Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Nutzung von E-Mail (ISi-Mail-Client)

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

Version 1.0

Vervielfältigung und Verbreitung

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-Clients befassen.

1.1 Funktion der Checklisten

Die Checklisten fassen die relevanten Empfehlungen der BSI-Studie „Sichere Nutzung von E-Mail“ [ISi-Mail-Client] 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-Client-Studie. Allgemeine Grundschutzmaßnahmen, die nicht spezifisch für die beschriebene E-Mail-Client-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 Kontrollfragen ersetzen *nicht* ein genaues Verständnis der technischen und organisatorischen Zusammenhänge für die Nutzung von E-Mail: 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 Grundschutzmaßnahmen zu beurteilen.

Der Zweck der Kontrollfragen besteht also vor allem darin, dem IT-Fachmann (z. B. Administratoren) bei der Konzeption, der Realisierung und der Nutzung einer E-Mail-Client-Architektur die jeweils erforderlichen Maßnahmen und die dabei verfügbaren Umsetzungsvarianten übersichtlich vor Augen zu führen. Die Checklisten sollen gewährleisten, dass alle wichtigen Aspekte berücksichtigt werden.

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-Client-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-Client-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 Studie ISi-Mail-Client 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 zugehörigen 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-Client-Architektur erstellt. Die Checklisten dieses Abschnitts hinterfragen, ob alle Empfehlungen für eine sichere Grundarchitektur korrekt umgesetzt sind.

Der sichere Einsatz von E-Mail-Clients kann nicht herausgelöst von der Gesamtarchitektur des Netzes betrachtet werden. Die Voraussetzung ist daher, dass eine entsprechende Netzarchitektur gemäß der Empfehlungen aus den Studien [ISi-LANA] und [ISi-Mail-Server] aufgebaut wurde.

2.1 Sichere E-Mail-Client-Architektur

Die sichere Architektur eines E-Mail-Clients umfasst verschiedene Komponenten,die sichere Anbindung des E-Mail-Clients an den E-Mail-Server und die sichere Verwendung von Adressbüchern, Zertifikatspeichern und Kalenderdaten.

Komponenten der E-Mail-Client-Architektur

☐ Ist in der E-Mail-Client-Architektur ein Virenschutzprogramm vorhanden?

☐ Ist in der E-Mail-Client-Architektur eine Personal Firewall vorhanden?

- ☐ *Werden alle von außen kommenden Zugriffe auf den Client-Rechner geprüft?*
- ☐ *Werden Verbindungen in das Internet nur lokal über definierte Ports zugelassen?*
- ☐ *Wird eine Prüfung auf zugelassene Programme durchgeführt?*

☐ **[optional]** Ist in der E-Mail-Client-Architektur eine Spam-Filter-Komponente vorhanden?

- Wird die Spam-Filter-Funktionalität durch die E-Mail-Client-Software erbracht? – **oder** –
- Wird die Spam-Filter-Funktionalität durch ein externes Programm (z. B. Plug-In) integriert?

☐ **[hohe Integrität]** Ist in der E-Mail-Client-Architektur ein Host-basiertes Intrusion Detection System (HIDS) vorgesehen? **[Variante 5.1.1 A]**

☐ **[hoher Schutzbedarf]** Werden Systeme, die nicht den aktuellsten Stand der Virenschutzprogramme einsetzen, nicht in das lokale Netz eingebunden? **[Variante 5.1.3 A]**

☐ **[hoher Schutzbedarf]** Ist vorgesehen, nur gepatchte Systeme in das lokale Netz einzubinden? **[Variante 5.1.8 A]**

Anbindung der E-Mail-Clients an den E-Mail-Server

☐ Werden zum Versenden von E-Mails geeignete Protokolle eingesetzt? Das heißt:

- Wird SMTP verwendet? – **oder** –
- Werden andere proprietäre Protokolle (z. B. MAPI) verwendet?

☐ Werden zum Empfang von E-Mails geeignete Protokolle eingesetzt? Das heißt:

- Wird POP3 eingesetzt? – **oder** –
- Wird IMAP eingesetzt? – **oder** –

- o Werden andere proprietäre Protokolle (z. B. MAPI) verwendet?

