**Sicherung der Netzübergänge mittels Session Border Controller**

Sicherheitsrichtlinie

**Autor:** Jürgen Schlereth

**Tel.: (0611) 340 -** 3058

Juergen.Schlereth**@hzd.hessen.de**

Dokumentinformationen

|  |  |
| --- | --- |
| Sperrvermerk | - |
| Redaktion | Jürgen Schlereth |
| Klasse | Sicherheitsrichtlinie |
| Dateiname | Policy-Sicherheit-SBC\_Ver\_01.09.docx |
| Letzte Bearbeitung (Speicherdatum) | 6. Mai 2020 |
| Letztes Druckdatum | 30. Dezember 2016 |
| Seitenzahl | 25 |

|  |  |  |
| --- | --- | --- |
| Dokumentstatus und –freigabe | | |
|  | Datum | Name und Abteilung / Firma |
| Entwurf | 5.4.2019 | F. Weberbauer |
| QS-Prüfung | 24.10.2019 | Jürgen Schlereth |
| Freigabe | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Änderungsnachweis | | | | |
| Versions-Nr. | Status | Bearbeiter | Datum | Änderung / Bemerkung |
| 00\_01 | Entwurf | F. Weberbauer | 5.4.2019 | Erstfassung |
| 00\_02 | QS | J. Schlereth | 15.4.2019 | QS |
| 00\_03 | Überarbeitung | J. Schlereth | 24.10.2019 | Änderungen aufgrund Aufhebung Blattschutz |
| 00\_04 | QS | J. Fritz-Weber | 11.2.2020 |  |
| 00\_05 | Überarbeitung | J. Schlereth | 11.2.20201 |  |
| 00\_05\_R6 | QS | M- Büßelberg |  |  |
| 00\_05\_D2 | QS | Dr. Domack | 7.4.2020 |  |
| 00\_06 | Überarbeitung | J. Schlereth | 8.4.2020 |  |
| 00\_07 | Formatierung | J. Schlereth | 8.4.2020 |  |
| 00\_08 | Überarbeitung | F. Weberbauer | 30.4.2020 | Einarbeitung von Kommentaren |
| 00\_09 | Prüfung | J. Schlereth | 4.5.2020 |  |

Inhaltsverzeichnis

1 Ziele und Geltungsbereich 5

1.1 Zweck des Dokuments 5

1.2 Begriffsdefinition und Abgrenzung 6

1.3 Geltungsbereich 6

1.4 Inkraftsetzen und Fortschreibung 7

2 Definition und Handlungsvorgaben 7

2.1 Allgemeine Beschreibung des Sprachfirewall-Übergangs 7

2.2 Sicherheitskonzept und IT-Sicherheitsarchitektur des Netzübergangs 8

2.3 Grundsätze 8

2.4 Ausnahmen 9

2.5 Allgemeine Anforderungen 10

2.5.1 Generisches Betriebshandbuch Sicherheitsgateway (SBC) 10

2.5.2 Konfiguration 11

2.5.3 Administrative Berechtigungen 12

2.5.3.1 Zutrittsschutz zu den Sicherheitsgateways 12

2.5.3.2 Zugangsrechte zu den Sicherheitsgateways (SBC) 12

2.5.4 Inventarisierung 13

2.5.5 Verfügbarkeit 13

2.5.6 Protokollierung und Reporting 14

2.5.6.1 Protokollierung 14

2.5.6.2 Reporting 14

2.5.6.3 Archivierung und Backup 15

2.5.7 Eskalationsstufen 15

2.6 Change-Management 15

2.6.1 Genehmigung 15

2.6.2 Auswirkungsanalyse 16

2.6.3 Implementierung 16

2.6.4 Notfalländerung 16

2.6.5 Kontrolle 17

3 Rollen und Verantwortlichkeiten 17

3.1 Gesamtverantwortlicher HessenVoice 17

3.2 Gesamt-Betriebsleitungen und Verfahrensleitungen (HessenVoice oder Dienststellen im TK – Eigenbetrieb) der Verfahren, die das Sicherheitsgateway (SBC) nutzen 18

3.3 IT-Sicherheitsplanung / Planung Sicherheitsgateways 18

3.4 IT- Sicherheitsadministration / Betrieb Sicherheitsgateways (SBC) 19

3.5 IT-Revision 20

3.6 IT-Sicherheitsbeauftragter 20

3.7 Behördlicher Datenschutzbeauftragte 20

4 Steuerung 21

4.1 Implementierung 21

4.2 Durchsetzung 21

4.3 Nichteinhaltung 21

4.4 Konsequenzen 21

5 Glossar ……………… 21

6 Mitgeltende Dokumente 22

6.1 Übergeordnete Dokumente 22

6.2 Nachgeordnete Dokumente 22

# Ziele und Geltungsbereich

## Zweck des Dokuments

Dieses Dokument stellt die Sicherheitsrichtlinie (gemäß M 2.299 BSI) für das Sicherheitsgateway am Übergang zu den Netzen von HessenVoice und den NGN-Netzen von Vodafone und anderen Providern dar. Eine Aktualisierung der Sicherheitsrichtlinie nach dem BSI Kompendium erfolgt nach Freigabe im Zusammenhang mit dem der Aktualisierung des allgemeinen Sicherheitskonzeptes für HessenVoice. Als konkrete Sicherheitsgateways (vergleichbar zu Firewalls bei Netzübergängen) kommen Session Border Controller (SBC) zum Einsatz.

Für die VoIP-Kommunikation über Vertrauensbereiche hinaus ist es erforderlich, den VoIP-Verkehr (Signalisierung und Medientransport) über ein Sicherheitsgateway (SBC) zu führen, welches zwischen den Vertrauensbereichen installiert wird. Im konkreten Szenario wird ein Sicherheitsgateway (SBC) am Übergang zu den Netzen von HessenVoice und den NGN-Netzen von Vodafone sowie anderen Providern vorgesehen. Hierbei wird ein Session Border Controller (SBC) als Sicherheitsgateway eingesetzt. Im Weiteren soll der Begriff Sicherheitsgateway (SBC) im Kontext der vorliegenden Sicherheitsrichtlinie verwendet werden. Ein Sicherheitsgateway (SBC) an einem Netzübergang kann hierbei mithilfe von einem oder mehreren SBCs realisiert werden, um bspw. Anforderungen der Verfügbarkeit bzw. der Kapazität umsetzen zu können. Weiterhin kann zwischen zentralem und dezentralem Sicherheitsgateway (SBC) unterschieden werden. Ein zentrales Sicherheitsgateway (SBC) wird am zentralen Netzübergang realisiert, wohingegen ein dezentrales Sicherheitsgateway (SBC) am lokalen Netzübergang am Standort einer Dienststelle realisiert wird. Werden zentrale Netzübergänge an unterschiedlichen RZ-Standorten realisiert, z.B. aus Gründen der Redundanz und Lastverteilung, dann kann zwischen einem zentralen Sicherheitsgateway (SBC) RZ1 und zentralen Sicherheitsgateway (SBC) RZ2 differenziert werden. Die zentral als Cluster betriebenen Sicherheitsgateways (SBC) werden im Folgenden als „hvsbc“-Cluster (HessenVoice SBC – Cluster) benannt.

