Telekom Austria wählt ISO 27001

- **In 6 Schritten von der Implementierung zum CIS-Zertifikat**
- **Interview mit dem Informationssicherheitsbeauftragten der Telekom Austria AG, Mag. Krzysztof Müller**

„Wir haben erkannt, dass Sicherheit für unsere Geschäftstätigkeit eine enorme Bedeutung hat und wir eine strukturierte Vorgangsweise für die komplexen Abläufe in der Informationssicherheit benötigen."

Als größter Serviceprovider Österreichs wurde die Telekom Austria AG nach der Norm für Informationssicherheit ISO/IEC 27001 zertifiziert. Die Zertifizierung umfasst den gesamten Bereich Service & Network Operation (SNO) mit 1.500 Mitarbeitern. SNO ist verantwortlich für weit über eine Millionen aon-Kunden, über 15.000 konzerninterne Benutzer und strategische IT-Dienstleistungen wie Housing oder Hosting.
Mag. Krzysztof Müller, Informationssicherheitsbeauftragter bei der Telekom Austria AG, hat die Zertifizierung operativ vorbereitet. Er schildert den Zertifizierungsprozess aus Sicht des Unternehmens und gibt Tipps aus der Praxis – für die Praxis.

Größter Serviceprovider Österreichs mit ISO-27001-Zertifizierung: Die Telekom Austria AG

Telekom Austria wählt ISO 27001

„Es war sinnvoller und kosteneffizienter, ein ISMS gleich für den gesamten SNO-Bereich mit 1.500 Mitarbeitern einzuführen. Sonst wäre es „doppelte" Arbeit gewesen."

Mag. Krzysztof Müller, Informationssicherheits-beauftragter der Telekom Austria AG

■ **Herr Mag. Müller, was waren die Motive für die Einführung eines Informations-SicherheitsManagementSystems, ISMS, nach ISO 27001?**

Wir haben erkannt, dass Sicherheit für unsere Geschäftstätigkeit eine enorme Bedeutung hat und wir eine strukturierte Vorgangsweise für die komplexen Abläufe in der Informationssicherheit benötigen. Auf der technischen Seite hatten wir sehr gute Security-Lösungen im Einsatz, aber die organisatorische Seite der Informationssicherheit sollte verbessert werden. So gab es zum Beispiel in jedem Bereich eine etwas andere Passwort-Politik oder auch andere Protokollierungsregeln. Letztere sind sehr wichtig für die **Nachvollziehbarkeit von Fehlern**, für die Fehlervermeidung und auch für Haftungsfragen. Die einheitliche Aufzeichnung von Sicherheitsereignissen in Form von Log-Files im Server-Bereich ist ein wesentlicher Sicherheitsfaktor bei der **Vermeidung von Datenmanipulation** oder unbefugten Zugriffen. Aber auch Fragen wie Zuständigkeiten oder das Informieren neu aufgenommener Mitarbeiter gehörten unter einer einheitlichen Struktur standardisiert.

Schritt 1: Informationsgespräch
Ein Erstgespräch mit der CIS liefert Details über den Zertifizierungsprozess.
Es folgen Registrierung und Projektplanung.

■ **Wie hat das Projekt begonnen?**

Der Projektstart begann mit ersten Gesprächen mit der Zertifizierungsstelle CIS. Dort wurde der Ablauf der Zertifizierung besprochen und der grobe Zeitplan fixiert. Unsere Fragen gingen vor allem in die Richtung, was geprüft wird und welche Norminhalte für unsere Anforderungen relevant sind.

■ **Hat das Erstgespräch auch bereits eine Richtungsweisung gegeben?**

Ja, denn wir hatten ursprünglich den Plan, nur einen kleinen Teil des SNO-Bereichs zu zertifizieren – sozusagen als Pilotprojekt. Aufgrund dieser Erfahrungen wollten wir später den gesamten SNO-Bereich nachziehen. Die CIS hat uns aber deutlich gemacht, dass es sinnvoller und kosteneffizienter wäre, ein ISMS gleich für den gesamten Bereich mit 1.500 Mitarbeitern einzuführen und zertifizieren zu lassen. Heute sehen wir uns in diesem Schritt bestätigt. Sonst wäre es „doppelte" Arbeit gewesen. Gleich nach diesem Erstgespräch haben wir, wenige Wochen vor dem Projektstart, ein Stage-Review in Anspruch genommen.