☐ Ist der verschlüsselte Austausch von Daten zwischen dem E-Mail-Client und dem E-Mail-Server vorgesehen?

- o Wird SSL/TLS eingesetzt? – **oder** –
- o **[hohe Vertraulichkeit]** Wird zur Verschlüsselung der Daten Secure Shell (SSH) mit Portweiterleitung für POP/IMAP und SMTP eingesetzt? **[Variante 5.3.3 A]** – **oder** –
- o **[hohe Vertraulichkeit]** Erfolgt der Austausch der Daten über ein (IPSec) Virtual Private Network (VPN)?**[Variante 5.3.3 B]**

☐ Ist auf dem Paketfilter (PF6) zwischen dem E-Mail-Server und den E-Mail-Systemen im Sicherheits-Gateway SMTP freigeschaltet?

☐ Ist die Authentifizierung des E-Mail-Servers gegenüber E-Mail-Clients mittels Zertifikaten vorgesehen?

☐ Erfolgt die Authentifizierung des E-Mail-Clients am E-Mail-Server mindestens über Benutzername und Passwort?

Adressbücher und Zertifikatsspeicher

☐ Verfügt die E-Mail-Client-Architektur über einen geeigneten Speicherort für Adressdaten und S/MIME-Zertifikaten bzw. OpenPGP-Schlüssel?

- o Ist ein zentraler Verzeichnisserver vorgesehen? – **oder** –
- o Erfolgt die Speicherung lokal auf dem E-Mail-Client-Rechner?

Die folgende Frage ist nur bei der Benutzung eines zentralen Verzeichnisservers zu beantworten:

☐ Werden für die Anbindung des E-Mail-Clients an den Verzeichnisserver geeignete Protokolle benutzt?

- ☐ *Erfolgt die Anbindung des E-Mail-Clients an den Verzeichnisserver mittels LDAP?*
- ☐ *Werden zur Authentifizierung des E-Mail-Clients am Verzeichnisserver sichere SASL-Mechanismen eingesetzt?*

Kalender

☐ Verfügt die E-Mail-Client-Architektur über einen geeigneten Speicherort für Kalenderdaten?

- o Ist einen zentraler Speicherort vorgesehen? – **oder** –
- o Erfolgt die Speicherung lokal auf dem E-Mail-Client-Rechner?

Die folgende Frage ist nur bei der Benutzung eines zentralen Speicherorts für Kalenderdaten zu beantworten:

☐ Werden für die Anbindung des E-Mail-Client an den zentralen Server für Kalenderdaten geeignete Protokolle benutzt?

- o Wird für Zugriffe CalDAV über HTTPS verwendet? – **oder** –
- o Wird für Zugriffe IMAPS mit dem Kolab-XML-Format verwendet? – **oder** –
- o Wird für Zugriffe MAPI mit RPC-Verschlüsselung verwendet?

Weitere Kontrollfragen

☐ **[hohe Vertraulichkeit]** Ist für Verschlusssachen eine Verschlüsselung mittels zugelassener Produkte vorgesehen? **[Variante 5.3.3 C]**

☐ **[hohe Vertraulichkeit]** Werden lokal gespeicherte E-Mails verschlüsselt? [**Variante 5.3.4 A]**

- Wird ein verschlüsselter Ordner angelegt? – **oder** –
- Wird die ganze Festplatte verschlüsselt?

2.2 Sichere Nutzung von S/MIME

Die Bearbeitung der Fragen dieses Abschnitts ist nur notwendig, wenn zur Absicherung der E-Mail-Kommunikation S/MIME eingesetzt werden soll.

☐ Befinden sich auf dem Client-Rechner das Schlüsselpaar des Nutzers und das zugehörige Zertifikat?

☐ Ist der private Schlüssel des Nutzers geschützt? Das heißt:

- Wird der private Schlüssel in einer mit einem Passwort gesicherten Datei gespeichert und wird der Export des privaten Schlüssels unterbunden? – **oder** –
- **[hohe Vertraulichkeit]** Wird der private Schlüssel auf einer passwortgeschützten Smart Card aufbewahrt? **[Variante 5.3.8 A]**

☐ Sind auf dem Verzeichnisserver im internen Netz Zertifikate zur Nutzung von S/MIME gespeichert und abrufbar?

