Informationssicherheit mit ISO/IEC 27001

Planung und Implementation einer Informationssicherheits-Strategie und ihre Integration in das Führungssystem des Unternehmens

Täglich erscheinen Berichte über Cyberangriffe auf Unternehmen jeglicher Grösse. Die Hard- und Software von IT-Systemen sowie die mit ihnen verarbeiteten Daten vor Diebstahl, Beschädigung und Missbrauch durch Dritte zu schützen, stellt Unternehmen vor grosse Herausforderungen.

Auch unternehmensinterne Risiken gilt es im Sinne der Informationssicherheit einzudämmen, beispielsweise nicht gepatchte Schwachstellen, schwache Konfigurationen oder die Verwendung veralteter Protokolle.

Wer nicht weiss, wie er seine unternehmenskritischen Daten richtig schützt, wird früher oder später das Nachsehen haben.

Verantwortungsvolle Entscheider zeichnen sich dadurch aus, dass sie ihr Informations-Sicherheits-Expertenteam aufstocken und der technischen Herangehensweise, beispielsweise dem Einsatz von Firewall, Applikations- und Netzwerksicherheit oberste Priorität einräumen.
Damit diese Massnahmen unternehmensweit erfolgreich sind, integrieren die Verantwortlichen die Informationssicherheit in ihr Führungssystem.

Baukasten eines Führungssystems für Informationssicherheit gemäss ISO/IEC 27001

Informationssicherheit-Experten und Unternehmensführer entscheiden sich für den Einsatz des breit akzeptierten und auf einem Standard basierten Führungssystems, mit dem die Informationssicherheit stets bewertet und der notwendige Handlungsbedarf festlegt wird. Es ermöglicht die Integration der Informationssicherheit in die Führungsstrategie eines Unternehmens und letztlich auch eine Zertifizierung nach dem internationalen Standard ISO/IEC 27001.

Diese Grundstruktur beinhaltet den Rahmen für den Aufbau der notwendigen Führungsinstrumente und die Festlegung der auf das Unternehmen angepassten Sicherheitsziele. Auch Unternehmen, die keine Zertifizierung anstreben, bietet dieser Standard die Anleitung zu Planung, Umsetzung, Betrieb, und Überwachung sowie zur kontinuierlichen Verbesserung der unternehmensweiten Sicherheitsmassnahmen.

Die Experten und erfahrenen Coaches der Glenfis AG begleiten und unterstützen Unternehmen auf dem Weg zu einem zertifizierbaren Führungssystem für die Informationssicherheit.

glenfis

Success Story Stadler Rail

Wie Stadler Rail AG und Glenfis AG sich gemeinsam auf eine erfolgreiche ISO/ IEC 27001 Zertifizierung vorbereiteten

Eine ISO/IEC 27001 Zertifizierung kann mitunter sehr komplex sein. Sie beinhaltet Anpassungen am bestehenden Führungssystem und umfasst mehr als 100 Massnahmen und Kontrollspezifikationen. Dabei ist ein formelles Change-Management erforderlich.

Andreas Bogk, CISO von Stadler, ist ISO/ IEC 27001 Auditor und führte mit Unterstützung von Glenfis AG erfolgreich eine Zertifizierung durch.

