|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Load-Balancer"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300063 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Load-Balancer" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc87632281)

[Dokumentenhistorie 3](#_Toc87632282)

[Inhaltsverzeichnis 4](#_Toc87632283)

[Allgemeine Festlegungen 6](#_Toc87632284)

[Ziel / Zweck 6](#_Toc87632285)

[Geltungsbereich 6](#_Toc87632286)

[Zuständigkeiten 7](#_Toc87632287)

[Genehmigungs- und Änderungsverfahren 7](#_Toc87632288)

[Aufbau des Dokuments 7](#_Toc87632289)

[Sicherheitsrichtlinie „Load-Balancer " 8](#_Toc87632290)

[Basismaßnahmen 8](#_Toc87632291)

[Festlegung einer Strategie für die Nutzung von Load-Balancern (NET.bd.1.A1) 8](#_Toc87632292)

[Beschaffung von Load-Balancern (NET.bd.1.A2) 8](#_Toc87632293)

[Einsatz von geschultem Personal (NET.bd.1.A3) 8](#_Toc87632294)

[Nutzung von funktionalen Erweiterungen (NET.bd.1.A4) 9](#_Toc87632295)

[Sicheres Betriebssystem und sichere Basiskonfiguration (NET.bd.1.A5) 9](#_Toc87632296)

[Installation, Konfiguration, Administration (NET.bd.1.A6) 9](#_Toc87632297)

[Protokollierung (NET.bd.1.A7) 10](#_Toc87632298)

[Betriebshandbuch für die Load-Balancer (NET.bd.1.A8) 10](#_Toc87632299)

[Sicherung der System-Konfiguration (NET.bd.1.A9) 11](#_Toc87632300)

[Verhaltensregeln bei Load-Balancer-Sicherheitsvorfällen (NET.bd.1.A10) 11](#_Toc87632301)

[Einsatz von Virtualisierungstechniken (NET.bd.1.A11) 11](#_Toc87632302)

[Implementierung von Heartbeats (NET.bd.1.A12) 11](#_Toc87632303)

[Einsatz von TLS -Offloading (NET.bd.1.A13) 11](#_Toc87632304)

[Standardmaßnahmen 11](#_Toc87632305)

[Zusätzlicher Schutz der Administrationsschnittstellen (NET.bd.1.A14) 12](#_Toc87632306)

[Berechtigungsmanagement in der Load-Balancer-Infrastruktur (NET.bd.1.A15) 12](#_Toc87632307)

[Regelmäßige Sicherheitschecks der Load-Balancer-Infrastruktur (NET.bd.1.A16) 12](#_Toc87632308)

[Administration über ein abgetrenntes Managementnetz (NET.bd.1.A17) 12](#_Toc87632309)

[Schutz vor DoS- und DDoS-Angriffen (NET.bd.1.A18) 12](#_Toc87632310)

[Vermeidung von Overlay-Technologien (NET.bd.1.A19) 12](#_Toc87632311)

[Einsatz von cloudbasierten Infrastrukturmanagementlösungen (NET.bd.1.A20) 13](#_Toc87632312)

[Maßnahmen bei erhöhtem Schutzbedarf 13](#_Toc87632313)

[Erweiterter Integritätsschutz für die Konfigurationsdateien (NET.bd.1.A21 - I) 13](#_Toc87632314)

[Zentrale Protokollierung (NET.bd.1.A22 - CI) 13](#_Toc87632315)

[Verwendung einer Hochverfügbarkeitslösung (NET.bd.1.A23 - A) 13](#_Toc87632316)

[Bandbreitenmanagement für kritische Anwendungen und Dienste (NET.bd.1.A24 - A) 14](#_Toc87632317)

[Vermeidung von Verknüpfungen von Sicherheitsbereichen (NET.bd.1.A25 - CIA) 14](#_Toc87632318)

# Allgemeine Festlegungen

## Ziel / Zweck

Ausgehend von der Leitlinie zur Informationssicherheit sind die wesentlichen Kernaspekte für einen sicheren Betrieb von Systemen einer Netzinfrastruktur zu konkretisieren. Das vorliegende Dokument definiert verbindliche Vorgaben für Load-Balancer.

