Bundesamt
für Sicherheit in der
Informationstechnik

Sicherer Betrieb von E-Mail-Servern (ISi-Mail-Server)

BSI-Checkliste zur Internet-Sicherheit (ISi-Check)

Version 1.0

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände finden Sie auf den Internet-Seiten des BSI.

http://www.bsi.bund.de oder http://www.isi-reihe.de

Bundesamt für Sicherheit in der Informationstechnik
ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Der vorliegende Checklisten-Katalog richtet sich vornehmlich an Administratoren und Sicherheitsrevisoren, die sich mit der Einrichtung, dem Betrieb und der Überprüfung von E-Mail-Servern befassen.

1.1 Funktion der Checklisten

Die Checklisten fassen die relevanten Empfehlungen der BSI-Studie „Sicherer Betrieb von E-Mail-Servern“ [ISi-Mail-Server] in kompakter Form zusammen. Sie dienen als Anwendungshilfe, anhand derer die Umsetzung der in der Studie beschriebenen Sicherheitsmaßnahmen im Detail überprüft werden kann.

Die Kontrollfragen beschränken sich auf die Empfehlungen der ISi-Mail-Server-Studie. Allgemeine Grundschutzmaßnahmen, die nicht spezifisch für die beschriebene E-Mail-Server-Architektur und ihre Komponenten sind, werden von den Fragen nicht erfasst. Solche grundlegenden Empfehlungen sind den BSI-Grundschutzkatalogen [ITGSK] zu entnehmen. Sie bilden das notwendige Fundament für ISi-Check. Auch Prüffragen, die bereits durch die Checkliste zur BSI Studie „Sichere Anbindung lokaler Netze an das Internet“ [ISi-LANA] abgedeckt wurden, werden hier nicht wiederholt.

Die Checklisten wenden sich vornehmlich an IT-Fachleute. Die Anwendung von ISi-Check setzt vertiefte Kenntnisse auf dem Gebiet der IP-Netze, der Administration von Betriebssystemen und der IT-Sicherheit voraus. Die Kontrollfragen ersetzen *nicht* ein genaues Verständnis der technischen und organisatorischen Zusammenhänge für den sicheren Betrieb von E-Mail-Servern: Nur ein kundiger Anwender ist in der Lage, die Prüfaspekte in ihrem Kontext richtig zu werten und die korrekte und sinnvolle Umsetzung der abgefragten Empfehlungen im Einklang mit den allgemeinen IT-Grundschutzmaßnahmen zu beurteilen.

Der Zweck der Kontrollfragen besteht also vor allem darin, dem Anwender bei der Konzeption, der Realisierung und dem Betrieb einer E-Mail-Server-Architektur die jeweils erforderlichen Maßnahmen und die dabei verfügbaren Umsetzungsvarianten übersichtlich vor Augen zu führen. Die Checklisten sollen gewährleisten, dass kein wichtiger Aspekt vergessen wird.

1.2 Benutzung der Checklisten

Der ISi-Reihe liegt ein übergreifender Ablaufplan zugrunde, der im Einführungsdokument [ISi-E] beschrieben ist. Die Checklisten des ISi-Mail-Server-Moduls haben darin ihren vorbestimmten Platz. Vor Anwendung der Checklisten muss sich der Anwender mit dem Ablaufplan [ISi-E] und mit den Inhalten der ISi-Mail-Server-Studie vertraut machen. Um die Kontrollfragen zu den verschiedenen Prüfaspekten zu verstehen und zur rechten Zeit anzuwenden, ist die genaue Kenntnis dieser Dokumente erforderlich.

Die Checklisten fragen die relevanten Sicherheitsempfehlungen der vorliegenden Studie ab, ohne diese zu begründen oder deren Umsetzung näher zu erläutern. Anwender, die den Sinn einer Kontrollfrage nicht verstehen oder nicht in der Lage sind, eine Kontrollfrage sicher zu beantworten, können vertiefende Informationen in der Studie nachschlagen. IT-Fachleute, die mit der Studie bereits vertraut sind, sollten die Kontrollfragen in der Regel jedoch ohne Rückgriff auf die Studie bearbeiten können.

Format der Kontrollfragen

Alle Kontrollfragen sind so formuliert, dass die erwartete Antwort ein JA ist. Zusammenhängende Kontrollfragen sind – soweit sinnvoll – hierarchisch unter einer übergeordneten Frage gruppiert. Die übergeordnete Frage fasst dabei die untergeordneten Kontrollfragen so zusammen, dass ein Bejahen aller untergeordneten Kontrollfragen ein JA bei der übergeordneten Kontrollfrage impliziert.

Bei hierarchischen Kontrollfragen ist es dem Anwender freigestellt, nur die übergeordnete Frage zu beantworten, soweit er mit dem genannten Prüfaspekt ausreichend vertraut ist oder die Kontrollfrage im lokalen Kontext nur eine geringe Relevanz hat. Die untergeordneten Fragen dienen nur der genaueren Aufschlüsselung des übergeordneten Prüfkriteriums für den Fall, dass sich der Anwender unschlüssig ist, ob die betreffende Vorgabe in ausreichendem Maße umgesetzt ist. Die hierarchische Struktur der Checklisten soll dazu beitragen, die Kontrollfragen effizient abzuarbeiten und unwichtige oder offensichtliche Prüfaspekte schnell zu übergehen.

Iterative Vorgehensweise

Die Schachtelung der Kontrollfragen ermöglicht auch eine iterative Vorgehensweise. Dabei beantwortet der Anwender im ersten Schritt nur die übergeordneten Fragen, um sich so einen schnellen Überblick über potenzielle Umsetzungsmängel zu verschaffen. Prüfkomplexe, deren übergeordnete Frage im ersten Schritt nicht eindeutig beantwortet werden konnte oder verneint wurde, werden im zweiten Schritt priorisiert und nach ihrer Dringlichkeit der Reihe nach in voller Tiefe abgearbeitet.

Normaler und hoher Schutzbedarf

Alle Kontrollfragen, die nicht besonders gekennzeichnet sind, beziehen sich auf obligatorische Anforderungen bei normalem Schutzbedarf. Diese müssen bei hohem Schutzbedarf natürlich auch berücksichtigt werden. Soweit für hohen Schutzbedarf besondere Anforderungen zu erfüllen sind, ist der entsprechenden Kontrollfrage ein „**[hoher Schutzbedarf]**“ zur Kennzeichnung vorangestellt. Bezieht sich die Frage auf einen bestimmten Sicherheits-Grundwert mit hohem Schutzbedarf, so lautet die Kennzeichnung entsprechend dem Grundwert zum Beispiel „**[hohe Verfügbarkeit]**“. Anwender, die nur einen normalen Schutzbedarf haben, können alle so gekennzeichneten Fragen außer Acht lassen.

