



## E-Interview mit Klaus Lenßen



<b>Titel des E-Interviews:</b>	IT-Sicherheit und –Outsourcing für kleine und mittelständische Unternehmen (KMU) – was das Management wissen muss
<b>Name:</b>	Klaus Lenßen
<b>Funktion/Bereich:</b>	Senior Business Development Manager Security
<b>Organisationen:</b>	Cisco Systems GmbH

### Liebe Leserinnen und Leser,

als verantwortlicher Manager oder IT-Leiter eines kleinen oder mittelständischen Unternehmens haben Sie es automatisch auch mit dem Thema Sicherheit in der IT zu tun. Damit Sie sich dem Kerngeschäft Ihres Unternehmens im täglichen Betrieb wirklich erfolgreich widmen können, benötigen Sie folglich leistungsfähige IT-Sicherheitsstrukturen – bei Ihnen im Unternehmen oder alternativ outgesourced bei einem Partner allokiert.

Leider besteht eine Flut von Informationen zu diesem Thema. Ein Teil dieser Informationen ist jedoch alles anderes als hilfreich oder aus Managementsicht auch nicht wirklich verständlich und somit nicht entscheidungsrelevant.

Worauf es wirklich ankommt und wie Sie bei der Eingrenzung der wichtigsten Sicherheitsaspekte für Ihr Unternehmen vorgehen sollten, ist Gegenstand dieses Interviews mit **Klaus Lenßen, Senior Business Development Manager**

Als praktische Erweiterung dieses Interviews existiert auch ein Leitfaden von Cisco mit den notwendigen Informationen aus einer Management-Perspektive, und nicht nur unter rein technischen Aspekten.

[Lesen Sie zu dem Thema auch - Nutzen Sie die IT optimal aus – zehn unverzichtbare Tipps für die Sicherheit in Ihrem Unternehmen](#)

Viel Spaß beim Lesen wünscht Ihnen

Ihr

NetSkill-Team



Sehr geehrter Herr Lenßen,

**Frage 1:**

Wie stellt sich aus Ihrer Erfahrung die Situation bzgl. der IT-Sicherheit bei kleinen oder mittelständischen Unternehmen in der Regel dar?

Worin bestehen aus Managementsicht die wesentlichen Risiken, sind diese Risiken v.a. technischer oder organisatorischer Natur?



**Antwort:**

Grundsätzlich ist festzustellen, dass das Bewusstsein für die Notwendigkeit von IT-Sicherheit stark zugenommen hat. Dies gilt für alle Arten von Unternehmen – vom Kleinstbetrieb bis hin zum Großkonzern. Doch mit der Erkenntnis alleine ist es nicht getan, sondern es bedarf einer situationsgerechten Umsetzung verschiedener Massnahmen, um das gewünschte Sicherheitsniveau zu erreichen – und hierbei sind enorme Unterschiede je nach Unternehmensgröße zu beobachten.

Der zweite Teil der Frage lässt sich nicht allgemeingültig beantworten, da sie von den Geschäftsprozessen des Unternehmens abhängen.

**Frage 2:**

Warum sind so viele der frei zugänglichen Informationen oft zu technisch oder liefern keine entscheidungsorientierten Handlungsanleitungen?

Bei welcher Art Partner sollten sich die Entscheider aus IT und Management gezielt informieren?



**Antwort:**

IT Sicherheit hängt immer vom Zusammenspiel verschiedener Massnahmen in unterschiedlichen technischen Disziplinen sowie über alle Bereiche eines Unternehmens hinweg ab.



Daher konzentrieren sich die meisten Dokumente auf Teilaspekte – und hiervon die meisten wiederum auf technische Funktionen. Ein weiterer Grund hierfür ist sicherlich auch, dass die meisten Hersteller von IT Sicherheitsprodukten über ein sehr fokussiertes Produktportfolio verfügen und daher alleine keine übergreifenden Konzepte mit aufeinander abgestimmten Sicherheitsfunktionen in jedem Gerät – beispielsweise für das gesamte Netzwerk – liefern können.

Rahmenwerke, die Orientierung und Handlungsanleitungen geben, sind beispielsweise das IT Grundschutzhandbuch, BS7799 bzw. der Nachfolger ISO 27001. Bevor man sich auf die technischen Details konzentriert, sollte geklärt sein, was die schützenswerte Information ist, wie hoch der Schutzbedarf ist, welche rechtlichen Rahmenbedingungen (Compliance) vorliegen und mit welcher Strategie sich diese Assets absichern lassen.

**Frage 3:**

Wie sehen Sie die zukünftige Risikosituation, v.a. in Bezug auf weiter zunehmende Kommunikationsintensität oder auch Vernetzungsgrad über eBusiness etc. zwischen Unternehmen?

**Antwort:**

Die Risiken werden weiter ansteigen, zu einen durch die Nutzung neuer Web 2.0 Techniken zum anderen durch Wirtschaftsspionage. Es gibt keinen klassischen Perimeter mehr, den man durch Einzelmaßnahmen absichern kann, Angriffe werden gezielter und neue Bedrohungen entstehen in immer kürzeren Abständen. Wichtige Informationen werden auf den verschiedensten Endgeräten verarbeitet werden und das überall und zu jeder Zeit. Data Leakage Prevention (DLP) – also die Absicherung gegen Verlust wichtiger Geschäftsinformationen – gewinnt daher immer mehr an Bedeutung. Agilität und Flexibilität bei der Umsetzung von Sicherungsmassnahmen sind daher sehr wichtig, da sich Technik, Bedrohungslage und Schutzziele ständig verändern. Diese Faktoren muss ein Sicherheitskonzept als Grundlage haben. Darüberhinaus darf man den Faktor Mensch nicht vergessen. Die Einbindung der Mitarbeiter in den Prozess durch Aufklärung (Awareness), Übertragung von Verantwortung und Auszeichnung von positivem Verhalten sind mindestens so wichtig wie neueste Sicherheitstechnik.

**Frage 4:**

Was würden Sie als die Top 3 Prios für Unternehmer und Geschäftsführer zu IT-Sicherheit formulieren?

**Antwort:**

Top Priorität für mich hat die Erkenntnis, dass Sicherheit kein notwendiges Übel ist, sondern Sicherheit dabei hilft Kosten zu sparen. Beispielsweise kann der Ersatz von signatur-basierten Antivirusprogrammen durch eine verhaltens-basierte Technik auf dem Endgerät die keine Updates mehr benötigt und so auch vor unbekanntem Bedrohungen schützt, helfen, Folgekosten im PC-Support für die Wiederherstellung von geschädigten PCs oder Servern einzusparen.

Eine weitere Priorität hat die Einbindung der Mitarbeiter, angefangen von der Geschäftsleitung bis hinunter zum Praktikanten, deren Training und Motivation verantwortungsvoll mit Daten umzugehen und sie zu schützen. Dazu gehört auch, dass im vollbesetzten ICE nicht per Handy über das letzte Angebot, einen Bewerber oder eine wichtige Änderung am neuesten Prototypen diskutiert wird.

Ebenfalls Priorität hat der effektive und kostenorientierte Einsatz von Sicherheitstechnik. Sicherheitsfunktionen werden mehr und mehr zum festen Bestandteil der Netzwerkinfrastruktur. Dort stehen sie bereits vielfach zur Verfügung, ohne jedoch genutzt zu werden. Potential, dass in vielen Unternehmen noch gehoben werden kann. Hierzu muss man jedoch das oft vorherrschende Silo-Denken aufbrechen um Sicherheit wirklich ganzheitlich betrachten zu können.

**Vielen Dank für das Interview!**