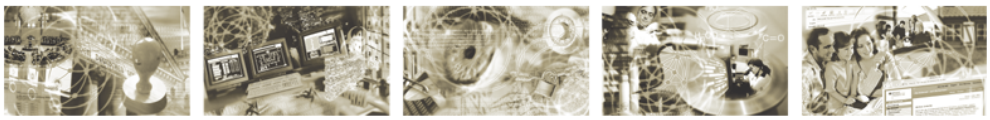
Bundesamt
für Sicherheit in der
Informationstechnik



Band M, Kapitel 10: Monitoring

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: Hochverfuegbarkeit@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Monitoring

Die nachfolgenden Maßnahmenkataloge beschreiben Maßnahmen im Sinne von Verfahren und Lösungen für die Erfassung, Darstellung und Auswertung der Zustandsinformationen einer HV-Architektur auf allen technischen und organisatorischen Ebenen sowie die geeignete Reaktion auf Störereignisse. Die Strukturierung der Maßnahmen erfolgt in Form von Maßnahmenclustern für die nachfolgend aufgeführten Subdomänen der HV-Domäne „Monitoring“:

- Überwachung
- (Früh-) Erkennung
- Reaktion
- Steuerung

1.1 Überwachung

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td>VM.10.1</td><td colspan="5">Auswahl der Überwachungsbereiche

Basierend auf der Monitoring-Strategie (vgl. 2.4) müssen die zu überwachenden Bereiche ausgewählt werden. Zur Realisierung hoher Verfügbarkeitsklassen müssen neben den Bereichen Hardware (inkl. Infrastrukturkomponenten), Software und Netze auch die Bereiche Infrastruktur, Personal und Organisation überwacht werden.</td></tr>
<tr><td></td><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td></td><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
<tr><td>VM.10.2</td><td colspan="5">Auswahl der zu überwachenden Komponenten

Es muss festgelegt werden, welche Komponenten in den verschiedenen Überwachungsbereichen überwacht werden sollen. In hohen Verfügbarkeitsklassen reicht die Überwachung der kritischen (SPoF) Komponenten nicht aus. Insbesondere müssen auch die Komponenten, die bereits redundant ausgelegt sind, überwacht werden.</td></tr>
<tr><td></td><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td></td><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.3</td><td>
Auswahl der Messgrößen
Im Rahmen der Überwachung sind insbesondere grundlegende Betriebsparameter zu erfassen (Vital-Monitoring), da diese essentielle Hinweise über den Zustand von Komponenten liefern. Im Bereich der Software- und Netzwerküberwachung sind Messgrößen wie z. B. Durchsatz, Antwortzeiten und Jitter von Bedeutung. Ebenso müssen im Bereich Personal und Organisation geeignete Messgrößen festgelegt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.4</td><td>
Auswahl der Sensorik
Es muss eine Auswahl darüber getroffen, welche Art der Sensorik eingesetzt werden soll. Zur Durchführung der Hardware-Überwachung werden Hardware-Sensoren eingesetzt, die durch die Verwendung eigenständiger Betriebsmittel gekennzeichnet sind. Sie verfügen über eine vom Zielsystem unabhängige Hardware sowie separate Software zur Erfassung und Aufbereitung der erfassten Werte.
Für die Überwachung der Systemaktivitäten und Parameter im Rahmen der Software-Überwachung ist die Integration von Software-Sensoren in das zu überwachende Zielsystem erforderlich. Das hybride Überwachungsverfahren stellt einen Kompromiss aus den beim Hardware-basierten sowie beim Software-basierten Überwachungsverfahren eingesetzten Prinzipien dar.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.5</td><td>
Festlegung der Abtastraten
Die Abtastrate muss in Abhängigkeit von der Dynamik der Messgrößen sowie der geforderten Reaktionszeiten festgelegt werden. Sollen sich schnell ändernde Größen mit einer hohen Genauigkeit wiedergegeben werden, ist eine hohe Abtastrate erforderlich. Kurze Reaktionszeiten fordern ebenso hohe Abtastraten, da auf Ereignisse in kürzester Zeit reagiert werden soll. Zu beachten ist, dass hohe Abtastraten zu hohen zusätzlichen Belastungen für das System führen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.6</td><td>
Auswahl der Übertragungsprotokolle
In allen Überwachungsbereichen muss festgelegt werden, mit welchen Übertragungsprotokollen die Messwerte zu einer zentralen Monitoring-Infrastruktur oder einem Überwachungs-Client übermittelt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*
VM.10.7	**Betrieb eines separaten Überwachungsnetzes** Eine hohe Anzahl von zu überwachenden Komponenten in Verbindung mit hohen Abtastraten machen ein separates Überwachungsnetz erforderlich. Ein separates Überwachungsnetz erhöht die Zuverlässigkeit der Überwachung auch bei Verbindungsbeeinträchtigung im Wirk-Netz.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung und Konzeption Implementierung Betrieb	Automatismen Fehlertoleranz Transparenz Redundanz Separation Skalierbarkeit Robustheit	Überwachung Reaktionszeit Fehlermeldung	Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)