Varianten

Mitunter stehen bei der Umsetzung einer Empfehlung verschiedene Realisierungsvarianten zur Wahl. In solchen Fällen leitet eine übergeordnete Frage den Prüfaspekt ein. Darunter ist je eine Kontrollfrage für jede der möglichen Umsetzungsvarianten angegeben. Die Fragen sind durch ein „– oder –“ miteinander verknüpft. Um das übergeordnete Prüfkriterium zu erfüllen, muss also mindestens eine der untergeordneten Kontrollfragen bejaht werden.

Befinden sich unter den zur Wahl stehenden Kontrollfragen auch Fragen mit der Kennzeichnung „**[hoher Schutzbedarf]**“, so muss mindestens eine der so gekennzeichneten Varianten bejaht werden, um das übergeordnete Prüfkriterium auch bei hohem Schutzbedarf zu erfüllen.

2 Konzeption

In der Konzeptionsphase des Ablaufplans gemäß [ISi-E] wird eine sichere E-Mail-Server-Architektur erstellt. Zur Integration des E-Mail-Dienstes muss das bestehende Netz zunächst überprüft werden, ob die Architektur des Netzes im derzeitigen Zustand dafür geeignet ist. Andernfalls muss das Netz angepasst werden, um die Anforderungen zu erfüllen und damit den späteren Einsatz des Dienstes E-Mail gewährleisten zu können.

Für den sicheren Betrieb von E-Mail-Servern wird vorausgesetzt, dass vor der Realisierung der E-Mail-Server-Architektur die Empfehlungen aus der Studie [ISi-LANA] umgesetzt beziehungsweise die zugehörigen Checklisten angewendet werden. Weiterhin sollten die Empfehlungen der Studie [ISi-Mail-Client] beachtet werden.

2.1 Sichere E-Mail-Server-Architektur

Die folgenden Kontrollfragen betreffen die Konzeption der E-Mail-Server-Architektur.

Aufbau der Grundarchitektur

☐ Wurden die Vorgaben aus [ISi-LANA] sowie [ISi-Mail-Server] der Grundarchitektur bezüglich korrekter Platzierung und Anbindung der Komponenten umgesetzt?

- ☐ *Befindet sich der interne E-Mail-Server in einer Serverzone im internen Netz?*
- ☐ *Ist der Content-Filter in der Zone Sicherheits-Gateway?*
- ☐ *Ist der SMTP-Proxy mit ALG-Funktionalität Teil des Sicherheits-Gateways?*
- ☐ *Ist in der Zone Sicherheits-Gateway ein DNS-Server vorgesehen?*

☐ **[optional]** Wurde eine der folgenden Varianten der Grundarchitektur gewählt?

- o Sind SMTP-Proxy und Content-Filter auf einem System zusammengelegt **[Variante 5.1.1 D]**? **– oder –**
- o Ist der Content-Filter am ALG und der SMTP-Proxy am ersten Paketfilter PF1 angeschlossen **[Variante 5.1.1 E]**? **– oder –**
- o Ist ein Content-Filter auf dem ALG implementiert und der SMTP-Proxy am ersten Paketfilter PF1 angeschlossen **[Variante 5.1.1 F]**? **– oder –**
- o Werden SMTP-Proxy und Content-Filter von einem Outsourcing-Unternehmen betrieben **[Variante 5.1.1 G]?**

Interner E-Mail-Server

☐ Ist der interne E-Mail-Server korrekt platziert und angebunden?

- ☐ *Ist der interne E-Mail-Server mit mindestens einem Paketfilter vom ALG/SMTP-Proxy getrennt?*
- ☐ *Ist der der interne E-Mail-Server nur vom internen Netz sowie vom ALG/SMTP-Proxy aus erreichbar und hat keine direkte Schnittstelle zum Internet?*
- ☐ *Erfolgt die Kommunikation des internen E-Mail-Servers mit dem ALG/SMTP-Proxy über SMTP oder SMTPS?*

☐ Wird auf dem internen E-Mail-Server ein Virenschutzprogramm verwendet, das von einem anderen Hersteller stammt als das, welches auf dem E-Mail-Client oder Content-Filter eingesetzt wird?

☐ **[optional]** Ist die Implementierung eines atypischen E-Mail-Adressen-Schemas vorgesehen **[Variante 5.3.2 A]**?

Content-Filter

☐ Kommuniziert der Content-Filter mit dem SMTP-Proxy über SMTP oder SMTPS?

☐ Ist die Spam-Filter-Software auf dem Content-Filter oder auf einem dedizierten System installiert (abhängig vom E-Mail-Volumen)?

☐ Wird auf dem Content-Filter ein Virenschutzprogramm verwendet, das von einem anderen Hersteller stammt als das, welches auf dem E-Mail-Client oder dem internen E-Mail-Server im internen Netz eingesetzt wird?

☐ Ist Black- und Whitelisting für Dateianhänge vorgesehen?

☐ *Ist ein Whitelisting von zugelassenen Dateiendungen für E-Mail-Anhänge vorgesehen?*

☐ *Ist ein Blacklisting von gefährlichen Dateianhängen auf Basis von Magic-Byte vorgesehen?*

☐ Sind geeignete Kontrollen vorgesehen, um Spam-E-Mails zu erkennen?[1]

- o Ist eine Prüfung auf Basis von DNSBLs vorgesehen? – **oder** –
- o Ist auf dem Spam-Filter eine statistische Inhaltsanalyse vorgesehen? – **oder** –
- o Ist auf dem Spam-Filter eine heuristische Inhaltsanalyse vorgesehen? – **oder** –
- o Ist eine Prüfung auf Basis von Prüfsummen vorgesehen? – **oder** –
- o Ist eine Prüfung auf Basis von URIDNSBLs vorgesehen? – **oder** –
- o Ist das Whitelisting spezifischer Domänen vorgesehen? – **oder** –
- o Ist ein Blacklisting bekannter Spam-Domänen vorgesehen?

☐ Ist für die Prüfungen ein Punktesystem zur späteren Bewertung von E-Mails auf Spam vorgesehen?

☐ **[hohe Integrität]** Werden verschlüsselte E-Mails auf dem Content-Filter blockiert **[Variante 5.1.2 A]**?

☐ **[hoher Schutzbedarf]** Werden E-Mails zusätzlich mit einem zentralen Unternehmensschlüssel verschlüsselt **[Variante 5.1.2 B]**?

ALG/SMTP-Proxy

☐ Hat der SMTP-Proxy ALG-Funktionalität?

☐ Ist der SMTP-Proxy durch Paketfiltern sowohl vorm Internet als auch vorm internen Netz (PF1 und PF2) geschützt?

☐ Sind auf dem SMTP-Proxy Anti-Spam-Maßnahmen vorgesehen?

