§ 6f IT-Sicherheitskonzept

(1) [1]Erlaubnisinhaber haben geeignete Sicherheitsmaßnahmen im IT-Sicherheitskonzept zu beschreiben und zu implementieren. [2]Das Sicherheitskonzept ist regelmäßig zu überprüfen und, soweit hierzu Veranlassung besteht, zu überarbeiten.

(2) Die Sicherheitsmaßnahmen müssen mindestens folgende Aspekte umfassen:

1. den jederzeitigen Schutz der personenbezogenen Daten der Spieler vor unrechtmäßiger Verarbeitung,

2. die Sicherstellung der dauerhaften und jederzeitigen Verfügbarkeit, Integrität und Vertraulichkeit von Daten, etwa durch Verschlüsselungsmechanismen, Zugriffskontrollen und Virenschutzprogramme,

3. die regelmäßige Sicherung aller relevanten Daten,

4. die Etablierung und den regelmäßigen Test von Prozessen, die eine schnelle Wiederherstellung gesicherter Daten ermöglichen,

5. den Schutz der verwendeten Systeme vor Manipulationen von innen und außen und

6. die lückenlose Nachvollziehbarkeit der Integrität der Systeme.

(3) [1]Die Wirksamkeit des Sicherheitskonzepts ist mindestens jährlich vom Erlaubnisinhaber auf eigene Kosten durch eine von ihm unabhängige, sachverständige Stelle überprüfen zu lassen. [2]Der zuständigen Erlaubnisbehörde ist der Prüfbericht vorzulegen.