Die Interpretation eines IT-Sicherheitskonzepts hat sich in den letzten Jahren massiv geändert. Je stärker die IT als Business Partner agiert und hochverfügbare Services für Geschäftsprozesse zur Verfügung stellt, umso umfassender und businessorientierter müssen solche Konzepte werden. Für **WOLFGANG GALLER, IT-LEITER DER ENERGIE STEIERMARK** *und ausgezeichnet mit dem* **CIO AWARD 2011,** *ist IT-Risikomanagement deshalb unerlässlich.*

Risikomanagement MUSS FÜR DIE IT ZUM GESCHÄFT GEHÖREN

Methodisches IT-Risikomanagement ist zur Erarbeitung eines vollständigen und organisationsweiten IT-Sicherheitskonzeptes unerlässlich. Um Risiken zu beherrschen, ist es zunächst erforderlich, sie zu kennen und zu bewerten. Abhängig von der in der Risikoanalyse angewandten Methodik drückt sich das Risiko als eine Menge identifizierter fehlender Maßnahmen oder in einem möglichen Schadensbetrag multipliziert mit der Wahrscheinlichkeit des Auftretens aus. Dazu wird in einer Risikoanalyse das Gesamtrisiko ermittelt. Verbleibt nach Durchführung aller im Sicherheitsplan vorgesehenen Maßnahmen ein Restrisiko, dessen weitere Reduktion nicht möglich oder unwirtschaftlich wäre, so ist es möglich, das Restrisiko bewusst zu akzeptieren.

Risikoanalyse in drei Schritten

In der Energie Steiermark wird die Risikoanalysestrategie in mehreren Schritten umgesetzt.

Schritt 1: Business Impact Analyse
Im ersten Schritt werden die Vermögenswerte beziehungsweise Assets – IT-Services und Informationskategorien – identifiziert und deren Wert für die Energie Steiermark ermittelt. Die Assets werden bezüglich der Kriterien Vertraulichkeit, Integrität und Verfügbarkeit (Confidentiality, Integrity, Availability – CIA) über ein definiertes Schema bewertet. Dabei ist eine Einstufung über die Business Impact Methode (BIA) von niedrig bis gravierend möglich.

Schritt 2: Risikoberechnung
Das Risiko ergibt sich aus dem Schadenspotenzial und der Frequenz (Eintrittswahrscheinlichkeit). Die Frequenz gibt an, mit welcher Eintrittswahrscheinlichkeit eine Bedrohung in Bezug auf ein bestimmtes Service eintritt.

Schritt 3: Restrisikoberechnung
Das Risiko multipliziert mit dem Umsetzungsgrad ergibt den Wert des Restrisikos, ebenso bezüglich der Kriterien Vertraulichkeit, Integrität und Verfügbarkeit. Der Umsetzungsgrad gibt an, inwieweit die Maßnahmen (Controls) in Bezug auf ein IT-Service umgesetzt wurden.
Der Endwert, der sich daraus ergibt, gibt Aufschluss über das Restrisiko. Der Wert des Restrisikos ist ein berechneter Wert und sagt aus, welcher Schaden verbleibt, obwohl Maßnahmen in die Wege geleitet wurden. Anhand des Restrisikowertes muss entschieden werden, ob das Risiko akzeptiert werden kann (Risikoakzeptanz) oder an externe, wie zum Beispiel an Versicherungen abgegeben wird (Risikoübertragung/Risikodelegation). Die Abbildung des IT-Risikomanagements basiert dabei auf der ÖNORM ISO/IEC 27001 und stützt sich zusätzlich auf das Konzern- Risk- und Krisenmanagement. Die Umsetzung erfolgte über ein aufwendiges Risk-Assessment im Zusammenspiel mit dem Business beziehungsweise mit den Organisations- und Prozessverantwortlichen.

Risiken rechtzeitig zu erkennen, um gezielt im Falle eines Eintritts darauf reagieren zu können und deren Eintrittswahrscheinlichkeit zu reduzieren beziehungsweise zu beseitigen, gehört heute zu den ganz zentralen Verantwortlichkeiten einer IT-Organisation, die als Service Provider und Business Partner hochverfügbare Dienste für das Kerngeschäft eines Unternehmens zur Verfügung stellt. □

WOLFGANG GALLER
ist seit 2008 als Leiter Konzern-Informationstechnologie in der Energie Steiermark für die gesamte IT und Telekommunikation und das externe Telekommunikationsgeschäft verantwortlich.

DIE ENERGIE STEIERMARK AG
ist das viertgrößte Energieunternehmen Österreichs mit den Kerngeschäftsfeldern Strom, Erdgas, Fernwärme und Restmüllverwertung. Mehrheitseigentümer ist das Land Steiermark, eine Beteiligung hält der französische Energiekonzern Electricité de France (EdF). Auf in- und ausländischen Märkten verkauft die Energie Steiermark 11.400 GWh Strom, mehr als 14.800 GWh Erdgas und 2.400 GWh Fernwärme. Der Konzernumsatz liegt bei rund 1,3 Milliarden Euro.
Die Energie Steiermark beschäftigt rund 1.800 MitarbeiterInnen und verfügt über 29 Betriebsstandorte in der Steiermark und eine Vertriebsgesellschaft in Wien, sowie über zahlreiche Beteiligungen im Ausland.