KLEINUNTERNEHMEN

PORTUGAL

Die Risk-Story 3

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

BEPREPARED

Kleinunternehmen aus Portugal

Kontext des Unternehmens und der Supply Chain

Mit rund 30 Mitarbeitern und fast 30 Jahren Erfahrung in der Verkehrsberatung ist das Unternehmen drei Hauptgeschäftsbereichen aktiv: Verkehrsstudien, Planung von Verkehrsnetzen und öffentlicher Straßenverkehr. Die Arbeit des Unternehmens reicht von der Planung von Bahnstrecken für öffentliche Einrichtungen bis hin zu Parkplätzen für Einkaufszentren.

Für einige ihrer Planungen hat das Unternehmen Zugang zu sensiblen Daten, die von ihren Kunden zur Verfügung gestellt werden, um Prognosemodelle zu entwickeln, z. B. detaillierte Finanzdaten von Kunden oder detaillierte Verkehrsdaten bestimmter Straßen.

Digitalisierung der Supply Chain

Das Unternehmen verfügt über zwei Hauptsysteme: eines zur Finanzverwaltung von Projekten und eins zur Verwaltung von Projektanforderungen. Beide Systeme sind einzigartig, speziell für das Unternehmen entwickelt und werden auf einem lokalen Server gehostet.

Allerdings sind sie schwerfällig, veraltet und weisen Einschränkungen hinsichtlich Nutzung, Rechenleistung und Skalierbarkeit auf, wodurch die tägliche Arbeit einige Umgehungen aus externen Quellen erfordert, z. B. die übermäßige Verwendung von Excel-Dateien.

Die Entwicklung beider Systeme wurde auf halbem Wege gestoppt. Die Migration der Daten in die Systeme ist ebenfalls ein problematisches und teures Unterfangen. Die Sicherungen wurden früher jeden Monat manuell auf Festplatten durchgeführt, seit kurzem sind sie aber auf eine tägliche Sicherung über einen Cloud-Dienst umgestiegen.

Aufgrund der Einschränkungen beider Systeme erfolgt die gesamte Interaktion mit dem Rest der Lieferkette anderweitig, wobei der Informationsaustausch meist über E-Mails erfolgt.

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

Risikomanagement

Durchführung des Risikomanagements

Die Vertraulichkeit sensibler Daten wird derzeit durch NDAs und Mehr-Faktoren-Authentifizierungen gewährleistet. Einige Daten auf höherer Ebene sind auch nur für Projektleiter zugänglich und werden nicht an andere Mitarbeiter weitergegeben. Das Unternehmen erstellt täglich Sicherungskopien der Daten, um Verluste zu verhindern.

Um die Abhängigkeit von den einzigartigen Systemen zu lösen, hat das Unternehmen externe Berater engagiert, um Alternativen zu den derzeitigen IT-Infrastrukturproblemen zu finden. Infolgedessen wurde ein großes Budget für die IT-Entwicklung im Jahr 2021 zur Verfügung gestellt. Das Unternehmen hofft, auf neue Systeme umsteigen zu können, die in der Lage sind, mit großen Datenmengen umzugehen, sich mit externen Stellen zu integrieren und in Zukunft skalierbar zu sein, um mit den Geschäftsanforderungen Schritt zu halten. Abgeschlossene Projekte werden im alten System und in den Backups verbleiben; nur aktive Projekte werden in die neuen Systeme migriert, um die Kosten für die Datenmigration zu senken.

Risiken

Durch die Abhängigkeit von den eigens entwickelten Systemen, die auf den Servern des Unternehmens gehostet werden, kann die Arbeit des gesamten Unternehmens durch einen einzigen Systemfehler für lange Zeit gefährdet werden. Die Systeme selbst sind störanfällig und im Unternehmen steht nur ein Techniker zur Verfügung.

Der Umgang mit detaillierten, sensiblen Daten erfordert besondere Aufmerksamkeit. Cybersicherheit ist daher ein Muss. Da jedoch nur ein IT-Mitarbeiter zur Verfügung steht und einige Informationen per E-Mail ausgetauscht werden, kann die Sicherheit stark beeinträchtigt werden.

Ein Ausfall beider Systeme würde die Arbeit des Unternehmens für die Dauer des Ausfalls zum Erliegen bringen. Wenn die alten Server ausfallen, wäre der

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

Schaden erheblich und könnte einen mehrwöchigen Stillstand der Unternehmenstätigkeit bedeuten, da entweder Zeit zur Behebung von Schäden aufgewendet werden müsste oder auf wichtige Daten nicht zugänglich wären.

Ein Leck bei sensiblen Daten wäre ebenfalls ein schwerwiegendes Problem. Es würde dem Ruf des Unternehmens schaden und gegen unterzeichnete NDAs verstoßen, was möglicherweise zu Reparaturen auf Grund von Vertragsverletzungen oder zum Ausschluss des Unternehmens von zukünftigen Arbeiten in vielen Bereichen mit sensiblen Daten führen könnte.

Cyber-Risiken

Der Umgang mit sensiblen Daten stellt ein Risiko dar, daher sollte die Exposition gegenüber Internet und Mitarbeitern so gering wie möglich gehalten werden. Die Aufbewahrung sensibler Daten im Intranet und die Beschränkung des Zugriffs auf bestimmte Personen tragen dazu bei, mögliche Lecks zu vermeiden.

Covid-19 bedingte Risiken

Seit der Covid19-Pandemie arbeiten die meisten Mitarbeiter von zu Hause und nutzen ihre privaten Netzwerke, um über VPN-Dienste auf arbeitsbezogene E-Mails und Systeme zuzugreifen. Diese Situation erhöht das Risiko, dass Malware in das System eindringt, und erfordert weitere Cybersicherheitsmaßnahmen, da mehr Zugangspunkte zu den Systemen auch potenziell mehr Sicherheitsverletzungen darstellen.

Nutzen des Risikomanagements

Mit Mehr-Faktor-Authentifizierung und NDAs reduziert das Unternehmen Verlusts- und Weitergaberisiken sensibler Informationen. Die künftigen Investitionen in neue IT-Lösungen stellen sicher, dass das Unternehmen mehr Informationen und Vorgänge verarbeiten kann, ohne dass das System zusammenbricht, und gewährleisten gleichzeitig mehr Skalierbarkeit.

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