In 3 Schritten zur ISO/IEC 27001 Zertifizierung auf der Basis von IT-Grundschutz bei der Versatel GmbH

Risikomanagement beim Einsatz von MPLS

Kunde
Versatel GmbH

Branche
Telekommunikation

Aufgabe
ISO/IEC 27001 Zertifizierungsbegleitung auf der Basis von IT-Grundschutz für den Einsatz von MPLS

Umsetzung
- Review
- Analyse
- Audit

Ergebnis
- Kosteneffizientes Risikomanagement
- Praxiserprobtes Management von potenziell möglichen und tatsächlichen Risiken
- Umfassende Sicherheitsmaßnahmen unter Einhaltung von unternehmensinternen und branchenspezifischen Gesetzen, Normen und Richtlinien
- Vollständige Identifikation und Definition von Prozessen der Informationssicherheit
- Konkrete Formulierung von Anforderungen und Zielsetzungen der Informationssicherheit
- Schnelle Anwendbarkeit der Handlungsanweisungen auf unterschiedliche Fälle

Das Telekommunikationsunternehmen Versatel ist ein deutschlandweit führender Anbieter von Daten-, Internet- und Sprachdiensten. Dabei zeichnet sich das Düsseldorfer Unternehmen durch umfassende und individuelle Kommunikationslösungen auf Basis einer leistungsstarken Infrastruktur und einem hochmodernen, flächendeckenden Glasfasernetz aus – dem zweitgrößten in Deutschland. Ein besonderer Fokus des Unternehmens liegt auf dem B2B-Markt, in dem vor allem das Geschäftsfeld Unternehmensvernetzung über Virtual Private Networks (VPN) einen wichtigen Stellenwert einnimmt.

Gerade im Unternehmensbereich spielt die Wirtschaftlichkeit von Vernetzungslösungen eine große Rolle. Dafür greift Versatel auf die Vermittlungstechnologie Multiprotocol Label Switching (MPLS) zurück. Hierüber werden VPN-Dienste für Sprache, Daten und Multimedia zur Erfüllung von Kundenanforderungen bezüglich des sicheren Informationsaustauschs bereitgestellt. Unternehmen mit mehreren Standorten sind damit in der Lage, auch räumlich entfernt liegende Standorte über ein virtuelles privates Netz (VPN) miteinander zu verbinden. Durch diese Variante der Datenübertragung können Datenpakete über mehrere Kundennetze viel schneller verarbeitet werden. Sie bietet aber auch viele Angriffsflächen und damit ein großes Gefahrenpotenzial.

Hintergrund

Gerade in der Telekommunikationsbranche ist es wichtig, dass Verantwortliche auf Steuerungs- und Verwaltungsebene sowie auf der Ebene des Kundenverkehrs zu jedem Zeitpunkt die Informationssicherheit gewährleisten, um Gefährdungen und damit Haftungsrisiken zu vermeiden. So können einem Telekommunikationsunternehmen beispielsweise dann Schäden entstehen, wenn das Transportnetz etwa durch Versagen wichtiger Netzkomponenten ausfällt. Ebenso muss es sich und auch seine Kunden vor Angriffen z. B. aus dem Internet sowohl auf das unternehmenseigene Netzwerk als auch auf Kunden-VPNs schützen. Eine weitere mögliche Gefahr droht, wenn Daten an nicht vertrauenswürdige Systeme gesendet wer-

den. All diese Fälle führen schnell dazu, dass ein Telekommunikationsunternehmen eine Leistung nicht rechtzeitig bis gar nicht erbringen kann, somit Umsatzausfälle oder Schadensersatzklagen hinnehmen muss und im schlimmsten Fall vielleicht sogar einen Imageschaden erleidet.

Motivation

Um die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit bei der Übertragung von Datenpaketen mittels MPLS zu gewährleisten, setzt Versatel auf maximale Sicherheit und höchste Qualität. Deshalb entschied sich das Unternehmen für die ISO/IEC 27001 Zertifizierung auf der Basis von IT-Grundschutz gemäß BSI (Bundesamt für Sicherheit und Informationstechnik), um unterschiedlichen möglichen Bedrohungen vorzubeugen oder gegebenenfalls frühzeitig darauf reagieren zu können. Für die Unterstützung der Zertifizierungsbegleitung beauftragte Versatel den Lösungsanbieter exceet Secure Solutions als erfahrenen Spezialisten für Machine-to-Machine (M2M) und IT Security mit besonderer Expertise im Bereich Industrie.

Ziele

Die ISO/IEC 27001 Zertifizierung auf Basis der IT-Sicherheit stellt ein bedeutendes und allgemein anerkanntes Hilfsmittel zur Sicherheitsanalyse sowie Identifizierung und Bewertung von Risiken dar. Ziel war es vorrangig, Risiken und Gefahrenpotenziale zu identifizieren, zu definieren sowie Handlungsanweisungen zu erarbeiten, mit denen man möglichen Risiken vorbeugen oder frühzeitig auf sie reagieren kann und damit einhergehend die Wahrscheinlichkeit von Schadensfällen zu senken. Dabei lag der Fokus der Zertifizierung auf „uniCore“, einer deutschlandweiten, nicht öffentlichen Netzwerkinfrastruktur der Versatel GmbH auf Basis des MPLS.

Umsetzung

Jede Branche und jedes Unternehmen hat jeweils eigene Gesetze, Normen und Richtlinien zu erfüllen und muss daher spezifischen Anforderungen gerecht werden. Diese gilt es bei der Analyse und Bewertung von Risiken zu kennen, zu beachten und darauf aufbauend eine individuelle ISO/IEC 27001 Zertifizierung durchzuführen.