Grundlagen sind die BSI-Maßnahmen M2.71 „Festlegung einer Policy für ein Sicherheitsgateway“, M2.299 „Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway“ und M2.78 „Sicherer Betrieb eines Sicherheitsgateways“ aus den IT- Grundschutzkatalogen für den Baustein B3.301 „Sicherheitsgateway (Firewall)“.

Informationssicherheit wird in dieser Sicherheitsrichtlinie als eine Kombination von Informationssicherheit und Datenschutz verstanden. Dabei bezeichnet Informationssicherheit diejenigen Maßnahmen, die den Schutz vor Verlust der Sicherheitsziele Verfügbarkeit, Integrität und Vertraulichkeit bezwecken. Datenschutz bedeutet Maßnahmen, die eine Beeinträchtigung des informellen Selbstbestimmungsrechts über die personenbezogenen Daten verhindern sollen. Ziel der Sicherheitsrichtlinie ist es, durch geeignete Auswahl von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen ein Sicherheitsniveau zu gewährleisten, so dass sowohl ein angemessener und ausreichender Schutz des oben genannten Netzbereiches gegeben ist.

Diese Sicherheitsrichtlinie versteht sich als verbindliches Dokument zur Erreichung des gesetzten Ziels. Sie legt Rechte und Pflichten aller mit dem Betrieb und der Nutzung der Systeme betrauten Personen fest und beschreibt die Grundsätze des Betreibers dieses Übergangs für die Kontrolle und den Schutz der in der Systemumgebung befindlichen Elemente. Sie definiert, welche Informationen, Dienste und Protokolle das Sicherheitsgateway wie behandelt und wer sie nutzen darf.

Diese Sicherheitsrichtlinie wird durch den Gesamtverantwortlichen des oben genannten Fachbereiches dem mit dem Betrieb der Sicherheitsgateways (SBC) beauftragten Organisationseinheit der HZD und dem IT-Sicherheitsmanagement der HZD zur Verfügung gestellt. Auf Nachfrage und nur für den internen Gebrauch bekommen z. B. andere Gesamt-Betriebsleitungen oder Verfahrensleitungen die Richtlinie bereitgestellt.

Die Konfigurationen des Sicherheitsgateways wird durch die für den Betrieb von Sicherheitsgateways (SBC) verantwortliche Organisationseinheit der HZD elektronisch gepflegt.

Eine detaillierte Beschreibung der Session Border Controller für HessenVoice ist im Dokument „HessenVoice Session Border Controller – Technik“ zur Nutzung in der jeweils aktuellen Fassung niedergelegt.

## Begriffsdefinition und Abgrenzung

Ein Session Border Contrller (SBC) zur Absicherung von Sprachnetzen ist gemäß BSI als Sicherheitsgateway definiert. Zur Abgrenzung zu anderen von der HZD betriebenen Sicherheitsgateways (z.B. Firewalls) und zur weiteren Begriffsdefinition wird in diesem Dokument von Session Border Controller (SBC) **oder** Sicherheitsgateway (SBC) gesprochen.

## Geltungsbereich

* **organisatorisch:**

Diese Sicherheitsrichtlinie gilt sowohl für die HZD und alle von ihr beauftragten Geschäftspartner, Lieferanten und Dienstleister, die Änderungen an dem durch das Sicherheitsgateway (SBC) gesicherten Übergang zu HessenVoice und TK –Anlagen des Landes vornehmen oder vornehmen lassen. Alle für die HZD tätigen Personen, d.h. Mitarbeiter, Drittunternehmer, Berater oder Lieferanten und Dienstleister, sind verpflichtet, diese Grundsätze sowie die daraus abgeleiteten Standards anzuwenden.

* **technisch:**

Die Sicherheitsrichtlinie bezieht sich ausschließlich auf das „hvsbc“-Cluster (HessenVoice SBC – Cluster) und dezentrale Session Border Controller Sicherheitsgateways (SBC).

* **Ausnahmen:**

Diese Sicherheitsrichtlinie ist als Ergänzung zur Informationssicherheitsleitlinie für die hessische Landesverwaltung (2016).) zu betrachten. Im Zweifel gelten die Anforderungen von übergeordneten Richtlinien. Ausnahmen bedürfen der schriftlichen Genehmigung der HZD und werden bei grundsätzlicher Bedeutung der Abteilung VII des HMdIuS (jetzt MinD) mitgeteilt.

## Inkraftsetzen und Fortschreibung

Diese Sicherheitsrichtlinie tritt nach Verabschiedung durch die Bereiche/Referate Sicherheit und der strategischen Planung des HMinD – spätestens aber mit Inbetriebnahme des Sicherheitsgateways (SBC) - in Kraft.

Durch eine permanente Fortschreibung der Sicherheitsrichtlinie mit jährlicher Überprüfung wird der Anforderung nach Aktualität entsprochen. Es werden Mitwirkungspflichten der nutzenden Organisationen, die für einen sicheren Gesamtbetrieb erforderlich sind, formuliert und bereitgestellt. Die Verantwortlichkeiten für die rechtzeitige Fortschreibung und Überprüfung sind in Kapitel 3 festgelegt.

# Definition und Handlungsvorgaben

## Allgemeine Beschreibung des Sprachfirewall-Übergangs

Die HZD stellt im Rahmen von HessenVoice allen Dienststellen des Landes Hessen Telekommunikationsdienste zur Verfügung. Der Ausbau von HessenVoice schreitet derzeit voran und soll zukünftig die Standardlösung für die Anschaltung an NGN-Anschlüsse darstellen. Dabei soll es ohne Belang sein, ob die Dienststelle oder der Standort ganzheitlich auf HessenVoice migriert wird oder nur eine Art Schnittstellenwandlung zwischen dem NGN-Anschluss und einer Bestandsanlage vollzogen wird. Hierzu soll eine VoIP-basierte Sicherheitskomponente, ein sogenannter Session Border Controller (kurz SBC) zum Einsatz kommen, um die notwendigen Sicherheitsanforderungen umsetzen zu können.

Im Vergabeverfahren „HessenVoice 2017“ wurde die notwendige vertragliche Grundlage geschaffen um eine flexible Bereitstellung von SBCs zu ermöglichen. So wurden sowohl zentral bereitgestellte und in den beiden Rechenzentren der HZD in Wiesbaden und Mainz aufgebaute, redundante und performante Session Border Controller ebenso berücksichtigt, wie dezentrale SBCs die sich für einen flächendeckenden Einsatz in den Dienststellen eignen. Die Abrechnung mit dem Managed Service Provider (MSP) erfolgt dabei auf beauftragte SIP-Kanäle und monatlicher Basis in Form von Ports.

Der Betrieb, insbesondere die vollumfängliche Konfigurationshoheit dieser Sicherheitskomponenten liegt in der Hoheit der HZD. Über eine vertragliche Klausel, kann zusätzlich zu bereits vereinbarten Wartungs- und Serviceleistungen auch der operative Betrieb übertragen werden.

Der MSP hat auf Anforderung der HZD zeitweise oder dauerhaft die vollumfängliche Konfigurationshoheit zu übergeben. Die vom MSP zu erbringende Leistung beinhaltet dann lediglich betriebssichernde Leistungen wie Hardwareaustauschservice, Softwarewartungsservice und allgemeine Betriebsdienstleistungen. Die Konfigurationshoheit des SBC hinsichtlich der SIP-Trunks und sicherheitsrelevanten Einstellungen obliegt der HZD.