☐ Erfolgt der Zugriff auf Verzeichnisserver im Internet ausschließlich über einen LDAP-Proxy im Sicherheits-Gateway?

- ☐ *Wird der direkte Zugriff des E-Mail-Clients auf Verzeichnisserver im Internet unterbunden?*
- ☐ *Befindet sich im Sicherheits-Gateway ein LDAP-Proxy?*
- ☐ *Kann der E-Mail-Client mit dem LDAP-Proxy kommunizieren?*
- ☐ *Kann der LDAP-Proxy mit Verzeichnisservern im Internet kommunizieren?*

☐ Ist auf dem Paketfilter (PF6) das Protokoll HTTP und HTTPS freigeschaltet?

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

2.3 Sichere Nutzung von OpenPGP

Die Bearbeitung der Fragen dieses Abschnitts ist nur notwendig, wenn zur Absicherung der E-Mail-Kommunikation OpenPGP eingesetzt werden soll.

☐ Befinden sich auf dem Client-Rechner das Schlüsselpaar des Nutzers und das zugehörige Zertifikat?

☐ Wird der private Schlüssel in einer mit einem Passwort gesicherten Datei gespeichert?

☐ Wird der Export des privaten Schlüssels unterbunden?

☐ Ist das Vorgehen für den sicheren Austausch der Schlüssel-ID und des Fingerabdrucks mit Kommunikationspartnern in einer E-Mail-Richtlinie festgelegt?

☐ Sind auf dem Verzeichnisserver im internen Netz öffentliche OpenPGP-Schlüssel abrufbar?

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

2.4 Organisatorische Regelungen

☐ Ist in einer E-Mail-Richtlinie definiert und für alle Mitarbeiter verbindlich vorgeschrieben, in welcher Form der E-Mail-Dienst genutzt werden darf:

- ☐ *Wird beschrieben, wer innerhalb der Institution einen E-Mail-Anschluss erhält?*
- ☐ *Sind Regelungen vorhanden, die von den E-Mail-Administratoren und den E-Mail-Benutzern zu beachten sind, um einen sicheren Betrieb zu gewährleisten (z. B. auch das Verhalten bei Auftreten von Schadprogrammen)?*
- ☐ *Ist beschrieben, dass schützenswerte Daten nur als verschlüsselte E-Mails übermittelt werden dürfen?*
- ☐ *Ist eine Beschreibung enthalten, bis zu welchem Anspruch an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit Informationen per E-Mail versandt werden dürfen?*
- ☐ *Ist beschrieben, wie die Benutzer geschult werden?*
- ☐ *Ist dargestellt, wie technische Hilfestellung für die Benutzer gewährleistet wird?*
- ☐ *Ist eine Darstellung enthalten, ob und in welchem Umfang der private Gebrauch von E-Mail erlaubt ist?*
- ☐ *Wird beschrieben, welche Regelungen für den Zugriff auf den E-Mail-Dienst und für die entsprechende Protokollierung einzuhalten sind?*
- ☐ *Sind Verhaltensregeln zur sicheren Aufbewahrung des privaten Schlüssels bei der Verwendung von S/MIME oder OpenPGP aufgestellt?*
- ☐ *Sind Verhaltensregeln zum Öffnen von Dateianhängen aufgestellt, insbesondere zum Ausführen enthaltener Anwendungen?*
- ☐ *Sind (restriktive) Verhaltensregeln zur Konfiguration von Stellvertreterberechtigungen aufgestellt?*
- ☐ *Ist eine Abstimmung mit dem Betriebs-/Personalrat geregelt, wenn persönliche Daten von Arbeitnehmern verarbeitet werden?*
- ☐ *Ist beschrieben, welche Regelungen im Hinblick auf die Zustimmungspflicht aller Mitarbeiter zur E-Mail-Richtlinie gelten?*

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 E-Mail-Client-Software/Plug-Ins

Die folgenden Kontrollfragen betreffen die Auswahl von E-Mail-Client-Software/Plug-Ins.

Allgemeine Anforderungen

☐ Unterstützt die E-Mail-Client-Software die Erstellung und Anzeige von E-Mails im Textformat?

