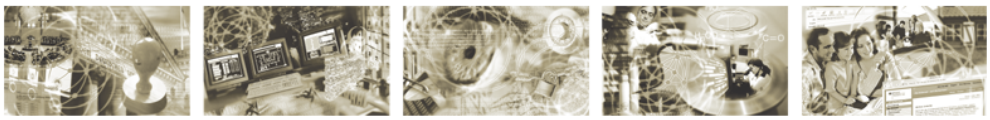
Bundesamt
für Sicherheit in der
Informationstechnik



Band M, Kapitel 3: Netzwerk

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

Tabellenverzeichnis

1 Netzwerk

Die nachfolgenden Maßnahmenkataloge beschreiben Maßnahmen im Sinne von Verfahren und Lösungen für die Realisierung hoch verfügbarer Netzwerkarchitekturen. Dies umfasst die folgenden Subdomänen:

- Komponenten
- Leitungsführung
- Protokolle
- Architekturen

1.1 Komponenten

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td>VM 3.1</td><td colspan="5">Einsatz hochwertiger Kabel und Lichtwellenleiter
Der Einsatz hochwertiger Kabel und Lichtwellenleiter gewährleistet garantierte Datenraten auf einem hohen Niveau (z. B. CAT-5-6-7). Die Beschaffung sowie der Einsatz solcher hochwertiger Komponenten in der Verkabelung tragen zur Zuverlässigkeit und Robustheit der Netzinfrastruktur bei.</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>Beschaffung
Implementierung</td><td>Robustheit</td><td>Durchsatz
EMV
Klimabeständigkeit</td><td>Technische Ermüdung
Fehler in Hard oder Software</td><td>HVK (Netzwerk)</td></tr>
<tr><td>VM 3.2</td><td colspan="5">Verwendung entstörter Geräte im Gebäude
Der Betrieb nicht ordnungsgemäß entstörter Geräte in Gebäuden (auch im Umfeld der Betriebsumgebung) kann Einfluss auf die Übertragungsqualität einer kabellosen Übertragung haben. Daher sollten nur ordnungsgemäß entstörte Komponenten beschafft und installiert werden. (z. B. Aufzug, Klimatisierung, Lüftung, etc.) um die Zuverlässigkeit und Betriebssicherheit der technischen Infrastruktur nicht durch Störeinflüsse zu beeinträchtigen.</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>Beschaffung</td><td>Robustheit</td><td>EMV</td><td>Sabotage
Manipulation
Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM 3.3</td><td>
Einsatz von Fibre Channel oder iSCSI.
In vielen Teilbereichen der HV-Architektur sind harte Garantien für den Netzdurchsatz nötig. Um diese zu erreichen, stehen spezialisierte Übertragungsprotokolle wie Fibre Channel oder iSCSI zur Verfügung, die einen hohen Durchsatz bei guter Zuverlässigkeit sicherstellen 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

Beschaffung</td><td>Robustheit

Fehlertoleranz</td><td>Durchsatz</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)

HVK (Storage)</td></tr>
</table>
</td></tr>
<tr><td>VM 3.4</td><td>
Einsatz von Fibre Channel-Switches
In SANs müssen Fibre Channel-Switches (FC-Switches) eingesetzt werden. Sie bilden das Rückgrat eines SANs, steuern den Datenfluss bei hohem Durchsatz und sind für die reibungslose und zuverlässige Kommunikation innerhalb des SANs verantwortlich.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>Wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption

Beschaffung</td><td>Robustheit

Fehlertoleranz</td><td>Durchsatz</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)

HVK (Storage)</td></tr>
</table>
</td></tr>
<tr><td>VM 3.5</td><td>
Einsatz von Switches für Punkt-zu-Punkt-Verbindung
Um die technologieimmanente Gefahr von Kollisionen zu vermeiden, müssen leistungsstarke Switches eingesetzt werden, die praktisch eine Punkt-zu-Punkt-Verbindung zwischen den Netzgeräten herstellen. Durch die Vermeidung von Kollisionen werden sowohl die Zuverlässigkeit als auch der Durchsatz der Netzkommunikation erhöht..
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>Wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption

Beschaffung</td><td>Robustheit

Fehlertoleranz</td><td>Durchsatz</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*				
VM 3.6	**Einsatz von NICs mit Diagnoseeinheiten** Es müssen NICs beschafft und eingesetzt werden, welche mittels Diagnoseschnittstellen die Funktionsbereitschaft (etwa ein Carrier-Signal) an das darüber liegende Betriebssystem melden und so den Einsatz von Automatismen im Monitoring erlauben.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Beschaffung	Automatismen	Überwachung	Fehler in Hard- oder Software	HVK (Netzwerk)
VM 3.7	**Einrichtung breitbandiger Uplinks der Switche mittels Trunking** Die breitbandigen Uplinks der Switche dürfen nicht nur über einen einzelnen Port erfolgen, sondern müssen über mehrere Ports miteinander gekoppelt werden. Dieses oft Trunking genannte Verfahren ermöglicht es dem Switch, die Verbindungen über mehrere Ports und mehrere physikalische Medien gleichzeitig zu führen. Darüber hinaus muss eine Logik zum Erkennen und Ausführen eines (Echtzeit-) Fail-Overs bereits im Switch realisiert (Hot-Stand-By). Durch diese Redundanz können SPoF vermieden werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption	Redundanz	SpoF	Fehler in Hard- oder Software	HVK (Netzwerk) Ref.
VM 3.8	**Einsatz von SSL-Proxies** Zur Erlangung einer Session-Transparenz verschlüsselter Sitzungen müssen SSL-Proxies eingesetzt werden. Diese erlauben bei einem Fail-Over redundanter Server im Cluster eine Fortführung bestehender Sessions und führen zu einer Minimierung der Aktivierungszeit der Redundanz.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption	Redundanz	Aktivierungszeit	Fehler in Hard- oder Software	HVK (Netzwerk)

Nr.	*Maßnahmen*				
VM 3.9	**Einsatz von Layer-4-Switches** Als präventive Maßnahme zur transparenten Lastverteilung sollten Layer-4-Switches eingesetzt werden, da sie eine Ende-zu-Ende-Betrachtung von Sitzungen gewährleisten können. Sie sind allerdings häufig nur für fest definierte Protokolle, wie insbesondere HTTP verfügbar. Sie erhöhen die Zuverlässigkeit sowie den Durchsatz der über das Protokoll abgewickelten Kommunikation.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption Beschaffung	Robustheit Fehlertoleranz	Durchsatz	Fehler in Hard- oder Software	HVK (Netzwerk)

Tabelle 1-1: Maßnahmenkatalog Netzwerk: Komponenten

1.2 Leitungsführung

Nr.	*Maßnahmen*				
VM 3.10	**Errichtung redundanter Netzanschlüsse** Topographisch sind geswitchte Netze zunächst sternförmig angeordnet, d. h. alle Server im Segment sind in der Regel an einem Switch zentral gekoppelt. Dies führt jedoch klassisch zu einem SPoF und ist daher zu vermeiden. Für Server-Systeme sollen idealerweise pro IT-System mehrere redundante Netzanschlüsse vorgesehen werden, die über dedizierte Kabel zu unabhängigen Switches führen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption Beschaffung	Redundanz	SpoF	Fehler in Hard- oder Software	HVK (Netzwerk)

