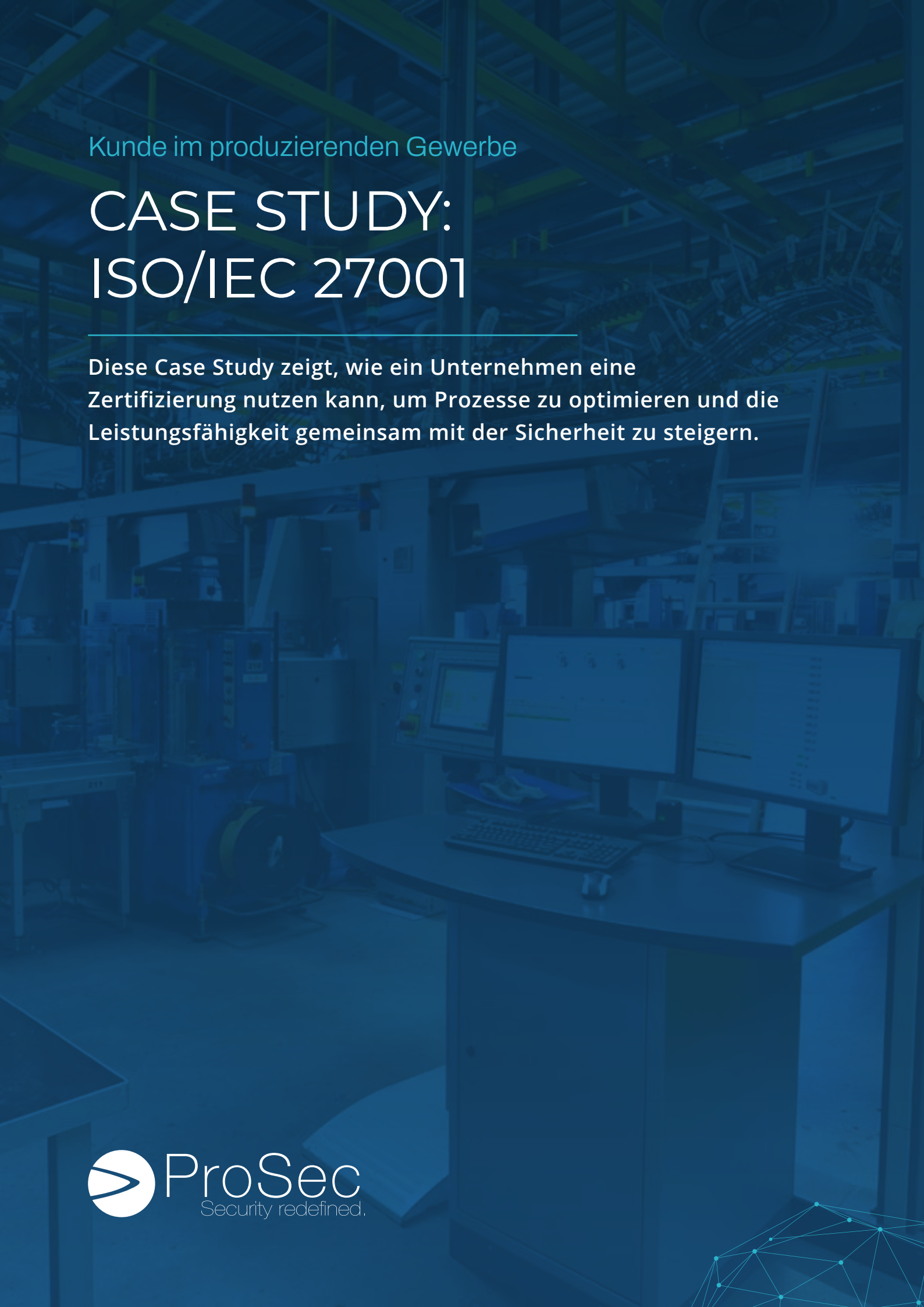

Kunde im produzierenden Gewerbe

CASE STUDY: ISO/IEC 27001

Diese Case Study zeigt, wie ein Unternehmen eine Zertifizierung nutzen kann, um Prozesse zu optimieren und die Leistungsfähigkeit gemeinsam mit der Sicherheit zu steigern.

ProSec
Security redefined.

Inhaltsverzeichnis

Case Study

ISO/IEC 27001 in einem Fertigungsunternehmen

ISO/IEC 27001 erfolgreich implementieren:

Eine Fallstudie mit Best Practices

Die ISO/IEC 27001 Zertifizierung bietet Unternehmen einen strukturierten Ansatz, um ihre Informationssicherheit zu verbessern und zu zertifizieren.