Durch Loadbalancing sollen folgende Effekte erzielt werden:

* Vermeidung von Gesamtausfällen von angebotenen Diensten bei Server-Wartungsarbeiten oder deren technischem Versagen
* Verbesserte Antwortzeiten der angebotenen Dienste
* Verbesserte Dimensionierung und Skalierbarkeit der Serversysteme
* Geeigneter Einsatz von Overflow-Servern für zusätzliche Service-Verbindungen
* Informationsauswertung aus der Anwendungs-Schicht des OSI-Modells bzw. der Datenteil der IP-Pakete, die für eine weitergehende Art der Lastverteilung herangezogen werden

Dabei sind folgende Einsatzzwecke für Load-Balancer möglich:

* Platzierung vom Load-Balancer zum Zwecke der Lastverteilung
* Platzierung vom Load-Balancer zur Verbesserung der Ausfallsicherheit von nachgelagerten Infrastrukturen.
* Platzierung vom Load-Balancer zum Schutze von DoS und DDOS
* Platzierung vom Load-Balancer in public Cloud-Infrastrukturen zur Realisierung von Cluster-Mechanismen (z. B. der Firewalls)

Aus diesen Einsatzzwecken ergeben sich unterschiedliche Gefährdungen für den Einsatz und den Betrieb von Load-Balancern, welche bei der Planung und Umsetzung von entsprechenden Maßnahmen berücksichtigt werden müssen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Load-Balancer“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Load-Balancer "

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Festlegung einer Strategie für die Nutzung von Load-Balancern (NET.bd.1.A1)

Die <Institution> muss eine angemessene Strategie für die Nutzung von Load-Balancern festlegen. Mindestens sind folgende Anforderungsaspekte zu berücksichtigen:

* Einsatzweck
  + Lastverteilung
  + Ausfallsicherheit von nachgelagerten Infrastrukturen
  + Zum Schutze von DoS und DDOS
  + Zur Realisierung von Cluster-Mechanismen in public Cloud-Infrastrukturen (z. B. der Firewalls)
  + Zur Anbindung der PaaS an die IaaS
* Homogenität der Load-Balancer-Komponenten (z. B. Anzahl der Hersteller und Modelle)
* Anzubindende IT-Systeme (private oder public Cloud)
* Zu erfüllende Segmentierungsanforderungen (Load-Balancer-Virtualisierung)
* Vertraulichkeit, Integrität und Verfügbarkeit
* Zu verwendende Protokolle (ISO – Layer 4 bis 7)

### Beschaffung von Load-Balancern (NET.bd.1.A2)

Vor der Beschaffung der Load-Balancer wird eine Anforderungsliste erstellt. Anhand den dort festgelegten Anforderungskriterien werden die am Markt bzw. vom Cloud-Dienstleister erhältlichen Produkte auf ihre Eignung in der Datacenter-Infrastruktur bewertet. Empfehlenswert ist zusätzlich die Durchführung eines Proof of Concept (PoC).

In der Anforderungsliste sind mindestens folgende Kriterien abzubilden:

* Grundlegende funktionale Anforderungen
* Sicherheit
* Wartbarkeit
* Zuverlässigkeit/Ausfallsicherheit
* Benutzerfreundlichkeit
* Kosten
* Funktionalität
* Protokollierung
* Infrastruktur

### Einsatz von geschultem Personal (NET.bd.1.A3)

Für den Betrieb der Load-Balancer-Komponenten ist ausschließlich geeignetes und geschultes Personal einzusetzen. Bei Schulungs- und Weiterbildungsbedarfen wird das Personal für die Load-Balancer-Komponenten geeignet in der Schulungsplanung berücksichtigt. Im Kontext „Schulung von Mitarbeitern“ ist der Standard „Sensibilisierung und Schulung“ zu berücksichtigen.

### Nutzung von funktionalen Erweiterungen (NET.bd.1.A4)

Bei der Verwendung von funktionalen Erweiterungen (z. B. TLS-Offloading, Malware Prevention/Detection, CA/OCSP Verifizierung, Scripte auf Basis von Perl) ist sicherzustellen, dass die definierten Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der Load-Balancer-Komponenten und der Netzinfrastruktur weiterhin erfüllt werden.

### Sicheres Betriebssystem und sichere Basiskonfiguration (NET.bd.1.A5)

Alle Load-Balancer-Komponenten werden so konfiguriert, dass sie den erforderlichen Schutzbedarf angemessen erfüllen. Durch die Administratoren werden passende Basiskonfigurationen der Load-Balancer entwickelt und als Blaupausen dokumentiert.

