compuTech

CASE STUDY | BALDAJA

Absolute Sicherheit. Schon ab der Buchung.

baldaja

Reise und Tourismus

Die Einhaltung des Datenschutz und der sensible Umgang mit personenbezogenen Daten ist heute nicht nur erst nach Einführung der DSGVO von hoher Relevanz. Gerade für Unternehmen und Kunden aus der Reisebranche bedeuten zusätzliche Richtlinien mehr Sicherheit der Daten, insbesondere bei der Erfassung von Kreditkarteninformationen.

So auch im Fall von unserem Kunden baldaja - ein Reisepartner für Geschäftsreisen und strategisches Travel Management. baldaja leistet mit der Umsetzung aktueller **PCI-DSS** Richtlinien einen wertvollen Beitrag zu mehr Sicherheit und Vertrauen im Umgang mit sensiblen Kreditkarteninformationen bei der Buchung. Wir begleiteten baldaja bei der Implementierung der PCI-DSS Richtlinien im Bereich der IT Infrastruktur, Netzwerk- und Systemadministration.

Was bedeutet PCI-DSS?

Die Abkürzung bedeutet Payment Card Industry Security Standard und beschreibt einen Industriestandard mit Best Practices zum Schutz von Kreditkartendaten bei Unternehmen und Kunden. Der industrielle Standard wurde 2005 von den großen Kreditkartenorganisationen (u.a. Visa, MasterCard und American Express) etabliert und wird seitdem fortlaufend vom PCI Security Standards Council weiterentwickelt.

Die Herausforderung

Die Erfassung von Kreditkartendaten unter Einhaltung der PCI-DSS Richtlinien, stellt Reiseunternehmen zunächst vor die Herausforderung die interne Datenverarbeitung, sowie die IT Sicherheit neu zu überdenken und gegebenenfalls umzustrukturieren. Im Rahmen der **PCI-DSS Compliance**, unter Berücksichtigung der SAQ Kategorie (SAQ: Self Assessment Questionnaire), ergeben sich dabei spezifische Anforderungen an die IT Infrastruktur.

baldaja
Official partner of BCD travel

baldaja / Expert Travel GmbH
www.baldaja.de

Zum Beispiel dürfen Kreditkartendaten nicht mehr elektronisch gespeichert, empfangen oder versendet werden. Zudem darf die Zahlungsabwicklung ausschließlich über ein isoliertes, virtuelles Terminal stattfinden, welches zwar nicht mit anderen Systemen des Firmennetzwerks verbunden ist, allerdings Zugang zu den branchenspezifischen Software-Produkten Amadeus und Midoco erlaubt.

CDE
Kreditkartenumgebung

Diese isolierte Umgebung wird als CDE, der Cardholder Data Environment bezeichnet.

Die Lösung

Um die genannten Anforderungen zu erfüllen, mussten eine Reihe an Maßnahmen bezüglich Netzwerk, Konfiguration, sowie Zugriffs- und Benutzerverwaltung vorgenommen werden. Eine umfassende IT Analyse der IT Struktur, sowie des zuvor etablierten Anforderungskatalogs, erlaubten uns dabei die Ausarbeitung eines strategischen Konzepts zur effizienten Umsetzung der Maßnahmen. Ganz ohne Neuanschaffung zusätzlicher Hardware oder Systemkomponenten.

Microsoft Hyper-V
Servervirtualisierung

Grundsätzlich setzten wir bei baldaja bereits schon vor der Einführung der PCI-DSS Richtlinie auf einen hochperformanten physikalischen Server mit mehreren virtuellen Serverinstanzen unter Verwendung der Servervirtualisierungs-Technologie Microsoft Hyper-V. Die virtuellen Server sind unter anderem für die Benutzerverwaltung zuständig, fungieren als Anwendungs- und Terminalserver und stellen virtuelle PC Systeme für die CDE zur Verfügung.