Schritt 2: Stage Review
Bei dieser freiwilligen Vorbeurteilung überprüft die CIS projektbegleitend die Zweckmäßigkeit der implementierten ISMS-Elemente und erstellt einen Stärken-Schwächen-Bericht.

■ **Was waren die Gründe für ein Stage-Review zu Projektbeginn und welchen Nutzen brachte dies konkret?**

Zuvor haben wir den Leitfaden zur Implementierung von Informationssicherheit, die ISO/IEC 27002, in Eigenregie durchgearbeitet und in eingeschränktem Ausmaß auch externe Beratung in Anspruch genommen. Dabei hat sich heraus kristallisiert, dass die Norm viel Interpretationsspielraum zulässt. So wird beispielsweise ein „angemessenes Risikomanagement" gefordert, aber nicht näher ausgeführt, was „angemessen" in der Praxis bedeutet – was ja auch von Unternehmen zu Unternehmen unterschiedlich sein kann, je nach den individuellen **Sicherheitsanforderungen**. Daher war uns eine Zustandsbestimmung von Seiten des Zertifizierers wichtig. Wenn die Auditoren, die später das ganze System begutachten, zu Projektbeginn eine **Kursbestätigung oder -korrektur** anzeigen, kann man später nicht so falsch liegen. Insgesamt ging es uns auch um die Präzisierung von Normforderungen, zugeschnitten auf den SNO-Bereich der Telekom Austria AG. Nach einem eintägigen Audit im Unternehmen erhielten wir einen sechsseitigen Bericht, der aufzeigte, in welchen Bereichen Handlungsbedarf bestand und wo wir uns bereits auf dem richtigen Weg befanden. So eine freiwillige Vorbegutachtung können wir empfehlen – als hilfreiche Wegbegleitung, weil die Umsetzung der Norm alles andere als Routine ist.

■ **Hat es aufgrund des Stage Reviews eine markante Kurskorrektur gegeben?**

Wir konnten unseren Zeitplan revidieren. Das Management wollte eine rasche Implementierung im Rahmen von elf bis zwölf Monaten, während die IS-Beauftragten eher mit 18 Monaten gerechnet hätten. Nach diesem Stage Review hatten wir aber einen relativ guten Überblick über die noch zu bewältigenden Aufgaben und konnten uns daraufhin das Ziel setzen, die Zertifizierung **schon nach elf Monaten** zu erreichen – was schließlich auch realisiert wurde.

„Nach einem Stage Review konnte der Zeitplan revidiert und die Zertifizierung schneller erreicht werden."

Schritt 3: Analyse
Evaluierung der Informationsrisiken und Bewertung vorhandener Sicherheitsmaßnahmen durch das Unternehmen. Die CIS als unabhängige Prüfstelle ist hier nicht involviert.

Wie wurde das Thema Risikomanagement in der Telekom Austria AG umgesetzt?

Risikomanagement ist ein abstraktes Thema, das eine neue Art des Denkens erfordert. Als Techniker kennt man „Ja" oder „Nein": entweder etwas funktioniert oder nicht. Bei Risiko handelt es sich um unklare Zustände: Man versucht eine Wahrscheinlichkeit zu errechnen, nach der ein bestimmtes Sicherheitsereignis und damit auch ein Verlust eintreffen kann. Aufgrund dieser Wahrscheinlichkeit werden Maßnahmen zur Vermeidung getroffen und **Notfallpläne** erarbeitet. Die Entscheidung, solche Maßnahmen zu budgetieren, fällt aufgrund von Schätzungen und Annahmen und nicht aufgrund einer vollkommen messbaren Realität. Daher hat der SNO-Bereich dieses komplexe Thema in enger Kooperation mit der Stabsstelle für Risikomanagement der Telekom Austria AG erarbeitet, wo fachliches Know-how dazu bereits vorhanden war. Es war eine große Herausforderung, die Risiken zu finden und zu definieren. Im technischen Bereich hat sich der **Change-Management-Prozess** als ein Hauptfokus heraus kristallisiert – denn bei jedem neuen System, das in Betrieb geht, können Fehler eingeschleust werden. Die meisten Risiken werden jedoch im Rahmen der Sicherheitsaudits entdeckt.

