Erläuterung zu Punkt V.3. der Betriebsvereinbarung für operative Systeme

- Einhaltung der Bestimmungen des § 14 DSG 2000 zur Datensicherheit;

  Beispiel:
  - Zutrittskontrollen zu den Serverräumen. Gerade um die Datensicherheit gewährleisten zu können wird der physische Zugang zu den Servern entsprechend geschützt. Andererseits müssen die TechnikerInnen entsprechend einfach und eventuell auch am Wochenende oder nachts Zugang zu den Serverräumen haben. Eine entsprechende Zugangskontrolle ist hier sinnvoll.

- Gewährleistung der Systemfunktionalität und Systemsicherheit;

  Beispiel:
  - Überwachung der Logins auf unbefugte Zugriffsversuche.
    Konkretes Beispiel dazu: Um zB unrechtmäßige Zugriffe durch Spammer/innen, die in den Besitz von User/innenpasswörtern gekommen sind, zu unterbinden, wird automatisiert die Zahl der via Webmail pro Stunde verschickten Nachrichten gemessen. Überschreitet diese einen festgesetzten Schwellwert werden die Administrator/innen gewarnt.
  - Durchführung von (automatisierten) Tests
  - Vergleich von Datenbeständen („Backup-Kontrolle")

- Analyse und Korrektur von technischen Fehlern im System;

  Beispiel:
  - Benutzer vermissen E-Mails -> Analyse des E-Mailflusses in den Logfiles, um den Weg der Mail bis zum Postfach nachzuvollziehen.
    Konkretes Beispiel: Anfrage bei „postmaster": Ich hätte angeblich vor 7 Tagen ein E-Mail von xyz@irgendwo.at erhalten sollen. Dies ist aber nie bei mir angekommen. Was ist damit passiert? Um dieser Frage nachgehen zu können, ist eine Protokollierung der Mailzustellung notwendig. Gerade durch das, in den letzten Jahren sehr gestiegene Spamaufkommen, hat die Zuverlässigkeit von E-Mail sehr gelitten und Anfragen über Probleme mit vermeintlich verschwundenen E-Mails sind nicht selten.

- Optimierung der Rechner- bzw Systemleistung;

  Beispiel:
  - Anzahl der verarbeiteten E-Mails pro Minute, reichen die Rechner aus, um die E-Mails schnell und zuverlässig zuzustellen.
  - Logfiles werden auch zu statistischen Zwecken analysiert, um Zahlen über die Auslastung (zB: E-Mailaufkommen, Spamaufkommen) zu erhalten. Meist, aber nicht immer, reicht dafür die laufende (und auch anonymisierte) Aufzeichnung von Daten. Manchmal ist es hilfreich, im Falle von Problemen anhand der zurückliegenden Logfiles eine historische Entwicklung bestimmter (damals eventuell noch nicht interessanter) Parameter zu haben.
    Konkretes Beispiel: Eine User/in meldet, sie hat manchmal, aber nicht immer, Probleme auf einem bestimmten System. Eine Analyse der Logfiles zeigt ein merkliches Ansteigen von entsprechenden Fehlermeldungen, das genau 13 Tage zurückliegt. Damit kann das Problem genau einem bestimmten Softwareupgrade auf einem anderen System zugeordnet werden, dass ebenfalls genau vor 13 Tagen erfolgte. Eine rein anonymisierte Statistik wäre hier nicht ausreichend gewesen da á priori noch nicht bekannt war, dass es an dieser Stelle ein Problem geben könnte.

- Leistungsverrechnung für den Betrieb der Rechner bzw der Systeme.

  Beispiel:
  - Ermittlung lizenzrelevanter Daten mittels Softwareinventur und Ermittlung der Anzahl gleichzeitiger Verwendung (Softwaremetering) für die Abrechnung mit den Herstellern

- Reaktion auf Fehler- sowie Problemmeldungen der Benutzer/innen

  Beispiel:
  - Klärung von Anfragen zum Berechtigungskonzept (Login-/Zutrittsprobleme)
  - Analyse und Rekonstruktion von Benutzer/innenverhalten im Fehlerfall (Klickpfade, Eingaben, etc)