## Sicherheitskonzept und IT-Sicherheitsarchitektur des Netzübergangs

Der IT-Verbund HessenVoice wird im Sicherheitskonzept K03\_IT Sicherheitskonzept SBC beschrieben. Er umfasst eine Kommunikationslösung basierend auf dem hybriden Kommunikations-System Mitel MiVoice MX-One (kurz MX-One) und SBC-Systeme des Herstellers AudioCodes. Eine Schutzbedarfsfeststellung und Schadensbetrachtung finden sich ebenfalls im oben genannten Sicherheitskonzept wieder.

Die Erzielung einer angemessenen Informationssicherheit beruht auf einem kontrollierten Übergang zentral (Wiesbaden/Mainz) oder dezentral (Lokation der Dienststelle) bereitgestellten NGN-Anschlüsse aus Providernetzen (insbesondere Vodafone), über den RZ-Backbone zum SBC-Frontend

Zentrales Element der Sicherheit bilden SBC Systeme, welche die entsprechenden Netzwerkschnittstellen zur Verfügung stellen. Die eingesetzten Systeme arbeiten dediziert als Sicherheitsgateways (SBC) auf eigener physikalischer Hardware. Es handelt sich dabei um speziell gehärtete Appliances. Auf den Sicherheitsgateways (SBC) werden keinerlei andere Anwendungen und/oder Prozesse installiert bzw. konfiguriert, da ansonsten der Herstellersupport verloren geht.

Aus Redundanzgründen wird i.d.R. ein Cluster eingesetzt, welches im Master- und Backup-Modus oder im Load-Balancing-Modus konfiguriert ist. Bei der Auswahl der Systeme für Sicherheitsgateways (SBC) wird neben Erfahrungswerten aus dem täglichen Betrieb entweder der Datendurchsatz des Vorgänger-Sicherheitsgateways (SBC) oder eines ähnlich ausgelasteten Sicherheitsgateways (SBC) zugrunde gelegt. Durch den Einsatz weiterer Systeme kann bei Bedarf skaliert werden.

## Grundsätze

Generell muss beim Betrieb der Sicherheitsgateways (SBC) („hvsbc“-Cluster und dezentralen SBCs) folgenden Anforderungen entsprochen werden:

1. **Jegliche Kommunikationsbeziehung, die nicht genehmigt wurde, ist verboten.**
2. **Über das „hvsbc“-Cluster (HessenVoice SBC – Cluster) und dezentrale Session Border Controller (SBC) werden nur folgende Kommunikationsbeziehungen ermöglicht:**

* **Kommunikation zwischen lokalen Sicherheitskomponenten in den Dienststellen des Landes und den SBC-Frontend**
* **Kommunikation zwischen den SBC-Systemen des Providers Vodafone und den SBC-Frontend**
* **Kommunikation zwischen SBC-Frontend und HessenVoice (MXOne Amtscluster)**

Für die jeweilige Konkretisierung der in dieser Sicherheitsrichtlinie gemachten Vorgaben zu den erlaubten Kommunikationsbeziehungen (in Bezug auf die Sprachkommunikation in das öffentliche Netz) und somit die korrekte und vollständige Konfiguration der jeweiligen Filterregeln ist es notwendig, dass durch die jeweilige Gesamt-Betriebsleitung (Rollendefinition siehe PLS-Beschluss vom 16.08.2010) jedes Verfahrens eine Kommunikationsmatrix erstellt und diese im Laufe des Produktlebenszyklus aktuell gehalten wird. Diese beschreibt (in tabellarischer Form) die Datenkommunikation zwischen Quelle und Ziel mit Angabe der benötigten Ports. Aufgrund der Verfahrensabhängigkeit werden diese konkreten Kommunikationsbeziehungen nicht in dieser Sicherheitsrichtlinie beschrieben, sondern müssen durch die jeweiligen Gesamt-Betriebsleitungen vorgehalten werden. Der Gesamt-Betriebsleitung und/oder der Verfahrensleitung (Rollendefinition siehe FS-Beschluss vom 14.03.2016) des jeweiligen Verfahrens obliegt daher auch die Information der Benutzer zu ihren Rechten und zur ggf. stattfindenden Nutzdaten-Filterung.

Die administrativen Zugriffe auf die Sicherheitsgateways (SBC) und die Überwachung der Sicherheitsgateways (SBC) finden über eine zentrale VPN Site-to-Site Verbindung statt.

Daraus folgt für den Betrieb des Sicherheitsgateways:

1. **Alles, was nicht ausdrücklich erlaubt ist, ist verboten.**
2. **Der Verbindungsaufbau erfolgt immer unidirektional. Das heißt, es ist immer eine Quelle-Ziel-Beziehung zu definieren. Bidirektionale Freischaltungen erfolgen grundsätzlich nicht.**
3. **Es sind nur die Dienste SIP / TLS SIP (Port 5060/5061) freigeschaltet.**
4. **Die RTP / UDP Ports werden erst nach Anforderung (SIP SDP) für die Verbindungsaufbau freigegeben.**
5. **Es sind für jede Quelle-Ziel-Beziehungen dedizierte Portfreischaltungen anzugeben. Eine „any“-Freischaltung ist grundsätzlich nicht zulässig.**
6. **Die Funktion „Pass through“ ist nicht eingerichtet**

Die Standardeinstellungen des Sicherheitsgateways müssen daher sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dieses muss auch bei einem Ausfall (ganz oder teilweise) des Sicherheitsgateways gewährleistet sein. Es darf zu keiner Zeit eine unkontrollierte und somit ungeschützte Kommunikation aus den zu schützenden hessischen Netzen heraus oder zu diesen aufgebaut werden.

Es gilt der Grundsatz: **Sicherheit geht vor Verfügbarkeit.**

Die nachstehenden Grundsätze, sowie die abgeleiteten Standards und Vorgaben schreiben vor, dass sämtliche Änderungen in einer kontrollierten Weise durchzuführen sind. Dies erfolgt in der HZD über den etablierten Changemanagement-Prozess.

## Ausnahmen

Im Notfall können Ausnahmen von den oben genannten Grundsätzen – insbesondere vom Grundsatz „Sicherheit geht vor Verfügbarkeit“ angeordnet werden. Die Autorisierung dieser Ausnahmen unterliegt hohen Sicherheitsanforderungen. Sie darf nur durch die Abteilungsleitung „Projekte“ für einen zeitlich eng befristeten Zeitraum erteilt werden. Die Freigabe ist im Changemanagement in den entsprechenden Changes zu dokumentieren. Der IT-Sicherheitsbeauftragte der HZD ist im Vorfeld zu informieren.

Die Umsetzung von Ausnahmen richtet sich nach dem HZD-Changemanagementprozess für das Verfahren HessenVoice. Zusätzlich sind als abschließende Freigabeinstanzen die Freigabegruppe der Abteilungsleitung „Rechenzentrum“ („HZD\_Abteilungsleiter\_P“) und der IT-Sicherheitsbeauftragte in den Change einzubinden. In diesen Change sind alle notwendigen Informationen aufzunehmen, die die freigebenden Gruppen in die Lage versetzen, eine sachgerechte Entscheidung zu treffen.