Unternehmensprofil

Branche: Produzierendes Gewerbe

Größe: 1.800 Mitarbeiter

Umsatz: 550 Mio. € Umsatz

Diese Fallstudie beleuchtet den erfolgreichen Weg eines Kunden aus dem produzierenden Gewerbe, der durch die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO/IEC 27001 nicht nur die Sicherheit seiner Daten, sondern auch die seiner Produktionsprozesse erheblich verbessert hat.

FRAGEN & HERAUSFORDERUNGEN

Risikomanagement in der IT und OT

Operational Security (OT)

Die Integration von Sicherheitskonzepten für die Operational Technology (OT) in bestehende IT-Sicherheitskonzepte stellte eine besondere Herausforderung dar. Die OT-Systeme des Unternehmens, darunter viele Maschinen mit langer Lebensdauer, nutzten veraltete Betriebssysteme wie Windows XP.

Veraltete Betriebssysteme

Zudem mussten Sicherheitsmaßnahmen so implementiert werden, dass sie den laufenden Betrieb nicht beeinträchtigten.

Physische Sicherheitsmaßnahmen

Weitere Herausforderungen umfassten die Integration von physischen Sicherheitsmaßnahmen mit den Arbeitsrealitäten, wie Arbeitshandschuhe vs. Fingerprint-Authentifizierung, die Entwicklung von minimalinvasiven Sicherheitslösungen, die laufende Prozesse nicht stören, und die Erstellung von Notfallplänen, die die speziellen Anforderungen der OT berücksichtigen.

Notfallpläne

Prozessbewertung

Zusätzlich war es notwendig, Geschäftsprozesse zu erfassen und zu bewerten, um Modernisierungsbedarf und sichere Workarounds zu identifizieren, sowie ein effizientes Management von personellen und monetären Ressourcen zur Umsetzung der Sicherheitsprozesse sicherzustellen.

Ressourcenmanagement

UNSERE LÖSUNGEN

Starke Sicherheitsstrukturen: Der integrierte Bottom-Up Ansatz

Unser Consulting-Team unterstützte den Kunden mit einem umfassenden Ansatz, der sowohl technische, personelle als auch organisatorische Kontrollen umfasste. Dieser Bottom-Up Ansatz stellte sicher, dass die Sicherheitsmaßnahmen auf realen Schwachstellen basierten, die durch detaillierte Analysen und praxisnahe Überprüfungen identifiziert wurden, bevor Maßnahmen ergriffen wurden.

1. Technische Kontrollen

Auf technischer Seite begann unser Ansatz mit gründlichen Analysen und Überprüfungen, um die tatsächlichen Probleme in der IT- und OT-Umgebung des Kunden zu identifizieren. Vorhandene Firewalls wurden für die spezifischen Anforderungen der OT optimiert, eine starke Passwort-Policy implementiert und die Netztrennung für die Verwaltung eingeführt. Standardisierte Pläne für regelmäßige Patches und Updates wurden entwickelt, und Backups sowie Desaster-Recovery geplant. Monitoring-Lösungen und Alarmierungsmechanismen wurden installiert, um die Sicherheit des Unternehmens weiter zu erhöhen. Alle Maßnahmen basierten auf den konkreten Ergebnissen der initialen Analysen, um sicherzustellen, dass sie in der Realität greifen.

2. Personelle Kontrollen

Im Bereich der personellen Kontrollen lag der Fokus auf Schulungen zur Bedrohungserkennung und der Schaffung eines Sicherheitsbewusstseins bei den Mitarbeitern. Wir etablierten eine fehlertolerante Meldekultur, um kritische Stunden nach einem möglichen Fehler zu gewinnen, wenn Vorkommnisse eintreten sollten. Der Aufbau eines Incident Response Teams, das zentrale Maßnahmen zur Begegnung von Vorfällen übernimmt, stellte sicher, dass alle Ebenen des Unternehmens aktiv in die Sicherheitsmaßnahmen eingebunden wurden. Durch praxisnahe Schulungen basierend auf realen Bedrohungsszenarien wurden die Mitarbeiter befähigt, ihre Rolle in der Sicherheitskette effektiv wahrzunehmen.

3. Organisatorische Kontrollen

Organisatorisch wurde ein maßgeschneiderter ISMS-Plan entwickelt, basierend auf einer gründlichen Analyse der bestehenden Sicherheitsmaßnahmen und der Identifikation von Schwachstellen. Die Geschäftsführung wurde sensibilisiert und aktiv in den Entscheidungsprozess eingebunden. Risikoanalysen und ein Risikobehandlungsplan wurden erstellt, um auf die spezifischen Bedrohungen und Bedürfnisse des Unternehmens einzugehen. Verschiedene Richtlinien, wie Dokumentenlenkungsplan und Passwortrichtlinie, wurden formuliert, um die Sicherheitsstandards zu gewährleisten. Dieser Prozess stellte sicher, dass alle organisatorischen Maßnahmen auf realen, identifizierten Risiken basierten.