„Risikomanagement ist ein abstraktes Thema, das eine neue Art des Denkens erfordert. Als Techniker kennt man „Ja" oder „Nein". Bei Risiko handelt es sich hingegen um unklare Zustände, die zu bewerten sind."

Schritt 4: Implementierung
Einführung von Sicherheitsmaßnahmen nach dem strategischen Aufbau der Norm ISO 27001 / ISO 27002. Die CIS als unabhängige Prüfstelle ist hier nicht involviert.

Die Hauptarbeit lag in der Implementierungsphase – wie lief diese ab?

Die Implementierungsphase hat insgesamt elf Monate gedauert. Ein Projektteam hat 2000 Personentage daran gearbeitet und 1.500 Mitarbeiter wurden nach dem kostengünstigen Train-the-Trainer-Prinzip über einige Monate geschult. Die Schulungen sind ein wichtiger Punkt, da beim Zertifizierungsaudit stichprobenartig geprüft wird, ob die Mitarbeiter das System leben.

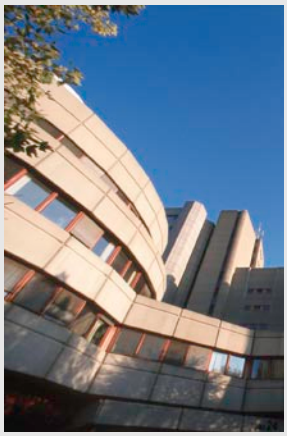
Zu Beginn der Implementierungsphase wurde die Information-Security-Policy verfasst, die unsere Grundsätze auf insgesamt acht Seiten wiedergibt. Dann folgte die Erstellung des 160 Seiten umfassenden Sicherheitshandbuches in einem Zeitraum von knapp drei Monaten. Dabei haben wir versucht, die mehr als **130 Steuerungsmaßnahmen** der ISO 27002, auch Controls genannt, auf die praktische Abwendbarkeit im SNO-Bereich herunter zu brechen. Daraus sind mehr als **40 IS-Richtlinien** entstanden, die nun unser normkonformes Regelwerk für Informationssicherheit darstellen. Erfasst werden alle informationssicherheitsrelevanten Themen wie zum Beispiel:

- **das Verhalten am Arbeitsplatz,**
- **Netzwerksicherheit,**
- **Usermanagement,**
- **private Nutzung von Netzwerkressourcen,**
- **Viren- und Spamschutz,**
- **WLAN u.a..**

Welche Unternehmensbereiche wurden bei der Implementierung einbezogen?

Die Verantwortlichen für die physische Sicherheit waren sehr wichtig, da die ISO 27001 / ISO 27002 auch physische Sicherheit wie Zutrittskontrollen verlangt. Juristen haben uns geholfen, das Sicherheitshandbuch und die enthaltenen Handlungsanweisungen gesetzeskonform zu verfassen, insbesondere in Hinsicht auf das E-Commerce-Gesetz, die Signaturverordnung und das Handelsgesetzbuch. Ebenso wurde die Leitung der internen Applikationsentwicklung einbezogen, weil sicherheitsrelevante Regeln zur Programmierung auch im Sicherheitshandbuch erfasst werden. Zur besseren Einschätzung von Risiken aus Versicherungssicht wurden die Versicherungsexperten der Telekom Austria AG hinzu gezogen. Die Personalabteilung half, die Richtlinie über die Sicherheitsaspekte bei der Aufnahme neuer Mitarbeiter oder Vorgangsweise bei Ausscheiden von Mitarbeitern zu erstellen.

„Keep it simple: man sollte nicht versuchen, alles bis in das kleinste Detail zu regeln."



Welchen Tipp können Sie zum Thema Sicherheitshandbuch geben?

Keep it simple – auf gut Deutsch: man sollte nicht versuchen, alles bis in das kleinste Detail zu regeln. Denn die Vorschriften aus dem Sicherheitshandbuch müssen auch auf ihre Einhaltung überprüft und bei Bedarf verbessert werden. Bei unserer ersten Ausgabe haben wir auch Security-Empfehlungen in das Handbuch aufgenommen – wie zum Beispiel: E-Mails von unbekannten Absendern sollten nicht geöffnet werden. Solche Empfehlungen lassen sich aber in der Realität nicht überprüfen. Im Release 2 unseres Handbuches haben wir all diese Empfehlungen heraus genommen und auf einem IS-Merkblatt zusammengefasst. In den Richtlinien finden sich jetzt nur mehr Hard-Facts, die sich verifizieren lassen.

