

ΜΙΚΡΗ ΕΠΙΧΕΙΡΗΣΗ ΠΟΡΤΟΓΑΛΙΑ

Ιστορία κινδύνου 3



Co-funded by the
Erasmus+ Programme
of the European Union



Μικρή επιχείρηση από την Πορτογαλία

Πλαίσιο της εταιρείας και της εφοδιαστικής αλυσίδας

Με περίπου 30 υπαλλήλους και σχεδόν 30 χρόνια στη συμβουλευτική μεταφορών, η εταιρεία έχει τρεις κύριους επιχειρηματικούς τομείς: κυκλοφοριακές μελέτες, σχεδιασμός δικτύων μεταφορών και δημόσιες οδικές μεταφορές. Το έργο τους μπορεί να κυμαίνεται από το σχεδιασμό σιδηροδρομικών γραμμών για δημόσιους φορείς έως χώρους στάθμευσης για εμπορικά κέντρα.

Για ορισμένους από τους σχεδιασμούς της, η εταιρεία έχει πρόσβαση σε ορισμένα ευαίσθητα δεδομένα που παρέχονται από τους πελάτες της για την ανάπτυξη μοντέλων πρόβλεψης, π.χ. λεπτομερή οικονομικά δεδομένα πελατών ή λεπτομερή δεδομένα κυκλοφορίας ορισμένων δρόμων.

Ψηφιοποίηση της Εφοδιαστικής Αλυσίδας

Η εταιρεία διαθέτει δύο κύρια συστήματα: ένα για τη διαχείριση των οικονομικών στοιχείων του έργου και ένα άλλο για τη διαχείριση των απαιτήσεων του έργου. Και τα δύο συστήματα είναι μοναδικά, έχουν αναπτυχθεί ειδικά για την επιχείρηση και φιλοξενούνται σε τοπικό διακομιστή.

Ωστόσο, και τα δύο συστήματα είναι βαριά και απαρχαιωμένα, παρουσιάζοντας περιορισμούς στη χρήση, την υπολογιστική ισχύ και την επεκτασιμότητα και, ως εκ τούτου, απαιτούν ορισμένες λύσεις από εξωτερικές πηγές για την καθημερινή εργασία, όπως η υπερβολική χρήση αρχείων excel.

Η ανάπτυξη και των δύο συστημάτων σταμάτησε στα μισά της διαδρομής. Η μετάβαση των δεδομένων στα συστήματα αυτά είναι επίσης ένα προβληματικό και δαπανηρό εγχείρημα. Τα αντίγραφα ασφαλείας του συστήματος γίνονταν χειροκίνητα κάθε μήνα σε σκληρούς δίσκους, αλλά πρόσφατα έχουν περάσει σε καθημερινό αντίγραφο ασφαλείας μέσω μιας υπηρεσίας cloud.

Λόγω των περιορισμών και των δύο συστημάτων, η όλη αλληλεπίδραση με την υπόλοιπη αλυσίδα εφοδιασμού γίνεται με άλλα μέσα, με την πιο συνηθισμένη ανταλλαγή πληροφοριών να γίνεται μέσω ηλεκτρονικού ταχυδρομείου.

Διαχείριση κινδύνων

Πρακτική της Διαχείρισης Κινδύνου

Η εμπιστευτικότητα των ευαίσθητων δεδομένων αντιμετωπίζεται επί του παρόντος μέσω των NDAs και των αυθεντικοποιήσεων πολλαπλών παραγόντων. Ορισμένα δεδομένα υψηλότερου επιπέδου είναι επίσης προσβάσιμα μόνο από τους διαχειριστές έργων και δεν αποκαλύπτονται σε άλλους υπαλλήλους. Η εταιρεία δημιουργεί καθημερινά αντίγραφα ασφαλείας των πληροφοριών για την αποφυγή απωλειών.

Για να λύσει την εξάρτησή της από τα μοναδικά συστήματα, η εταιρεία προσέλαβε εξωτερικούς συμβούλους για να βρουν εναλλακτικές λύσεις στα τρέχοντα προβλήματα της υποδομής πληροφορικής. Ως αποτέλεσμα, έχει διατεθεί μεγάλος προϋπολογισμός για την ανάπτυξη της Τεχνολογίας Πληροφορικής το 2021. Ελπίζουν να μεταβούν σε νέα συστήματα με δυνατότητα διαχείρισης μεγάλων δεδομένων, ενσωμάτωσης με εξωτερικές οντότητες και μελλοντικής επεκτασιμότητας για να συμβαδίζουν με τις επιχειρηματικές απαιτήσεις. Τα κλειστά έργα θα παραμείνουν στο παλιό σύστημα και τα αντίγραφα ασφαλείας- μόνο τα ενεργά έργα θα μεταφερθούν στα νέα συστήματα για να μειωθεί το κόστος μετάβασης δεδομένων.

