OTS0011 5 WI 0350 NEF0015 II Mi, 15.Okt 2008
Technologie/Software/Sicherheit/Unternehmen/Recht

IT-Risikomanagement - auch für KMU: Push durch neue Norm ISO 27005

Utl.: Druck durch Datenverlust und Gesetze. IT ist Vorreiter: 2009 folgt ISO-Norm für Enterprise-RM =

Wien (OTS) - Der lang erwartete Standard für "Information Security Risk Management", ISO/IEC 27005, wurde als Leitfaden zu der bekannten Norm für Informationssicherheit ISO/IEC 27001 veröffentlicht. Damit wird das abstrakte Thema Risikomanagement besser umsetzbar - auch in KMU. Der IT kommt Themenführerschaft zu, denn erst 2009 soll mit ISO 31000 eine Norm für Enterprise-RM folgen. Risikomanagement (RM) gehöre zu den großen Herausforderungen, auch aufgrund aktueller Gesetze, so DI Herfried Geyer, RM-Experte der Zertifizierungsorganisation CIS, im Interview. (www.cis-cert.com)

Herr Geyer, was bedeutet IT-Risikomanagement im Business-Kontext?

Datenverlust und -diebstahl sind ein massives Problem. Im Vorjahr wurden weltweit mehr als 167 Mio. Persondaten entwendet. Derzeit wird diskutiert, ob Unternehmen künftig den sorgfältigen Umgang mit Daten aktiv nachweisen müssen. Sicherheitslücken lassen sich mittels Risikomanagement aufdecken und minimieren, was Regressforderungen entgegenwirkt. Die akkreditierte Gesellschaft CIS führt Zertifizierungen nach ISO 27001 durch, wobei der Security-Standard Riskmanagement vorsieht sowie den Aufbau ganzheitlicher Security-Systeme mit Prozessverbesserung und Kontrollen ermöglicht. Für viele IT-Manager noch Neuland.

Wird IT-Risikomanagement durch die neue Norm gepusht?

Datensicherheit beginnt mit solidem Risikomanagement, was auch vom Verbandshaftungsgesetz und Richtlinien wie Basel II oder Euro-Sox gefordert wird. Weiter aufgewertet wird das Thema, wenn Mitte 2009 die ISO 31000 für unternehmensweites Risikomanagement kommen soll. IT-Verantwortliche mit RM-Erfahrung sind dann Vorreiter.

Ist Risikomanagement für KMU ein Thema?

Gerade kleinere und mittlere Unternehmen in sensiblen Branchen wie Automotive, Health, Software oder Telekommunikation sind hier angesprochen und haben meist großen Aufholbedarf.

Inwieweit ist ISO 27005 für KMU anwendbar?

Der Leitfaden ist branchen- und größenunabhängig. Durch Adaptierung seiner Inhalte auf die betrieblichen Anforderungen können KMU ein schlankes und effektives IT-Riskmanagement etablieren. ISO 27005 bietet eine Anleitung zum Risikomanagement mit Checklisten, Erklärungen und Beispielen.

Wie passen die IT-Norm ISO 27005 und Enterprise-RM zusammen?

ISO 27005 lässt sich aufgrund ähnlicher Strukturen in ein unternehmensweites Riskmanagement integrieren, kann aber auch "solo" umgesetzt werden. Der Trend geht hin zu integrierten Systemen und vernetzten Teams. (Mehr Info: www.cis-cert.com)

Fotos + Volltext: http://www.cis-cert.com/aktuell/presse.php

Rückfragehinweis:
Heike Galley, h.galley@cis-cert.com, Tel.: 0699 1974 5647

OTS0011 2008-10-15/08:00

150800 Okt 08

Link zur Aussendung:
http://www.ots.at/presseaussendung/OTS_20081015_OTS0011