„Das größte Problemfeld ist wohl, wenn Mitarbeiter bestimmte Abläufe plötzlich anders vollziehen müssen."

- **Das Handbuch stellt den Soll-Zustand dar. Wie wurde der Ist-Zustand erhoben?**

Da haben wir zwei bis drei Monate harter Arbeit hinter uns. Denn das Projektteam wollte möglichst genaue Ergebnisse über den Ist-Zustand in Bezug auf Informationssicherheit erheben, als solide Grundlage für die Implementierung. So wurden Abteilungs- und Gruppenleiter zu den einzelnen Punkten des Sicherheitshandbuchs befragt.
Zusätzlich wurde stichprobenartig in den technischen Protokollen der **Systeme überprüft**, wie der tatsächliche Zustand ist. Auf diese Weise konnten wir ganz konkrete Angaben eruieren – und zwar **im Vergleich zu den Richtlinien** unseres Sicherheitshandbuches. Daher ist es sinnvoll das Handbuch zuerst zu erstellen.

- **Können Sie Beispiele nennen?**

Durch die Befragungen wurde dem beteiligten Management auch frühzeitig Einsicht in die Inhalte des ISMS gewährt, so dass das neue System in der Breite mitgetragen wurde. Praktische Beispiele für Überprüfungen sind etwa die Passwort-Policy. Hier wurde überprüft wie oft und mit welchen Merkmalen die Passwörter geändert wurden. Im Bereich Change Management wurden die Abläufe erhoben, nach denen neue Software in Betrieb genommen wird. Oder ein organisatorischer Bereich: Es wurde überprüft, welche Unterlagen bei Aufnahme von neuem Personal weitergegeben und welche Berechtigungen vergeben werden. Diese Vorgangsweise wurde **flächendeckend** über alle Hierarchieebenen durchgeführt. Der Aufwand hat sich aber ausgezahlt. Denn aufgrund der exakten **Standortbestimmung** konnte bereits parallel mit der Implementierung von Maßnahmen und Abläufen begonnen werden. Es geht bei der ISO 27001 / ISO 27002 ja darum, für alle Kernabläufe einen Verbesserungsprozess nach dem Muster Plan-Do-Check-Act einzuführen.

- **Wie lang dauerte die Umsetzung von Maßnahmen und worauf kommt es dabei an?**

Insgesamt haben wir rund fünf Monate für die Umsetzung sämtlicher Maßnahmen für Informationssicherheit benötigt. Natürlich kommt es dabei zu menschlichen Reibungspunkten, denn das Projekt musste von den Beteiligten zusätzlich zur laufenden Arbeit bewältigt werden. Das größte Problemfeld ist wohl, wenn Mitarbeiter bestimmte Abläufe plötzlich anders vollziehen müssen, als sie es bisher gewohnt waren. In diesen Fällen haben wir immer den Konsens gesucht und uns **Zeit für Gespräche genommen** – denn das System kann nur funktionieren, wenn die Mitarbeiter von der Sinnhaftigkeit überzeugt sind und die Richtlinien in der täglichen Praxis umsetzen. Sehr wichtig dabei war auch die Absegnung der Maßnahmen durch das oberste Management. Somit wurde klar kommuniziert, dass es zu Änderungen kommen muss.

Schritt 5: CIS-System-&-Risk-Review (Vorbegutachtung)
Die CIS begutachtet die Interpretation der Normforderungen sowie die ISMS-Dokumentation. Mängel und Verbesserungspotenziale werden in einem Kurzbericht festgehalten. So wird das Unternehmen auf das Certification-Audit gezielt vorbereitet.

Welche Bedeutung hatte das Stage-One-Audit oder CIS-System-&-Risk-Review?

Einige Wochen vor der Zertifizierung fand diese Vorbegutachtung statt und stellte als **„Generalprobe"** eine optimale Vorbereitung auf das Finale dar. Der erstellte Zwischenbericht zeigt klar auf, wo man steht und wie wahrscheinlich eine erfolgreiche Zertifizierung ist. Die angestrebte Zertifizierung sollte unbedingt beim ersten Anlauf erreicht werden, um nicht eine Demotivation der Mitarbeiter hervor zu rufen.