☐ *Ist vorgesehen, die Existenz der E-Mail-Adresse eines Empfängers (z. B. über eine lokale Datei) zu prüfen und bei unbekannten E-Mail-Adressen keine weiteren Prüfungen durchzu-*

1 Es wird empfohlen, zur Reduzierung von Spam möglichst viele der oben genannten Maßnahmen zu realisieren.

führen und die E-Mail zu löschen?

- ☐ *Ist vorgesehen E-Mails, die von außerhalb an interne Verteilerlisten gesendet werden, zu blockieren?*
- ☐ *Ist vorgesehen E-Mails, die den Regeln des SMTP-Protokolls nicht genügen durch protokollbasierte Verfahren (Prüfung des Envelopes) zu blockieren?*
- ☐ *Ist ein Greylisting von E-Mail-Servern vorgesehen?*

☐ **[hohe Integrität]** Werden auf dem SMTP-Proxy die Methoden SenderID, SPF und DKIM umgesetzt **[Variante 5.2.2 A]**?

☐ **[hohe Vertraulichkeit]** Wird der SMTP-Verkehr mit externen Kommunikationspartnern verschlüsselt [**Variante 5.3.3 A]**?

☐ **[hoher Authentizität]** Ist eine Verschlüsselung der internen Kommunikation zwischen SMTP-Proxy, Content-Filter und E-Mail-Server vorgesehen **[Variante 5.3.3 C]**?

☐ **[hohe Verfügbarkeit]** Sind Token-basierte und Challenge-Response-Verfahren im Einsatz **[Variante 5.4.4 B]**?

☐ **[hohe Verfügbarkeit]** Ist die Implementierung einer Bounce Address Tag Validation (BATV) vorgesehen **[Variante 5.4.4 C]**?

Management und die Überwachung

☐ Ist für das Management und die Überwachung der E-Mail-Komponenten ein separates Management- und Überwachungsnetz vorgesehen?

☐ Werden alle benötigten Protokolldaten der beteiligten Server (SMTP-Proxy, ALG, Content-Filter, E-Mail-Server, DNS) zentral in der Management-Zone gespeichert?

☐ Sind die Uhren aller LAN-Komponenten, einschließlich der des Sicherheits-Gateways, synchronisiert?

Virtuelle Poststelle

Die folgenden Fragen sind zusätzlich zu den bisherigen zu beantworten, wenn der Einsatz einer Virtuellen Poststelle geplant ist.

☐ Ist die Virtuelle Poststelle korrekt platziert und angebunden?

- ☐ *Ist die Virtuelle Poststelle direkt am ALG/SMTP-Proxy angeschlossen?*
- ☐ *Kommuniziert die Virtuelle Poststelle mit dem SMTP-Proxy über SMTP?*
- ☐ *Hat die VPS (über den ALG/SMTP-Proxy) Zugriff auf externe Verzeichnisservern, OCSP-Auskunftsdienste und CRL-Server?*

3 Auswahl sicherer Komponenten

Die Realisierungsphase des Ablaufplans gemäß [ISi-E] beginnt mit der Auswahl geeigneter Komponenten, die über die notwendigen Sicherheitseigenschaften verfügen, um das Sicherheitskonzept umzusetzen. Die Checklisten in diesem Abschnitt hinterfragen die Eignung der vorgesehenen Komponenten. Die Kontrollfragen können als Hilfsmittel bei der Erstellung von Ausschreibungen oder als Bewertungsmaßstab beim Vergleich konkurrierender Produkte dienen.

3.1 Interner E-Mail-Server

Die folgenden Kontrollfragen betreffen die Auswahl des interner E-Mail-Servers sowie dessen Komponenten.

Allgemein

☐ Unterstützt das Produkt SMTP und SMTP-Auth?

☐ Können mit dem Produkt POP3, IMAP und SMTP in Verbindung mit SSL/TLS verwendet werden?

☐ Unterstützt das Produkt unterschiedliche E-Mail-Routing-Funktionalitäten (MX-Routing, Relaying)?

☐ Sind Einschränkungen bei der Benutzung von Verteilerlisten möglich, so dass beispielsweise nur authentisierte Benutzer E-Mails an eine Verteilerliste senden dürfen?

☐ Ist mit dem Produkt eine Integration unterschiedlicher Virenschutzprogramme möglich?

☐ **[optional]** Ermöglicht das Produkt das Hinzufügen von E-Mail-Disclaimern, die die Integrität der S/MIME-Signatur einer E-Mail nicht gefährden?

Virenschutzprogramm

☐ Bietet das Virenschutzprogramm die Möglichkeit E-Mails vor jedem Zugriff ohne Benutzeraktion auf Schadprogramme zu prüfen?

☐ Bietet das Virenschutzprogramm die Möglichkeit ein- und ausgehende E-Mails auf Schadprogramme zu prüfen?

☐ Ist ein mindestens tägliches (besser öfter) automatisches Virenschutz-Update (Signaturen und Virenschutzprogramm) möglich?

☐ Unterstützt die Software einen Quarantäne-Bereich für Schadprogramme?

☐ Wird eine auf Virenschutz-Signaturen basierende Prüfung unterstützt?

☐ Wird eine heuristische Prüfung auf Schadprogramme unterstützt?

3.2 Application Level Gateway

Hinsichtlich der Auswahl eines Application Level Gateways wird auf die Checkliste [ISi-LANA] (Abschnitt 3.6) verwiesen, in der die entsprechenden Kontrollfragen aufgeführt sind.

3.3 Content-Filter

Die folgenden Kontrollfragen betreffen die Auswahl eines Content-Filters.

Allgemein

☐ Unterstützt das Produkt unterschiedliche E-Mail-Routing-Funktionalitäten (MX-Routing, Relaying)?

☐ Können für eingehende und ausgehende E-Mails verschiedene Richtlinien (Policies) definiert werden?

☐ Ist bei dem Produkt die Integration eines Spam-Filters möglich?

☐ Ist mit dem Produkt die Verwendung von SMTP mit SSL/TLS möglich?

☐ Kann die Existenz der Empfängeradresse (z. B. mittels einer lokalen Datei) geprüft werden?

☐ Unterstützt das Produkt die gängigen Archivformate für Dateianhänge unterstützen (z. B. ZIP). Es muss möglich sein Dateianhänge, die in einem Archivformat vorliegen, vor einer Prüfung zu entpacken.

☐ Unterstützt das Produkt das Filtern von Dateianhängen auf der Basis von Magic-Byte?

☐ Bietet das Produkt die Möglichkeit, die Magic-Byte-Datei so zu ergänzen, dass alle für die Institution wichtigen Dateitypen erkannt werden?

☐ Kann das Produkt E-Mails anhand von MIME-Types blockieren?

☐ Erlaubt das Produkt das Hinzufügen neuer nicht vordefinierter MIME-Types?

☐ **[hoher Schutzbedarf]** Erlaubt das Produkt eine Konvertierung von Dateianlagen in das PDF-Format **[Variante 5.1.1 B]**?