Alle bekanntgewordenen und identifizierten Schwachstellen der betreuten Load-Balancer werden durch die Verantwortlichen zeitnah in Abhängigkeit vom Schutzbedarf und der Kritikalität behoben. Es werden ausschließlich Patches und Updates aus vertrauenswürdigen Quellen bezogen. Für die Patches und Updates sind die Vorgaben der Sicherheitsrichtlinie „Patch- und Änderungsmanagement“ anzuwenden.

### Installation, Konfiguration, Administration (NET.bd.1.A6)

Für die Installationen, Konfigurationen und Administrationen der Load-Balancer-Komponenten sind folgende Regelungen einzuhalten:

* Vorgehensweisen für die Erstinstallation
* Überprüfung der Default-Einstellungen hinsichtlich Sicherheitsgefährdungen
* Regelungen zur physikalischen Zutritts- Zugriffs- und Zugangskontrolle
* Geregelte Verwendung und Konfiguration sonstiger Zugriffsarten
* Die Einbindung von Load-Balancern in die Infrastruktur darf nicht das etablierte Sicherheitszonenmodell aufweichen
* Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen
* Entwicklung und Etablierung eines Rollenkonzepts für die Administration
* Regelungen zur Einrichtung und Nutzung von virtuellen Load-Balancern
* Regelungen zu Erstellung und Pflege von Dokumentation sowie der Form der Dokumentation
* Vorgaben über zugelassene und nicht zugelassene Dienste, Protokolle und Netze
* Absicherung der Administrationsschnittstelle
* Einsatz von freigegebenen kryptographischen Verfahren, Algorithmen und Protokolle
* Einhaltung der Passwortvorgaben
* Angemessene Nutzung der Werkzeuge für Betrieb und Wartung
* Integration in ein bestehendes Netzmanagement bzw. die Automatisierungsinfrastruktur
* Berechtigungen und Vorgehensweisen bei Softwareupdates und Konfigurationsänderungen
* Einbindung in das Datensicherungskonzept
* Regelungen für die Reaktion auf Betriebsstörungen, technische Fehler und Sicherheitsvorfälle
* Einbindung in das organisationsweite Notfallvorsorgekonzept

Für die Installation, Konfiguration und Administration der Load-Balancer-Komponenten sind folgende ISMS-Dokumente zu beachten:

* Standard „IT-Administration"
* Sicherheitsrichtlinie „Kryptokonzept“
* Sicherheitsrichtlinie „Patch- und Änderungsmanagement“
* Sicherheitsrichtlinie „Netzarchitektur und -design sowie Netzmanagement“
* Sicherheitsrichtlinie „Protokollierung“
* Sicherheitsrichtlinie „Virtualisierung“
* Sicherheitsrichtlinie „Fernwartung“
* Beantragung von Kryptographieausnahmen
* Umgang mit Passwörtern

### Protokollierung (NET.bd.1.A7)

Zum Zwecke einer übergreifenden Auswertung von Ereignissen wird eine Zeit-Synchronisation mit freigegebenen Zeitquellen vorausgesetzt.

Die Load-Balancer protokollieren alle sicherheitsrelevanten Ereignisse und Konfigurationsänderungen und speichern diese unverändert ab. Durch die Regelungen im Identitäts- und Berechtigungsmanagement können nur Befugte die erhobenen Daten einsehen und auswerten. Bei der Protokollierung werden die gesetzlichen und internen Regelungen eingehalten (siehe Sicherheitsrichtlinie "Protokollierung"). Für die Auswertungen der Protokollierungen wird ein Plan erstellt. Dabei wird geregelt, welche Protokolldaten regelmäßig, sporadisch oder nur bei Bedarf auszuwerten sind.

Für die Protokollierung gelten zusätzlichen die zentralen Vorgaben der Sicherheitsrichtlinie „Protokollierung“.

### Betriebshandbuch für die Load-Balancer (NET.bd.1.A8)

Die Inhalte eines Betriebshandbuchs für die Load-Balancer sind nachvollziehbar zu dokumentieren. Das Betriebshandbuch beinhaltet, angelehnt an den Lebenszyklus, folgende inhaltliche Phasen:

* Inbetriebnahme
* Betrieb
* Aussonderung
* Wiederanlauf

Die Dokumentation wird gegen unbefugten Zugriff geschützt. Alle Änderungen sind nachvollziehbar zu dokumentieren bzw. zu referenzieren. Für die Betriebshandbücher ist die Handlungsempfehlung „Template für die Erstellung von Betriebshandbüchern“ zu nutzen.