Nr.	*Maßnahmen*
VM.10.8	**Überwachung im SAN** Sollen die Komponenten in einem SAN überwacht werden, ist ein separates (Überwachungs-) Netz erforderlich. Die zur Überwachung verwendeten Übertragungsprotokolle können i. d. R. nicht mittels fibre-channel übermittelt werden. In SANs sollten zu Zwecken der Verkehrsmessung s. g. Fibreoptic-TAPS eingesetzt werden. Beinhalten SAN-Management-Systeme bereits Monitoring-Komponenten, sollten diese eingesetzt werden. Zur Performance-Überwachung in SANs muss die Überwachung auf die SCSI-Ebene der Host-Systeme erweitert werden.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung und Konzeption Implementierung Betrieb	Automatismen Transparenz Redundanz Separation	Überwachung Reaktionszeit Fehlermeldung	Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.9</td><td>
Überwachung der Leistungsdaten des Netzwerks
Im Rahmen eines Netzwerk-Monitoring soll eine gezielte Überwachung der Parameter und Leistungsdaten eines Netzwerkes realisiert werden. Die Überwachung sollte auch die im Netzwerk befindliche Hardware sowie aktive Komponenten und Dienste umfassen. Die Überwachung der Netzwerkservices sollte die Funktionalität der DNS-Auflösung, die Dauer von DNS-Abfragen, die Korrektheit der Netzwerk-Uhrzeit, die Dauer der Beantwortung von NTP-Abfragen, die Anzahl der gerouteten Pakete bzw. die Auslastung der Router, die Anzahl der verworfenen Pakete, die Netzwerkantwortzeiten, die Hops zum Host, der Netzwerkdurchsatz bzgl. der Netzwerkbandbreite, der Durchsatz der Firewall, die Latenz der Firewall, die verworfenen (abgelehnten) Pakete der Firewall, die Latenz des VPN-Server, der ISAKMP- und IPSec-Status bzw. der Tunnelstatus sowie der Durchsatz des VPN-Services umfassen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.10</td><td>
Auswahl der Messmethode im Netz
Kann in einem Netz keine passive Verkehrsmessung im Durchfluss durchgeführt werden, muss mittel aktivem Injizieren von Test- oder Probepakten eine Indirekte Verkehrsmessung durchgeführt werden. Die dafür notwendigen Probepakete müssen mit einer hohen Rate einige Millisekunden bis einige Sekunden in das Netz injiziert werden. Die Abstände zwischen zwei Injektionen dürfen nicht größer als die Zeit sein, in der ein Ausfall erkannt werden soll.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit
Fehlermeldung</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td rowspan="3">VM.10.11</td><td colspan="5">Einsatz von TAPs
Zur passiven Verkehrsmessung im Durchfluss müssen TAPs eingesetzt werden. Auf das übliche Auslesen der Datenpakete an den Mirror-Ports sollte verzichtet werden.</td></tr>
<tr><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
<tr><td rowspan="3">VM.10.12</td><td colspan="5">Überwachung der Servicequalität
Im Rahmen eines Endanwender-Monitorings (EAM) soll eine Überwachung der für den Endanwender sichtbaren und spürbaren Service-Qualität durchgeführt werden. Die hierbei erfassten Messgrößen gehen über technische Betriebsparameter hinaus und sollen eine Aussage über die Einhaltung der im Service-Level-Agreement (SLA) vereinbarten Dienste-Qualität liefern.</td></tr>
<tr><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td>Betrieb</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit</td><td>Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td rowspan="3">VM.10.13</td><td colspan="5">Auswahl des Überwachungsverfahren im Überwachungsbereich Personal und Organisation
Für den Überwachungs-Bereich Personal und Organisation muss festgelegt werden, ob die Überwachung aufgrund von Selbsteinschätzung (internes Monitoring) oder aufgrund von Audits und Revisionen (externes Monitoring) erfolgen soll.</td></tr>
<tr><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
<tr><td rowspan="3">VM.10.14</td><td colspan="5">Einsatz des Nutzers als Sensor
Der Nutzer muss im Rahmen der Früherkennung in die Monitoring-Prozesse integriert werden. Es muss dazu ein Prozess etabliert werden, der den Nutzer kontinuierlich auffordert, bestimmte Indikatoren mit seinem subjektiven Empfinden zu beschreiben. Die Indikatoren sollten in Form von Fragebögen, bspw. als Online-Fragebögen im Intranet, den Nutzern angeboten werden.</td></tr>
<tr><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Transparenz</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.15</td><td>
Überwachung des Betriebssystems
Das Monitoring soll die Erfassung und Darstellung von verfügbarkeitsrelevanten Parametern des Betriebssystems, wie der Prozesstabelle, der Anzahl der Prozesse, der RAM-Auslastung, der CPU-Auslastung, der Systemzeit, der Uptime, der Auslastung des virtuellen Speichers (Page-File; Swap), der Auslastung des physikalischen Speichers, der Log-Dateien, der Gültigkeit bzw. des Status der Lizenzen sowie der verfügbaren Patches / Update beinhalten.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.16</td><td>
Überwachung eines Datenbankservers
Bei der Überwachung der Datenbankserver sind die wesentlichen Verfügbarkeitsparameter der Gültigkeit bzw. des Status der Lizenzen, der verfügbaren Patches / Updates, der Log-Dateien, der Funktionalität des Verbindungsaufbaus, der Dauer des Verbindungsaufbaus (Anfrage bis zur Antwort), der Funktionalität und Qualität der Anfragebearbeitung, der Anfragenbearbeitung, des verfügbaren (allozierten) Speicherplatzes, des belegten Speicherplatzes sowie des letzten Backups zu erfassen und darzustellen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*
VM.10.17	**Überwachung eines E-Mail-Servers** Zur Überwachung eines E-Mail-Servers kann ein Monitoring der verfügbaren Patches und Updates, der Log-Dateien, der Auslastung der zugehörigen Antivirus-/Antispam-Komponente, Status und Dauer des Verbindungsaufbaus zu einem POP3-Server, Funktionalität, Qualität und Dauer der Anfragebearbeitung durch einen POP3/SMTP/IMAP oder http(s)-Server sowie die Länge der Mailqueue durchgeführt werden.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung und Konzeption Betrieb	Automatismen	Reaktionszeit	Menschliches Versagen Sabotage, Manipulation Technische Ermüdung	HVK (Überwachung)