☐ **[optional]** Erlaubt das Produkt potenziell gefährliche Dateitypen, Dateinamen, Dateiendungen und/oder zugeordnete MIME-Types der Dateianhänge mit Mail Defang oder MIME Defang zu ändern **[Variante 5.1.1 C]**?

Virenschutzprogramm

☐ Ist ein mindestens tägliches (besser öfter) automatisches Virenschutz-Update (Signaturen und Virenschutzprogramm) möglich?

☐ Unterstützt das Produkt eine auf Virenschutz-Signaturen basierende Prüfung?

☐ Ist mit dem Produkt eine heuristische Prüfung auf Schadprogramme möglich?

☐ Kann das Produkt Aktive Inhalte auf Schadprogramme (z. B. VBScript, JavaScript, ActiveX-Controls und Java Applets) prüfen?

☐ Kann eingestellt werden, dass Dateien, die auf dem Content-Filter gelesen oder geschrieben werden, sofort auf Schadprogramme geprüft werden (On-Access)?

Spam-Filter

☐ Unterstützt das Produkt Spam-Filter-Mechanismen?

- ☐ *Unterstützt das Produkt ein Auto-Whitelisting von Domänen?*
- ☐ *Wird das DNS-basierte Blacklisting unterstützt?*

- ☐ *Kann mit dem Produkt eine statistische Inhaltsanalyse durchgeführt werden?*
- ☐ *Kann mit dem Produkt eine heuristische Inhaltsanalyse durchgeführt werden?*
- ☐ *Sind Prüfsummenvergleiche möglich und werden mindestens „fuzzy checksums" unterstützt?*
- ☐ *Unterstützt das Produkt URIDNSBLs (Uniform Resource Identifier DNS Blacklist)?*

☐ **[optional]** Ist die Erkennung von Spam-E-Mail möglich, die in verschiedenen Dateiformaten (z. B. gif, pdf, xls, rtf) versteckt ist?

☐ Ist die Spam-Bewertung von E-Mails mittels eines Punktesystems (Schwellenwert) möglich?

3.4 ALG/SMTP-Proxy

Die folgenden Kontrollfragen betreffen die Auswahl eines ALG/SMTP-Proxy.

☐ Unterstützt das Produkt unterschiedliche E-Mail-Routing-Funktionalitäten (MX-Routing, Relaying)?

☐ Unterstützt das Produkt Spam-Filter-Mechanismen?

- ☐ *Unterstützt das Produkt das IP-Blacklisting durch Frequenzanalyse?*
- ☐ *Unterstützt das Produkt protokollbasierte Verfahren zur Abwehr von Spam?*
- ☐ *Bietet das Produkt die Möglichkeit, eingehende E-Mails auf nicht routingfähige IP-Adressen zu überprüfen?*
- ☐ *Ist eine Überprüfung der Existenz einer Domäne mittels Reverse Lookup möglich?*
- ☐ *Kann das Produkt die eigene Domäne als Absenderadresse aus dem Internet blockieren?*
- ☐ *Kann eine leistungsfähige Datenbank für das Greylisting eingebunden werde*n?

☐ Unterstützt das Produkt SMTP mit SSL/TLS?

3.5 Virtuelle Poststelle

Die folgenden Fragen sind zusätzlich zu den bisherigen zu beantworten, wenn der Einsatz einer Virtuellen Poststelle geplant ist.

☐ Ist eine Validierung des Zertifikat eines Absenders für Verschlüsselung und digitale Signatur möglich?

- ☐ *Wird der Gültigkeitszeitraum des Zertifikats geprüft?*
- ☐ *Wird geprüft, ob ein Zertifizierungspfad existiert, der zu einem vertrauenswürdigen Wurzelzertifikat führt?*
- ☐ *Wird der Zertifikatsstatus entweder mittels einer Sperrliste (CRL) oder einem OCSP-Auskunftsdienst geprüft?*
- ☐ *Werden die Sperrlisten und OCSP-Antworten anhand der Signatur des Ausstellers auf Integrität geprüft?*
- ☐ *Wird der Gültigkeitszeitraum der Sperrliste verifiziert?*
- ☐ *Wird, falls im Zertifikat eine E-Mail-Adresse angegeben ist, geprüft, ob diese mit der E-Mail-*

Adresse des Absenders übereinstimmt?

☐ Kann die Integrität der digitalen Signatur geprüft werden?

☐ Kann konfiguriert werden., dass dass Ergebnis der Signaturprüfung der E-Mail beigefügt wird?

4 Konfiguration

Nach der Beschaffung der benötigten Software erfolgt die Konfiguration der Komponenten durch die Administratoren. Die Punkte, welche für eine sichere Konfiguration zu beachten sind, werden durch folgende Checkliste dargestellt. Des Weiteren kann die Checkliste von Revisoren eingesetzt werden, um die bestehende E-Mail-Server-Architektur zu überprüfen.

4.1 E-Mail-Server

Für den E-Mail-Server sind folgende Prüfaspekte zu berücksichtigen.

Allgemein

- ☐ Ist der E-Mail-Server auf einem dedizierten System installiert?
- ☐ Wurde für das verwendete System eine systematische und strukturierte Sicherheitsanalyse durchgeführt?
- ☐ Sind nicht benutzte Dienste ausgeschaltet?
- ☐ Ist zwischen Betriebssystem und Postfächern eine logische und/oder eine physische Trennung konfiguriert?
- ☐ Sind die E-Mail-Domänen konfiguriert?
- ☐ Ist das Routing zum ALG/SMTP-Proxy konfiguriert?
- ☐ Werden Größenbeschränkungen (Quotas) für Postfächer genutzt?
- ☐ Ist die Ausgabe von Versionsinformationen der eingesetzten Software über die verwendeten Protokolle SMTP, POP und IMAP ausgeschaltet?
- ☐ Ist das automatische Antworten (z. B. Out-of-Office-Reply und Empfangsbestätigung) an externe Empfänger ausgeschaltet?
- ☐ Ist nur authentisierten Benutzern erlaubt E-Mails an eine Verteilerliste zu senden?
- ☐ Ist nur authentisierten Benutzern das Versenden und Abfragen von E-Mails erlaubt?
- ☐ Ist für die Kommunikation mit E-Mail-Clients auf dem internen E-Mail-Server SMTP, IMAP und POP3 über TLS konfiguriert?
- ☐ Findet die Authentisierung der SMTP-Verbindung mittels SMTP-Auth in Kombination mit einer der SASL-Methoden statt?
- ☐ Ist beim Einsatz von S/MIME und dem Hinzufügen eines E-Mail-Disclaimers durch den E-Mail-Server der E-Mail-Server so konfiguriert, dass die Integrität der digitalen Signatur und/oder der Verschlüsselung gewährleistet ist?
- ☐ Sind gefährliche und nicht benutzte SMTP-Befehle, z. B. VRFY und EXPN, deaktiviert?

