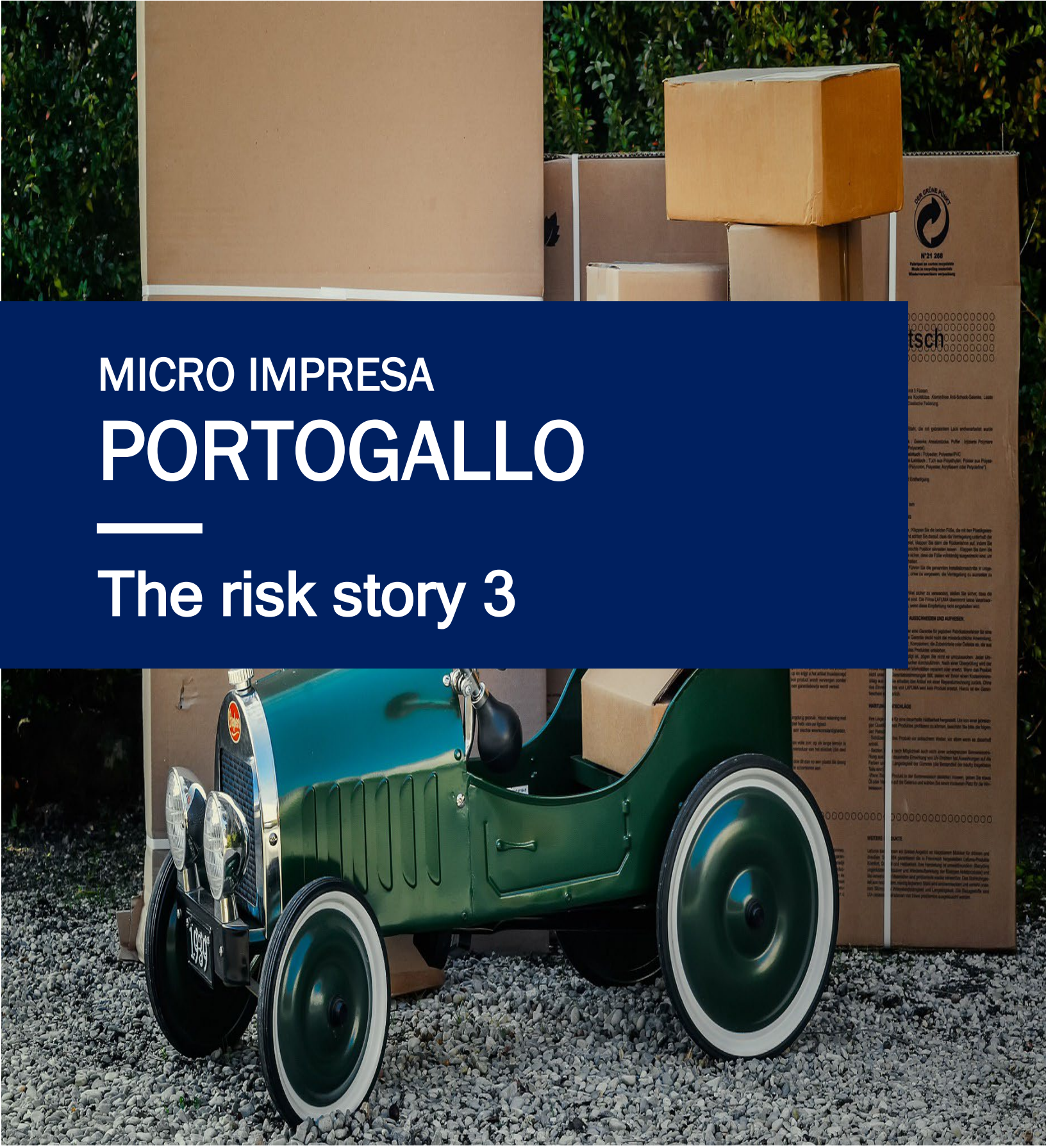

MICRO IMPRESA

PORTOGALLO

The risk story 3

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

BEPREPARED

Micro impresa del Portogallo

Descrizione dell'azienda e della sua Supply Chain

Con circa 30 dipendenti e quasi 30 anni di attività nella consulenza sui trasporti, l'azienda ha tre aree di attività principali: studi sul traffico, pianificazione delle reti di trasporto e trasporti pubblici su strada. Il loro lavoro può spaziare dalla pianificazione di ferrovie per enti pubblici ai parcheggi per centri commerciali.
Per alcune delle loro pianificazioni, l'azienda ha accesso ad alcuni dati sensibili forniti dai clienti per sviluppare modelli di previsione, ad esempio dati finanziari dettagliati dei clienti o dati dettagliati sul traffico di alcune strade.