Nr.	*Maßnahmen*				
VM 3.11	**Herstellung wechselseitiger Raumverkabelung** Eine wechselseitige Raumverkabelung der Client-Systeme zur Vermeidung von SPoF mittels unabhängiger Switches muss hergestellt werden. So können die Server bei Ausfall eines Switches noch von der verbleibenden Hälfte der Clients erreicht werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption	Redundanz	SpoF	Fehler in Hard- oder Software	HVK (Netzwerk)
VM 3.12	**Unterschiedliche Wegstrecken der Kabelführung** Um die Gefahr der Nichtverfügbarkeit durch mechanische Unterbrechungen der Kabelführung zu minimieren, müssen unterschiedliche Wegstrecken der Kabelführung durch redundante Verkabelung realisiert und SPoF vermieden werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption Implementierung	Redundanz	SpoF Strukturell	Naturkatastrophen Menschliches Versagen	HVK (Netzwerk)
VM 3.13	**Einsatz alternativer Übertragungsstrecken/-technik** Zur Wiederherstellung einer Verbindung sollte eine alternative Übertragungsstrecke und Übertragungstechnik eingerichtet werden (z. B. Richtfunk, Wireless LAN nach IEEE 802.11a/b/g und WiMax). Die Diversität der eingesetzten Redundanz erhöht die Zuverlässigkeit der Kommunikation und reduziert die Gefahr der Kommunikationsstörung durch den Ausfall einer Strecke bzw. einer Kommunikationstechnik.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption Beschaffung Implementierung	Redundanz	SpoF Diversität	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Netzwerk)

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td>VM 3.14</td><td colspan="5">Erzeugung von Mehrpfadigkeit durch Switch-Redundanz
Zur Realisierung einer Pfadredundanz müssen mehrere Switche eingesetzt werden, die es ermöglichen, alternative Pfade zwischen zwei Netzgeräten anzubieten.
<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>Redundanz</td><td>SpoF</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table></td></tr>
<tr><td>VM 3.15</td><td colspan="5">Errichtung redundanter Trassenführung
Redundante Trassenführung bedeutet eine parallele, aber unabhängige Topographie der Übertragungsmedien. So können Kabel unterschiedlich geführt werden. Dabei kann die Topologie auch über unterschiedliche Vermittlungsstellen erfolgen. Sehr wirkungsvoll ist hier die Ringtopologie, da von jedem Standort zu jedem anderen Standort stets zwei Wege bei geringem Aufwand bereitstehen. Auch bei Richtfunk oder Satellitenfunk ist eine Verbindung zu verschiedenen Vermittlungssystemen denkbar. Richtfunkstrecken können bei Einsatz von Relais über topographisch unterschiedliche Trassen geführt werden. Durch diese Redundanz werden SPoF vermieden sowie die Anfälligkeit der Kommunikationsarchitektur gegenüber Störeinflüssen reduziert.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>Wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Beschaffung
Implementierung</td><td>Redundanz</td><td>SpoF</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation
Technische Ermüdung

Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table></td></tr>
</table>

Nr.	*Maßnahmen*				
VM 3.16	**Entwicklung eines Hierarchiekonzepts für alternative Kommunikationswege** Es muss eine hierarchische Architektur der alternativen Kommunikationsgesamtlösung entwickelt werden, die in Abhängigkeit von der durch die Kommunikation zu überbrückende Distanz unterschiedliche Basis-Technologien zum Einsatz bringt. Den hierbei zum Einsatz kommenden Basis-Technologien liegt hierbei eine Clusterung der Kommunikation hinsichtlich bestimmter Hierarchie-Ebenen zugrunde, die sich an der räumlichen Lokation orientiert. Durch geeignete Auswahl und Separation der Kommunikationswege können so SPoF vermieden und die Aktivierungszeit der Redundanz im Fehlerfall erheblich reduziert werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption Beschaffung Implementierung	Redundanz	SpoF	Naturkatastrophen Menschliches Versagen Sabotage Manipulation Technische Ermüdung Fehler in Hard- oder Software	HVK (Netzwerk)

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td>VM 3.17</td><td colspan="5">Verwendung alternativer Übertragungsmedien
Es müssen Alternativmedien verwendet werden, welche unempfindlich gegen eine oder mehrere Gefährdungen des im Normalbetrieb genutzten Übertragungsmediums sind. Die implementierte Redundanz sollte eine weitestmögliche Diversität aufweisen.</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

