ΣΥΝΟΨΗ ΤΩΝ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ ΤΗΣ HP

Για την προστασία των δεδομένων των Πελατών, η HP τηρεί ένα ισχυρό σύνολο ελέγχων ασφάλειας πληροφοριών, συμπεριλαμβανομένων πολιτικών, πρακτικών, διαδικασιών και οργανικών δομών για τη διασφάλιση του απορρήτου, της ακεραιότητας και της διαθεσιμότητας των δικών της πληροφοριών και των πληροφοριών των πελατών της (συμπεριλαμβανομένων των προσωπικών δεδομένων όπως ορίζονται στις Προσθήκες της HP σχετικά με τους πελάτες και την επεξεργασία δεδομένων). Παρακάτω παρατίθεται μια επισκόπηση των τεχνικών/οργανωτικών μέτρων ασφαλείας της HP σε όλη την εταιρεία.

1. Πολιτική ασφαλείας

   Η HP διατηρεί καθολικά εφαρμόσιμες πολιτικές, πρότυπα και διαδικασίες που αποσκοπούν στην προστασία των δεδομένων της HP και των πελατών. Οι λεπτομέρειες των πολιτικών ασφαλείας της HP είναι εμπιστευτικές για την προστασία της ακεραιότητας των δεδομένων και των συστημάτων της HP. Ωστόσο, περιλήψεις των βασικών πολιτικών μας περιλαμβάνονται παρακάτω.

2. Οργάνωση ασφάλειας πληροφοριών

   Το πρόγραμμα για την ασφάλεια των πληροφοριών της HP έχει σχεδιαστεί για να κατευθύνει και να διατηρεί τη στρατηγική και τους ελέγχους ασφάλειας πληροφοριών του οργανισμού. Το σύστημα αυτό διασφαλίζει τη συμμόρφωση σε επίπεδο επιχειρήσεων με τις πολιτικές και τους ελέγχους ασφαλείας της HP, καθώς και την τήρηση των απαιτήσεων ασφαλείας των πελατών της. Το Πλαίσιο, το οποίο είναι δομημένο σύμφωνα με τα τυποποιημένα πλαίσια, τους νόμους και τους κανονισμούς κυβερνοασφάλειας, αναθεωρείται ετησίως για να προσαρμόζεται στο εξελισσόμενο τοπίο απειλών της HP.

3. Διαχείριση κινδύνων κυβερνοασφάλειας

   Το πρόγραμμα διαχείρισης κινδύνων κυβερνοασφάλειας της HP έχει σχεδιαστεί για τη διατήρηση του απορρήτου, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών πόρων της. Το πρόγραμμα παρέχει μια συνεπή προσέγγιση για τον εντοπισμό, την αξιολόγηση, την ιεράρχηση, την αντιμετώπιση, την αποκατάσταση, την παρακολούθηση και την αναφορά των κινδύνων κυβερνοασφάλειας. Η HP καθορίζει τη διάθεση για ανάληψη κινδύνων ως το αποδεκτό επίπεδο έκθεσης σε απώλειες και την ανοχή κινδύνου ως τον βαθμό απόκλισης από την εν λόγω διάθεση. Οι κίνδυνοι αξιολογούνται με τη χρήση καθορισμένης μεθοδολογίας, η οποία δίνει στην HP τη δυνατότητα να μετριάσει τους κινδύνους ασφάλειας των πληροφοριών σε αποδεκτό επίπεδο. Το πρόγραμμα αυτό ευθυγραμμίζεται με τη διαδικασία Διαχείρισης επιχειρηματικών κινδύνων της HP.

Τελευταία ενημέρωση: Σεπτέμβριος 2024

4. Ασφάλεια ανθρώπινου δυναμικού

   Η πολιτική ασφάλειας για το ανθρώπινο δυναμικό της HP διασφαλίζει την ασφάλεια των πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής των εργαζομένων, δημιουργώντας διαδικασίες για την πρόσβαση σε εγκαταστάσεις, συστήματα πληροφοριών και άλλα περιουσιακά στοιχεία. Περιλαμβάνει τη λήψη γραπτών επιβεβαιώσεων μέσω συμφωνιών απόρρητου και μη κοινοποίησης, καθώς και τη διεξαγωγή διαδικασιών ελέγχου ιστορικού. Όλοι οι υποψήφιοι για πρόσληψη στην HP πρέπει να ολοκληρώνουν έναν έλεγχο ιστορικού σύμφωνα με τη σχετική νομοθεσία, τους κανονισμούς και τη δεοντολογία.

