

12 Fragen zur Sicherheit

- 1 **Haben Sie Prozesse für den etwaigen IT-Notfall oder Ausfall im Unternehmen definiert und dokumentiert (z.B. in einem Handbuch) und sind diese den Mitarbeitern bekannt? Werden diese Prozesse regelmäßig auf Aktualität, Angemessenheit und Einhaltung überprüft?**
- 2 **Sind diese Prozesse im laufenden Betrieb auf Funktionsfähigkeit überprüft worden?**
- 3 **Haben Sie klare Regelungen in Ihrem Netzwerk zu den Benutzerrechten, zur Datensicherung und Verwahrung und zur etwaig notwendigen Wiederherstellung?**
- 4 **Wissen Sie, wie lange es im Ernstfall dauert, den Normalbetrieb wieder aufzunehmen?**
- 5 **Haben Sie schon einmal einen Web-Angriff auf Ihre Systeme durchgeführt oder durchführen lassen (ethical hack)?**
- 6 **Verwenden Sie Standardprodukte (Hardware und Software) im Unternehmen, die einfacher zu pflegen und zu warten und auch meist schneller zu ersetzen sind?**
- 7 **Werden Software- und Hardware-Komponenten auch unter dem Aspekt der Sicherheit und Verfügbarkeit eingekauft?**
- 8 **Haben Sie einen IT-Sicherheitsbeauftragten oder einen Berater, der sich mit diesem Schwerpunkt regelmäßig befasst?**
- 9 **Haben Sie ständig verfügbare IT-Mitarbeiter oder Berater, die Ihre Systeme betreuen, sich bei Abwesenheit Einzelner gegenseitig vertreten können und sich regelmäßig fortbilden?**
- 10 **Sind die Aufgaben und Kompetenzen dieser Mitarbeiter klar geregelt?**
- 11 **Lassen Sie Ihre hausinternen Regeln und Prozesse regelmäßig durch externe Fachleute prüfen?**
- 12 **Wussten Sie, dass nach dem Gesetz zur Kontrolle und Transparent im Unternehmensbereich (KontraG) sowohl an Aktiengesellschaften, als auch an GmbHs, die gewissen Größenkriterien genügen, die Forderung gestellt wird, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit der Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“? (§ 91 Abs. 2 AktG)**