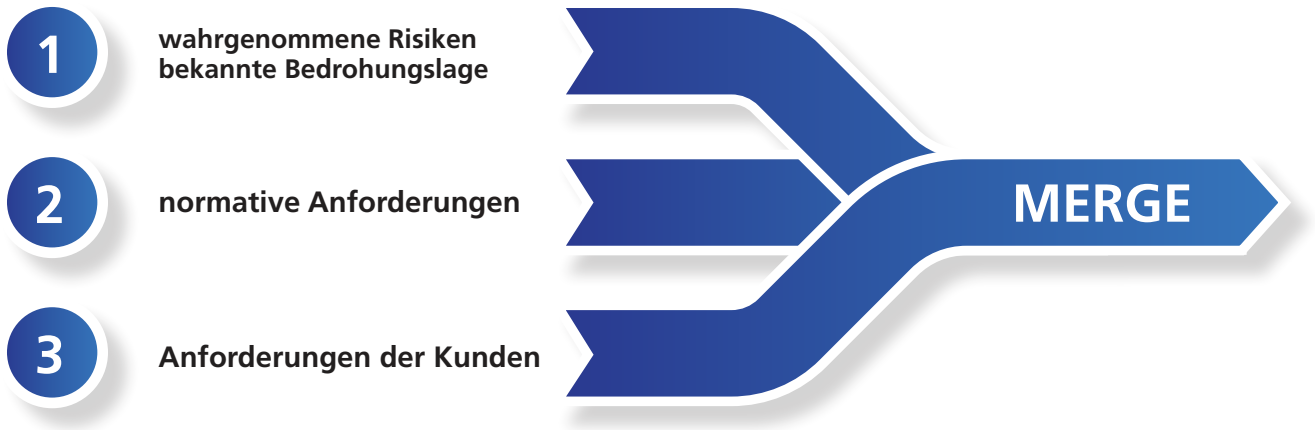
«Die ISO/IEC 27001 Zertifizierung bei Stadler umfasst alle strategischen Unternehmensbereiche, die gesamte Wertschöpfungskette unseres Unternehmens und mehrere Produktionsbetriebe», berichtet Bogk. «Die Überprüfung vorhandener Prozesse, Stakeholder Management und Mitarbeiter-Briefings gehören zu den wichtigsten Tätigkeiten».

Priorisierung und Ressourcen

«Die von uns ergriffenen Massnahmen basieren auf 3 Säulen: das sind erstens die wahrgenommenen Risiken sowie die bekannte Bedrohungslage, zweitens normative Anforderungen seitens der Schweizer Eisenbahnverordnung und drittens die Anforderungen der Kunden. Sie liegen der Entscheidung zur ISO/IEC 27001 zu Grunde».

«Um dieses Projekt zum Erfolg zu führen, ist der Freiraum, der dem ISO/IEC 27001 Zertifizierungs-Team durch die vom Vorstand eingeräumte Priorisierung gewährt wurde, von grosser Wichtigkeit», unterstreicht Bogk.

«Weitere wichtige Voraussetzungen für den Erfolg eines solchen Projekts sind ein klares Mandat seitens der Geschäftsleitung sowie die richtige Zusammensetzung des Projekt-Teams. Letzteres bestand aus IT-, HR- und Facility-Mitarbeitenden sowie Experten von Glenfis», ergänzt Bogk. Das Stadler ISO/IEC 27001-Team, bestehend aus 15 Mitarbeitenden, verfügte über theoretisches Wissen und baute



fehlendes Know-how auf. Die Erfahrung aus vielen ISO/IEC 27001 Zertifizierungsvorbereitungen brachte die Mitarbeit von Glenfis mit ins Zertifizierung-Team.
Die Symbiose aus internem theoretischem Wissen und externer Praxiserfahrung führte zum Erfolg.

Der Faktor «Mensch»
«Den Prozessverantwortlichen kam eine wichtige Rolle zu. Sie wurden von Beginn an aktiv eingebunden. Unser Fokus lag dabei auf dem Faktor Mensch», erläutert Bogk. «Als CISO sollte man wissen, wie und warum Menschen agieren und reagieren. Man muss ihren Bedarf analysieren und mittels technischer Systeme deren Verhalten kompensieren können», erklärt Bogk.

«Durch Interaktion verändern sich das Verhalten und das Bewusstsein der Akteure. Wichtig dabei ist die Sprache des Anderen zu verstehen. Zuhören und das Gespräch suchen sind manchmal wichtiger als das Wissen um die Theorie», erläutert Bogk.
In Einzelgesprächen mit den Prozessverantwortlichen wurden Vorgehensweisen, die Bedeutung der jeweiligen Arbeit und die Einhaltung von Zielen analysiert und überprüft. «Dieser Prozess endet nicht nach einer durchlaufenen Zertifizierung. Wir holen uns fortlaufend Feedback bei den Prozessverantwortlichen, um bei einer Re-Zertifizierung nicht wieder von vorne anzufangen», ergänzt Bogk.

Internationale Projekte in der Pandemie
«Die Beschränkungen der Pandemie haben dazu geführt, dass virtuelles Kommunizieren und Zusammenarbeiten zur Normalität geworden sind. In einem internationalen Unternehmen kann das dazu führen, dass man zusammenwächst», betont Bogk. «Ich gebe aber gerne zu, dass ich bei bestimmten Themen zur Erläuterung gerne vor Ort gestanden hätte», ergänzt er.