### Sicherung der System-Konfiguration (NET.bd.1.A9)

Vor Installationen, Konfigurationsänderungen und in zyklischen Abständen sind Systemsicherungen der Load-Balancer vorzunehmen. Es gelten die Vorgaben der Sicherheitsrichtlinie „Datensicherung“.

### Verhaltensregeln bei Load-Balancer-Sicherheitsvorfällen (NET.bd.1.A10)

Bei einem Load-Balancer-Sicherheitsvorfall leiten die Verantwortlichen in Übereinstimmung mit der Sicherheitsvorfallsbehandlung passende Gegenmaßnahmen einleiten. Die möglichen Konsequenzen sicherheitskritischer Ereignisse werden dazu geeignet untersucht. Letztlich werden alle erforderlichen Maßnahmen ergriffen, um auszuschließen, dass durch Load-Balancer-Sicherheitslücken auf das Netz sowie auf vertrauliche Informationen zugegriffen werden kann.

Für die Behandlung und Bereinigung von Sicherheitsmeldungen, sicherheitsrelevanten Ereignissen und Sicherheitsvorfällen gelten die nachfolgenden ISMS-Dokumente:

* Sicherheitsrichtlinie „IT-Forensik und Bereinigung von Sicherheitsvorfällen“
* Sicherheitsrichtlinie „Behandlung von Sicherheitsvorfällen“
* Sicherheitsrichtlinie „Detektion von sicherheitsrelevanten Ereignissen“
* Beurteilung von Sicherheitsmeldungen

### Einsatz von Virtualisierungstechniken (NET.bd.1.A11)

Beim Einsatz von Load-Balancern in virtuellen Umgebungen gefährdet ein einzelner gestörter Prozess der angewandten Virtualisierungstechnik des Load-Balancers nicht die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit des gesamten Systems oder eines parallel betrieben virtuellen Systems. Beim Einsatz von Virtualisierungstechniken gelten die Vorgaben der Sicherheitsrichtlinie „Virtualisierung“.

### Implementierung von Heartbeats (NET.bd.1.A12)

Sofern Heartbeats für Instanzen zur Auswertung durch die Load-Balancer implementiert werden, wird darauf geachtet, dass die etablierten Heartbeats keine eingesetzten und vorgeschriebenen Sicherheitsmechanismen umgehen oder außerkraftsetzen.

### Einsatz von TLS -Offloading (NET.bd.1.A13)

Für die <Institution> kann TLS-Offloading bei den Load-Balancer-Komponenten eingesetzt werden, um hierdurch die mittels TLS transportiert Daten auf Verletzung der Compliance bzw. potentielle Schadsoftware überprüfen zu können.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Zusätzlicher Schutz der Administrationsschnittstellen (NET.bd.1.A14)

Die Zugänge zu den Load-Balancern sind auf einzelne Quelladressen (der ursprünglichen Clients) eingeschränkt. Der direkte Zugriff auf die Administrationsschnittstellen aus nicht-vertrauenswürdigen Netzen wird verhindert.

### Berechtigungsmanagement in der Load-Balancer-Infrastruktur (NET.bd.1.A15)

Für die Load-Balancer-Infrastruktur wird ein dokumentiertes Berichtigungskonzept angewandt. Den Auditoren, Administratoren und technischen Konten für die Überwachung werden nur so viele Berechtigungen eingeräumt, wie für die Aufgabenerfüllung notwendig ist (Minimalprinzip). Es ist regelmäßig zu überprüfen, ob die zugeteilten Rechte noch angemessen sind.

Für das Berechtigungsmanagement in der Load-Balancer-Infrastruktur gelten die Regelungen der Sicherheitsrichtlinie „Identitäts- und Berechtigungsmanagement“.

### Regelmäßige Sicherheitschecks der Load-Balancer-Infrastruktur (NET.bd.1.A16)

Mittels Penetrationstests erfolgt eine regelmäßige Überprüfung auf eventuelle Sicherheitslücken in der Load-Balancer-Infrastruktur. Die Ergebnisse von den Sicherheitsuntersuchungen werden nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen. Allen erkannten Abweichungen werden im Nachgang angemessen behandelt.

