Checkliste: IT-Sicherheit in IT-Konsortien

- ☐ **Gemeinsame IT-Sicherheitsausrichtung**
  Die Kooperationspartner sollten eine einheitliche Sicherheitsstrategie entwickeln – hierfür eignet sich besonders eine Informationssicherheitsrichtlinie, auf die sich die Partner einigen.

- ☐ **Mindeststandards setzen**
  Um ein hohes IT-Schutzniveau innerhalb der Kooperation zu erreichen, sollte sich auf verbindliche IT-Sicherheits-Mindeststandards verständigt werden. Diese können ebenfalls Bestandteil einer Informationssicherheitsrichtlinie sein.

- ☐ **Etablierung eines Informationssicherheitsmanagementsystems (ISMS)**
  Die Kooperationspartner müssen zwingend Regeln, Verfahren und Methoden etablieren, um den Umgang mit der Informationssicherheit klar zu regeln und zu kontrollieren.

- ☐ **Schutzmaßnahmen implementieren**
  Natürlich müssen neben den Management-Maßnahmen auch technische Schutzmaßnahmen wie z.B. Firewalls, Deep Packet Inspection oder Malware-Erkennung* zum Einsatz kommen.

- ☐ **Risiko- und Sicherheitsanalysen durchführen**
  Um Sicherheitslücken und Schwachstellen zu detektieren, eignen sich insbesondere Pentesting- und Vulnerability-Scans*.

- ☐ **Verschlüsselung nutzen**
  Um Vertraulichkeit zu gewährleisten, sollten sämtliche Verbindungen zu Plattformen, Ressourcen und Schnittstellen ausschließlich verschlüsselt nutzbar sein.

- ☐ **Logging und Monitoring**
  Vertrauen ist gut, Kontrolle ist besser: Netzwerkverkehr sollte überwacht und auf Unregelmäßigkeiten überprüft werden. Der Zugriff auf Systeme oder Ressourcen ist ebenfalls zu protokollieren.

- ☐ **Awareness-Bildung erhöhen**
  IT-Sicherheit ist ein proaktiver Prozess, deshalb gilt es, die Beteiligten einschließlich des Managements, bestmöglich für Informationssicherheit zu sensibilisieren und zu schulen.

* *siehe Glossar, Seite 42*