5. Διαχείριση πόρων

   Η HP διαθέτει μια διαδικασία για τον εντοπισμό πόρων τεχνικών πληροφοριών, την κατηγοριοποίηση κρίσιμων πόρων και τη διατήρηση τεκμηριωμένων διαδικασιών χειρισμού για κάθε τύπο ταξινόμησης πληροφοριών, συμπεριλαμβανομένων εκείνων που περιέχουν προσωπικά δεδομένα. Οι εν λόγω διαδικασίες καλύπτουν την αποθήκευση, τη διαβίβαση, την κοινοποίηση, την πρόσβαση, την καταγραφή, τη διατήρηση, την καταστροφή, τη διάθεση, τη διαχείριση συμβάντων και τη γνωστοποίηση παραβίασης. Οι πολιτικές και τα πρότυπα ασφαλείας της HP επιβάλλουν επίσης την ασφαλή απόρριψη των μέσων.

6. Ασφάλεια δεδομένων

   Το πρόγραμμα για την ασφάλεια δεδομένων της HP περιγράφει τις πρακτικές ασφαλείας και τους τεχνικούς ελέγχους που πρέπει να εφαρμόζονται για την προστασία του απόρρητου, της αυθεντικότητας και της ακεραιότητας των δεδομένων. Οι νομικές απαιτήσεις, η σημαντικότητα, η κρισιμότητα και η ευαισθησία σε μη εξουσιοδοτημένη αποκάλυψη ή τροποποίηση είναι μερικοί από τους παράγοντες που καθορίζουν τον τρόπο ταξινόμησης των πληροφοριών σύμφωνα με την πολιτική της HP για την ασφάλεια των δεδομένων. Εκτός από τις διαδικασίες χειρισμού των δεδομένων, η πολιτική περιγράφει την κρυπτογράφηση, τη διαγραφή, τη συλλογή και την επεξεργασία, τη διατήρηση, τη δημιουργία αντιγράφων ασφαλείας και την πρόληψη της απώλειας των δεδομένων.

7. Έλεγχος πρόσβασης

   Η HP εφαρμόζει την αρχή των ελάχιστων προνομίων για τον έλεγχο λογικής πρόσβασης, παρέχοντας πρόσβαση στους χρήστες μέσω μοναδικών αναγνωριστικών και κωδικών πρόσβασης χρήστη. Η πολιτική κωδικών πρόσβασης ορίζει τους ελέγχους πολυπλοκότητας, ισχύος, εγκυρότητας και ιστορικού των κωδικών πρόσβασης. Τα δικαιώματα πρόσβασης επανεξετάζονται περιοδικά και αφαιρούνται κατά την αποχώρηση του προσωπικού. Οι συμφωνημένες διαδικασίες για τη δημιουργία και διαγραφή λογαριασμών χρήστη εφαρμόζονται για τη χορήγηση και την αφαίρεση πρόσβασης σε συστήματα πελατών κατά τη διάρκεια των δεσμεύσεων.

8. Κρυπτογράφηση

   Η HP έχει καθορίσει ένα σύνολο ισχυρών διαδικασιών για την κρυπτογράφηση, ώστε να διασφαλίζεται το απόρρητο, η ακεραιότητα και η διαθεσιμότητα των πληροφοριακών πόρων. Τα εγκεκριμένα πρωτόκολλα απαιτούν κρυπτογράφηση για ορισμένους πόρους, συμπεριλαμβανομένων αυτών που περιέχουν προσωπικά δεδομένα. Το πρόγραμμα κρυπτογράφησης περιλαμβάνει τη χρήση μαθηματικών τεχνικών για την ασφάλεια των πληροφοριών και των επικοινωνιών, διασφαλίζοντας ότι μόνο εξουσιοδοτημένα μέρη μπορούν να έχουν πρόσβαση στα δεδομένα. Ένα κρίσιμο στοιχείο του προγράμματος ασφάλειας των πληροφοριών της HP είναι η προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση και παραποίηση.

9. Φυσική και περιβαλλοντική ασφάλεια

   Οι εγκαταστάσεις της HP προστατεύονται με τη χρήση διαφόρων φυσικών και ηλεκτρονικών ελέγχων πρόσβασης, συμπεριλαμβανομένων των φρουρών ασφαλείας, του ηλεκτρονικού ελέγχου πρόσβασης και της τηλεόρασης κλειστού κυκλώματος (CCTV). Οι εγκαταστάσεις είναι επίσης εξοπλισμένες με την απαραίτητη υποστήριξη υποδομών, συμπεριλαμβανομένου του ελέγχου της θερμοκρασίας και της εφεδρικής τροφοδοσίας ρεύματος, χρησιμοποιώντας UPS ή/και γεννήτριες ντίζελ για την υποστήριξη κρίσιμων υπηρεσιών. Όλο το προσωπικό της HP είναι καταγεγραμμένο και απαιτείται να φέρει τα κατάλληλα διακριτικά αναγνώρισης.