Κίνδυνοι

Με την εξάρτησή τους από τα μοναδικά κατασκευασμένα συστήματα που φιλοξενούνται στους διακομιστές της εταιρείας, η εργασία ολόκληρης της εταιρείας μπορεί να τεθεί σε κίνδυνο για μεγάλο χρονικό διάστημα με ένα μόνο ελάττωμα του συστήματος. Τα ίδια τα συστήματα είναι επιρρεπή σε βλάβες και μόνο ένας τεχνικός είναι διαθέσιμος στην εταιρεία.

Η χρήση λεπτομερών, ευαίσθητων δεδομένων απαιτεί ιδιαίτερη προσοχή. Έτσι, η ασφάλεια στον κυβερνοχώρο καθίσταται απαραίτητη. Ωστόσο, με έναν μόνο υπάλληλο πληροφορικής και κάποια ανταλλαγή πληροφοριών μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, η ασφάλεια μπορεί να τεθεί σε σοβαρό κίνδυνο.

Μια αποτυχία των δύο συστημάτων θα σήμαινε διακοπή των εργασιών της εταιρείας κατά τη διάρκεια της αποτυχίας. Εάν λήξουν οι παλιοί διακομιστές, η ζημία θα ήταν σημαντική. Θα μπορούσε να σημαίνει αρκετές εβδομάδες διακοπής των εργασιών της εταιρείας, είτε λόγω του χρόνου αποκατάστασης των ζημιών είτε λόγω έλλειψης πρόσβασης σε κρίσιμα δεδομένα.

Μια διαρροή ευαίσθητων δεδομένων θα αποτελούσε επίσης σοβαρό πρόβλημα. Θα έβλαπτε τη φήμη της εταιρείας και θα ερχόταν σε αντίθεση με τις υπογεγραμμένες Συμβάσεις Εμπιστευτικότητας, με πιθανό αποτέλεσμα την επισκευή για παραβίαση των συμβάσεων ή τον περαιτέρω αποκλεισμό της εταιρείας από μελλοντικές εργασίες σε πολλούς τομείς με ευαίσθητα δεδομένα.

Κίνδυνοι στον κυβερνοχώρο

Η διαχείριση ευαίσθητων δεδομένων ενέχει κινδύνους, οπότε η έκθεσή τους στο διαδίκτυο και στους υπαλλήλους θα πρέπει να είναι όσο το δυνατόν πιο περιορισμένη. Η διατήρηση των ευαίσθητων δεδομένων μόνο στο εσωτερικό δίκτυο και ο περιορισμός της πρόσβασης μόνο από ορισμένα άτομα συμβάλλει στη μείωση των πιθανών διαρροών.

Κίνδυνοι που σχετίζονται με το Covid-19

Μετά την επιδημία του covid19, οι περισσότεροι εργαζόμενοι εργάζονται από το σπίτι τους χρησιμοποιώντας τα ιδιωτικά τους δίκτυα για να έχουν πρόσβαση σε ηλεκτρονικά μηνύματα και συστήματα που σχετίζονται με την εργασία τους μέσω υπηρεσιών VPN. Η κατάσταση αυτή αυξάνει τους κινδύνους εισόδου κακόβουλου λογισμικού στο σύστημα και απαιτεί περαιτέρω μέτρα κυβερνοασφάλειας, καθώς τα περισσότερα σημεία εισόδου στα συστήματα αντιπροσωπεύουν επίσης δυνητικά περισσότερες παραβιάσεις ασφαλείας.

Οφέλη από τη διαχείριση κινδύνων:

Με τον έλεγχο ταυτότητας πολλαπλών παραγόντων και τις Συμβάσεις Εμπιστευτικότητας, η εταιρεία μειώνει τον κίνδυνο απώλειας και διαρροής ευαίσθητων πληροφοριών.

Η μελλοντική επένδυση σε νέες λύσεις πληροφορικής διασφαλίζει ότι η εταιρεία μπορεί να διαχειρίζεται περισσότερες πληροφορίες και λειτουργίες χωρίς κατάρρευση του συστήματος, ενώ παράλληλα εξασφαλίζει μεγαλύτερη επεκτασιμότητα.