☐ Wird das Ausführen von Aktive Inhalte im Vorschau-Fenster verhindert?

- Fehlt dem Produkt die Fähigkeit Aktive Inhalte im Vorschaufenster auszuführen? – **oder** –
- Ist das Ausführen von Aktiven Inhalten im Vorschaufenster deaktivierbar? – **oder** –
- Ist die Vorschaufunktionalität abschaltbar?

☐ Können HTML-Strukturelemente ohne Ausführung Aktiver Inhalte angezeigt werden?

☐ Können Header-Informationen von E-Mails angezeigt werden?

☐ Unterstützt die Software die Zeichensätze 7-Bit ASCII, UTF-8, ISO 8859-1 (Latin-1) und ISO-8859-15?

☐ Kann neben einem Hyperlink auch die tatsächliche URL bzw. nur diese angezeigt werden?

☐ Können gefährliche Dateianhänge mittels einer Blacklist blockiert werden?

☐ Ist die Liste mit gefährlichen Dateianhängen (Blacklist) für spezifische (neue) Schwachstellen in der Infrastruktur erweiterbar?

☐ **[Optional:]** Können gefährliche MIME-Types mittels einer Blacklist blockiert werden? **[Variante 5.1.1 B]**

Sichere Kommunikation auf Protokollebene

☐ Unterstützt die E-Mail-Client-Software die Protokolle POP3S, IMAPS und SMTPS ?

Sichere Kommunikation auf Anwendungsebene mittels S/MIME

Die nachfolgenden Kontrollfragen müssen geprüft werden, wenn zur Absicherung der Kommunikation auf Anwendungsebene S/MIME verwendet wird:

☐ Unterstützt die E-Mail-Client-Software oder das eingesetzte Plug-In S/MIME?

☐ Werden starke Kryptoalgorithmen unterstützt[1]?

1 Im Bundesanzeiger werden geeignete Algorithmen sowie die empfohlenen Schlüssellängen für Verschlüsselung, für digitale Signatur und für das Hashen von Daten veröffentlicht.

- ☐ Können Schlüssel mit einer entsprechenden Länge für eine sichere Kommunikation verwendet werden?
- ☐ Ist eine sichere Aufbewahrung des privaten Schlüssels gewährleistet?
  - ☐ *Kann das Exportieren des Schlüssels verhindert werden?*
  - ☐ *Ist der private Schlüssel durch ein Passwort geschützt?*
- ☐ Wird das Zertifikatsformat X.509 unterstützt?
- ☐ Wird das Sperrlistenformat ab CRLv2 unterstützt?
- ☐ Können Zertifikate verwendet werden, die keine E-Mail-Adresse enthalten?
- ☐ Werden die S/MIME-Nachrichtenaustauschformate Signed-Data und Multipart-Signed für signierte E-Mails sowie Enveloped-Data für verschlüsselte E-Mails unterstützt?
- ☐ Enthält das Produkt Schnittstellen zu kryptografischen Token (wie PKCS#11 oder das proprietäre Microsoft CSP), um X.509-Zertifikaten auf Smart Cards einbinden zu können?
- ☐ Können Wurzelzertifikate nachträglich zum lokalen Zertifikatsspeicher hinzugefügt werden?
- ☐ Wird für den Import von Zertifikaten und privaten Schlüsseln aus Dateien das Format PKCS#12 unterstützt?
- ☐ Wird für den Abruf von CRLs HTTP/HTTPS oder LDAP unterstützt?
- ☐ Werden Mehrfachsignaturen unterstützt?
- ☐ Ist das Versenden von S/MIME-Quittungen möglich?

