Gehört Ihnen Ihr Wissen „allein“?

Gehört Ihnen Ihr Wissen allein? Vermutlich – und hoffentlich – reagiert das Gros der Wissensgesellschaft auf diese Frage mit einem entpörten „Nein!“. Denn Wissen vermehrt sich schließlich vor allem durch den Austausch mit anderen; „Wissen ist Macht“-Denken gilt daher längst als überholt. Unter dem Stichwort IT-Sicherheit stellt sich dieser Aspekt allerdings in einem ganz anderen Licht dar: Wer den falschen Leuten Zugriff auf seine immateriellen Werte gewährt – womöglich noch unfreiwillig, der wird im schlimmsten Fall um sein wertvollstes Gut gebracht. Und auch wenn sich das Wort Wirtschaftsspionage anhört wie aus einem Agententhriller – erst kürzlich hat Bayerns Verfassungsschutzchef Burkhard Körner die Unternehmen des Freistaats vor Wirtschaftsspionage gewarnt. Der Grund: Eine bisher unveröffentlichte Studie aus dem Jahr 2008 brachte ans Licht, dass allein in Bayern wahrscheinlich jede zweite Hightech-Firma bereits Opfer von Wirtschaftsspionage geworden ist. Die Dunkelziffer liege aber vermutlich deutlich höher. Betroffen seien vor allem kleine und mittelständische Unternehmen – mit Folgeschäden im Wert von bis zu zwei Millionen Euro pro Betrieb!

Doch die Gefahr lauert nicht nur von außen. Auch innerbetrieblich hört (bzw. liest) „der Feind“ mit. So ergab eine aktuelle Studie von Cyber-Ark Software, dass 41 Prozent der IT-Mitarbeiter ihre Administratoren-Rechte nutzen, um auf vertrauliche Informationen wie Kundendatenbanken oder Personaldaten zuzugreifen. 27 Prozent der befragten Unternehmen bestätigten zudem, dass sie bereits Opfer von Insider-Sabotage geworden sind. Aber nicht nur IT-Verantwortliche haben Zugriff auf sensible Daten – egal ob Personalabteilung, Buchhaltung oder Sekretariat: Jeder Mitarbeiter ist gefordert, die ihm zugänglichen Firmendaten zu schützen. Bereits die Wahl von Passwörtern, das Speichern von Informationen auf mobilen Speichergeräten oder der ungeschützte Austausch via E-Mail & Co. können neugierigen Wettbewerbern Tür und Tor öffnen. In der Regel passiert so etwas ungewollt, die Folgen sind dennoch verheerend. Bayerns Verfassungsschutzchef Körner führt 70 Prozent der Fälle von Wirtschaftsspionage auf das Fehlverhalten von Mitarbeitern zurück.

Unternehmen sind folglich gefordert, ihre Mitarbeiter für das Thema IT-Sicherheit zu sensibilisieren. Sie müssen sie dabei aber auch durch entsprechende Software unterstützen. Denn Irren ist bekanntlich menschlich. Werden Passwörter aber durch biometrische Identifikationsverfahren ersetzt und Daten auf USB-Sticks und anderen Speichermedien verschlüsselt, dann springt die IT ein, wenn der Mensch im bewussten Umgang mit sensiblen Informationen einmal irrt. Mehr dazu lesen Sie in unserem Titelthema ab Seite 22.

Ihr

Oliver Lehnert