Nr.	*Maßnahmen*
VM.10.18	**Überwachung eines DBMS** Für die Überwachung eines DBMS können die aktiven Mechanismen der DBMS (z. B. Trigger) können genutzt werden, indem jede Datenmanipulation einen Trigger auslöst, der geänderte Datensätze in eine Datei oder eine andere Datenstruktur schreibt. Jedem Datensatz kann darüber hinaus ein Zeitstempel zugeordnet werden, der im Fall einer Änderung auf den Zeitpunkt der Änderung gesetzt wird. An Hand der Zeitstempel kann später entschieden werden, welcher Datensatz sich nach dem Zeitpunkt der letzten Extraktion geändert hat. Eine fortlaufende Überwachung der Datenobjekte und Services muss über eine feste Zeitdauer erfolgen. Eine ereignisbasierte Überwachung liefert darüber hianus detaillierte Informationen über Datenbanken, Tabellen, Deadlocks, Table Spaces, Buffer Pools, Connections oder Transaktionen.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung und Konzeption Betrieb	Automatismen	Reaktionszeit	Menschliches Versagen Sabotage, Manipulation Technische Ermüdung	HVK (Überwachung)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.19</td><td>
Überwachung Netzwerksoftware / -services
Die Überwachung der Netzwerkservices sollte die Funktionalität der DNS-Auflösung, die Dauer von DNS-Abfragen, die Korrektheit der Netzwerk-Uhrzeit, die Dauer der Beantwortung von NTP-Abfragen, die Anzahl der gerouteten Pakete bzw. die Auslastung der Router, die Anzahl der verworfenen Pakete, die Netzwerkantwortzeiten, die Hops zum Host, der Netzwerkdurchsatz bzgl. der Netzwerkbandbreite, der Durchsatz der Firewall, die Latenz der Firewall, die verworfenen (abgelehnten) Pakete der Firewall, die Latenz des VPN-Server, der ISAKMP- und IPSec-Status bzw. der Tunnelstatus sowie der Durchsatz des VPN-Services umfassen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.20</td><td>
Überwachung der Mitarbeiterqualifikation
Für das Monitoring der Qualifaktion der Mitarbeiter können der Bildungsgrad bzgl. Aus- und Fortbildung bzw. der Anteil von Mitarbeitern, die Bildungsmaßnahmen erhalten haben, die Bildungszeit bzw. der durchschnittliche Umfang von Aus- und Fortbildungsmaßnahmen in Tagen pro Mitarbeiter (z. B. 5 Tage pro Jahr und Mitarbeiter), die Weiterbildungsbereiche / -gebiete, die Spezialisierung sowie ISMS-Trainings herangezogen werden. Diese erlauben eine durchgängige Überwachung und Bewertung als Basis für eine Steuerung und Optimierung der Qualifikation der Mitarbeiter.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.21</td><td>
Überwachung der Personal-Fluktuation
Die Erfassung und geeignete Auswertung der Fluktuationsrate der Mitarbeiter kann Hinweise auf mögliche, die Verfügbarkeit beeinträchtigender Faktoren in der Mitarbeitermotivation sowie sich abzeichnende personelle Engpässe liefern.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.22</td><td>
Überwachung der Ressourcenplanung
Durch die Überwachung der Ressourcenplanung und die Erfassung wesentlicher Kenngrößen, wie z. B. der Personaldeckung, der Krankheitsquote, der Mitarbeitereinsatzplanung entsprechend der Geschäftszeiten, der Mitarbeitervertretungsregelungen, der Inspektions- und Wartungsplanung sowie der Mobilität bei dezentraler Administration oder des Ressourcen- und Bedarfsmanagements können Informationen über die Qualität und Leistungsfähigkeit der Ressourcenplanung gewonnen sowie Optimierungsprozesse überwacht und gesteuert werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.23</td><td>
Überwachung des Supports
Das Monitoring des Support durch die Erfassung und Auswertung von Kenngrößen, wie Realisierungszeit bis zur vollständigen Verfügbarkeit bei Supportanfragen / Störungen, der Anzahl der Supportanfragen pro IT-Service-Komponenten, der Anzahl der Supportmitarbeiter sowie der Supportsysteme und –prozesse ermöglicht die Überwachung der Support-Qualität sowie insbesondere deren Steuerung und Optimierung.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.24</td><td>
Überwachung der Festplatte(n)
Im Rahmen des Monitorings der Festplattensysteme sollte eine Überwachung der verfügbaren Festplattenkapazität, des Status der Festplatte(n), der Filesystem- bzw. Partitionskapazität sowie eine Prüfung der Integrität (Konsistenz) der Dateisysteme erfolgen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Sabotage, Manipulation
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.25</td><td>
Überwachung der externen Storageeinheiten
Zur Überwachung und frühzeitigen Störungserkennung sollte ein Monitoring der Kapazität externer Storageeinheiten, des Status der externen Storageeinheit, der verfügbaren Filesystem- bzw. Partitionskapazität sowie der Integrität (Konsistenz) von Speichermedien und Dateisystemen erfolgen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Sabotage, Manipulation
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.26</td><td>
Überwachung RAID-Systeme
Sofern innerhalb der HV-Architektur RAID-Systeme eingesetzt werden, sollte zu deren Überwachung ein Monitoring der pro Zeiteinheit gelesenen und geschriebenen Datenmengen (Belastung des RAID-Systems, I/O-Rate) sowie der Lesefehler und Schreibfehler pro Zeiteinheit erfolgen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*				
VM.10.27	**Überwachung Serverlüftung / -Kühlung** Im Rahmen des Health-Monitoring sollte eine Überwachung des Lüfters bzw. der Lüftergeschwindigkeit sowie der Systemtemperatur erfolgen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Betrieb	Automatismen	Reaktionszeit	Sabotage, Manipulation Technische Ermüdung Fehler in Hard- oder Software	HVK (Überwachung)
VM.10.28	**Überwachung Backup** Im Rahmen des Monitoring sollten eine Überwachung des Zeitpunkts des letzten Backups sowie der Aktualität des Backups und dessen Status erfolgen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Betrieb	Automatismen	Reaktionszeit	Menschliches Versagen Sabotage, Manipulation Technische Ermüdung Fehler in Hard- oder Software	HVK (Überwachung)

Nr.	*Maßnahmen*				
VM.10.29	**Überwachung Arbeitsspeicher (RAM)** Im Rahmen des Health-Monitoring sollte eine Überwachung des verfügbaren physikalischen Arbeitsspeichers erfolgen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Betrieb	Automatismen	Reaktionszeit	Technische Ermüdung Fehler in Hard- oder Software	HVK (Überwachung)
VM.10.30	**Überwachung Systemspannung** Im Rahmen des Health-Monitoring sollte eine Überwachung der Systemspannung und der Energieversorgung erfolgen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Betrieb	Automatismen	Reaktionszeit	Menschliches Versagen Sabotage, Manipulation Technische Ermüdung Fehler in Hard- oder Software	HVK (Überwachung)

