεων.

73. Στο πλαίσιο των σχεδίων αντιμετώπισης και ανάκτησης, οι επιχειρήσεις θα πρέπει να εξετάζουν και να εφαρμόζουν μέτρα συνέχειας για τον περιορισμό της αποτυχίας των παρόχων υπηρεσιών, τα οποία είναι καθοριστικής σημασίας για τη συνέχεια των υπηρεσιών ΤΠΕ των επιχειρήσεων (σύμφωνα με τις διατάξεις των κατευθυντήριων γραμμών της ΕΙΟΡΑ σχετικά με το σύστημα διακυβέρνησης και των κατευθυντήριων γραμμών σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους).

Κατευθυντήρια γραμμή 23 – Δοκιμές σχεδίων

74. Οι επιχειρήσεις θα πρέπει να δοκιμάζουν τα οικεία Σχέδια Επιχειρησιακής Συνέχειας και να διασφαλίζουν ότι η λειτουργία των κρίσιμων επιχειρηματικών διαδικασιών και δραστηριοτήτων τους, οι επιχειρησιακές λειτουργίες, ρόλοι και πόροι (π.χ. πληροφοριακοί πόροι) και οι πόροι ΤΠΕ και οι αλληλεξαρτήσεις τους (συμπεριλαμβανομένων εκείνων που παρέχονται από παρόχους υπηρεσιών) ελέγχονται τακτικά με βάση τα χαρακτηριστικά κινδύνου των επιχειρήσεων.

75. Τα σχέδια επιχειρησιακής συνέχειας θα πρέπει να επικαιροποιούνται τακτικά, με βάση τα αποτελέσματα των δοκιμών, τις τρέχουσες πληροφορίες σχετικά με απειλές και τα διδάγματα που αντλούνται από προηγούμενα συμβάντα. Τυχόν σχετικές αλλαγές στους στόχους ανάκτησης (συμπεριλαμβανομένου του χρονικού στόχου ανάκτησης και του στόχου σημείου ανάκτησης) ή/και αλλαγές στις επιχειρηματικές διαδικασίες και δραστηριότητες, στις επιχειρηματικές λειτουργίες, στους ρόλους και τους πόρους (π.χ. πληροφοριακοί πόροι και πόροι ΤΠΕ) θα πρέπει επίσης να περιλαμβάνονται.

76. Οι δοκιμές των Σχεδίων Επιχειρησιακής Συνέχειας θα πρέπει να αποδεικνύουν ότι είναι σε θέση να διατηρήσουν τη βιωσιμότητα της επιχείρησης έως ότου ανακτηθούν κρίσιμες λειτουργίες σε προκαθορισμένο επίπεδο υπηρεσίας ή η ανοχή στους κραδασμούς.

77. Τα αποτελέσματα της δοκιμής θα πρέπει να τεκμηριώνονται, ενώ επίσης τυχόν διαπιστωθείσες ελλείψεις που προκύπτουν από τις δοκιμές θα πρέπει να αναλύονται, να αντιμετωπίζονται και να αναφέρονται στο διοικητικό, διαχειριστικό ή εποπτικό όργανο.

Κατευθυντήρια γραμμή 24 - Επικοινωνία σε καταστάσεις κρίσεων

78. Σε περίπτωση διακοπής λειτουργίας ή έκτακτης ανάγκης, και κατά τη διάρκεια της εφαρμογής των σχεδίων επιχειρησιακής συνέχειας, οι επιχειρήσεις θα πρέπει να διασφαλίζουν την εφαρμογή αποτελεσματικών μέτρων επικοινωνίας σε καταστάσεις κρίσεων, ούτως ώστε όλοι οι σχετικοί εσωτερικοί και εξωτερικοί ενδιαφερόμενοι φορείς, συμπεριλαμβανομένων αρμόδιων εποπτικών αρχών, όταν απαιτείται από την εθνική νομοθεσία, καθώς και οι σχετικοί πάροχοι υπηρεσιών, να ενημερώνονται με έγκαιρο και κατάλληλο τρόπο.