Im Einzelnen sind dies folgende Informationen:

* Detaillierte Beschreibung der benötigten Ausnahme
* Fachliche Begründung der Ausnahme. Diese muss nachvollziehbar und detailliert sein. Ein Hinweis auf die „Aufrechterhaltung des Betriebs“ ist nicht ausreichend.
* Zeitliche Befristung der Ausnahme. Diese Befristung muss im Change durch die notwendigen Rückbauschritte schon verankert sein.
* Quantitative und/oder qualitative Folgen und Auswirkungen, wenn diese Ausnahme abgelehnt wird.
* Betrachtungen zu Alternativ-Lösungen, die ohne diese Ausnahmegenehmigung möglich wären, aber aus wirtschaftlichen, organisatorischen oder anderen Gründen nicht wünschenswert sind.
* Ergebnis der Auswirkungsanalyse gem. Kap. 2.6.2, insbesondere die durch die Ausnahme zusätzlich erhöhten Sicherheits-Risiken auf alle davon unmittelbar oder mittelbar betroffenen Kunden und Dienste

Die Informationen sind mit Ausnahme der Auswirkungsanalyse vollständig vom Antragsteller der Ausnahmegenehmigung bereit zu stellen.

In Notfällen ist ein Notfall-Change vorzunehmen.

## Allgemeine Anforderungen

### Generisches Betriebshandbuch Sicherheitsgateway (SBC)

Für die durch die HZD betriebenen Sicherheitsgateways (SBC) wird ein generisches Betriebshandbuch die übergeordneten, standardisierten und daher für alle Sicherheitsgateways geltenden Anforderungen gemäß M 2.71 des BSI umgesetzt. Die Verantwortung für die Erstellung des generischen Betriebshandbuchs für Sicherheitsgateways liegt bei der Sicherheitsplanung/Sicherheitsgateway-Planung unter Hinzuziehung von Spezialisten aus dem für den Betrieb der Sicherheitsgateways zuständigen Betriebsteam der HZD (und Managed Service Provider).

Die aktuelle und spezifische Dokumentation der Sicherheitsgateways (SBC) und deren jeweiliger Konfiguration wird durch die für den Betrieb von Sicherheitsgateways (SBC) verantwortlichen Organisationseinheit der HZD elektronisch Tool-unterstützt gepflegt.

Das generische Betriebshandbuch muss in der jeweils aktuellen Version allen mit dem Betrieb und der Betreuung des Sicherheitsgateways (SBC) beauftragten Personen unaufgefordert zur Verfügung gestellt werden. Die Gesamt-Betriebsleitung des Sicherheitsgateways (SBC) ist zudem dafür verantwortlich, dass diesem Personenkreis alle für die Erfüllung ihrer Aufgaben notwendigen Werkzeuge (z.B. Software und Workflows) zur Verfügung gestellt werden.

Hingegen liegt die Verantwortung für die Pflege des verfahrensspezifischen Betriebshandbuchs für HessenVoice bei der jeweiligen Gesamt-Betriebsleitung. Die Pflege der verfahrensspezifischen Betriebshandbücher bei Eigenbetrieb von TK – Anlagen obliegen den Dienststellen. Die initiale Erstellung eines verfahrensspezifischen Betriebshandbuchs erfolgt gemäß dem Prozess „VM Projekte“ (siehe MAP) bzw. den Vorgaben nach ITIL V3.

Bei Bedarf sind das verfahrensspezifische Betriebshandbuch für HessenVoice sowie die in Eigenverantwortung liegenden Betriebshandbücher der Dienststellen durch die jeweiligen Betriebsleitungen der Verfahren dem mit dem Betrieb der Sicherheitsgateways (SBC) verantwortlichen Organisationseinheit der HZD zur Verfügung zu stellen.

### Konfiguration

Folgende Grundregeln und Vorgaben gelten für das Sicherheitsgateway (SBC) und dessen Regelwerk:

* Jegliche Konfigurationsänderung des Sicherheitsgateways muss schriftlich bzw. über den in der HZD etablierten Changemanagement-Prozess beauftragt werden (siehe Kapitel 2.6).
* Auf den eingesetzten Komponenten des Sicherheitsgateways sind nur die vom Hersteller vorgegebenen und unterstützten Programme installiert, die für die ordnungsgemäße Funktion des Sicherheitsgateways notwendig sind (siehe auch Kap. 2.2). Nach Möglichkeit sind Maßnahmen zur Integritätsprüfung zu etablieren.
* Es ist sicherzustellen, dass sich die eingesetzten Produkte immer auf dem relevanten, sichersten Stand der Entwicklung befinden. Bekanntwerdende Sicherheitsprobleme werden unter Anwendung des Genehmigungsverfahrens schnellstmöglich nach Verfügbarkeit von Patches behoben.
* Für die Administration des Sicherheitsgateways werden die vom Hersteller für die Administration vorgegebenen und unterstützen Werkzeuge eingesetzt.
* Es muss sichergestellt werden, dass das Sicherheitsgateway (SBC) bei einem Systemabsturz nach einem Neustart nur mit der letzten validierten Konfiguration wieder in Betrieb geht.
* Grundlegende Anforderungen an die Hardware-Konfiguration und Funktionalität der Sicherheitsgateways werden jeweils im Rahmen einer EU-weiten Ausschreibung eines Rahmenvertrags bzw. dessen Fortschreibung berücksichtigt. Auf Aktualität und Vollständigkeit der Anforderungen ist dabei zu achten. Die Anforderungen sind im Einzelnen in der Leistungsausschreibung zum aktuellen Rahmenvertrag enthalten.

### Administrative Berechtigungen

Im Rahmen der in der HZD etablierten Prozesse ist durch die für den Betrieb der Sicherheitsgateways verantwortlichen Organisationseinheit der HZD sicherzustellen, dass berechtigte Personen nur für die Dauer ihrer Tätigkeit für das Betriebsteam die entsprechenden Berechtigungen für den Zugriff auf die Komponenten der Sicherheitsgateways (SBC) erhalten. Darüber hinaus sind alle Autorisierungen für den Zugriff auf die Komponenten durch die für den Betrieb der Sicherheitsgateways (SBC) verantwortliche Organisationseinheit der HZD regelmäßig, aber zumindest einmal im Jahr, zu validieren.

Alle ausgesprochenen Berechtigungen und die diesbezüglichen Überprüfungen sind so zu führen, dass jederzeit ersichtlich ist, wer welche Berechtigungen wann hat(te). Der Nachweis kann auch über geeignete Tools – z.B. im Rahmen des Betriebskonzeptes HessenVoice– geführt werden. Die Verantwortung und die Nachweispflicht hierfür liegen ebenfalls bei der für den Betrieb von Sicherheitsgateways (SBC) verantwortlichen Organisationseinheit der HZD.

#### Zutrittsschutz zu den Sicherheitsgateways

Die Komponenten des zentralen Sicherheitsgateways (SBC) sind in einen geschlossenen Sicherheitsbereich innerhalb der Räumlichkeiten der HZD integriert. Ein dezentrales Sicherheitsgateway muss durch geeignete Sicherheitsmaßnahmen in der jeweiligen Dienstelle geschützt werden.

