



PICCOLA IMPRESA AUSTRIA

The risk story 5



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



PICCOLA IMPRESA DALL'AUSTRIA

Descrizione dell'azienda e della sua Supply Chain

L'azienda è una società di medie dimensioni, fondata nel 2006, con circa 30 dipendenti specializzati in servizi di sicurezza e consulenza sulla sicurezza. L'azienda esegue test di sicurezza o di penetrazione informatica. Intere aziende vengono testate per le misure di protezione e vengono fatti tentativi per ottenere il controllo del sistema IT senza conoscenza preliminare. Questa è una parte del portafoglio, la seconda è il complesso di consulenza completa che va oltre l'attacco cyber. In seguito, si elaborano delle road map per rendere il cliente più preparato per il futuro e più capace di difendersi.

Digitalizzazione della SC

L'azienda ha un alto livello di digitalizzazione. L'intero modello di business si basa su tecnologie moderne che sono emerse nel corso della digitalizzazione.

Risk Management

Tutti i partner sono responsabili della gestione del rischio.

Pratiche di Risk Management: Gli impiegati hanno un alto numero di diritti di lettura e modifica, perché hanno un alto livello di consapevolezza della sicurezza. Una separazione molto rigorosa è fatta tra le aree dei compiti e le aree dei clienti, in modo che ogni dipendente possa accedere ai documenti in cui si sta sviluppando un prodotto. Si può accedere a qualsiasi metodologia, qualsiasi informazione sul prodotto o qualsiasi tecnologia. Ma solo i pochi impiegati che sono coinvolti con un cliente possono accedere alle informazioni del cliente. Il principio del need-to-know viene applicato e c'è un accesso estremamente limitato a tutto ciò che è dato dal cliente.

Rischi: Attualmente, l'azienda è esposta principalmente ai rischi operativi e COVID-19.

o Rischio operativo. Dopo che un cliente entra in una cooperazione, viene fatta una valutazione iniziale della situazione, le possibilità di miglioramento vengono elaborate e migliorate nel dialogo con il cliente. Il rischio è che l'informazione del cliente sia gestita in modo negligente o non attento, e che i dati vengano persi o

venduti dai dipendenti. Se questo accade, questo attira una causa legale e l'azienda affronta una grave perdita di reputazione.

o Rischio finanziario. Non sono stati segnalati rischi specifici.

o Rischio di mercato. Non sono stati segnalati rischi specifici.

o Rischio informatico. Non sono stati segnalati rischi specifici.

o Il rischio legato a COVID-19. Soprattutto durante una pandemia, il problema che i concetti di sicurezza devono essere dotati di risorse sufficienti, sia finanziarie che umane, e che la gestione e anche la gestione IT devono prendersi il tempo necessario, è in aumento. La sfida più grande è quella delle risorse e della consapevolezza.

Benefici del risk management: Il principio della need-to-know dà il controllo e la standardizzazione della comunicazione. I dati al cliente passano solo attraverso persone selezionate per il cliente. Tutti i tecnici coinvolti presso quel cliente, sono consultati di nuovo prima di inviare qualsiasi cosa. Per quanto riguarda la gestione del rischio, vengono utilizzate diverse cose per proteggere i dati e i dati dei clienti. Classificazione, soluzioni multiple di crittografia, autenticazione multipla a più fattori, diversi sistemi di protezione delle e-mail, certificati delle e-mail, sistemi di backup e posizioni multiple dei sistemi di backup e dei dati.