Beschaffung</td><td>Redundanz</td><td>SpoF</td><td>Fehler in Hard- oder Software
Naturkatastrophen
Sabotage
Manipulation
Fehler in Hard oder Software</td><td>HVK (Netzwerk)</td></tr>
<tr><td>VM 3.18</td><td colspan="5">Vermeidung von Lagehinweisen
Kommunikationskabel müssen so verlegt werden, dass keine unmittelbaren Lagehinweise ersichtlich sind. Die Vermeidung von Lagehinweisen dient zur Erschwerung von gezielten Angriffen auf die Übertragungsmedien. Zu dieser Maßnahme gehört auch die unauffällige Installation von technischem Equipment im Freien oder an entfernten Orten (z. B. Relais).</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
Beschaffung

Implementierung</td><td>Robustheit</td><td>Resistent</td><td>Sabotage
Manipulation</td><td>GSK M 1.12</td></tr>
</table>

Tabelle 1-2: Maßnahmenkatalog Netzwerk: Leitungsführung

1.3 Protokolle

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td rowspan="3">VM 3.19</td><td colspan="5">Verwendung von Spanning-Tree-Protocol (STP)
Das Spanning-Tree-Protocol (STP, IEEE Std 802.1D-2004) wird zur Vermeidung von Netzwerkblockaden verwendet und erlaubt darüber hinaus mittels Heartbeat-Mechanismus und HELLO-Paketen die Auswahl alternativer Pfade.</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>Redundanz</td><td>SpoF</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
<tr><td rowspan="3">VM 3.20</td><td colspan="5">Verwendung von RSTP oder MSTP
Es können verbesserte Alternativen zu STP eingesetzt werden, welche die Konvergenzzeit deutlich reduzieren. Mit RSTP (IEEE 802.1w) und MSTP (IEEE 802.1s, besonders im Umfeld des Einsatzes von VLANs) wurden leistungsfähigere Nachfolger entworfen, die eine durchschnittliche Fail-Over-Zeit von circa einer Sekunde ermöglichen.</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>Redundanz</td><td>Aktivierungszeit</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table>

Nr.	*Maßnahmen*				
VM 3.21	**Dynamisches Routing mit BGP (äußeres Fail-Over)** Die Wegewahl zwischen Übergabepunkten von Autonomen Systemen kann über spezialisierte Protokolle wie dem Exterior Gateway Protocol (EGP) bzw. seiner fast ausschließlich anzutreffenden Realisierung durch das Border Gateway Protocol (BGP) realisiert werden (s. RFC 1654 (BGP-4)). Durch die Verwendung dieser Protokolle wird auch ein dynamisches Routing ermöglicht, welches die Zusendung von Datenpaketen über verschiedene Service Provider ohne Änderung der IP-Adressen erlaubt. So kann eine erhebliche Reduzierung der Aktivierungszeit im Fehler- bzw. Störfall erreicht werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption	Redundanz	Aktivierungszeit	Fehler in Hard- oder Software	HVK (Netzwerk)