Die für das Sicherheitsgateway (SBC)-Management notwendigen Management- und Log-Server stehen ebenfalls in den gesicherten Rechenzentrumsräumen der HZD. Darüber hinaus müssen sich diese Systeme in einem durch Firewall-Systeme zugangsgesichertem Netzsegment befinden. Der administrative Zugriff erfolgt jederzeit verschlüsselt.

Der physikalische Zutritt zu den Sicherheitsgateways und den Management-Systemen wird geregelt und kontrolliert, so dass nur berechtigte Personen Zutritt erhalten. Die zu den Räumen erteilten Zutrittsberechtigungen werden zentral verwaltet und können in der Sicherheitszentrale der HZD eingesehen werden.

#### Zugangsrechte zu den Sicherheitsgateways (SBC)

Zugangsrechte auf die Sicherheitsgateways (SBC) werden nur den Mitgliedern des für den Betrieb der Sicherheitsgateways (SBC) in der HZD zuständigen Betriebsteams gewährt. Zusätzlich kommt ein externer Servicepartner zum Einsatz, dessen Mitarbeiter namentlich benannt und sicherheitsüberprüft sind.

Die Zugangsrechte müssen von der Funktion abhängig sein, die eine Person wahrnimmt. Dazu wird im Betriebshandbuch ein entsprechendes Rollenkonzept beschrieben, in dem die Zugangsrechte zu den Sicherheitsgateways (SBC) bestimmten Rollen zugewiesen werden. Dabei werden immer nur so viele Zugriffsrechte vergeben, wie für die Aufgabenwahrnehmung notwendig sind. Für die Autorisierung gegenüber den Komponenten der Sicherheitsgateways (SBC) sind die seitens der hessischen Landesverwaltung vorgegebenen Standards zur Anwendung zu bringen.

Alle Berechtigten müssen eine eindeutige Benutzerkennung für den persönlichen und ausschließlichen Gebrauch besitzen. Gemäß den „Datensicherheitsstandards der HZD (DS-S)“ müssen diese administrativen Konten von den „normalen“ Benutzerkonten getrennt sein (im DS-S wird dies für das Active Directory gefordert, dies wird auf die Sicherheitsgateways (SBC) übertragen). Außerdem obliegen die administrativen Konten zusätzlichen Anforderungen wie z.B. der Vergabe von komplexen Kennwörtern.

Diese administrativen Kennungen dürfen keinen Aufschluss über den Berechtigungsstatus aufweisen. Besteht die Notwendigkeit, in Ausnahmefällen eine gemeinsame administrative Kennung zu verwenden, so ist dieses vom IT-Sicherheitsbeauftragten der HZD zu genehmigen. Darüber hinaus ist ein Inhaber für die Verwaltung dieses Kontos zu bestimmen.

Es ist zudem durch technische und/oder organisatorische Maßnahmen sicherzustellen, dass die Administration ausschließlich von explizit festgelegten Arbeitsplätzen erfolgt. Der administrative Zugriff auf das Sicherheitsgateway (SBC) erfolgt ausschließlich verschlüsselt über eine zentralen VPN Site-to-Site Verbindung. Für die Administration des Sicherheitsgateways werden die vom Hersteller für die Administration vorgegebenen und unterstützen Werkzeuge eingesetzt.

### Inventarisierung

Sämtliche Elemente des Sicherheitsgateways und ihre Beziehungen sind in der mitgeltenden Dokumentation und einem Inventar zu dokumentieren Die Verantwortung für die Aktualisierung und Fortschreibung des Inventars liegt bei der für den Betrieb der Sicherheitsgateways verantwortlichen Organisationseinheit.

### Verfügbarkeit

Die Möglichkeit für die Verfahren (HessenVoice und dezentrale TK – Anlagen), die Kommunikationsdienste auf Basis der Sicherheitsgateways (SBC) zu nutzen, steht diesen an allen Wochentagen zu allen Tageszeiten zur Verfügung, ausgenommen ist das Standard-Wartungsfenster der HZD (Dienstag von 18 bis 22 Uhr).

Ein den Verfügbarkeitsanforderungen entsprechendes organisationsweites Notfallkonzept ist im „Notfallkonzept des Verfahrens HessenVoice“ beschrieben. Es beschreibt u.a. alle Maßnahmen für Gebäude, Räume und Energie, die nach Eintritt eines Notfalls zu ergreifen sind und stellt alle benötigten Informationen zur Verfügung. Dies ist Grundlage der Funktionalität der Sicherheitsgateways.

Die SBC-spezifische Notfallvorsorge umfasst alle Maßnahmen, die auf die Wiederherstellung der Betriebsfähigkeit nach Ausfall eines Systems ausgerichtet sind, unabhängig von der Ursache des Ausfalls. Das Service-Continuity-Management für das Verfahren HessenVoice gilt entsprechend. Für die Sicherheitsgateways (SBC) liegen generisch gehaltene Wiederanlaufpläne vor.

Beim Wiedereinspielen von gesicherten Datenbeständen ist insbesondere darauf zu achten, dass alle für den gesicherten Betrieb der Komponenten des Sicherheitsgateways (SBC) relevanten Daten auf dem aktuellen Stand sind. Wird hierfür die Unterstützung Dritter benötigt, so sind diese durch entsprechende Verträge zu verpflichten.

Dieses gilt ebenso für den Abschluss entsprechender Wartungs- und Serviceverträge für die installierten Komponenten. Die Verantwortung für den Abschluss von Wartungs- und Supportverträgen liegt zurzeit bei der mit der Planung von Sicherheitsgateway-Infrastrukturen beauftragten Organisationseinheit der HZD.

### Protokollierung und Reporting

#### Protokollierung

Sämtliche Vorkommnisse und Handlungen das Sicherheitsgateway (SBC) betreffend, sowie sämtliche Zugriffe auf die Komponenten sind zu protokollieren. Es muss sichergestellt werden, dass sowohl alle korrekt aufgebauten als auch alle abgewiesenen Verbindungen protokolliert werden. Dieses gilt gleichermaßen für alle administrativen und produktiven Vorgänge. Ausnahmen von der Protokollierung sind in der Betriebsdokumentation festzuhalten.

Die Protokolle werden geschützt auf gesonderten Log-Servern abgelegt (siehe Betriebshandbuch). Diese sind redundant vorhanden. Für die Aufbewahrung der Protokolldaten gelten die allgemeinen Aufbewahrungsfristen zum Verfahren HessenVoice, es sei denn, der Auftraggeber beauftragt aus besonderen Gründen eine längere Aufbewahrung. Nach Ablauf der Aufbewahrungsfrist werden die Protokolldaten automatisiert gelöscht.

Zugriff auf die Protokolle hat nur das für den Betrieb von Sicherheitsgateways (SBC) zuständige Team der HZD und des Servicepartners (siehe Rollenkonzept im Betriebshandbuch). Sicherheitsrelevante Protokollierungsdaten werden datenschutzkonform ggf. an eine zentrale Stelle in der HZD weitergeleitet, soweit eine Protokollierungsrichtlinie der HZD dies vorsieht.

Die Protokolldaten werden im Rahmen der ordnungsgemäßen Betriebsführung regelmäßig auf Auffälligkeiten und Unregelmäßigkeiten kontrolliert. Bei Verdacht eines Angriffs auf das Sicherheitsgateway (SBC) wird umgehend ein Troubleticket des Typs „Sicherheitsvorfall“ eröffnet.