Betriebssystem-spezifische Maßnahmen

Die Maßnahmen in diesem Abschnitt werden empfohlen, wenn diese vom Betriebssystem unterstützt werden. Dies ist beispielsweise derzeit bei Unix/Linux der Fall.

- ☐ Ist die E-Mail-Server-Software unter einem separaten Benutzer mit eingeschränkten (minimalen)

Rechten installiert und konfiguriert?

☐ Werden temporäre Dateien in einem eigenen Ordner mit gesonderten Rechten abgelegt?

☐ Wurde die E-Mail-Server-Software gekapselt?

- o Wurden Rootverzeichnisse der E-Mail-Server-Software geändert? – **oder** –
- o Wurden UNIX/Linux-Sicherheitserweiterungen (z. B SELinux, AppArmor, grsecurity, Systrace, LIDS, RSBAC, LSM) eingesetzt und für die E-Mail-Server-Software mit eingeschränkten, möglichst minimalen, Rechten konfiguriert?

Virenschutzprogramm

☐ Ist konfiguriert, dass ein- und ausgehende E-Mails mittels Virenschutzprogramm geprüft werden?

☐ Ist konfiguriert, dass vor jedem Zugriff auf E-Mails diese ohne weitere Benutzeraktion auf Schadprogramme geprüft werden?

☐ Ist konfiguriert, dass mindestens einmal täglich (besser öfter) automatisch ein Virenschutz-Update (Signaturen, Heuristiken und Virenschutzprogramm) erfolgt?

☐ Führt das Produkt eine auf Virenschutz-Signaturen basierende Prüfung durch?

☐ Ist konfiguriert, dass eine heuristische Prüfung auf Schadprogramme erfolgt?

☐ Werden durch Filterung gefundene Schadprogramme gelöscht oder in einen eigenen Quarantäne-Ordner verschoben?

Kommunikation mit den E-Mail-Clients

☐ Ist der E-Mail-Server so konfiguriert, dass dieser die Übermittlung der Authentisierungsdaten ablehnt, wenn kein Verschlüsselungsverfahren (also unverschlüsselt) oder kein geeigneter Verschlüsselungsalgorithmus vom E-Mail-Client verwendet wird?

☐ Ist der E-Mail-Server so konfiguriert, dass dieser von den E-Mail-Clients beim Verbindungsaufbau eine schwache oder unverschlüsselte Verbindung ablehnt?

4.2 Application Level Gateway

Hinsichtlich der sicheren Konfiguration eines Application Level Gateways wird auf die Checkliste [ISi-LANA] (Abschnitt 4.6) verwiesen, in der die entsprechenden Kontrollfragen aufgeführt sind.

4.3 Content-Filter

Für den Content-Filter sind folgende Prüfaspekte zu berücksichtigen.

Allgemein

☐ Wurde der Content-Filter gemäß Grundkonfiguration oder einer der angegebenen Varianten installiert?

- o Ist der Content-Filter auf einem dedizierten System installiert? **– oder –**

- Sind der Content-Filter und ALG/SMTP-Proxy auf einem System zusammengelegt **[Variante 5.1.1 D]**? **– oder –**
- Ist der Content-Filter auf dem ALG implementiert **[Variante 5.1.1 F]**? **– oder –**
- Werden SMTP-Proxy und Content-Filter von einem Outsourcing-Unternehmen betrieben **[Variante 5.1.1 G]?**

☐ Wurde für das verwendete System eine systematische und strukturierte Sicherheitsanalyse durchgeführt?

☐ Sind nicht benutzte Dienste ausgeschaltet?

☐ Werden temporäre Dateien in einem eigenen Ordner mit gesonderten Rechten abgelegt?

☐ Ist die Ausgabe von Versionsinformationen der eingesetzten Software ausgeschaltet?

☐ Ist das automatische Antworten (z. B. Meldungen bezüglich gefilterter E-Mails) an externe Empfänger ausgeschaltet?

☐ Ist ein Maximalwert dafür eingestellt, wie oft Komprimierungen ineinander geschachtelt werden dürfen und werden E-Mails, die dieser Anforderung nicht genügen, abgewiesen?

☐ Ist ein Maximalwert für die in einer komprimierten Datei enthaltenen Dateien eingestellt und werden E-Mails, die dieser Anforderung nicht genügen, abgewiesen?

☐ Werden nur die E-Mails auf dem Content-Filter gespeichert, die aufgrund der E-Mail-Richtlinie gefiltert und in den Quarantäne-Ordner geschoben werden – und sonst keine?

Betriebssystem-spezifische Maßnahmen

Die Maßnahmen in diesem Abschnitt werden empfohlen, wenn diese vom Betriebssystem unterstützt werden. Dies ist beispielsweise derzeit bei Unix/Linux der Fall.

☐ Ist die Content-Filter-Software unter einem separaten Benutzer mit eingeschränkten (minimalen) Rechten installiert und konfiguriert?

☐ Werden temporäre Dateien in einem eigenen Ordner mit gesonderten Rechten abgelegt?

☐ Wurde die Content-Filter-Software gekapselt?

- Werden Rootverzeichnisse der Content-Filter-Software geändert? – **oder** –
- Werden UNIX/Linux-Sicherheitserweiterungen (z. B SELinux, AppArmor, grsecurity, Systrace, LIDS, RSBAC, LSM) eingesetzt und für die Content-Filter-Software mit eingeschränkten, möglichst minimalen, Rechten konfiguriert?

Schutz vor Schadprogrammen

☐ Ist konfiguriert, dass ein- und ausgehende E-Mails mittels Virenschutzprogramm geprüft werden?

☐ Ist konfiguriert, dass E-Mails vor jedem Zugriff ohne weitere Benutzeraktion auf Schadprogramme geprüft werden?

☐ Ist konfiguriert, dass mindestens einmal täglich (besser öfter) automatisch ein Virenschutz-Update (Signaturen, Heuristiken und Virenschutzprogramm) erfolgt?

☐ Führt das Produkt eine auf Virenschutz-Signaturen basierende Prüfung durch?

☐ Ist konfiguriert, dass eine heuristische Prüfung auf Schadprogramme erfolgt?