Nr.	*Maßnahmen*				
VM.10.31	**Überwachung Unterbrechungsfreie Stromversorgung (USV)** Zur Durchführung des Monitorings der eingesetzten USV-Anlagen sollte eine Überwachung des Status der USV (z. B. unbekannt, normal, niedrig, entladen), der Spannung der USV, der Stromstärke der USV sowie des Ladezustands der USV erfolgen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Betrieb	Automatismen	Reaktionszeit	Menschliches Versagen Sabotage, Manipulation Technische Ermüdung Fehler in Hard- oder Software	HVK (Überwachung)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.32</td><td>Überwachung der Netzwerkkomponenten
Zur Überwachung und Störungserkennung der Netzkomponenten sollte eine Überwachung der Erreichbarkeit des Hosts, des Servers bzw. der externen Speichereinheit (RTA-Round Trip Average Time & PL-Package Loss), des operativen Status des Netzwerkinterfaces (Aufzählung: up, down, testing, dormant, notPresent, lowerLayerDown), des Statuswechsels, der Menge eingehender Daten (Last des Netzwerkinterfaces), der Anzahl fehlerhafter eingehender Pakete, der Menge ausgehender Daten, der Anzahl fehlerhafter ausgehender Pakete, des Link-Status von Ports sowie der Netzwerkkabel erfolgen.</td></tr>
<tr><td></td><td>
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.33</td><td>Einsatz eines Hardware-Watchdog
Durch den Einsatz dedizierter Hardwarebausteine zur Überwachung der Hardware eines Systems können zuverlässig Störungen bzw. sich abzeichnende Ausfälle von Systemkomponenten erkannt und kritische Systembausteine auf ihre Funktionsfähigkeit überwacht werden.</td></tr>
<tr><td></td><td>
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Überwachung)</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-1: Maßnahmenkatalog Monitoring: Überwachung