#### Reporting

Ein Reporting erfolgt anlassbezogen auf Wunsch der Beteiligten. Die Reports werden in Form von Log-Auszügen (.csv-Datei) von dem für den Betrieb der Sicherheitsgateways (SBC) zuständigen Servicepartner im Auftrag der Organisationseinheit der HZD erstellt.

Bei der Auswertung von Reports ist – soweit sie personenbezogene Daten enthalten – der jeweilige behördliche Datenschutzbeauftragte und ein Vertreter des jeweiligen örtlichen Personalrats zu beteiligen. Die Verantwortung für die Auswertungen sowie für die Einbindung der o.g. Stellen liegt bei der jeweiligen Gesamt-Betriebsleitung und/oder Verfahrensleitung. Reports können diesen Personen entsprechend übermittelt werden (z.B. per Mail).

#### Archivierung und Backup

Eine Archivierung findet nicht statt.

Die vorgenommenen Änderungen im Regelwerk oder an der Konfiguration erfolgen über das Changemanagement-System der HZD und dem explizit für HessenVoice entwickelten Verfahren Auftragscenter. Die Change-Nummern werden entsprechend im Regelwerk mit dokumentiert. Damit sind Änderungen am Sicherheitsgateway (SBC) jederzeit nachvollziehbar.

Die komplette Konfiguration des Sicherheitsgateways (SBC) unterliegt einem täglichen Backup (siehe Betriebshandbuch). Diese Sicherungen werden auf einem gesonderten Server im firewallgeschützten Managementsegment vorgehalten. Dieser Server ist gehärtet und der Zugriff nur entsprechend berechtigten Personen erlaubt, siehe Rollenkonzept im Betriebshandbuch.

### Eskalationsstufen

Eskalationsstufen sind gemäß dem Rahmenvertrag für HessenVoice festgelegt.

Der Entscheidungsprozess über Ausnahmen von dieser Sicherheitsrichtlinie ist in Kapitel 2.4 beschrieben.

## Change-Management

Systemverändernde Eingriffe in die Struktur der Sicherheitsgateways (SBC) unterliegen dem Change-Management-Prozess. Dies umfasst neben Regeländerungen auch Patches und Upgrades der Hard- und Software der beteiligten Komponenten.

Die verbindlichen Dokumente zum Change-Management-Prozess sind im Organisationshandbuch der HZD veröffentlicht und unter dem Stichwort „Change-Management“ im Intranet der HZD sowie der Betriebsdokumentation für das Verfahren HessenVoice zu finden.

### Genehmigung

Jede Änderung des Sicherheitsgateways (SBC) (Regelwerk und sonstige Änderungen) muss der Sicherheitsrichtlinie entsprechen, im betrieblichen Sinn erforderlich sein und bedarf einer autorisierten Genehmigung im Rahmen eines festgelegten Verfahrens (wie z.B. des Change-Managements).

An der Freigabe des Changes sind mindestens die folgenden Personen bzw. Gruppen zu beteiligen:

* die Gruppe des Change Requestors (Rolle Vorortbetreuer (VOB) und Genehmiger Dienststelle bei HessenVoice oder Dienststellen des Landes), sofern nicht deckungsgleich mit einer der untenstehenden Gruppe
* abhängig von der Betroffenheit, die zuständigen Gesamt-Betriebsleitung(en) und/oder Verfahrensleitung(en) (HessenVoice oder Dienststellen des Landes bei TK - Eigenbetrieb) der Verfahren, die das Sicherheitsgateway (SBC) nutzen
* Freigabe durch die Verfahrens- und Gesamtbetriebsleitung HessenVoice
* ggf. weitere, betroffene Gruppen

Darüber hinaus sind bei Ausnahmen die Gruppe „IT\_Sec“ (Sicherheitsbeauftragter HZD) und die Abteilungsleitung Rechenzentrum („HZD\_Abteilungsleiter\_P“) mit einzubinden.

Alle Konfigurationsänderungen müssen den in Kapitel 2.3 und 2.4 erhobenen Grundsätzen entsprechen.

### Auswirkungsanalyse

Vor der Implementierung einer Änderung muss eine Bewertung im Hinblick auf potentielle Auswirkungen auf die Daten des Sicherheitsgateways (SBC) und das Sicherheitsniveau durchgeführt und – bei Bedenken gegen die Freischaltung – im Vorfeld der Umsetzung der Änderung und ggf. auch im Change entsprechend kommuniziert bzw. dokumentiert werden. Die Bewertung wird sowohl von der mit dem Betrieb der Sicherheitsgateways (SBC) beauftragten Organisationseinheit (siehe 3.4) als auch durch die Sicherheitsplanung/Sicherheitsgateway-Planung (siehe 3.3) in der HZD durchgeführt. Über die Ergebnisse der Analyse wird im Rahmen des Genehmigungsprozesses nach Kapitel 2.6.1 entschieden.

### Implementierung

Es werden nur genehmigte Änderungen implementiert. Die Konfiguration des Sicherheitsgateways (SBC) erfolgt ausschließlich in der Verantwortung des für den Betrieb von Sicherheitsgateways (SBC) zuständigen Organisationseinheit der HZD.

Jede Änderung muss abgenommen und dokumentiert werden. Die Verantwortung für die endgültige ordnungsgemäße Abnahme und Dokumentation liegt bei den jeweiligen Gesamtbetriebsleitungen bzw. Verfahrensleitungen (siehe 3.2) oder bei einer dem Change Requestor nahestehende Organisationseinheit. Die Dokumentation erfolgt im Rahmen des Changemanagement-Tools der HZD bzw. dem Auftragscenter für HessenVoice.

### Notfalländerung

Wird im Rahmen einer Problemanalyse von den Verantwortlichen der mit dem Betrieb beauftragten Organisationseinheit der HZD ein Problem festgestellt, so wird dieses umgehend dokumentiert. Ist ein sofortiges Eingreifen aus sicherheitstechnischen Gründen notwendig, so kann dieses durch die mit dem Betrieb beauftragte Organisationseinheit der HZD ohne weitere Rücksprache erfolgen. In diesem Fall ist ein Trouble-Ticket „Sicherheitsvorfall“ zu erzeugen.

Besteht der Verdacht auf Kompromittierung der Sicherheitsinfrastruktur, beinhaltet dieses auch die Außerbetriebnahme des Sicherheitsgateways (SBC) und somit die Nichterreichbarkeit des dadurch geschützten Netzbereichs und darin integrierter Systeme. Der Informationssicherheitsbeauftragte ist unverzüglich zu informieren. In diesem Fall ist ein Trouble-Ticket „Sicherheitsvorfall“ zu erzeugen.

Es gilt der Grundsatz: **Sicherheit geht vor Verfügbarkeit.**

Ergibt sich die Notwendigkeit, in der Folge eines Notfalls eine Änderung (der Konfiguration) des Sicherheitsgateways (SBC) vorzunehmen, so muss den Anforderungen dieser Sicherheitsrichtlinie und den daraus hergeleiteten Standards nachträglich entsprochen werden.