- ☐ Werden durch Filterung gefundene Schadprogramme gelöscht oder in einen eigenen Quarantäne-Ordner verschoben?
- ☐ Ist konfiguriert, dass Aktive Inhalte aus der E-Mail entfernt oder alternativ die gesamte E-Mail blockiert wird?
- ☐ Werden nur E-Mail-Anhänge durchgelassen, die ausgepackt und geprüft werden können?
  - ☐ *Ist für jedes verwendete komprimierte Dateiformat ein Entpack-Programm vorhanden*
  - ☐ *Ist das Aussortieren oder Blockieren von Dateien konfiguriert, die nicht entpackt und somit nicht geprüft werden können?*
- ☐ Ist Black- und Whitelisting für Dateianhänge konfiguriert?
  - ☐ *Ist das Whitelisting von zugelassenen Dateiendungen aktiviert, damit Dateien mit erlaubten Endungen durchgelassen werden?*
  - ☐ *Erfolgt das Blacklisting von gefährlichen Dateianhängen auf Basis von Magic-Byte, damit Dateien mit gefährlichen Endungen blockiert werden?*
- ☐ Ist die Prüfung der Header konfiguriert?
  - ☐ *Wird auf Bad Headers geprüft?*
  - ☐ *Werden Received Headers mittels Reverse Lookup geprüft?*
- ☐ Ist das Whitelisting von zugelassenen MIME-Types aktiviert?
- ☐ Wurde eine entsprechende Liste von MIME-Types erstellt?
- ☐ Ist das automatische Senden einer gesonderten Warn-E-Mail vom E-Mail-Server an den Benutzer konfiguriert, wenn eine verschlüsselte E-Mail (S/MIME und PGP) nicht vom Virenschutzprogramm geprüft werden kann?
- ☐ Ist die Prüfung eingehender E-Mails auf Mailbomben aktiviert?
- ☐ **[hoher Schutzbedarf]** Ist für die Ermittlung von gefährlichen Dateianhängen eine Erkennung anhand von Whitelisting mittels Magic-Byte konfiguriert **[Variante 5.1.1 A]**?
- ☐ **[hoher Schutzbedarf]** Werden Dateianlagen in PDF konvertiert **[Variante 5.1.1 B]**?
- ☐ **[optional]** Werden potenziell gefährliche Dateitypen, Dateinamen, Dateiendungen und/oder zugeordnete MIME-Types der Dateianhänge mit Mail Defang oder MIME Defang geändert **[Variante 5.1.1 C]**?

Filterung auf Spam

Nachfolgende Empfehlungen gelten zur Filterung von Spam, abhängig von in der Konzeption (siehe Abschnitt 2) gewählten Methoden.

- ☐ Sofern Blacklisting verwendet wird: Ist das Blacklisting von IP-Adressen auf bekannte Spam-Domänen so konfiguriert, dass E-Mails von diesen Domänen blockiert werden?
- ☐ Ist das Whitelisting von IP-Adressen von legitimen E-Mail-Domänen aktiviert, um E-Mails dieser Domänen nicht zu filtern?
- ☐ Sind bei Verwendung von heuristische Inhaltsanalyse die Header- und Body-Regeln konfiguriert, um E-Mails mit bestimmten ungewollten Zeichenketten im Header und Body zu blockieren?
- ☐ Sofern eine statistische Inhaltsanalyse durchgeführt wird: Ist diese ausreichend konfiguriert/trai-

niert?

- ☐ *Wurde eine Trainingsphase der statistischen Filter durchgeführt, damit diese lernen, was als Spam und was als „Ham“ behandelt werden soll?*
- ☐ *Wird ein fortlaufendes Training des statistischen Filters durchgeführt?*

☐ Sofern Prüfsummenvergleiche durchgeführt werden: Werden E-Mails nicht nur auf Basis der Prüfung einer einzelnen Prüfsumme eines Anbieters, sondern auf Basis der Prüfsummen mehrerer Anbieter bewertet?

☐ Werden E-Mails nach der Durchführung aller Prüfungen anhand der ermittelten Punktzahl und des Schwellenwerts bewertet?

☐ Ist ein Schwellenwert konfiguriert, ab welcher Punktzahl Spam-verdächtige E-Mails gekennzeichnet werden und ab welchem Schwellenwert sie blockiert werden?

☐ Ist ein Mechanismus zur Ermittlung von in verschiedenen Dateiformaten verstecktem Spam konfiguriert/aktiviert?

☐ Ist die Ablage blockierter Spam-verdächtiger E-Mails in einem speziellen Quarantäne-Ordner so konfiguriert, dass false positives freigegeben werden können?

☐ Ist die Speicherung von E-Mails auf dem Content-Filter mit Ausnahme der E-Mails, die aufgrund der E-Mail-Richtlinie gefiltert und in den Quarantäne-Ordner geschoben werden, verboten?

4.4 ALG/SMTP-Proxy

Für den ALG/SMTP-Proxy sind folgende Prüfaspekte zu berücksichtigen.

Allgemein

☐ Ist der ALG/SMTP-Proxy auf einem dedizierten System installiert?

☐ Wurde für das verwendete System eine systematische und strukturierte Sicherheitsanalyse durchgeführt?

☐ Sind nicht benutzte Dienste ausgeschaltet?

☐ Ist die Ausgabe von Versionsinformationen über das SMTP-Protokoll der eingesetzten Software ausgeschaltet?

☐ Sind erlaubte Relay-Domänen konfiguriert?

☐ Ist die Benutzung des ALG/SMTP-Proxy als Open Relay nicht möglich?

- ☐ *Nimmt der SMTP-Proxy ausgehende E-Mails nur vom E-Mail-Server an?*
- ☐ *Wird der E-Mail-Server vom SMTP-Proxy auf Basis der IP-Adresse authentisiert?*
- ☐ *Werden eingehende E-Mails nur für vordefinierte Domänen angenommen?*

☐ Ist eine maximale Größe von E-Mails konfiguriert?

☐ Ist konfiguriert, dass unzustellbare E-Mails für eine festgelegte Zeit zunächst in einer Warteschlange verbleiben, bevor diese abgewiesen werden?

☐ Ist die Handhabung automatischer Antworten konfiguriert:

- Sind automatische Antworten ausgeschaltet (z. B. Delivery Status Notifications, Message Delivery Notifications und Spam-Filter Notifications)? – **oder** –
- Wenn dennoch automatische Antworten erfolgen sollen: Ist eine Benutzerdatenbank mit bekannten E-Mail-Domänen in der Zone des Sicherheits-Gateways eingerichtet? Ist die Generierung der Antwort „E-Mail-Adresse nicht bekannt“ bei unbekannten Benutzern untersagt?

☐ Werden E-Mails von externen Absendern an interne Verteilerlisten blockiert?

☐ Wird die Verwendung von Produktinformationen in Headern unterbunden?

☐ **[optional]** Wird die Beschreibung des „From“-Feldes ausgeblendet **[Variante 5.2.3 A]**?

Betriebssystem-spezifische Maßnahmen

Die Maßnahmen in diesem Abschnitt werden empfohlen, wenn diese vom Betriebssystem unterstützt werden. Dies ist beispielsweise derzeit bei Unix/Linux der Fall.

☐ Ist die SMTP-Proxy-Software unter einem separaten Benutzer mit eingeschränkten (minimalen) Rechten installiert und konfiguriert?

☐ Werden temporäre Dateien in einem eigenen Ordner mit gesonderten Rechten abgelegt?

☐ Wurde die SMTP-Proxy-Software gekapselt?