Κατευθυντήρια γραμμή 25 – Εξωτερική ανάθεση υπηρεσιών ΤΠΕ και συστημάτων ΤΠΕ

79. Με την επιφύλαξη των κατευθυντήριων γραμμών της ΕΙΟΡΑ σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους, οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι όταν οι υπηρεσίες ΤΠΕ και τα συστήματα ΤΠΕ έχουν ανατεθεί σε εξωτερικούς συνεργάτες, πληρούνται οι σχετικές απαιτήσεις για την υπηρεσία ΤΠΕ ή το σύστημα ΤΠΕ.

80. Σε περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών λειτουργιών, οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι οι συμβατικές υποχρεώσεις του παρόχου υπηρεσιών (π.χ. σύμβαση, συμβάσεις διασφάλισης επιπέδου ποιότητας υπηρεσιών, διατάξεις καταγγελίας στις σχετικές συμβάσεις) περιλαμβάνουν, τουλάχιστον, τα ακόλουθα:

    a) κατάλληλους και αναλογικούς στόχους και μέτρα ασφάλειας πληροφοριών, συμπεριλαμβανομένων απαιτήσεων όπως ελάχιστες απαιτήσεις ασφάλειας πληροφοριών, προδιαγραφές του κύκλου ζωής δεδομένων των επιχειρήσεων, δικαιώματα ελέγχου και πρόσβασης και τυχόν απαιτήσεις σχετικά με την τοποθεσία των κέντρων δεδομένων και απαιτήσεις κρυπτογράφησης δεδομένων, ασφάλειας δικτύου και διαδικασιών παρακολούθησης της ασφάλειας

    b) συμβάσεις διασφάλισης επιπέδου ποιότητας υπηρεσιών, για την εξασφάλιση της συνέχειας των υπηρεσιών ΤΠΕ και των συστημάτων ΤΠΕ και στόχων επιδόσεων υπό κανονικές συνθήκες, καθώς και εκείνων που παρέχονται από σχέδια έκτακτης ανάγκης σε περίπτωση διακοπής παροχής υπηρεσίας· και

    c) διαδικασίες χειρισμού περιστατικών λειτουργικού κινδύνου και περιστατικών ασφάλειας, συμπεριλαμβανομένης της υποβολής εκθέσεων και της παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας.

81. Οι επιχειρήσεις θα πρέπει να παρακολουθούν και να ζητούν διαβεβαίωση σχετικά με το επίπεδο συμμόρφωσης των εν λόγω προμηθευτών υπηρεσιών με τους αντικειμενικούς σκοπούς, τα μέτρα και τους στόχους επιδόσεών τους όσον αφορά την ασφάλεια.

Συμμόρφωση και κανόνες αναφοράς

82. Το παρόν έγγραφο περιέχει κατευθυντήριες γραμμές οι οποίες εκδίδονται δυνάμει του άρθρου 16 του κανονισμού (ΕΕ) αριθ. 1094/2010. Σύμφωνα με το άρθρο 16 παράγραφος 3 του εν λόγω κανονισμού, οι αρμόδιες αρχές και οι επιχειρήσεις καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις εκάστοτε κατευθυντήριες γραμμές και συστάσεις.

83. Οι αρμόδιες αρχές που συμμορφώνονται ή προτίθενται να συμμορφωθούν προς τις παρούσες κατευθυντήριες γραμμές θα πρέπει να τις ενσωματώσουν δεόντως στο ρυθμιστικό ή εποπτικό τους πλαίσιο.

84. Οι αρμόδιες αρχές πρέπει να επιβεβαιώνουν στην EIOPA αν συμμορφώνονται ή προτίθενται να συμμορφωθούν προς τις παρούσες κατευθυντήριες γραμμές, αναφέροντας τους λόγους της ενδεχόμενης μη συμμόρφωσης, εντός δύο μηνών από την ημερομηνία έκδοσης της μετάφρασης των κατευθυντήριων γραμμών.

85. Ελλείψει απάντησης εντός της προθεσμίας αυτής, θα θεωρείται ότι οι αρμόδιες αρχές δεν συμμορφώνονται προς τους κανόνες αναφοράς και θα αποτελούν αντικείμενο σχετικής αναφοράς.

Τελική διάταξη περί επανεξέτασης

86. Οι παρούσες κατευθυντήριες γραμμές υπόκεινται σε επανεξέταση από την EIOPA.