### Kontrolle

Durch regelmäßige Überprüfungen (empfohlen: mindestens einmal jährlich) ist sicherzustellen, dass alle Änderungen korrekt umgesetzt sind und der vereinbarten Sicherheitspolitik entsprechen. Die Verantwortung für die korrekte Umsetzung der übergeordnet gültigen und der verfahrensspezifischen Filterregeln teilt sich auf, siehe dazu Kap. 3. Über die Ergebnisse und offene Maßnahmen wird der Informationssicherheitsbeauftragte der HZD informiert.

# Rollen und Verantwortlichkeiten

Für die Beschreibung der für die Erstellung und Umsetzung der Sicherheitsrichtlinie verantwortlichen Rollen gelten folgende Definitionen.

## Gesamtverantwortlicher HessenVoice

Der Gesamtverantwortliche HessenVoice trägt die übergeordnete Verantwortung für alle Aspekte, die einen sicheren Betrieb der Sicherheitsgateways (SBC) „hvsbc“- Cluster und die dezentralen Sicherheitsgateways (SBC) für das Verfahren HessenVoice ermöglichen. Im Rahmen dieses Dokumentes sind dies die folgenden Aufgaben:

* Abstimmung aller Änderungsvorhaben hinsichtlich dieses Sicherheitsgateways (SBC) in der HZD
* Verantwortung für anlassbezogene Auswertungen von Reports sowie ggf. für die Einbindung des Personalrats und des Datenschutzbeauftragten bei personenbezogenen Daten. Auswertungen werden ausschließlich nach Abstimmung durchgeführt. Außer für den Betreiber besteht kein Zugriff auf die Systeme und darauf liegenden Daten.
* Genehmigung der über das Sicherheitsgateway (SBC) eingerichteten Kommunikationsbeziehungen einschließlich deren Dokumentation
* Freigabe von Regelwerksänderungen
* Freigabe von anderen konfigurationsverändernden Maßnahmen im Sicherheitsgateway
* Veranlassung der Fortschreibung dieser Richtlinie sowie der zugehörigen Dokumente einschließlich der Mitwirkungspflichten der Kunden
* Freigabe der Fortschreibung des generischen Betriebshandbuchs
* Beauftragung von regelmäßigen Überprüfungen der korrekten Umsetzung der übergeordnet gültigen Filterregeln sowie der Einhaltung der Grundsätze (siehe Kap. 2.3) gemäß Kap. 2.6.5. Der Dienstleister wird beauftragt regelmäßig im Rahmen des Service Level Management das Regelwerk der SBC bereitzustellen.
* Unterstützung bei einer möglichen IT-Revision des Sicherheitsgateways

Der Gesamtverantwortliche HessenVoice kann diese Aufgaben ganz oder in Teilen (z.B. die Freigabe von Regelwerksänderungen) an von ihm benannte Personen oder Arbeitsgruppen delegieren.

## Gesamt-Betriebsleitungen und Verfahrensleitungen (HessenVoice oder Dienststellen im TK – Eigenbetrieb) der Verfahren, die das Sicherheitsgateway (SBC) nutzen

Wird das Sicherheitsgateway (SBC) von mehreren Verfahren gemeinsam genutzt, so müssen die jeweiligen Gesamt-Betriebsleitungen und Verfahrensleitungen für ihre Verfahren bestimmte Aufgaben übernehmen. Dies umfasst neben Aufgaben, die bereits im Vorfeld der Integration von Verfahren in diese Zone anfallen, auch laufende Aufgaben im Rahmen des Regelbetriebs des Verfahrens.

Zu den Aufgaben der Gesamt-Betriebsleitungen und Verfahrensleitungen zählen:

* Freigabe von konfigurationsverändernden Maßnahmen im Sicherheitsgateway (SBC) und Abstimmung aller verfahrensbezogenen Änderungsvorhaben hinsichtlich dieses Sicherheitsgateways (SBC) in der HZD
* Wahrnehmung der verfahrensbezogenen Aufgaben in Zusammenhang mit diesen Änderungen
* Erstellung bzw. Fortschreibung eines verfahrenseigenen Sicherheitskonzepts einschließlich Schutzbedarfsfeststellung und eines Notfallkonzeptes
* Erstellung einer Kommunikationsmatrix für sein Verfahren und deren Pflege im Rahmen des Verfahrens-Lebenszyklus
* Erstellung von Changes zu Regelwerksänderungen (sowohl für das initiale Regelwerk als auch für den laufenden Betrieb), die sein Verfahren betreffen
* Freigabe von Changes zu Regelwerksänderungen, die sein Verfahren betreffen
* Initialisierung und Steuerung des Ausnahmeprozesses nach Kapitel 2.4
* Information der Benutzer des Verfahrens zu ihren Rechten und zur ggf. stattfindenden Nutzdaten-Filterung
* regelmäßige Überprüfung der korrekten Umsetzung der verfahrensspezifischen Filterregeln in Zusammenarbeit mit dem für den Betrieb des Sicherheitsgateways (SBC) verantwortlichen Organisationseinheit (d.h. ob nur die Dienste zugelassen werden, die in der Policy des Sicherheitsgateways (SBC) erlaubt sind und ob neue Zugänge unter Umgebung des Sicherheitsgateways (SBC) geschaffen worden sind). Der Informationssicherheitsbeauftragte der HZD wird über wesentliche sicherheitsrelevante Ergebnisse informiert.

## IT-Sicherheitsplanung / Planung Sicherheitsgateways

Der Bereich Unified Communication (P6) ist u.a. auch für die Planung und Organisation der Sicherheitsgateway (SBC)-Infrastruktur zuständig.

Zu den Aufgaben zählen:

* Ansprechpartner in sicherheitsrelevanten Fragestellungen
* Überprüfung und Freigabe von Regelwerksänderungen
* Freigabe von anderen konfigurationsverändernden Maßnahmen im Sicherheitsgateway
* Unterstützung und Beratung des Gesamtverantwortlichen HessenVoice bei der Fortschreibung der Sicherheitsrichtlinie und der relevanten Dokumente
* Ansprechpartner sowie Unterstützung des Gesamtverantwortlichen HessenVoice bei der Klärung von Sicherheitsfragen hinsichtlich bestehender und neu einzurichtender Dienste und Anwendungen
* Beschaffung der notwendigen Sicherheitsgateways (SBC) und der notwendigen Wartungsverträge mit dem Hersteller bzw. Lieferanten aus dem bestehenden Rahmenvertrag nach Abklärung der Anforderungen mit den betroffenen Verantwortlichen (Sicherheitsgateway-Betrieb, Verfahrens-Owner, ggf. weitere).
* Unterstützung einer möglichen IT-Revision des Sicherheitsgateways
* Bewertung im Rahmen der Auswirkungsanalyse

## IT- Sicherheitsadministration / Betrieb Sicherheitsgateways (SBC)

Die IT- Sicherheitsadministration ist für den korrekten Betrieb und Administration des Sicherheitsgateways (SBC) zuständig. Zu ihren Aufgaben zählen:

