versatel

exceet SECURE SOLUTIONS

3 Steps to BSI-Compliant ISO/IEC 27001 Certification at Versatel GmbH

Risk Management for MPLS Protection

Client
Versatel GmbH

Sector
Telecommunications

Contracted for
ISO/IEC 27001 certification support based on IT Basic Protection for MPLS deployment

Implementation

- Review
- Analysis
- Audit

Result

- Cost-efficient risk management
- Proven management of potential and actual risks
- Comprehensive security measures in compliance with company and sector-specific regulations, norms and guidelines
- Complete identification and definition of information security processes
- Concrete formulation of information security requirements and targets
- Rapid application of procedural instructions to a wide range of cases

The telecommunications enterprise Versatel, headquartered in Düsseldorf, is a leading German provider of data, internet and language services. The company offers comprehensive, customized communication services via a high-performing infrastructure and an extensive, state-of-the-art fiber-optic network – the 2nd largest in Germany. Versatel devotes special attention to the B2B market, with a major focus on virtual private networks (VPNs) for its Corporate Connectivity business segment.

The economy of connectivity solutions plays a major role for businesses. Versatel relies on the Multiprotocol Label Switching (MPLS) technology to provide VPN-based language, data and multimedia services and satisfy customer requirements for secure exchanges of information. MPLS lets enterprises link geographically remote branch offices via a virtual private network (VPN). This method of data transmission enables very rapid processing of data packages across a range of customer networks. However, VPNs are highly susceptible to attack and thus represent considerable hazard potential.

Background

Particularly in the telecommunications industry, it's crucial for management at the control, administration and customer relations levels to safeguard information security at all times and thus avoid hazards and possible liability risks. For example, a telecoms enterprise can be harmed by the failure of the transport network due to a breakdown of important network components. Equally, it has to protect itself and its customers against (Internet) attacks on the enterprise network and client VPNs. Threats also loom when data is sent to untrustworthy systems. Such cases can quickly render a telecoms enterprise unable to provide its services, or unable to provide them on time. This in turn can entail severe earnings losses, may expose the enterprise to claims for damages and could, in a worst-case scenario, cause lasting damage to its reputation.

Motivation

Versatel pursues maximum security and quality standards to continually protect its business assets – availability, integrity and confidentiality – when transferring data via MPLS. For this reason, the company decided to pursue ISO/IEC 27001 certification based on Baseline IT Protection as defined by the BSI (German Federal Office for Security in Information Technology). This shields Versatel against potential threats and provides rapid response capabilities in the event of a breach. For support services during the certification process, Versatel turned to solutions provider exceet Secure Solutions, an experienced specialist for machine-to-machine (M2M) and IT security with special expertise in the industry field.

Targets

ISO/IEC 27001 certification based on the BSI IT security standard represents a range of meaningful and widely acknowledged resources for security analysis and risk assessment. The prime objective was to identify and define potential risks and hazards and develop guidelines for action that would ensure cross-board protection, enable effective responses and reduce the likelihood of damaging events. Specifically, the certification focused on “uniCore”, a Germany-wide, non-public, MPLS-based network infrastructure maintained by Versatel GmbH.

Implementation

Every industry segment and every enterprise has to observe certain regulations, norms and guidelines and is thus obliged to comply with its own specific set of requirements. When analyzing and evaluating risks, a company must therefore be aware of these requirements and continually keep them in mind in the course of its individual ISO/IEC 27001 certification.

Security consultants from exceet Secure Solutions assisted Versatel by providing a transfer of knowhow on BSI Baseline Protection methodology and standards (BSI 100-1 to 100-4) and contributing support throughout the ISO/IEC 27001 certification project. To this end, exceet Secure Solutions adopted a three-step approach:

Step 1: Review

- ✓ Determining project scope
- ✓ Defining the framework conditions
- ✓ Developing the required concepts and guidelines

During the first step, the project team determined the scope of the project. The object of the investigation was the network of MPLS core routers (deployed at separate locations) with its defined provider edge, as well as the infrastructure-related, organizational, personnel and technical components and processes required to operate it.

In the event of a liability claim, a provider can rely on such boundary-setting to clearly identify the responsibilities and accountabilities of participants in the affected, security-critical business processes. The project team applied the Basic Protection security check to this delineated sphere and developed the required concepts and guidelines.

Step 2: Analysis

- ✓ Assessing security measures
- ✓ Evaluating information risks
- ✓ Developing a risk response plan

Building on Step 1, the team prepared a security analysis, a risk analysis and a risk response plan. This step, taken to facilitate future budgeting decisions, calculated the probability that particular security events will occur and estimated the attendant damage. Building upon this calculation, the team defined potential risks, developed measures aimed at preventing the respective events, and prepared emergency response plans.

The challenge of conducting the analysis was that it had to create a budget for measures based on estimates and assumptions rather than a measurable set of circumstances.

For Versatel, help from exceet Secure Solutions was particularly important here: Versatel has extensive enterprise know-how on potential and actual liability cases, while the security consultants were able to contribute deep industry expertise and long-term experience in the field.

Step 3: Audit

- ✓ Conducting the formal ISO/IEC 27001 certification (by independent experts)
- ✓ Reviewing the security and coverage of all implemented measures

To bring the project to completion, exceet Secure Solutions also provided assistance during certification auditing. One might have considered the process complete at this stage, but as it turned out the formal ISO/IEC 27001 certification followed immediately thereafter, by way of an audit conducted by specially accredited experts.

The audit fulfills a very important function: It is a formal process in which an independent authority validates the results of the project and confirms that the implemented measures were indeed appropriate and comprehensive.

Results

Having gained ISO/IEC 27001 certification in line with BSI Baseline IT Protection (information security), Versatel can demonstrate that it takes a systematic, formally approved approach to safeguarding its IT systems against security hazards. To this end it has developed catalogs that address all potential threats and define the countermeasures needed to protect its MPLS-based network infrastructure.

The project team focused on developing highly specific instructions for actions to prevent liability risks, at the personnel, organizational, technical and infrastructure level. The action plans are cost-efficient, comprehensive, consistent, complete and proven on the ground, and yet can be applied quickly to a wide range of use cases.

With its involvement in the Versatel certification project, exceet Secure Solutions was able to demonstrate that in addition to established business fields such as the health and M2M segments, its competencies can be successfully applied to the telecommunications sector as well.

Benefits: Overview

- ✓ Cost-efficient risk management
- ✓ Tried and proven management of potential and actual risks
- ✓ Comprehensive security measures in compliance with enterprise- and sector-specific regulations, norms and guidelines
- ✓ Comprehensive identification and definition of information security processes
- ✓ Concrete formulation of information security requirements and targets
- ✓ Rapid application of response plans to a wide range of use cases

Errors, modification and availability with respect to cited products, services, properties and uses reserved. exceet Secure Solutions assumes no warranty for the correctness of information provided by third parties with respect to properties, performance and availability. During the course of product development, exceet Secure Solutions reserves the right to alter products and services without prior notice. No statement or representation contained herein constitutes legal advice, nor may they be interpreted as such. In the event of deviation between this document and related contract documents or general terms and conditions of exceet Secure Solutions and its subsidiaries, the contract documents and/or general terms and conditions shall always take precedence over this document.