KLEINUNTERNEHMEN
PORTUGAL

Die Risk-Story 2

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

BEPREPARED

Kleinunternehmen aus Portugal

Kontext des Unternehmens und der Supply Chain

Das Unternehmen wurde in den 1980er Jahren gegründet und ist in der Kunststoff-Spritzgussindustrie tätig. Das Kerngeschäft ist die Herstellung der innovativsten und effizientesten vollelektrischen Anbausysteme, entwickelt durch verschiedener Technologien, die seinen Kunden nachhaltigere und flexiblere Lösungen bieten.

Als Ingenieurbüro setzt es Ideen in Endprodukte um. Diese werden intern in Zusammenarbeit mit den Kunden entwickelt. Während sich das Unternehmen sich um den Forschungs- und Entwicklungsprozess kümmert, werden alle fertigungsbezogenen Aktivitäten von Subunternehmern übernommen. Jeder Zulieferer erhält einen Teil der Ausrüstung, wie ein Lego-Stein, ohne zu wissen, in welches Puzzle ein solches Teil passt. Zusammen mit vielen anderen wird dieses in das Endprodukt eingebaut.

Digitalisierung der Supply Chain

Das Unternehmen arbeitet mit verschiedenen IT-Systemen, die über ein Intranet mit unterschiedlichen Zugriffsebenen je nach Funktion und Zuständigkeit der Mitarbeiter verfügbar sind. Sie können auch aus der Ferne über ein VPN auf diese Systeme zugreifen.

Weder Kunden noch Lieferanten haben Zugang zum Intranet des Unternehmens. Die Interaktion mit den Kunden erfolgt hauptsächlich über E-Mail, während ein FTP-Server auch für den Dateitransfer genutzt werden kann – z. B. bei der gemeinsamen Nutzung größerer Dateien.

Das Unternehmen verwendet ein COTS-ERP-System, das mit dem Produktionsmanagement-System verbunden ist.

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

Risikomanagement

In Unternehmen 2 gibt es tatsächlich eine Risikomanagementstrategie. Das Cyber-Risiko wird jedoch nicht berücksichtigt, obwohl man sich der Bedeutung dieses Risikos bewusst ist.

Durchführung des Risikomanagements

Anhand der durchgeführten internen und externen Analyse ist es möglich, eine SWOT-Analyse zu erstellen und die Folgen und Auswirkungen auf die Geschäftstätigkeit des Unternehmens zu überprüfen. Diese Risikoidentifizierung und -bewertung wird in einer Matrix angewandt. Unter Berücksichtigung der Qualitäts- und Innovationspolitik werden Ziele definiert und Maßnahmen ergriffen, um die Ziele zu erreichen, sowie die notwendigen Schritte, um die in der Matrix identifizierten Risiken zu bewältigen.

Risiken

Operationale Risiken

Vertraulichkeitsvereinbarungen schützen die eigenen Interessen des Unternehmens und die seiner Kunden. Solche Vereinbarungen können erweitert werden, um andere Stellen in den Prozess einzubeziehen, wie Universitäten oder – selten, aber möglich, wenn es um komplexe Systeme geht – Lieferanten.

Mit Kunden werden nur Produktanforderungen ausgetauscht, mit Lieferanten nur technische Zeichnungen. Das Unternehmen fühlt sich in Bezug auf seine Zulieferer sicher: Erstens sind sie in einem anderen Geschäftsbereich tätig als ihre Zulieferer, zweitens stellt jeder Zulieferer nur eine Ausrüstungskomponente her, sodass sie keinen Zugang zum gesamten technischen Design haben.

Das Unternehmen setzt Software ein, um die Risiken aus mechanischer und elektrischer Sicht bei der Entwicklung eines Produkts zu analysieren.

Finanzielle Risiken

Das Unternehmen ist zu 75 % finanziell unabhängig und nimmt keine Bankkredite für seine Tätigkeit in Anspruch.

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

Marktrisiken

Wenn das Unternehmen etwas Innovatives entwickelt, meldet es ein Patent an, bevor es auf den Markt kommt.

Cyber-Risiken

Cyber-Risiken werden nicht berücksichtigt. Daher kann das Unternehmen diese Art von Risiko nicht quantifizieren, obwohl ein gewisses Bewusstsein für ihre potenzielle Schwere vorhanden ist. Das einzige Risiko, das auf der Cyber-Ebene festgestellt wurde, war ein Hackerangriff. Aus Sicht des Unternehmens sei dies jedoch nicht so katastrophal, da täglich Sicherheitskopien erstellt werden, die sich außerhalb des Unternehmens befinden. Außerdem ist es nicht einfach, ein vom Unternehmen patentiertes Produkt zu replizieren.

Das Unternehmen verlässt sich lediglich auf eine Person zur Verwaltung der IT-Systeme. Was die Informationssicherheitspolitik des Unternehmens anbelangt, so werden folgende Präventivmaßnahmen erwogen: Im Vertrag mit den Mitarbeitern wird die unrechtmäßige Nutzung von Unternehmensdaten abgedeckt (obwohl nichts jemanden daran hindert, wichtige Daten herunterzuladen); es werden täglich Sicherheitskopien an einem Ort außerhalb des Unternehmens erstellt; Firewall und Antivirus werden zum Schutz vor Bedrohungen eingesetzt.

Tatsächlich herrscht ein allgemeiner Wissensmangel, der auch zu einer Abwertung solcher Risiken führt. Es ist jedoch wichtig, darauf hinzuweisen, dass die Unternehmensleitung trotz der Tatsache, dass diese Art von Risiken bisher nicht formell berücksichtigt wurde, offen für die Einführung eines Informationsrisikomanagements war.

Covid-19 bedingte Risiken

Obwohl einige Mitarbeiter des Unternehmens aus der Ferne arbeiten mussten, war man der Meinung, dass in Bezug auf die Risiken der Informationssicherheit kein zusätzliches Bewusstsein erforderlich war. In diesem Sinne wurden auch keine zusätzlichen Maßnahmen ergriffen.

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