Sichere Kommunikation auf Anwendungsebene mittels OpenPGP

Die nachfolgenden Kontrollfragen müssen geprüft werden, wenn zur Absicherung der Kommunikation auf Anwendungsebene OpenPGP verwendet wird:

- ☐ Unterstützt die E-Mail-Client-Software die Integration von OpenPGP?
- ☐ Werden starke Kryptoalgorithmen unterstützt?
- ☐ Können Schlüssel mit einer entsprechenden Länge für eine sichere Kommunikation verwendet werden?
- ☐ Ist eine sichere Aufbewahrung des privaten Schlüssels möglich?
  - ☐ *Kann das Exportieren des Schlüssels verhindert werden?*
  - ☐ *Ist der private Schlüssel durch ein Passwort geschützt?*
- ☐ Wird das Sperren von OpenPGP-Schlüsselpaaren unterstützt (*key revocation certificate*)?
- ☐ Können öffentliche Schlüssel von Empfängern durch den Client vom OpenPGP-Keyserver abgerufen werden?
- ☐ Kann zur Gewährleistung der Integrität eine digitale Signatur über den eigenen öffentlichen Schlüssel (Eigensignatur) erzeugt werden?
- ☐ Ist eine Funktion zur Wiederherstellung von Schlüsseln (*key recovery*), die zur Verschlüsselung von Daten verwendet wurden, vorhanden?
- ☐ Wird eine Key ID (Schlüsselnummer, die einen Schlüssel eindeutig identifiziert) für die Zuordnung von öffentlichem Schlüssel zu einer Person unterstützt?

Verzeichnisdienst

☐ Können in den E-Mail-Client über das Protokoll LDAP verschiedene Verzeichnisdienste eingebunden werden?

☐ Wird ein sicherer SASL-Mechanismus zur Authentifizierung des Clients an den Verzeichnisserver unterstützt?

3.2 Virenschutzprogramm

Die folgenden Kontrollfragen betreffen die Auswahl eines Virenschutzprogramms, das Schutz vor Schadprogrammen wie Viren, Würmer, Trojanische Pferde, Spyware und Adware bieten soll.

☐ Können das Virenschutzprogramm sowie die Virenschutz-Signaturen unverzüglich und automatisch nach Veröffentlichung neuer Virenschutz-Signaturen aktualisiert werden?

☐ Kann die Aktualisierung so gesteuert werden, dass eine Aktualisierung erst nach Freigabe des Administrators erfolgt?

☐ Prüft das Virenschutzprogramm verschlüsselte E-Mails unmittelbar nach dem Entschlüsseln auf Schadprogramme?

☐ Verfügt die Software über einen Quarantäne-Bereich für Schadprogramme?

☐ Ist eine Prüfung auf Schadprogramme basierend auf Virenschutz-Signaturen möglich?

☐ Unterstützt das Produkt eine heuristische Prüfung auf Schadprogramme?

☐ Unterstützt das Virenschutzprogramm die mittels TLS abgesicherten Protokolle POP3, IMAP und SMTP?

☐ Kann das Virenschutzprogramm Aktive Inhalte auf Schadprogramme (z. B. VBScript, JavaScript, ActiveX Controls und Java Applets) prüfen, sofern das E-Mail-Programm Aktive Inhalte ausführen kann?

☐ Kann der Nutzer mit dem Produkt eine Prüfung auf Schadprogramme selbst initiieren (*on-demand*)?

☐ Kann bei dem Programm eingestellt werden, dass Dateien, die auf dem Client-Rechner gelesen oder geschrieben werden, sofort auf Schadprogramme geprüft werden (*on-access*)?

☐ Läuft die Prüfung auf Schadprogramme im Hintergrund ab?

☐ Stellt das Virenschutzprogramm eine Schnittstelle für die E-Mail-Client-Software bereit, so dass der E-Mail-Client die Software integrieren und für eine Prüfung auf Schadprogramme aufrufen kann?

3.3 Anti-Phishing-Software

Die folgenden Kontrollfragen betreffen die Auswahl einer Anti-Phishing-Software.

☐ Verfügt die Software über einen Quarantäne-Bereich für E-Mails, die Phishing-Merkmale aufweisen?

☐ Kann das Produkt E-Mails auf Basis von Prüfsummen auf Phishing-Merkmale prüfen und ggf. die diesbezüglichen Inhalte blockieren?

- ☐ Ist eine automatische Aktualisierung der Prüfsummen für Phishing-Merkmale mit dem Produkt möglich?
- ☐ Kann das Produkt eine URL-Blacklist für Phishing-Seiten verwenden und ggf. die diesbezüglichen E-Mails blockieren?
- ☐ Ist eine automatische Aktualisierung der URL-Blacklist mit dem Produkt möglich?
- ☐ Stellt das Produkt eine Schnittstelle für den E-Mail-Client bereit, so dass der E-Mail-Client diese Software integrieren und für eine Prüfung aufrufen kann?