1.2 (Früh-) Erkennung

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.34</td><td>
Auswahl der Erkennungsmethode
Ereignisse müssen erkannt werden. Es muss definiert werden, ob das Erkennen manuell oder automatisch erfolgen soll. Das manuelle Erkennen erfordert eine ständige Beobachtung der Messgröße durch das Überwachungspersonal. Das eingesetzte Überwachungspersonal muss dahingehend fachkundig sein, die Messwerte interpretieren und ggf. entsprechend reagieren zu können. Im Rahmen des automatischen Erkennens kontrolliert i. d. R. Software die Messwerte und löst bei Abweichungen von Soll-Werten entsprechende Reaktionen aus.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen
Transparenz
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.35</td><td>
Darstellung der Messwerte
Für die Darstellung der Messwerte ist eine geeignete Visualisierungstechnik auszuwählen, die eine schnelle, aussagefähige Darstellung von Echtzeitdaten sowie die kurzfristige Erkennung und Lokalisierung von Beeinträchtigungen der Verfügbarkeit ermöglicht. Zu diesem Zweck sollten neben einfachen Visualisierungstechniken (z. B. tabellarische Darstellung) insbesondere auch grafische Visualisierungstechniken (z. B. Dashboard-, Cockpit-, Ampel- oder Thermometerdarstellung) eingesetzt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen
Transparenz
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.36</td><td>
Auswahl der Analysemethode
Zum automatisierten Erkennen müssen geeignete Analysemethoden ausgewählt werden. Im Rahmen des Monitorings muss eine Erhebung, Sammlung (z. B. durch Polling) und Protokollierung von historischen Daten als Grundlage für Trendanalysen und Berichte durchgeführt werden. Dabei werden u. a. Ressourcen- und Performance-Messdaten von Anwendungen, Datenbanken, Netzwerken und Systemen eingesammelt, protokolliert und zusammengefasst. Diese historischen Daten können anschließend statistischen Analyse- und Berichtsprogrammen zur Verfügung gestellt werden. Über die Konsolidierung hinaus müssen durch Analysen der Messwerte und Meldungen Zusammenhänge, Abhängigkeiten und zeitliche Entwicklungen aufgedeckt werden. Die Analysen sollen nicht nur zur Beurteilung der aktuellen Situation herangezogen werden, sondern dienen vielmehr zur Unterstützung einer mittel- bis langfristige Planung und Steuerung des IT-Designs. Die folgenden Analysemethoden stehen zur bspw. zur Verfügung: Schwellwertanalyse, Auswertung von Event-Logs, Ereigniskorrelation und Ursachenanalyse.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Transparenz
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.37</td><td>
Auswahl der Visualisierungstechnik
Für die Visualisierung der Monitoring-Informationen ist eine geeignete Visualisierungstechnik auszuwählen, die eine schnelle, aussagefähige Darstellung von Echtzeitdaten sowie die kurzfristige Erkennung und Lokalisierung von Beeinträchtigungen der Verfügbarkeit ermöglicht. Zu diesem Zweck sollten neben einfachen Visualisierungstechniken (z. B. tabellarische Darstellung) insbesondere auch grafische Visualisierungstechniken (z. B. Dashboard-, Cockpit-, Ampel- oder Thermometerdarstellung) eingesetzt werden. Neben der Darstellung von Echtzeitdaten sollten auch statistische Informationen erhoben und visualisiert werden, die auf der Erhebung von historischen Daten beruhen. Das Überwachungspersonal muss anhand eines übersichtlichen Lagebildes jederzeit den aktuellen Gesamtzustand eines IT-Systems erkennen können. Im Rahmen der Fehlerdiagnostik und Problemlösung können bei Bedarf weitere Informationen aus einer zentralen Konfigurations-Datenbank angezeigt werden. Über das aktuelle Lagebildes hinaus müssen auch langfristige Informationen in Form von Reports und Trends in geeigneter Form (wie z. B. Tabellen, Diagramme und Histogramme) visualisiert werden können.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen
Transparenz
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*
VM.10.38	**Auswahl der Alarmierungsmethode** Im HV-Umfeld verlangen Alarme des Monitoring-Systems eine kurzfristige Reaktion. Diese Reaktion kann automatisiert (z. B. Ausführung eines Skriptes) oder manuell (z. B. durch Administrationspersonal) stattfinden. Dies beinhaltet eine Benachrichtigung der erforderlichen Personen- bzw. Personengruppen über Warnungen, Alarme, Probleme und Fehler nach vorher definierten Regeln. Diese Benachrichtigung kann u. a. per Web, Pager, Blackberry, E-Mail erfolgen und an bestimmte Regeln, z. B. zeitliche Bedingungen, wie innerhalb und außerhalb der Arbeitszeit, an Sonn- und Feiertagen, gebunden sein. So sollte zum Beispiel bei Verfügbarkeitsverlust des IT-Services "E-Mail" keine Benachrichtigung per Email erfolgen. Weiterhin sollten die Benachrichtigungen entsprechend der negativen Auswirkungen des eingetretenen Events, z. B. als kritisch, klassifiziert werden können. Auch Eskalationsregeln sind dabei zu berücksichtigen. Bei der Konfiguration der Benachrichtigungsregeln sind die Policy-Vorgaben des Unternehmens bzw. der Organisation zu beachten. Die Benachrichtigungstexte müssen klar und verständlich definiert sein und dürfen keine irreführenden Aussagen enthalten.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung und Konzeption	Automatismen Skalierbarkeit Priorisierung	Überwachung Reaktionszeit	Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.39</td><td>
Einsatz von Früherkennung
Zur Erreichung hoher Verfügbarkeitsklassen müssen Prognosen, die es ermöglichen, Aussagen über das zukünftige Verhalten des IT-Systems oder der Komponenten zu geben, eingesetzt werden. Im Wesentlichen basieren die Prognosen auf Methoden der mathematischen Statistik, auf Simulation und Berechnungsmodellen. Die folgenden Methoden können bspw. eingesetzt werden: Richtlinien und Daumenregeln, Zeitreihenanalysen, Historische Daten, Trendanalyse, Lastsimulation und Modellierungsverfahren.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.40</td><td>
Einsatz von Data Mining
Der Einsatz von Data Mining ist dann erforderlich, wenn in den höchsten Verfügbarkeitsklassen eine „always up“ Verfügbarkeit realisiert werden muss. Um auf sämtliche Eventualitäten vorbereitet zu sein, müssen Methoden angewendet werden, die z. B. derzeit noch nicht bekanntes Verhalten des IT-Systems vorhersagen können.
Data Mining ist eine weitere Form der Früherkennung. Ziel des Data Mining ist es, neues, gültiges und handlungsrelevantes Wissen, ohne konkrete Fragestellung zu entdecken. Grundlagen des Data-Minings sind Methoden der deskriptiven und induktiven Statistik. Darauf setzen die eigentlichen Data Mining-Verfahren, wie künstliche neuronale Netze, Clustering-Verfahren, Diskriminanzanalysen, Multifaktorielle Regressionsanalyse, Einsatz genetischer Algorithmen usw. auf. Ziel dabei ist das Aufspüren von Regeln und Mustern bzw. statistischen Auffälligkeiten.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Redundanz
Autonomie</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.41</td><td>
Einsatz von Visueller Daten Exploration
Eine weitere Form des Data Minings ist die Visuelle Datenexploration. Die Grundidee der visuellen Datenexploration ist die geeignete Darstellung der Daten in visueller Form, um einen Einblick in die Struktur der Daten zu bekommen. Dies ermöglicht darüber hinaus Schlussfolgerungen aus den visualisierten Daten zu ziehen sowie direkt mit den Daten zu interagieren und Hypothesen über die Daten aufzustellen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Redundanz
Autonomie</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.42</td><td>
Durchführung von Insepktionen
Um Phänomene (früh-) zu erkennen, die das Monitoring-System nicht erkennen kann, weil bspw. für bestimmte Überwachungsbereiche keine Sensorik vorhanden ist oder es zu kostspielig oder sogar unmöglich ist, diese automatisch zu überwachen, müssen Inspektionen durchgeführt werden. Dazu muss ein Inspektions-Plan erstellt werden. Der Inspektions-Plan muss mindestens die zu inspizierenden Komponenten, einen Zeitplan sowie die dafür notwendigen Mitarbeiter beinhalten. Auf die im Rahmen der Inspektion erkannten Mängel muss geeignet reagiert werden. Die Mängel müssen z. B. in Form von Meldungen zur zentralen Monitoring-Infrastruktur übermittelt werden. Die Durchführung der Inspektion muss ebenso überwacht werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.43</td><td>
Erhebung von Historiedaten
Im Rahmen des Monitorings sollte ebenfalls eine Erhebung, Sammlung (z. B. durch Polling) und Protokollierung von historischen Daten als Grundlage für Trendanalysen und Berichte durchgeführt werden. Dabei werden u. a. Ressourcen- und Performance-Messdaten von Anwendungen, Datenbanken, Netzwerken und Systemen eingesammelt, protokolliert und zusammengefasst. Diese historischen Daten können anschließend statistischen Analyse- und Berichtsprogrammen zur Verfügung gestellt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.44</td><td>
Durchführung geeigneter Analysen
Über die Konsolidierung hinaus müssen durch Analysen der Messwerte und Meldungen Zusammenhänge, Abhängigkeiten und zeitliche Entwicklungen aufgedeckt werden. Die Analysen sollen nicht nur zur Beurteilung der aktuellen Situation herangezogen werden, sondern dienen vielmehr zur Unterstützung einer mittel- bis langfristige Planung und Steuerung des IT-Designs.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen
Autonomie</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.45</td><td>
Auswertung von Event-Logs
Das Monitoring sollte in jedem Fall auch eine Auswertung protokollierter Ereignisse ggf. unter Anwendung von Tools (z. B. SIEM-Tools – Security Information and Event Management) umfassen um im Rahmen einer Steuerung und Optimierung Ursachen für Störereignisse zu erkennen und zu beheben.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.46</td><td>
Ursachenanalyse
Die Grundlage für die im Rahmen des Monitorings durchzuführende Ursachenanalyse bildet der Erkennungsprozess (auch Discovery-Prozess genannt). Ziel der Ursachenanalyse ist die Reduzierung der Mean Time to Repair (MTTR) und die Erhöhung der Betriebseffizienz im Rahmen eines Steuer- und Optimierungsprozesses. Dabei werden voneinander abhängige Störungsströme untersucht. Die Ursachenanalyse für Probleme und Störungen kann automatisch-deterministisch erfolgen oder probabilistisch (wahrscheinlichkeitstheoretisch).
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.47</td><td>
Ereigniskorrelation (Event Correlation)
Ein Problem kann eine Flut von Ereignissen auslösen. Diese Flut von Ereignissen muss effizient verwaltet werden, um eine optimale Steuerung und letztendlich eine optimale Bearbeitung aller Ereignisse sicherstellen zu können. Dabei ist der Informationsinhalt von Ereignissen durch die Unterdrückung nicht gewollter, redundanter Events und das Hinzufügen neuer, mehr informativer Events mittels der Nutzung von Event-Reduzierung-Strategien (wie z. B. Deduplizierung) zu verbessern. Die Event-Correlation-Funktion setzt Ereignisse untereinander in Beziehung und dient der Entdeckung und Analyse komplexer Störeinflüsse.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*
VM.10.48	**Trendanalyse** Die Trendanalyse dient der Identifizierung von Trends und zur dynamischen Erkennung von Ressourcen- und Performance-Engpässen, die zu Verfügbarkeitsverlusten führen können, und damit zur Bestimmung der optimalen Konfiguration, der Ersetzung und /oder der Erweiterung der entsprechenden Komponenten. Dieses Verfahren trifft Vorhersagen basierend auf den gesammelten Historiedaten. Dazu werden Langzeitbeobachtungen der entsprechenden Komponenten mit Hilfe von Monitoring-Werkzeugen vorgenommen und die gewonnenen Daten werden entsprechend verdichtet. Häufig werden lineare Extrapolierungsansätze verwendet. Dieser Ansatz, den Zusammenhang zwischen Last und Performance-Maßen durch eine lineare Gleichung zu beschreiben, berücksichtigt allerdings nicht den rasanten Anstieg von Leistungsmaßen in der Nähe der Sättigungspunkte und berücksichtigt in der Regel auch nicht das Zusammenwirken unterschiedlicher Arbeitslasten.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Betrieb	Automatismen	Überwachung Reaktionszeit	Sabotage, Manipulation Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.49</td><td>
Analytische Modellierung
Die analytische Modellierung (Verifikation, stochastisch, deterministisch) beschreibt die Performance des IT-Service durch eine Reihe von Gleichungen. Das Performance-Verhalten wird durch mathematische Größen und Beziehungen zwischen ihnen beschrieben. Das analytische stochastische Modell berücksichtigt zufällig auftretende Ereignisse. Die Erstellung einer solchen Modellierung kann sehr aufwendig sein, da in der Regel eine Vielzahl von Abstraktionen, Vereinfachungen und Annahmen nötig ist, um das Performanceverhalten auf einige wenige Parameter zu reduzieren. Die Genauigkeit der Modellierung hängt sehr stark davon ab, wie genau sich die Realität durch die Modellierungselemente beschreiben lassen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.50</td><td>
Simulative Modellierung
Die simulative Modellierung (Black-Box-Test, deterministisch) beschreibt das Performanceverhalten mittels mathematischer Größen und Beziehungen zwischen ihnen. Diese Modelle beinhalten aber auch Größen, die sich in Abhängigkeit von der Zeit dynamisch ändern (Ereignis-diskret oder kontinuierlich). Sie ermöglichen genauere Performance-Ergebnisse als analytische Modelle, da sie mehr Details des realen IT-Service nachbilden kann. Sie ist in der Regel aufwendiger als die analytische Modellierung. Die simulative Modellierung sollte hauptsächlich zur Analyse und Bewertung von wichtigen Details eingesetzt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.51</td><td>Schwellwertanalyse mit festen Schwellwerten
Feste (auch fixe) Schwellwerte werden für einzelne, meist kritische, Komponenten (Messobjekte) der IT-Services anhand von Daumenregeln oder vereinbarten Service Level Agreements festgelegt. Die Erreichung der Schwellwerte wird im Rahmen der Überwachung geprüft. In der Regel werden zwei Schwellwerte pro Messobjekt definiert. Der erste Wert löst bei Erreichung eine Warnmeldung aus, der zweite einen Alarm. An die definierten Schwellwerte ist damit auch der Status des Messobjekts (der Komponente) geknüpft.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table></td></tr>
<tr><td>VM.10.52</td><td>Schwellwertanalyse mit dynamischen Schwellwerten
Einige Monitoringwerzeuge ermöglichen die dynamische Anpassung von Schwellwerten anhand von statistischen Verfahren (z. B. Standardabweichungen). Auch bei diesem Verfahren werden in der Regel zwei Schwellwerte bestimmt. Der erste Wert löst bei Erreichung eine Warnmeldung aus, der zweite einen Alarm. An den definierten Schwellwerten ist damit auch der Status des Messobjekts (der Komponente) geknüpft. Kombiniert wird dieses Verfahren mit festen Schwellwerten, die die Grenzen für die dynamische Anpassung nach oben bzw. nach unten hin, je nach Definition und Messparameter, darstellen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table></td></tr>
</table>