Vorbereitung ist alles!
«Am Ende des Tages geht es darum, dass alle Prozess- und die involvierten IT-Verantwortlichen darauf vorbereitet sind, dem Auditor Auskunft zu geben. Das gelingt nur, wenn man sich vorher genau fragt, warum man dieses Zertifizierungsprojekt vorantreiben will», sagt Bogk. «Bei einer ISO/IEC 27001 Zertifizierung ist es nicht damit getan, eine Checkliste abzuarbeiten. Es geht darum, wie man als Unternehmen mit Informationsrisiken umgeht».

«Im Vorfeld des Auditor-Besuchs haben wir alle Eventualitäten abgeklopft. Da den Prozessverantwortlichen eine Schlüsselrolle zukam, haben wir sie in der Vorbereitung darauf eng begleitet» begründet Bogk. «Jedes Auditthema wurde aufwändig aufbereitet. Das ging so weit, dass wir mit den Verantwortlichen Trockenübungen der Präsentationen der zu zertifizierenden Prozesse durchführten», unterstreicht er.

Zu guter Letzt
«Das alles hat nicht nur dazu geführt, dass das Wissen und Können der IT-Abteilung für eine grössere Gruppe von Mitarbeitenden sichtbarer wurde, sondern auch, dass die Prozessverantwortlichen und Entscheider die Expertise der IT heute öfter als vor der ISO/IEC 27001 Zertifizierung in Anspruch nehmen», fasst Bogk zusammen.

Quote von Daniel Heinzmann, Group CIO bei Stadler Rail AG
«Sicherheit ist Grundvoraussetzung für ein vertrauensvolles Verhältnis zu unseren Kunden und Geschäftspartnern. Informationssicherheit ist dabei das oberste Gebot. Um dies deutlich zu machen und transparent zu dokumentieren, haben wir die ISO/IEC 27001 umgesetzt. Die erfahrenen Experten von Glenfis haben uns bei der Vorbereitung auf die entsprechende Zertifizierung auf Basis effizienter Methoden kompetent und tatkräftig unterstützt.»

Zur Person
Andreas Bogk hat das IT-Handwerk von der Pike auf gelernt. Seine Bandbreite umfasst IT-Administration, Security-Architektur und Programmierung, forensische und Crypto-Expertise bis hin zu Governance, Risk and Compliance (GRC)-Wissen. Als CISO vermittelt er zwischen der IT-Welt mit der ihr eigenen Sprache und den Anwenderwünschen und Unternehmensnotwendigkeiten, die er ebenso versteht.

Über Stadler Rail AG

Stadler baut seit 80 Jahren Züge. Der Systemanbieter von Lösungen im Schienenfahrzeugbau hat seinen Hauptsitz im ostschweizerischen Bussnang. An mehreren Produktions- und Engineering-Standorten sowie über 60 Servicestandorten arbeiten rund 13.000 Mitarbeitende. Das Unternehmen ist sich seiner gesellschaftlichen Verantwortung für zukunftsfähige Mobilität bewusst und steht daher für innovative, nachhaltige und langlebige Qualitätsprodukte. Die Produktpalette im Bereich der Vollbahnen und des Stadtverkehrs umfasst Highspeed-Züge, Intercity-Züge, Regio- und S-Bahnen, U-Bahnen, Tram-Trains und Trams. Überdies stellt Stadler Streckenlokomotiven, Rangierlokomotiven und Reisezugwagen her. Stadler ist der weltweit führende Hersteller von Zahnradbahnfahrzeugen.

Über Glenfis
Glenfis ist ein Consulting-Unternehmen mit einer breiten und erfolgreichen Expertise in den Bereichen Organisationsentwicklung, Governance, Security und Service Management sowie ISO-Zertifizierungen. Basierend auf einer Vielzahl von erfolgreich durchgeführten Zertifizierungs-Prozessen trug die Expertise des Unternehmens massgeblich zur Verkürzung der Projektlaufzeit bei.

Glenfis AG
Service & Sourcing Excellence
Kennen. Können. Tun.

Badenerstrasse 623
8048 Zürich
+41 44 202 81 10
info@glenfis.ch
glenfis.ch