### Administration über ein abgetrenntes Managementnetz (NET.bd.1.A17)

Die Komponenten der Load-Balancer-Infrastruktur werden ausschließlich über ein dediziertes Management-Netz administriert, welches nicht die etablierte Sicherheitsinfrastruktur umgeht. Eine gegebenenfalls vorhandene In-Band-Konfigurierbarkeit ist in diesem Fall nicht erforderlich und deaktiviert. Bei der Integration der Load-Balancer in die Netz-Infrastruktur sind die Anforderungen der Sicherheitsrichtlinie „Netzarchitektur und -design sowie Netzmanagement“ zu beachten und umzusetzen.

### Schutz vor DoS- und DDoS-Angriffen (NET.bd.1.A18)

Ein erfolgreicher DoS- oder DDoS-Angriff kommt einer Einladung zu weiteren Angriffen gleich. Aus diesem Grunde sind Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen und TCP-State-Exhaustion Angriffen implementiert.

### Vermeidung von Overlay-Technologien (NET.bd.1.A19)

Seitens der <Institution> wird auf den Einsatz von Overlay-Technologien nach Möglichkeit verzichtet. Sofern erforderlich wird Network function virtualization (NFV) eingesetzt. Dabei werden die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit hinsichtlich der Absicherung der Steuerungskommunikation und der Nutzdatenübertragung beachtet und eingehalten.

### Einsatz von cloudbasierten Infrastrukturmanagementlösungen (NET.bd.1.A20)

Vor dem Einsatz von cloudbasierten Lösungen für das Management von Load-Balancer-Komponenten werden die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit werden folgende Sicherheitsaspekte eingehalten:

* Cloud-Dienst-Regelungen
* Absicherung der Steuerungskommunikation
* Absicherung der Nutzdatenübertragung

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Erweiterter Integritätsschutz für die Konfigurationsdateien (NET.bd.1.A21 - I)

Durch einen Integritätsschutz für die Konfigurationsdateien wird bei erhöhtem Schutzbedarf sichergestellt, dass auch dann keine alten oder fehlerhaften Konfigurationen benutzt werden, wenn es einem Angreifer gelingt, einen Neustart der Load-Balancer-Komponente zu verursachen.

### Zentrale Protokollierung (NET.bd.1.A22 - CI)

Bei erhöhtem Schutzbedarf erfolgt die Protokollierung auf einem zentralen gesonderten System und wird fortlaufend durch geeignete Mechanismen automatisiert ausgewertet. Die Administration des Protokollierungssystems ist von der Administration der protokollierenden Systeme personell zu trennen.

Für die Protokollierung gelten zusätzlichen die zentralen Vorgaben der Sicherheitsrichtlinie „Protokollierung“.

### Verwendung einer Hochverfügbarkeitslösung (NET.bd.1.A23 - A)

Um einem erhöhten Schutzbedarf im Sicherheitsziel Verfügbarkeit zu entsprechen, ist eine Hochverfügbarkeitslösung für die Load-Balancer-Infrastruktur zu implementieren. Diese darf nicht den Betrieb der Load-Balancer-Komponenten bzw. deren Sicherheitsfunktionen behindern. Das Sicherheitsniveau ist weiterhin aufrechtzuerhalten. Damit zum Beispiel im Fall einer Wiederherstellung des Load-Balancers oder eines Gesamtsystems ausreichend Zeit zur Verfügung steht, werden folgende Möglichkeiten zur Steigerung der Verfügbarkeit vorgesehen:

* Cold-Standby (nicht aktiver baugleicher Load-Balancer)
* Warm-Standby (aktiver baugleicher Load-Balancer mit Timeout)
* Hot-Standby (aktiver baugleicher Load-Balancer ohne Timeout)

### Bandbreitenmanagement für kritische Anwendungen und Dienste (NET.bd.1.A24 - A)

Bei erhöhtem Verfügbarkeitsschutzbedarf ist ein Bandbreitenmanagement vorzusehen. Bei den Load-Balancer-Komponenten werden zu diesem Zweck Funktionen zur Erkennung der Applikationen sowie zur festen oder dynamischen Priorisierung von Bandbreiten genutzt.

### Vermeidung von Verknüpfungen von Sicherheitsbereichen (NET.bd.1.A25 - CIA)

Mittels einem physischen Load-Balancer werden nicht gleichzeitig zwei unterschiedliche Sicherheitsbereiche bzw. zwei Sicherheitszonen mit unterschiedlichen Schutzbedarfen angebunden.