Tabelle 1-2: Maßnahmenkatalog Monitoring: Früherkennung

1.3 Reaktion

Nr.	*Maßnahmen*
VM.10.53	**Auswahl der Reaktionsart** Die durch den Alarm ausgelöste Reaktion muss innerhalb eines wohl definierten Fehlerbehandlungs- bzw. Eskalationsprozesses erfolgen. Es muss festgelegt werden, wie auf Alarme oder Meldungen aus der (Früh-) Erkennung reagiert werden soll. Die möglichen Reaktionsarten sind autonom, automatisch, manuell. Autonom bedeutet, dass IT-Systeme eigenständig die Verfügbarkeitsanforderungen realisieren. Die IT-Systeme erfüllen diese autonom (selbständig) und transparent für die Anwender. Eine Eigenschaft autonomer Systeme ist die s. g. Selbststabilisierung. Das System führt eine eigenständige, automatisierte Behebung von Fehlerzuständen durch. In diesem Fall sind keine weiteren Reaktionen durch das Überwachungspersonal oder der Instandsetzung notwendig. Die automatischen Reaktionen auf der Monitoring-Ebene sind häufig das automatisierte Ausführen von Skripten, das automatische Rekonfigurieren von Routern, das automatisierte Rebooten von Systemen oder der automatisierte „Umzug“ von virtualisierten Systemen auf andere Host-Systeme. Bei dieser Reaktionsart ist ein manuelles Eingreifen nicht notwendig, sie werden durch den Monitoring-Prozess (Früh-) Erkennung automatisch ausgelöst und ggf. werden die auslösenden Ereignisse zur Information des Überwachungspersonals angezeigt. Manuelles Eingreifen ist immer dann erforderlich, wenn Ereignisse aufgetreten sind, die sich durch automatische Reaktionen aufgrund der Fehlerart nicht korrigieren lassen oder eine automatische Reaktion nicht implementiert wurde. Hierzu zählen u. a. Totalausfälle von Systemen aufgrund von Hardware- oder Software-Problemen. Der so ausgelöste Alarm muss durch einen Prozess der Instandsetzung aufgefangen werden und adäquate Reaktionen müssen erfolgen.