4. Physische Kontrollen

Physische Kontrollen wurden überarbeitet, um Zugangskontrollsysteme zu optimieren und eine Harmonisierung von Werkschutz und Informationssicherheit zu erreichen. Ein Prozess zur Überwachung des Besucher-Lifecycles wurde etabliert, der die Anmeldung, Bewegung und Abmeldung von Besuchern im Unternehmen kontrolliert. Die Überarbeitung der Zugangskontrollsysteme basierte auf einer Analyse der tatsächlichen physischen Sicherheitsbedrohungen, die durch praxisnahe Überprüfungen identifiziert wurden.

5. Integration und kontinuierliche Verbesserung

Ein integraler Bestandteil des Bottom-Up Ansatzes ist die kontinuierliche Verbesserung und Anpassung der Sicherheitsmaßnahmen an die sich verändernden Anforderungen und Bedrohungslagen. Durch regelmäßige Analysen und praxisnahe Überprüfungen, die Praxisnähe sicherstellen, werden die Sicherheitsstrategien kontinuierlich angepasst und verbessert. Die Installation einer Stabsstelle direkt unterhalb der Geschäftsführung verdeutlicht die strategische Bedeutung, die diesem Ansatz beigemessen wird, und stellt sicher, dass die Sicherheitsmaßnahmen stets auf realen, aktuellen Bedrohungen basieren.

DAS ERGEBNIS

Ganzheitliche Optimierung

Durch die umfassende Implementierung dieser Maßnahmen konnte das Unternehmen seine Sicherheit sowohl in der Verwaltung als auch in den Produktionswerken erheblich verbessern. Die Informationssicherheit wurde ganzheitlich optimiert, was potenzielle Angreifer vor größere Herausforderungen stellt. Die erzielten Vorteile umfassen eine höhere Sicherheit und Zuverlässigkeit der Produktionsprozesse, eine Stärkung des Sicherheitsbewusstseins aller Mitarbeiter, die Optimierung der Geschäftsprozesse durch Identifikation und Umsetzung von Verbesserungsmöglichkeiten sowie die Vorbereitung auf eine zukünftige Zertifizierung, die dank der ergriffenen Maßnahmen zur Formsache wird.

Fazit

Die erfolgreiche Implementierung der ISO/IEC 27001 ist ein kontinuierlicher Prozess, der sowohl technisches als auch organisatorisches Engagement erfordert. Die Fallstudie zeigt, dass durch eine systematische Herangehensweise und die enge Zusammenarbeit mit erfahrenen Beratern selbst komplexe Herausforderungen gemeistert werden können.

Für Unternehmen, die ähnliche Ziele verfolgen, empfiehlt sich eine gründliche Bestandsaufnahme und Bewertung des Ist-Zustands, die Identifikation und Einbindung von Schlüsselpersonen im Unternehmen, die Priorisierung der wichtigsten Geschäftsprozesse, eine sorgfältige Ressourcenplanung und die harmonische Implementierung der Änderungen.

Ihr Kontakt zu uns

Bereit, Ihre Informationssicherheit auf das nächste Level zu heben? Kontaktieren Sie uns und erfahren Sie, wie wir Ihr Unternehmen auf die ISO/IEC 27001 Zertifizierung vorbereiten können.

Kontaktieren Sie uns für eine persönliche und kostenfreie Beratung!

Weitere Informationen zur Zertifizierung und unserem Service finden Sie auf unserer Website:
https://www.prosec-networks.com/it-security-consulting/iso27001-zertifizierung/

Per Telefon & E-Mail
+49 (0) 261 450 930 90
info@prosec-networks.com

ProSec GmbH
Campus Mendig (Nähe Koblenz):
Karl-Schiller-Straße 9–17,
56743 Mendig

ProSec
Security redefined.

WHO WE ARE

2016
gegründet

50+
Team-Mitglieder

1000+
durchgeführte Assessments

100%
Systemübernahmen

UNSERE MISSION

Menschenleben retten und schützen, indem wir die digitale Infrastruktur von Unternehmen nachhaltig sicher machen.

UNSERE VISION

Wir wollen IT Security viral gehen lassen.

HOW WE SUPPORT YOUR INFORMATION SECURITY

Penetration Testing IT Security Consulting Ethical Hacker Courses

„IT Security aus der Eifel
für Kunden weltweit."