Tabelle 1-3: Maßnahmenkatalog Netzwerk: Protokolle

1.4 Architekturen

Nr.	*Maßnahmen*				
VM 3.22	**Entwicklung eines Router Cluster** Bei einem Router Cluster werden zwei oder je nach Verfügbarkeitsanforderungen mehrere funktional gleichartige Router mit jeweils eigenen IP-Adressen in einem Subnetz aufgebaut. Zusätzlich wird eine virtuelle IP-Adresse vergeben, die funktional den gesamten Cluster abbildet, unabhängig davon, welcher Cluster-Knoten gegenwärtig aktiv ist. Die einzelnen Knoten stehen über ein Heartbeat-Protokoll in dauerhaftem Kontakt. Fällt der aktive Knoten aus, so übernimmt ein bis dahin passiver Knoten innerhalb kürzester Zeit die IP-Adresse des Clusters.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**Wirkt gegen**	**Querverweis**
	Planung und Konzeption Beschaffung	Redundanz	Aktivierungszeit	Fehler in Hard- oder Software	HVK (Netzwerk)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM 3.23</td><td>Fail-Over-Protokolle (internes Fail-Over)
Zur Realisierung eines Cluster-internen Fail-Overs können die folgenden Fail-Over-Protokolle verwendet werden: VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Stand-By Routing Protocol) oder in begrenztem Umfang CARP (Common Address Redundancy Protocol).
<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>Aktivierungszeit</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table></td></tr>
<tr><td>VM 3.24</td><td>Errichtung von Round Robin DNS
Wenn Web-Server in einem Cluster betrieben werden, muss erreicht werden, dass eine gleichmäßige Verteilung der Web-Anfragen mittels HTTP (Hypertext Transfer Protocol) stattfindet. Im Domain Name Service können zu diesem Zweck unter einem Namen mehrere IP-Adressen abgelegt werden. Diese werden theoretisch in undeterministischer Weise bei Abfragen zurückgeliefert und führen zu einer Lastverteilung.
<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>Aktivierungszeit</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM 3.25</td><td>
Errichtung einer Cluster-fähigen Firewall
Eine Firewall muss umfangreiche Statusinformationen sammeln, die sie für ihre Funktionsweise benötigt. Die innerhalb der HV-Architektur eingesetzte Firewall muss cluster-fähig sein, d. h. sie muss Status- und Zustandsinformationen mit den weiteren Firewalls im Cluster austauschen können. Im Fail-over muss eine andere Firewall im Cluster die Steuerung der Sitzung mit einer für den Benutzer hinreichenden Sitzungstransparenz innerhalb kürzester Zeit übernehmen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>Wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption

Beschaffung</td><td>Redundanz</td><td>Aktivierungszeit</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table>
</td></tr>
<tr><td>VM 3.26</td><td>
Redundanz statischer Schlüssel im Gateway-Cluster
Statische Schlüssel (Preshared Keys, PSK) müssen optimalerweise schon a priori auf die Stand-By-Systeme aufgebracht werden, damit diese bei einem Fail-Over unmittelbar eingesetzt 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>Redundanz</td><td>Aktivierungszeit</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM 3.27</td><td>Einsatz eines DNS Baum-Cluster
Bei DNS-Servern sollte das Konzept des „Versteckten Primärservers“ (Hidden primary) verwendet werden. Von dem Primär-Server erfolgt hierbei ein Zonentransfer auf alle Sekundär-Server, die so alle auf dem gleichen Stand gehalten werden und die Client-Anfragen bearbeiten. Es handelt sich dabei um eine Ausprägung eines Baum-Clusters, bei dem jedoch auf den Wurzel-Knoten nicht zugegriffen wird.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>Wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption

Beschaffung

Implementierung</td><td>Redundanz</td><td>SpoF</td><td>Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table></td></tr>
<tr><td>VM 3.28</td><td>Bildung von logischen Netzsegmenten (VLAN)
Zur Vermeidung von Überlastung und zur Optimierung der Verfügbarkeit kann ein bestehendes einzelnes physisches Netzwerk in mehrere logische Netzwerke (Virtuelles LAN, sog. VLAN) aufgeteilt werden. Mittels VLANs ergibt sich die Möglichkeit, Gruppen ohne Eingriff in die physikalische Vernetzung dynamisch und zeitnah neu zu bilden bzw. umzugruppieren. Aufgrund der systembedingt verwendeten Netzkomponenten sind VLANs robust gegen spezielle Gefährdungen hinsichtlich der Vertraulichkeit.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>Wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung und Konzeption
Beschaffung
Konzeption</td><td>Separation
Priorisierung</td><td>Verkehrsvorrangklassen</td><td>Sabotage
Manipulation
Fehler in Hard- oder Software</td><td>HVK (Netzwerk)</td></tr>
</table></td></tr>
</table>

Tabelle 1-4: Maßnahmenkatalog Netzwerk: Leitungsführung