10. Διαχείριση λειτουργιών

    Η HP έχει θεσπίσει ελάχιστες απαιτήσεις σχετικά με την ενίσχυση της ανθεκτικότητας των υποδομών τεχνολογίας, συμπεριλαμβανομένων των σταθμών εργασίας, των διακομιστών και του δικτυακού εξοπλισμού. Αυτές οι συσκευές χρησιμοποιούν εικόνες λειτουργικού συστήματος που έχουν ήδη ενισχυθεί ως προς την ανθεκτικότητα, με τις απαιτήσεις να διαφέρουν ανάλογα με το λειτουργικό σύστημα και τους ελέγχους που εφαρμόζονται. Επιπλέον, η HP έχει αναπτύξει συστήματα ανίχνευσης/πρόληψης εισβολών στο δίκτυο (NIDS/NIPS), στα οποία η παρακολούθηση και η διαχείριση πραγματοποιείται 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα.

11. Ασφάλεια επικοινωνιών

    Η ασφάλεια επικοινωνιών διασφαλίζει την προστασία των πληροφοριών στα εταιρικά δίκτυα. Περιλαμβάνει την εγκατάσταση και τη διαχείριση στοιχείων ασφάλειας δικτύου (π.χ. τείχη προστασίας), το διαχωρισμό δικτύων, καθώς και ελέγχους φιλτραρίσματος Web και χειρισμού των email. Επιπλέον, περιλαμβάνει την παρακολούθηση και τη διαχείριση των καναλιών επικοινωνίας για τον εντοπισμό και την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή παραβίασης δεδομένων.

12. Ασφάλεια συστημάτων

    Η πολιτική της HP επιβάλλει μια ασφαλή μεθοδολογία ανάπτυξης συστημάτων και λογισμικού καθ' όλη τη διάρκεια του κύκλου ζωής τους. Ο κύκλος ανάπτυξης λογισμικού καλύπτει την έναρξη, την ανάπτυξη/απόκτηση, την εφαρμογή, τις λειτουργίες και τη διάθεση του λογισμικού. Όλα τα στοιχεία του συστήματος αξιολογούνται ως προς τις επιπτώσεις τους στη συνολική ασφάλεια. Η HP έχει καθιερώσει ελέγχους για τις συναλλαγές των εφαρμογών υπηρεσιών, συμπεριλαμβανομένης της επικύρωσης των διαπιστευτηρίων των χρηστών, των ψηφιακών υπογραφών, της κρυπτογράφησης, των πρωτοκόλλων ασφαλούς επικοινωνίας και της αποθήκευσης των στοιχείων των συναλλαγών εντός της κατάλληλης ζώνης ασφαλείας του δικτύου. Πραγματοποιούνται επίσης τακτικές εσωτερικές σαρώσεις ευαλωτότητας.

13. Τρίτα μέρη και υπεργολάβοι

    Η HP διαθέτει διαδικασίες για την επιλογή υπεργολάβων, οι οποίες συμμορφώνονται με τις ολοκληρωμένες συμβατικές απαιτήσεις ασφαλείας. Για τους ισχύοντες προμηθευτές που χειρίζονται δεδομένα της HP ή δεδομένα των πελατών της HP ή έχουν πρόσβαση στο δίκτυο HP, η ομάδα της HP για την ασφάλεια στον κυβερνοχώρο (HP Cybersecurity) διενεργεί αξιολόγηση κινδύνων για την επαλήθευση του προγράμματος ασφαλείας πληροφοριών σχετικά με την προστασία με φυσικά, τεχνικά και οργανωτικά μέτρα. Η εν λόγω αξιολόγηση απαιτείται προτού ο προμηθευτής αποκτήσει πρόσβαση στις πληροφορίες της HP.

14. Διαχείριση περιστατικών ασφάλειας πληροφοριών

    Η HP διαθέτει μια ολοκληρωμένη διαδικασία διαχείρισης περιστατικών στον κυβερνοχώρο, η οποία περιγράφει τον σκοπό, το πεδίο εφαρμογής, τους ρόλους, τις αρμοδιότητες, τη δέσμευση της διοίκησης, τον συντονισμό της οργάνωσης, τις διαδικασίες εφαρμογής και τον έλεγχο συμμόρφωσης. Η διαδικασία αυτή επανεξετάζεται και επικαιροποιείται ετησίως. Η ομάδα αντιμετώπισης περιστατικών στον κυβερνοχώρο (Cyber Incident Response Team), συμπεριλαμβανομένου του προσωπικού της HP Cybersecurity, εκπαιδευμένη στην αντιμετώπιση περιστατικών και στη διαχείριση κρίσεων, πραγματοποιεί επί χάρτου επισκοπήσεις της διαδικασίας και τυχόν περιστατικών ή συμβάντων.