Die Security Consultants von exceet Secure Solutions unterstützten Versatel zum einen bei einem Know-how-Transfer zur BSI-Grundschutz-Methodik und den Standards (BSI 100-1 bis 100-4). Zum anderen begleiteten sie das ISO/IEC 27001 Zertifizierungsprojekt. Dabei ging exceet Secure Solutions in drei Schritten vor:

Schritt 1: Review

- Festlegung des Geltungsbereichs
- Ermittlung von Rahmenbedingungen
- Erstellung der erforderlichen Konzepte und Richtlinien

Im ersten Schritt legte das Projektteam den Geltungsbereich fest. Der Untersuchungsgegenstand umfasste den Verbund der MPLS-Core-Router mit realisierter Netzbetreibergrenze (Provider Edge), sowie die für deren Betrieb notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten und Prozesse an unterschiedlichen Standorten.

Eine solche Abgrenzung ist wichtig, um im Haftungsfall die Verantwortung und Zuständigkeiten der an den sicherheitskritischen Geschäftsprozessen beteiligten Akteure eindeutig nachvollziehen zu können. Hierauf wurde der Basis-Sicherheitscheck angewendet und die erforderlichen Konzepte und Richtlinien erstellt.

Schritt 2: Analyse

- Bewertung der Sicherheitsmaßnahmen
- Evaluierung der Informationsrisiken
- Erstellung des Risikohandlungsplans

Darauf aufbauend erfolgten die Erstellung der ergänzenden Sicherheitsanalyse, Risikoanalyse und die Unterstützung bei der Erstellung des Risikobehandlungsplans. Die Notwendigkeit dieses Schrittes lag in der Budgetierung von Maßnahmen. Dafür wurde eine Wahrscheinlichkeit errechnet, nach der ein bestimmtes Sicherheitsereignis und damit auch ein Verlust eintreten können. Darauf auf-

bauend wurden mögliche Risiken definiert und Maßnahmen zur Vermeidung solcher Sicherheitsereignisse erarbeitet sowie Notfallpläne erstellt.

Die Herausforderung dieser Analyse bestand darin, die Budgetierung von Maßnahmen auf Basis von Schätzungen und Annahmen anstelle einer vollständig messbaren Realität vorzunehmen. Die Hinzuziehung von Security Consultants der exceet Secure Solutions war für Versatel daher besonders wichtig, da sie das Know-how des Unternehmens zu möglichen und tatsächlichen Haftungsfällen mit umfassendem Know-how aus der Branche sowie langjährigen Erfahrungen optimal ergänzen konnten.

Schritt 3: Audit

- Durchführung der formalen ISO/IEC 27001 Zertifizierung durch unabhängige Gutachter
- Überprüfung der Sicherheit und Vollständigkeit aller implementierten Maßnahmen

Abgeschlossen wurde das Projekt mit der Zertifizierungsbegleitung im Audit. An dieser Stelle könnte man den Prozess eigentlich als abgeschlossen betrachten. Tatsächlich schloss sich hier jedoch die formale ISO/IEC 27001 Zertifizierung an. Sie erfolgte in Form eines Audits, die von speziell akkreditierten Gutachtern durchgeführt wurde.

Dieses Audit erfüllte eine wesentliche Funktion: bei diesem formalen Prozess wurde das Projektergebnis durch eine unabhängige Stelle nochmals bestätigt und Angemesseneheit sowie Vollständigkeit aller Maßnahmen überprüft.

Ergebnisse

Mit der ISO/IEC 27001 Zertifizierung auf der Basis von IT-Grundschutz (Informationssicherheit) kann Versatel ihr systematisches Vorgehen zur Absicherung ihrer IT-Systeme gegen Gefährdungen der IT-Sicherheit mithilfe des ISO/IEC 27001-Zertifikats auf der Basis von IT-Grundschutz nachweisen. Hierfür wurden Kataloge entwickelt, die sämtliche erforderliche Gefährdungen und Maßnahmen für die Netzwerkinfrastruktur auf Basis der MPLS-Vermittlungstechnologie umfassen.

Der Schwerpunkt lag hierbei auf der Erarbeitung von sehr konkreten Handlungsanweisungen auf personeller, organisatorischer, technischer und infrastruktureller Ebene zur Vermeidung von Haftungsrisiken. Diese zeichnen sich vor allem dadurch aus, dass sie kostengünstig, praxiserprobt, umfassend, konsequent, vollständig und doch auf viele Anwendungsfälle schnell anwendbar sind.

exceet Secure Solutions wiederum konnte mit der Beteiligung am Zertifizierungsprojekt bei Versatel zeigen, dass sie ihre Kompetenzen neben etablierten Geschäftsfeldern – dem Gesundheits- und M2M-Segment – auch im Telekommunikationsbereich erfolgreich anwenden kann.

Vorteile im Überblick

- Kosteneffizientes Risikomanagement
- Praxiserprobtes Management von potenziell möglichen und tatsächlichen Risiken
- Umfassende Sicherheitsmaßnahmen unter Einhaltung von unternehmensinternen und branchenspezifischen Gesetzen, Normen und Richtlinien
- Vollständige Identifikation und Definition von Prozessen der Informationssicherheit
- Konkrete Formulierung von Anforderungen und Zielsetzungen der Informationssicherheit
- Schnelle Anwendbarkeit der Handlungsanweisungen auf unterschiedliche Fälle

exceet Secure Solutions GmbH
Phone +49 211 436989 0
Email info@exceet-secure-solutions.de
Web www.exceet-secure-solutions.de