Umsetzungsphase	Prinzip	Kriterien	wirkt gegen	Querverweis

Nr.	*Maßnahmen*				
	Planung und Konzeption	Automatismen Autonomie Priorisierung Separation	Überwachung Reaktionszeit	Menschliches Versagen Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)
VM.10.54	**Manuelle Reaktion** Manuelles Eingreifen ist immer dann erforderlich, wenn Ereignisse aufgetreten sind, die sich durch automatische Reaktionen aufgrund der Fehlerart nicht korrigieren lassen oder eine automatisierte Behandlung nicht vorgesehen. Die manuelle Reaktion muss zeitnah erfolgen. Dies bedeutet, dass das Administrations- und Instandsetzungspersonal mit entsprechender Fachkunde und in ausreichender Anzahl zur Verfügung stehen muss. Um den HV-Anforderungen gerecht zu werden müssen im Rahmen der Instandsetzung organisatorische Prozesse und Zuständigkeiten definiert werden, die im Fall einer Alarmierung eine geeignete Reaktion ermöglichen. Dafür müssen Einsatz- und Dienstpläne entwickelt werden, die neben der Fachkunde des Personals auch eventuelle Anreise- und Rüstzeiten berücksichtigen. Ein Personalkonzept, dass den Verfügbarkeitsanforderungen genügt, muss entwickelt werden. Gegebenenfalls muss auf externes Personal zurückgegriffen werden. Dazu müssen entsprechende SLAs getroffen werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung und Konzeption Betrieb	Separation	Überwachung Reaktionszeit	Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)

Nr.	*Maßnahmen*
VM.10.55	**Wartung** Die Wartung im HV-Umfeld dient in erster Linie zur Erhöhung der Zuverlässigkeit von Komponenten und damit zur Erhöhung der Gesamtverfügbarkeit eines IT-Systems. Die Wartung umfasst z. B. Nachstellen, Schmieren, funktionserhaltendes Reinigen, Konservieren, Nachfüllen oder Ersetzen von Betriebsstoffen oder Verbrauchsmitteln (z. B. Kraftstoff, Schmierstoff oder Wasser) und planmäßiges Austauschen von Verschleißteilen (z. B. Filter oder Dichtungen) oder ganzer Komponenten (z. B. Festplatten oder USV-Batterien) im Rahmen der manuellen Reaktion. Neben der Wartung von Komponenten muss auch die eingesetzte Software gewartet werden. Dazu zählt das Einspielen von Up-Dates, Up-Grades oder Patches. Für die zu wartenden Komponenten müssen Wartungspläne entwickelt werden. In den Wartungsplänen müssen die Wartungszyklen und die durchzuführenden Wartungsarbeiten festgelegt werden. Ferner müssen Rollen, und damit Mitarbeiter, bestimmt werden, die die Wartungsarbeiten ausführen. Die Festlegung der Wartungszyklen orientiert sich in erster Linie an den Vorgaben des Herstellers. Zudem sollten die durch das Monitoring erlangten Erkenntnisse in die Bestimmung der Zyklen und der durchzuführenden Arbeiten einfließen. Die Durchführung der Wartung muss durch einen Monitoring-Prozess überwacht werden.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung und Konzeption Betrieb	Redundanz Fehlertoleranz	Überwachung Reaktionszeit	Technische Ermüdung	HVK (Monitoring)

Tabelle 1-3: Maßnahmenkatalog Monitoring: Reaktion

1.4 Steuerung

Nr.	*Maßnahmen*
VM.10.56	**Entwicklung einer geeigneten Monitoring-Strategie, Planung und Auswahl der Monitoring-Szenarien** Die Monitoring-Strategie muss sich an den Verfügbarkeitsanforderung der Wirkumgebung orientieren. Je höher die Anforderungen, umso schneller müssen Ereignisse erkannt, auf erkannte Ereignisse reagiert oder Ereignisse sogar im Vorfeld verhindert werden. Es ist eine geeignete Monitoring-Strategie zu entwickeln, deren Ziel es ist, durch Überwachungsmethoden und -techniken in einem möglichst frühen Stadium Gefährdungen der Verfügbarkeit zu erkennen und Maßnahmen zu deren Beseitigung zu veranlassen.