- Werden Rootverzeichnisse der SMTP-Proxy-Software geändert? – **oder** –
- Werden UNIX/Linux-Sicherheitserweiterungen (z. B SELinux, AppArmor, grsecurity, Systrace, LIDS, RSBAC, LSM) eingesetzt und für die SMTP-Proxy Software mit eingeschränkten, möglichst minimalen, Rechten konfiguriert**?**

Filterung auf Spam

Nachfolgende Empfehlungen gelten zur Filterung von Spam, abhängig von in der Konzeption (siehe Abschnitt 2) gewählten Methoden.

☐ Wird die Einhaltung des SMTP-Protokolls und dessen Ablauf auf Protokollverstöße geprüft und werden E-Mails, die dieses Protokoll nicht einhalten, abgewiesen?

☐ Ist das Blockieren nicht routingfähiger Absenderadressen (z. B. 127.0.0.1) aktiviert?

☐ Wird geprüft, ob die in der Absenderadresse angegebene Domäne existiert und wird eine leere Absenderadresse akzeptiert?

☐ Werden E-Mails mit nicht existierenden Empfängeradressen im Kommando RCPT TO: aussortiert?

☐ Ist das Versenden von SMTP-Statusmeldungen bei nicht existierenden E-Mail-Adressen deaktiviert?

☐ Ist das SMTP-Pipelining ausgeschaltet, damit nicht mehrere Befehle nacheinander ohne Bestätigung des Servers gesendet werden können?

☐ Ist der SMTP-Proxy gegen (D)DoS Angriffe geschützt?

- ☐ *Wird ein IP-Blacklisting durch Frequenzanalyse durchgeführt?*
- ☐ *Ist für das IP-Blacklisting durch Frequenzanalyse ein Maximalwert für gleichzeitige Verbindungen per Client konfiguriert?*

- ☐ *Ist ein Maximalwert für die Anzahl der Empfängeradressen pro E-Mail konfiguriert?*

☐ Ist Greylisting konfiguriert?

- ☐ *Ist eine Whitelist konfiguriert?*
- ☐ *Sind in der Whitelist keine vollständige IP-Subnetze enthalten?*
- ☐ *Sind wichtige E-Mail-Server in die Whitelist aufgenommen?*
- ☐ *Ist in der Whitelist die Adresse 127.0.0.1/32 (localhost) enthalten?*
- ☐ *Wird bei der Benutzung mehrerer SMTP-Proxys die Datenbank für das Greylisting synchronisiert?*
- ☐ *Ist ein Zeitraum festgelegt, in dem ein E-Mail-Server aus der Greylisting-Datenbank entfernt wird, wenn keine neuen E-Mails eingetroffen sind?*
- ☐ *Ist eine Karenzzeit konfiguriert, in der die Zustellung von E-Mails, die noch nicht in die Datenbank aufgenommen wurden, durch den SMTP-Proxy untersagt wird?*
- ☐ *Ist bei der Verzögerung einer E-Mail aufgrund des Greylistings das Hinzufügen eines Headers in der E-Mail konfiguriert?*

☐ Wird an der Schnittstelle zum Content-Filter und E-Mail-Server kein Greylisting durchgeführt?

4.5 Virtuelle Poststelle

Die folgenden Fragen sind zusätzlich zu den bisherigen zu beantworten, wenn der Einsatz einer Virtuellen Poststelle geplant ist.

☐ Ist die Validierung des Zertifikat eines Absenders für Verschlüsselung und digitale Signatur konfiguriert?

- ☐ *Ist konfiguriert, dass der Gültigkeitszeitraum des Zertifikats geprüft wird?*
- ☐ *Wird geprüft, ob ein Zertifizierungspfad existiert, der zu einem vertrauenswürdigen Wurzelzertifikat führt?*
- ☐ *Wird der Zertifikatsstatus entweder mittels einer Sperrliste (CRL) oder einem OCSP-Auskunftsdienst geprüft?*
- ☐ *Werden die Sperrlisten und OCSP-Antworten anhand der Signatur des Ausstellers auf Integrität geprüft?*
- ☐ *Wird der Gültigkeitszeitraum der Sperrliste verifiziert?*
- ☐ *Wird, falls im Zertifikat eine E-Mail-Adresse angegeben ist, geprüft, ob diese mit der E-Mail-Adresse des Absenders übereinstimmt?*

☐ Ist konfiguriert, dass die Integrität der digitalen Signatur geprüft wird?

☐ Ist konfiguriert, dass dass Ergebnis der Signaturprüfung der E-Mail beigefügt wird?

☐ Wird das Zertifikat zur Verschlüsselung entweder lokal auf der VPS gespeichert oder von einem externen Verzeichnisserver abgerufen?

5 Betrieb

Die Anforderungen für einen sicheren Betrieb der Komponenten für ein sicheres Bereitstellen von E-Mail-Servern werden auch zu einem großen Teil durch die BSI IT-Grundschutz-Kataloge [ITGSK] abgedeckt. Für den sicheren Betrieb sind neben technischen auch organisatorische Tätigkeiten wichtig. Die folgenden Kontrollfragen sollen noch einmal explizit hervorgehoben werden.

5.1 Übergreifende Aspekte

Die nachfolgenden Kontrollfragen betreffen Prüfaspekte, die für alle Komponenten relevant und übergreifend für die gesamte E-Mail-Infrastruktur von Bedeutung sind.

Allgemein

☐ Ist eine E-Mail-Richtlinie festgelegt, in der die sichere Nutzung von E-Mail und entsprechende Verhaltensregeln für den Benutzer beschrieben werden?

☐ Sind in der E-Mail-Richtlinie mögliche Änderungen von E-Mails bei der Weiterleitung beschrieben (z. B. Filterung Aktiver Inhalte)?

Überwachung

☐ Werden die Auslastung der Systeme und deren Verfügbarkeit ständig überwacht?

☐ Wird die Speicherkapazität (Festplatten und interner Speicher) überwacht?

☐ Werden die eingehende und ausgehende E-Mail-Warteschlange (Active Queue und Deferred Queue) kontinuierlich beobachtet?

☐ Wird der Spam-Quarantäne-Ordner regelmäßig auf false positives überwacht?

☐ Wird die Aktualität der Virenschutz-Signaturen auf den unterschiedlichen E-Mail-Komponenten mindestens einmal täglich (besser öfter) geprüft?

☐ Sind Prozeduren festgelegt, wie auf Exploits zu reagieren ist?

☐ Wird eine „8x5“-Überwachung von Exploits durchgeführt und werden verdächtige Anhänge gezielt blockiert?

☐ **[hoher Schutzbedarf]** Wird eine „12x7“-Überwachung von Exploits durchgeführt und werden verdächtige Anhänge gezielt blockiert **[Variante 5.1.5 A]**?

Protokollierung

☐ Werden die Protokolldateien täglich auf Warnungen und Fehler geprüft?