15. Διαχείριση επιχειρηματικής συνέχειας

    Το παγκόσμιο πρόγραμμα συνέχισης των δραστηριοτήτων της HP διασφαλίζει τη συνέχεια από την αρχή έως το τέλος μέσω συνεργατικών, τυποποιημένων και τεκμηριωμένων διαδικασιών σχεδιασμού. Η εταιρεία εφαρμόζει περιοδικά τα σχέδια επιχειρηματικής συνέχειας για να διασφαλίσει την αποτελεσματικότητά τους, δοκιμάζοντας και επικαιροποιώντας όλα τα σχέδια τουλάχιστον μια φορά το χρόνο. Επιπλέον, όλο το προσωπικό που συμμετέχει στο σχέδιο επιχειρηματικής συνέχειας λαμβάνει κατάλληλη εκπαίδευση.

16. Συμμόρφωση

    Η συμμόρφωση διαμορφώνει την προσέγγιση της HP για την τήρηση των νομικών, συμβατικών και εσωτερικών προσδοκιών για ένα αποτελεσματικό πρόγραμμα ασφάλειας πληροφοριών. Οι τακτικοί έλεγχοι ασφάλειας πληροφοριών διασφαλίζουν ότι τα πρωτόκολλα ενσωματώνονται στις λειτουργίες κάθε επιχειρηματικής ομάδας. Η διαδικασία επανεξέτασης διατηρεί επίσης τα έγγραφα επικαιροποιημένα, ώστε να αντικατοπτρίζουν τις τρέχουσες νομικές υποχρεώσεις καθώς εξελίσσονται οι απαιτήσεις.

17. Κλάδος καρτών πληρωμής

    Το πλαίσιο που αφορά τον κλάδο καρτών πληρωμής (Payment Card Industry - PCI) καθοδηγεί την προσέγγιση της HP για την επίτευξη συμμόρφωσης με το PCI, περιγράφοντας τις επιχειρηματικές ευθύνες και τους ελέγχους ασφαλείας που συμμορφώνονται με το πρότυπο ασφάλειας δεδομένων του κλάδου καρτών πληρωμής (PCI DSS). Εγκαθιστώντας και διατηρώντας ελέγχους ασφαλείας δικτύου, όπως τείχη προστασίας, η HP διασφαλίζει ότι πληροί τις απαιτήσεις συμμόρφωσης PCI.

18. Ασφάλεια προϊόντων της HP

    Η ασφάλεια προϊόντων της HP περιλαμβάνει βασικές πρακτικές για την ασφάλεια των προϊόντων HP, όπως η υπογραφή κώδικα, η διαχείριση των ευπαθειών ασφαλείας των προϊόντων, η έκδοση ανακοινώσεων ασφαλείας και η αναφορά ζητημάτων ασφαλείας των προϊόντων. Τα μέτρα αυτά διασφαλίζουν ότι τα προϊόντα HP παραμένουν ασφαλή και αξιόπιστα για τους χρήστες. Η ασφάλεια των προϊόντων είναι υψίστης σημασίας για την HP, καθώς βοηθά στη διατήρηση της εμπιστοσύνης των πελατών και στην προστασία από πιθανές απειλές.

19. Ασφάλεια υπηρεσιών της HP

    Η ασφάλεια υπηρεσιών της HP περιλαμβάνει βασικές πρακτικές για την ασφάλεια των υπηρεσιών που παρέχονται στους πελάτες της HP. Η πολιτική αυτή αφορά διάφορους τομείς σχετικά με την ασφάλεια των υπηρεσιών, συμπεριλαμβανομένων των περιβαλλόντων που φιλοξενούνται από τις υποδομές της HP, από τρίτους, από συνεργάτες και από πελάτες. Τα μέτρα αυτά διασφαλίζουν ότι οι υπηρεσίες της HP παραμένουν ασφαλείς και αξιόπιστες για τους χρήστες. Με την εφαρμογή ισχυρών πρακτικών ασφαλείας, η HP διασφαλίζει την ασφάλεια και την ακεραιότητα των προϊόντων και των υπηρεσιών της, δημιουργώντας ένα ασφαλές και αξιόπιστο περιβάλλον για όλους τους χρήστες.