RDP
Remote Verbindung

Die mehr als 30 Arbeitsplätze sind dabei vorwiegend mit kosteneffizienten Thin Clients ausgestattet, sodass Mitarbeiter unkompliziert per Remote Desktop Protocol (RDP) auf den Terminalserver, sowie die virtuellen PCs zugreifen und somit ohne klassische PC Hardware arbeiten können. Der externe Zugriff auf die normale Office Umgebung wird über eine sichere VPN Verbindung mit IPSec Verschlüsselung ermöglicht, sodass Mitarbeiter auch mobil und standortunabhängig auf den Terminalserver zugreifen können.

Um die PCI-DSS Compliance vollständig zu erfüllen, segmentierten wir zunächst die Netzwerke und Systeme in zwei unabhängige Bereiche, sodass keine Kommunikation zwischen der regulären Netzwerkumgebung für die Bürokommunikation und der CDE möglich ist. Anschließend wurden weitere Anpassungen und Konfigurationen der Hyper-V Netzwerkumgebung vorgenommen und mehrere Firewall Regeln implementiert, die alle unautorisierten Verbindungen blockieren.

Doch neben Anpassungen der Server und Netzwerkstruktur, musste auch der E-Mail Verkehr an die PCI-DSS Richtlinien angepasst werden. Auch hier etablierten wir unternehmensweite E-Mail Regeln und passten die Office 365 Pakete an, um E-Mails mit Kreditkartendaten serverseitig zu blockieren. Schließlich dürfen nach PCI-DSS, Kreditkartendaten nicht mehr elektronisch übermittelt werden.

Neben den primären Anforderungen, erfordert die PCI-DSS Compliance zudem ein langfristiges, zeitnahes Patch-Management der Systeme, um diese geeignet gegen externe Bedrohungen zu schützen. Durch unseren Einsatz von Managed Services und Managed Antivirus erfüllen wir nicht nur das Patch-Management, sondern können durch 24/7 Monitoring proaktiv auf Auffälligkeiten und Schwachstellen reagieren.

Michael Holdkamp, Geschäftsführer

“Als Unternehmen für Geschäftsreisen und Travel Management suchen wir immer wieder neue Wege und Lösungen unsere Kunden mit maßgeschneiderten, modernen Prozessen zu begeistern. Dabei sehen wir uns häufig mit neuen, technischen, wie auch sicherheitsrelevanten Herausforderungen konfrontiert, sodass ein zuverlässiger IT-Partner essentiell ist. Mit der Firma compuTech haben wir diesen Partner nun schon seit vielen Jahren gefunden. compuTech unterstützt und betreut dabei nicht nur unser Day-to-Day Business im Bereich der IT, sondern bietet ganzheitliche und zeitgemäße Lösungen, die auch die wachsenden Anforderungen im Datenschutz und der Datensicherheit berücksichtigen.”

Zusammenfassung und Ergebnis

Die Erfüllung der PCI-DSS Richtlinien bedeutet für Reiseunternehmen und deren Kunden mehr Vertrauen und mehr Sicherheit. Diese Sicherheit beginnt heutzutage mit einer langfristig gedachten und flexiblen IT Infrastruktur, die sich dynamisch an die wachsenden Anforderungen an Datensicherheit und Datenschutz anpassen sollte.

Wir begleiteten baldaja bei der Umsetzung der neuen PCI-DSS Richtlinien und konnten die CDE durch infrastrukturelle IT Maßnahmen erfolgreich implementieren. Durch den fortschreitenden Einsatz von Servervirtualisierungen, erfolgte die Anpassung frei von neuer Hardware und ermöglichte auch den Mitarbeitern einen nahtlosen Übergang zu mehr Datensicherheit im Geschäftsalltag, ohne an Produktivität einbüßen zu müssen.

Auch heute betreuen und schützen wir die Systeme von baldaja und freuen uns einen kleinen Beitrag zu mehr Datensicherheit im Reiseverkehr geleistet zu haben.

HYPER-V SERVER VIRTUALISIERUNG

ANPASSUNG VON OFFICE 365 RICHTLINIEN

TERMINALSERVER MIT RDP ZUGRIFF

NETZWERKSEGMENTIERUNG

24/7 MANAGED SERVICES

256 BIT VERSCHLÜSSELUNG

compuTech GmbH
Heiderhöfen 23a
46049 Oberhausen
Deutschland

+49 (0) 208 84 83 910
www.computech-oberhausen.de

compuTech