* Installation, Konfiguration, Wartung und Überprüfung der Hard- und Softwarekomponenten des Sicherheitsgateways
* Erstellung und Pflege der relevanten Dokumentationen des Sicherheitsgateways (SBC) (eigene Vorgaben zur Betriebsführung und Dokumentation, auch siehe u.a. Kap. 2.5)
* Regelmäßige Überprüfung der Log-Dateien der Sicherheitsgateways (SBC) zur Erkennung von Angriffen
* Unterstützung einer möglichen IT-Revision bei der Kontrolle des Sicherheitsgateways
* Ergreifen von notwendigen Maßnahmen entsprechend dem Incident- und Problem-Management zur Störungsbeseitigung (gemäß SLA aus der Standardleistungsbeschreibung)
* Eskalation von Incidents und Problemen an den Support-Partner bzw. den Hersteller gemäß vertraglicher Vereinbarung
* Umsetzung des Change-Managements
* Bewertung im Rahmen der Auswirkungsanalyse
* Bereitstellung von Muster-Changes für die Administration der Sicherheitsgateways
* Kontinuierliche Beschaffung und Auswertung von Informationen über Weiterentwicklungen bzw. Sicherheitslücken der eingesetzten Systeme und Komponenten
* Durchführung von Backups bzw. Wiederherstellungsmaßnahmen gemäß der Wiederanlaufpläne gemäß Betrieb HessenVoice
* Erstellung von Reports gemäß den Vorgaben aus Kapitel 2.5.6.2
* Regelmäßige Information der IT-Sicherheitsplanung/Planung Sicherheitsgateways (SBC) über durchgeführte Tätigkeiten und den Zustand des Sicherheitsgateways. Die Administration berichtet ausschließlich den in diesem Dokument aufgeführten Stellen im Rahmen ihrer jeweiligen Aufgabengebiete. Mit Ausnahme der momentanen Verfügbarkeit von Verbindungen ist sie nicht berechtigt, irgendwelche Informationen über das Sicherheitsgateway (SBC) an Dritte weiterzugeben.

## IT-Revision

Die IT-Revision überprüft entsprechend Beauftragung durch die Direktion stichprobenartig sicherheitskritische Objekte und stößt je nach Ergebnis der Revision Sicherheitsmaßnahmen an.

Die Tätigkeit der IT Revision umfasst grundsätzlich die Prüfung der Sicherheit und Ordnungsmäßigkeit der IT-Infrastruktur der HZD gemäß den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Rechte und Pflichten der IT-Revision sind dokumentiert in der DA Regeleinhaltung OH 1.2.1.1. Weitere Informationen zu den Inhalten und dem Ablauf einer IT-Revision finden sich in der Prozessbeschreibung IT-Revision, die im MAP veröffentlicht ist.

## IT-Sicherheitsbeauftragter

Die Dienststellenleitung ist gemäß Sicherheitsleitlinie für die hessische Landesverwaltung vom 01.01.2010 verantwortlich für eine angemessene Informationssicherheit seiner Dienststelle, d.h. im Rahmen dieser Sicherheitsrichtlinie die Verantwortung für alle Aspekte, die einen sicheren Betrieb der Sicherheitsgateways (SBC) ermöglichen.

Der IT-Sicherheitsbeauftragte der HZD ist verantwortlich für die Wahrnehmung aller Belange des Informationssicherheitsmanagements innerhalb der HZD gemäß seiner Aufgabenbeschreibung. Detaillierte Aufgabenzuordnungen sind im Mitarbeiterportal der HZD beschrieben.

## Behördlicher Datenschutzbeauftragte

Der behördliche Datenschutzbeauftragte der HZD (im Bedarfsfall unter Einbeziehung des HBDI) hat die Aufgabe, die datenverarbeitende Stelle bei der Ausführung des Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) in tagesaktueller Version sowie anderer Vorschriften über den Datenschutz zu unterstützen und Hinweise zur Umsetzung zu geben. Seine Aufgaben sind im HDSIG im Einzelnen beschrieben. Seine Aufgabe im Rahmen dieses Dokuments ist es, die gesetzlichen Auflagen bezüglich des Datenschutzes (beratend) sicherzustellen.

# Steuerung

## Implementierung

Der Gesamtverantwortliche HessenVoice hat sicherzustellen, dass die Sicherheitsrichtlinie umgesetzt und die notwendige Infrastruktur bereitgestellt wird. Die dazu notwendigen Beschaffungsaufträge für die Sicherheitsgateways (SBC) sowie für ggf. notwendige Erweiterungen sind zu erteilen.

## Durchsetzung

Dem Gesamtverantwortlichen HessenVoice obliegt die Kontrolle über die Einhaltung und Aktualität dieser Sicherheitsrichtlinie. Änderungen der Vorgaben in dieser Sicherheitsrichtlinie werden mit dem IT-Sicherheitsmanagement der HZD und mit der für den Betrieb von Sicherheitsgateways (SBC) verantwortlichen Organisationseinheit der HZD entsprechend vor deren Umsetzung abgestimmt.

## Nichteinhaltung

Bei der vorliegenden Sicherheitsrichtlinie handelt es sich um eine Rahmenrichtlinie, deren Regelungen uneingeschränkt gelten. Die Nichteinhaltung der Vorgaben ist nur mit einer schriftlichen Genehmigung durch den Leiter der Abteilung Rechenzentrum gestattet.

## Konsequenzen

Bei Verstoß gegen die Sicherheitsrichtlinie gelten die Instrumente des Dienst- und Arbeitsrechts. Es wird auf die Informationssicherheitsrichtlinie der Hessischen Landesverwaltung verwiesen.

# Glossar

Das Glossar enthält keine komplette Auflistung der relevanten Begriffe. Es werden nur die grundlegenden, zum Verständnis der Grundsätze erforderlichen Begrifflichkeiten erläutert.

| Abkürzung, Begriff | Erläuterung |
| --- | --- |
| SBC | Session Border Controller |
| Sicherheitsgateway (SBC) | Mit Sicherheitsgateway (SBC) wird eine Kombination aus Hard- und Software, insbesondere der für das Management benötigten Komponenten [Management Server und GUI Client („Graphical User Interface“/“Grafische Benutzerschnittstelle“)], bezeichnet, die als alleiniger Übergang zwischen zwei, oder mehreren zu trennenden NGN/All-IP Netzen dient. |
| Regelwerksänderung | Unter Regelwerksänderung wird eine Konfigurationsänderung der Sicherheitsgateways (SBC) verstanden, um die Parameter einer Kommunikationsbeziehung zu ändern. |
| GSKat | Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI), jeweils im aktuellen Stand |
| LMO | „List of managed Objects“ = Liste der Standards in Hessen |

# Mitgeltende Dokumente

## Übergeordnete Dokumente

* alle in der HZD geltenden Dokumente in ihrer jeweils aktuellen Fassung, insbesondere auch die, die in Zusammenhang mit IT-Sicherheit stehen
* Dokument Konzept\_SBC.doc in der jeweils aktuellen Fassung
* K03\_IT Sicherheitskonzept SBC in der jeweils aktuellen Fassung

## Nachgeordnete Dokumente

* Muster-Changes für Regelwerksänderungen/Sicherheitsgateways,
* Changemanagement Prozess im Auftragscenter
* Generisches Betriebshandbuch im Rahmen des allgemeinen Betriebshandbuchs des Verfahrens „HessenVoice“ inklusive Rollenkonzept (In Vorbereitung nach Freigabe Policy
* Wiederanlaufpläne
* Betriebsdokumentation
* Sicherheitskonzept (in finaler Abstimmung)