☐ Wird die Protokollierung auf Basis der für die Organisation geltenden Gesetze und Vorschriften, wie beispielsweise Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und Datenschutzbestimmungen, zu beachten. durchgeführt?

☐ Werden Protokolldateien zentral in einer Management-Station gesammelt?

☐ Wird eine Datensicherung der Protokolldateien durchgeführt?

5.2 E-Mail-Server

Für den E-Mail-Server sind folgende Kontrollfragen zu berücksichtigen.

☐ Wird mindestens einmal pro Tag (besser öfter) die Aktualisierung der Virenschutz-Signatur-Datei, der Heuristiken sowie des Virenschutzprogramms geprüft?

☐ Wird die E-Mail-Warteschlange überwacht, um beispielsweise Probleme bei der Zustellung von E-Mails festzustellen?

☐ Werden nach jeder Aktualisierung von Virenschutz-Signaturen die Postfächer neu auf Schadprogramme geprüft?

Protokollierung

Die Protokollierung wird aus Sicherheitsgründen empfohlen, jedoch hat jede Organisation die für sie geltenden Gesetze und Vorschriften, wie beispielsweise Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und Datenschutzbestimmungen, zu beachten.

☐ Ist eine Protokollierung von wichtigen Inhalten/Ereignissen auf dem E-Mail-Server aktiviert?

- ☐ *Wird die Absenderadresse protokolliert?*
- ☐ *Wird die Empfängeradresse protokolliert?*
- ☐ *Wird die Uhrzeit des Ereignisses protokolliert?*
- ☐ *Wird die Message-ID protokolliert?*
- ☐ *Wird die erfolgreiche bzw. fehlgeschlagene Zustellung einer E-Mail protokolliert?*

☐ Werden bei der Protokollierung die geltenden Gesetze und Vorschriften beachtet?

5.3 Content-Filter

Für das Content-Filter sind folgende Kontrollfragen zu berücksichtigen.

Virenschutzprogramm

☐ Wird mindestens einmal pro Tag (besser öfter) die Aktualisierung der Virenschutz-Signatur-Datei, der Heuristiken sowie des Virenschutzprogramms geprüft?

☐ Werden spezifische Dateianhänge anhand von Dateinamen, Dateitypen oder MIME-Types auf dem Content-Filter blockiert, für die gemäß aktueller Sicherheitswarnungen Schwachstellen bestehen und für die noch keine Pachtes verfügbar oder installiert sind?

Protokollierung für Virenschutzprogramme

Die Protokollierung wird aus Sicherheitsgründen empfohlen, jedoch hat jede Organisation die für sie geltenden Gesetze und Vorschriften, wie beispielsweise Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und Datenschutzbestimmungen, zu beachten.

☐ Ist eine Protokollierung von wichtigen Inhalten/Ereignissen auf dem Content-Filter aktiviert?

- ☐ *Wird die Absenderadresse protokolliert?*
- ☐ *Wird die Empfängeradresse protokolliert?*
- ☐ *Wird die Uhrzeit des Ereignisses protokolliert?*

- ☐ *Wird die Message-ID protokolliert?*
- ☐ *Wird die erfolgreiche bzw. fehlgeschlagene Zustellung einer E-Mail protokolliert?*
- ☐ *Wird zum Ereignis der Name der Scan-Engines protokolliert?*
- ☐ *Wird der Name des Schadprogramms protokolliert?*

Filterung auf Spam

- ☐ Wird bei Verwendung einer internen DNSBL-, URIDNSBL- oder Prüfsummenvergleichs-Datenbank alle 20 Minuten eine Aktualisierung der Datenbanken durchgeführt?
- ☐ Wird die Aktualisierung der Datenbanken überwacht?
- ☐ Wird bei der statistischen und heuristischen Inhaltsanalyse der Spam-Filter regelmäßig aktualisiert?
- ☐ Werden Spam-behaftete E-Mails in einen eigenen Quarantäne-Ordner verschoben?
- ☐ Werden Quarantäne-Ordner auf false positives geprüft?
- ☐ Wird die vom Betreiber von Listen benutzte Richtlinie geprüft, mit der Blacklisting durchgeführt wird?

Protokollierung für Spam-Filter

- ☐ Ist eine Protokollierung von wichtigen Inhalten/Ereignissen auf dem Spam-Filter aktiviert? Das heißt:
  - ☐ *Wird die Punktzahl (Spam-Level) protokolliert?*
  - ☐ *Werden die ausgeführten Spam-Prüfungen und die Punktzahl je Prüfung protokolliert?*
  - ☐ *Werden Kennzeichen für Spam oder Ham protokolliert?*
  - ☐ *Wird die Quarantäne ID (Kennnummer) protokolliert?*

5.4 Application Level Gateway

Hinsichtlich des sicheren Betriebs eines Application Level Gateways wird auf die Checkliste [ISi-LANA] (Abschnitt 5) verwiesen, in der die entsprechenden Kontrollfragen aufgeführt sind.

5.5 ALG/SMTP-Proxy

Für den SMTP-Proxy sind folgende Kontrollfragen zu berücksichtigen.

- ☐ Wird die E-Mail-Warteschlange überwacht?
- ☐ Wird zur Vorbeugung vor Sicherheitslücken eine Überwachung von Exploits dahingehend durchgeführt, ob Schwachstellen des verwendeten Betriebssystems, der installierten Anwendungen oder Dienste bekannt werden?

Protokollierung

☐ Ist eine Protokollierung von wichtigen Inhalten/Ereignissen auf dem ALG/SMTP-Proxy aktiviert?

- ☐ *Wird die Absenderadresse (E-Mail-Adresse und IP-Adresse des Absender-Gateways) protokolliert?*
- ☐ *Wird die Empfängeradresse protokolliert?*
- ☐ *Wird die Uhrzeit des Ereignisses protokolliert?*
- ☐ *Wird die Message-ID protokolliert?*
- ☐ *Wird die erfolgreiche bzw. fehlgeschlagene Zustellung einer E-Mail protokolliert?*
- ☐ *Werden unzulässige SMTP-Befehle protokolliert?*
- ☐ *Werden STARTTLS Fehlermeldungen protokolliert?*

6 Literaturverzeichnis

[ISi-Mail-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Sicherer Betrieb von E-Mail-Servern, 2009, http://www.bsi.bund.de/fachthem/sinet/

[ITGSK] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzkataloge, Stand 2008, http://www.bsi.bund.de/gshb/

[ISi-LANA] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Sichere Anbindung lokaler Netze an das Internet, 2007, http://www.bsi.bund.de/fachthem/sinet/

[ISi-E] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise, in Bearbeitung, http://www.bsi.bund.de/fachthem/sinet/

[ISi-Mail-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Sichere Nutzung von E-Mail, 2009, http://www.bsi.bund.de/fachthem/sinet/