Schritt 6: CIS-Certification-Audit
CIS-Auditoren überprüfen das InformationsSicherheitsManagementSystem durch multiple Stichproben auf allen Ebenen der Organisation. Ein Abschlussbericht zeigt zukünftige Verbesserungspotenziale auf.

Wie haben Sie sich auf das Audit vorbereitet und wie war der Ablauf?

Es ist empfehlenswert alle benötigten Unterlagen wie Dokumentationen aus den Abteilungen im Vorhinein zu sammeln. Während dem Audit bleibt keine Zeit dafür. Wichtig ist auch das Vorbereiten von Beweisen und Beispielen: Wann und von wem wurde das Sicherheitshandbuch freigegeben? **Welche Nachweise** gibt es für die Schulungen der Mitarbeiter? Insgesamt geben die Auditoren Themen vor, die genauer überprüft werden. Dafür sind **Interviewpartner** aus dem operativen Bereich bereitzustellen. Die Auditoren wollen sehen, ob das ISMS von den Beteiligten gelebt wird.
Im SNO-Bereich mit 1.500 Mitarbeitern hat das Schluss-Audit eine Woche gedauert und insgesamt drei Standorte einbezogen. Im ersten Teil des Audits wurden das Handbuch, die Dokumentation und die Nachweise gesichtet. Geprüft wurde, ob die Abläufe formell richtig beschrieben sind. Im zweiten Teil des Audits ging es um die operative Umsetzung. Dabei wurden Interviews mit von uns ausgewählten Mitarbeitern geführt. Darüber hinaus wurden stichprobenartig auch Mitarbeiter überraschend am Arbeitsplatz befragt. Und schließlich wurden auch die Serverräume und die **Systemtechnik begutachtet.** Hier wurde geprüft, ob technische Sicherheitseinrichtungen wie zum Beispiel die strenge Zutrittskontrolle zum Serverraum den im Handbuch definierten Richtlinien tatsächlich entsprechen.

■ **Als Schlussbilanz: Wie groß ist der Aufwand im täglichen Betrieb des ISMS?**

Tatsächlich minimal. Technische Einrichtungen wie Access Controls, Prozess- oder Systemtechnik arbeiten automatisch. Auch ein Großteil der Dokumentation erfolgt mit Hilfe der Technik.
In der IT ergibt sich zwar ein erhöhter Aufwand durch Einhaltung der Prozesse, dafür sinkt aber die Fehlerquote. Extern profitiert das Unternehmen bei Ausschreibungen: Das ISO-27001-Zertifikat macht einen klaren Unterschied zum Mitbewerb.

Von der Implementierung zum Zertifikat

Informationsgespräch
CIS-Erstgespräch: Details über Zertifizierungsprozess. Dann Registrierung, Projektplanung.

Analyse
Interne Evaluierung des Verbesserungspotentials, Bewertung vorhandener Maßnahmen.*

Implementierung
Maßnahmenumsetzung nach ISO 27001 und/oder ISO 20000 im Unternehmen.*

*Die CIS als unabhängige Prüfstelle ist nicht involviert

CIS Stage Review (Vorbeurteilung)
Optional: Projektbegleitende Prüfung der implementierten Elemente durch CIS-Auditoren.

CIS System & Risk Review (Vorbegutachtung)
CIS prüft Interpretation der Normforderungen und Dokumentation, „Generalprobe".

CIS Certification Audit
Überprüfung des Systems durch multiple Stichproben. Auditbericht mit zukünftigem Verbesserungspotenzial. Das CIS-Zertifikat nach ISO 27001 / ISO 20000 gilt 3 Jahre.

CIS Surveillance Audit
Das einmal pro Jahr durchgeführte Surveillance Audit überprüft die Effektivität des gesamten Managementsystems sowie seine ständige Verbesserung.

CIS Recertification Audit
Nach 3 Jahren haben Sie die Möglichkeit, das abgelaufene Zertifikat erfolgreich zu erneuern.

„Heute ist der zusätzliche Aufwand minimal. Denn die technischen IS-Einrichtungen wie Access Controls, Prozess- oder Systemtechnik arbeiten automatisch."