Nr.	*Maßnahmen*				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung und Konzeption	Automatismen Autonomie Fehlertoleranz Redundanz Skalierbarkeit Separation	Überwachung Reaktionszeit Fehlermeldung Reifegrad	Menschliches Versagen Sabotage, Manipulation Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)
VM.10.57	**Bestimmung der Verfügbarkeitsanforderungen für das Monitoring-System** Auch für das Monitoring-System müssen Verfügbarkeitsanforderungen definiert werden. Das Monitoring-System dient nicht dem Selbstzweck, es trägt vielmehr zur Erreichung der angestrebten Verfügbarkeit des Wirksystems bei. Insbesondere bei hohen Verfügbarkeitsklassen ist die Verfügbarkeit des Monitoring-Systems entscheidend für die Gesamtverfügbarkeit. Die Abhängigkeiten des Wirksystems vom Monitoring-System müssen untersucht werden. Bei einer starken Abhängigkeit der Verfügbarkeit des Wirksystems von der Verfügbarkeit des Monitoring-Systems muss dass Monitoring-Systems mindestens genauso verfügbar sein wie das Wirksystem sein.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung und Konzeption	Fehlertoleranz Redundanz	Überwachung Reaktionszeit Fehlermeldung Reifegrad	Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.58</td><td>
Einsatz einer zentralen Monitoring-Infrastruktur
Es muss ein zentraler Log- oder Monitorserver zur Speicherung und Konsolidierung der anfallenden Monitoring-Daten betrieben werden. Die Aufgaben dieses Servers sind u. a. Entgegennahme von Überwachungs-Daten, sichere Archivierung der Überwachungs-Daten, übersichtliche Darstellung der aktuellen Situation und ggf. des Systemstatus, Erkennung und Visualisierung von Trends, Auswertung von Überwachungs-Daten z. B. anhand von Mustern und Regeln, automatische Alarmierung bei besonderen Ereignissen. Darüber hinaus kann dieser Server auch automatisierte Reaktionen auslösen.
Zur Erreichung höherer Verfügbarkeitsklassen muss die Monitoring-Infrastruktur Fehlertolerant (z. B. durch redundante Systeme) ausgelegt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Sabotage, Manipulation</td><td>HVK (Monitoring))</td></tr>
</table>
</td></tr>
<tr><td>VM.10.59</td><td>
Einsatz eines Intusion Detection System (IDS)
Zum Erreichen höherer Verfügbarkeitsklassen genügt es nicht, nur Ereignisse, die sich aufgrund von technischem Versagen ereignen, zu erkennen oder zu verhindern. Auch Ereignisse die auf einem Angriff auf das Netzwerk oder dessen Komponenten basieren und zu einem Verfügbarkeitsverlust führen, müssen erkannt oder verhindert werden. Ein IDS muss zur Erkennung oder Verhinderung von Angriffen eingesetzt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Überwachung
Reaktionszeit</td><td>Sabotage, Manipulation</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.60</td><td>
Überwachung in virtuellen Umgebungen
Zur Überwachung virtueller Umgebungen müssen die Besonderheiten dieser Technik berücksichtigt werden. Das Monitoring muss sowohl aus physikalischer Sicht (Host-Systeme) als auch aus virtueller Sicht (Guest-Systeme) erfolgen. Nur die gemeinsame Überwachung beider Welten kann einen Aufschluss über das Verhalten und der Performance des „sichtbaren“ Systems geben.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Skalierbarkeit
Separation</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.61</td><td>
Überwachung im WAN
Die Besonderheiten eines WANs müssen bei dessen Überwachung berücksichtigt werden. Bei einem Leitungs- oder Komponentenausfall kann via WAN nicht mehr steuernd reagiert werden. Komponenten wie Router müssen bspw. in solchen Fällen autonom handeln und neue Wege (Routen) im Netz finden (BGP).
Neben der reinen Komponentenüberwachung des WANs muss auch dessen Performance überwacht werden. Dies kann dadurch erfolgen, dass die Verkehrsmessung im Durchfluss erfolgt. Ist dies, z. B. in Fremd-Netzen, nicht möglich, muss die Performance-Messung indirekt durch aktives Injizieren von Probepakten erfolgen. Dazu müssen u. a. geeignete Injektionsstellen bestimmt werden.
Werden von einem Netzbetreiber Überwachungsdaten zur Verfügung gestellt, müssen diese in das eigenen Monitoring-System integriert werden.
Die möglicherweise auftretenden langen Anreise- und Rüstzeiten müssen im Rahmen der Reaktion berücksichtigt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Implementierung
Betrieb</td><td>Automatismen
Autonomie
Redundanz</td><td>Überwachung
Reaktionszeit</td><td>Technische Ermüdung
Fehler in Hard- oder Software</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*				
VM.10.62	**SLA-Monitoring** Werden bestimmte Dienste im Outsourcing betrieben, muss die Einhaltung der vereinbarten Service-Parameter überwacht werden. Die Überwachung der Service-Parameter sollte idealer weise in die zentrale Monitoring-Infrastruktur integriert werden. Die SLA-Überwachung kann bspw. mittels Endanwender-Monitoring erfolgen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung und Konzeption Implementierung Betrieb	Automatismen Separation	Überwachung Reaktionszeit	Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)
VM.10.63	**Nutzung von ITIL-Tools** Sind in einer Organisation ITIL Management-Prozesse definiert und existiert eine dafür vorgesehene Konfigurations-Datenbank (CMDB), sollte diese im Rahmen des Monitoring genutzt werden. Die CMDB enthält i. d. R. Informationen die für eine Fehlerdiagnostik und Problemlösung herangezogen werden können.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung und Konzeption Betrieb	Redundanz Separation	Überwachung Reaktionszeit	Technische Ermüdung Fehler in Hard- oder Software	HVK (Monitoring)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.10.64</td><td>
Planung der Alarmierung und Eskalation
Im HV-Umfeld verlangen Alarme des Monitoring-Systems eine kurzfristige Reaktion. Diese Reaktion kann automatisiert (z. B. Ausführung eines Skriptes) oder manuell (z. B. durch Administrationspersonal) stattfinden. Die durch den Alarm ausgelöste Reaktion muss innerhalb eines wohldefinierten Fehlerbehandlungs- bzw. Eskalationsprozesses erfolgen. Dies beinhaltet eine Benachrichtigung der erforderlichen Personen- bzw. Personengruppen über Warnungen, Alarme, Probleme und Fehler nach vorher definierten Regeln. Diese Benachrichtigung kann u. a. per Web, Pager, Blackberry, E-Mail erfolgen und an an bestimmte Regeln, z. B. zeitliche Bedingungen, wie innerhalb und außerhalb der Arbeitszeit, an Sonn- und Feiertagen, gebunden sein. So sollte zum Beispiel bei Verfügbarkeitsverlust des IT-Services "E-Mail" keine Benachrichtigung per Email erfolgen. Weiterhin sollten die Benachrichtigungen entsprechend der negativen Auswirkungen des eingetretenen Events, z. B. als kritisch, klassifiziert werden können. Auch Eskalationsregeln sind dabei zu berücksichtigen. Bei der Konfiguration der Benachrichtigungsregeln sind die Policy-Vorgaben des Unternehmens bzw. der Organisation zu beachten. Die Benachrichtigungstexte müssen klar und verständlich definiert sein und dürfen keine irreführenden Aussagen enthalten.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
<tr><td>VM.10.65</td><td>
Planung einer geeigneten (automatischen) Reaktion im Fehler(stör)fall
Im HV-Umfeld muss sichergestellt sein, dass Alarme nicht ins Leere laufen und dass durch fachkundiges Personal sowohl kurzfristige als auch langfristige Reaktionen erfolgen. Zur Sicherstellung der hohen Verfügbarkeit müssen auf allen Reaktionsebenen entsprechende Eskalationspfade und –mechanismen definiert werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Betrieb</td><td>Automatismen</td><td>Reaktionszeit</td><td>Menschliches Versagen
Sabotage, Manipulation
Technische Ermüdung</td><td>HVK (Monitoring)</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-4: Maßnahmenkatalog Monitoring: Steuerung