Digitalizzazione della SC

L'azienda ha due sistemi principali: uno per la gestione finanziaria dei progetti e un altro per la gestione dei requisiti dei progetti. Entrambi i sistemi sono unici, sviluppati esplicitamente per l'azienda e ospitati su un server locale.

Tuttavia, entrambi i sistemi sono pesanti e arcaici, presentano limitazioni nell'uso, nella potenza di calcolo e nella scalabilità e richiedono quindi alcuni workaround da fonti esterne per il lavoro quotidiano, come l'uso eccessivo di file excel.

Lo sviluppo di entrambi i sistemi è stato interrotto a metà strada. Anche la migrazione dei dati in questi sistemi è un'impresa problematica e costosa. I backup del sistema venivano eseguiti manualmente ogni mese su dischi rigidi, ma di recente sono passati a un backup giornaliero tramite un servizio cloud.

A causa delle limitazioni di entrambi i sistemi, l'intera interazione con il resto della catena di fornitura avviene attraverso altri mezzi, con la condivisione di informazioni più comunemente tramite e-mail.

Risk Management

La riservatezza dei dati sensibili è attualmente gestita attraverso autenticazioni a più fattori. Inoltre, alcuni dati di livello superiore sono accessibili solo ai project manager e non vengono divulgati agli altri dipendenti. L'azienda esegue quotidianamente il backup delle informazioni per evitarne la perdita.

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

Per risolvere la dipendenza dai sistemi unici, l'azienda ha assunto consulenti esterni per trovare alternative agli attuali problemi dell'infrastruttura IT. Di conseguenza, è stato stanziato un budget consistente per lo sviluppo dell'IT nel 2021. L'azienda spera di passare a nuovi sistemi con la capacità di gestire i big data, l'integrazione con entità esterne e la futura scalabilità per tenere il passo con i requisiti aziendali. I progetti chiusi rimarranno nel vecchio sistema e nei backup; solo i progetti attivi migreranno ai nuovi sistemi per ridurre i costi di migrazione dei dati.

Rischi:

La dipendenza dai sistemi unici ospitati sui server dell'azienda può mettere a rischio l'intero lavoro dell'azienda per molto tempo con un singolo difetto del sistema. I sistemi stessi sono soggetti a guasti e l'azienda dispone di un solo tecnico.

L'utilizzo di dati dettagliati e sensibili richiede un'attenzione particolare. La cybersecurity diventa quindi un must. Tuttavia, con un solo dipendente IT e la condivisione di alcune informazioni tramite e-mail, la sicurezza potrebbe essere gravemente compromessa.

Un guasto dei due sistemi rappresenterebbe un arresto del lavoro dell'azienda per tutta la durata del guasto. Se i vecchi server scadono, il danno sarebbe significativo. Potrebbe significare diverse settimane di arresto dell'attività dell'azienda, sia per il tempo speso a riparare i danni sia per la mancanza di accesso ai dati critici.

Anche una fuga di dati sensibili rappresenterebbe un grave problema. Danneggerebbe la reputazione dell'azienda e andrebbe contro gli NDA firmati, causando potenzialmente riparazioni per violazioni del contratto o l'ulteriore esclusione dell'azienda dal lavoro futuro in molte aree con dati sensibili.

Rischi informatici

La gestione di dati sensibili è un rischio, quindi la loro esposizione a Internet e ai dipendenti deve essere il più possibile limitata. Mantenere i dati sensibili solo nell'intranet e limitarne l'accesso solo ad alcune persone aiuta a ridurre le potenziali fughe di notizie.

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

Rischi legati al Covid-19

Da quando è scoppiata l'epidemia di covid19, la maggior parte dei dipendenti lavora da casa utilizzando le proprie reti private per accedere alle e-mail e ai sistemi legati al lavoro tramite servizi VPN. Questa situazione aumenta i rischi di penetrazione di malware nel sistema e richiede ulteriori misure di cybersecurity, poiché un maggior numero di punti di accesso ai sistemi rappresenta anche un numero potenzialmente maggiore di violazioni della sicurezza.

Benefici del Risk Management

Grazie all'autenticazione a più fattori e agli NDA, l'azienda riduce il rischio di perdita e fuga di informazioni sensibili.
L'investimento futuro in nuove soluzioni informatiche assicura che l'azienda possa gestire un numero maggiore di informazioni e operazioni senza che il sistema collassi, garantendo al contempo una maggiore scalabilità.

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