3.4 Anti-Spam-Software

Die folgenden Kontrollfragen betreffen die Auswahl einer optionalen Anti-Spam-Software.

- ☐ Können Spam-verdächtige E-Mails in einen Quarantäne-Bereich verschoben werden?
- ☐ Wird eine Sortierung von E-Mails auf der Basis von Blacklisting/Whitelisting von Wörtern und E-Mail-Adressen unterstützt?
- ☐ Ist die Filterung von E-Mails auf der Basis einer statistischen Inhaltsanalyse möglich?
- ☐ Kann die Software mit Spam und Ham trainiert werden, um Spam-Filter für gewünschte und nicht gewünschte E-Mails zu konfigurieren?
- ☐ Können Einträge des Adressbuchs in eine Whitelist aufgenommen werden?
- ☐ Stellt das Produkt eine Schnittstelle für die E-Mail-Client-Software bereit, so dass die E-Mail-Client-Software die Anti-Spam-Software integrieren und für eine Prüfung aufrufen kann?
- ☐ Unterstützt die Software die Prüfung verschiedener Dateiformate (z. B. pdf, xls, rtf) zur Ermittlung von in Anhängen verstecktem Spam?

3.5 Personal Firewall

Die folgenden Kontrollfragen betreffen die Auswahl einer Personal Firewall.

- ☐ Besteht das Produkt aus mindestens einem zustandslosen Paketfilter?
- ☐ Kann das Produkt auch ausgehende Pakete von unzulässigen Protokollen blockieren?
- ☐ Unterstützt das Produkt eine Protokollierung zur Aufzeichnung von Angriffsversuchen?

4 Konfiguration

Die Checklisten zur Konfiguration sind vor allem für Administratoren bestimmt, die eine sichere E-Mail-Client-Architektur einrichten wollen. Daneben dient der folgende Abschnitt auch als Hilfsmittel für Revisoren, die eine bestehende E-Mail-Client-Architektur einer Sicherheitsrevision unterziehen wollen.

4.1 E-Mail-Client-Software

Für die E-Mail-Client-Software sind folgende Prüfaspekte zu berücksichtigen.

Allgemein

☐ Ist das automatische Starten von Anwendungen, die mit Dateianhängen verknüpft sind (z. B. .ods mit OpenOffice) deaktiviert, so dass Anwendungen erst nach Abfrage und Bestätigung durch den Anwender gestartet werden?

☐ Ist der automatische Zugriff von Programmen – außer der E-Mail-Client-Software selbst – auf das Adressbuch über den E-Mail-Client ausgeschaltet?

☐ Ist das Versenden von automatischen Lesebestätigungen deaktiviert?

☐ Ist als Antwortadresse eine externe E-Mail-Adresse, also eine im Internet nutzbare E-Mail-Adresse, konfiguriert (z. B. name@firma.de)?

☐ Wird die Konfiguration von Stellvertreterberechtigungen restriktiv gehandhabt? Dies bedeutet, dass die Berechtigung des Zugriffs nur erteilt werden sollte, wenn unbedingt notwendig und nur die Funktionen freigeschaltet werden sollten, die für die Stellvertretung notwendig sind.

☐ Ist die automatische Weiterleitung von E-Mails deaktiviert?

☐ **[hohe Vertraulichkeit]** Werden lokal gespeicherte E-Mails verschlüsselt? **[Variante 5.3.4 A]**

- Wird ein verschlüsselter Ordner angelegt? – **oder** –
- Wird die ganze Festplatte verschlüsselt?

Bei E-Mail-Clients, die bei Verweisen auf externe Dateien und Schriftarten diese automatisch heruntergeladen können, ist folgende Prüffrage relevant:

☐ Ist der E-Mail-Client so konfiguriert, dass bei Verweisen auf externe Dateien und Schriftarten diese nicht automatisch heruntergeladen werden?

Bei E-Mail-Clients, die MIME-Types in einer E-Mail blockieren können, ist folgende Prüffrage relevant:

☐ **[hoher Schutzbedarf]** Ist das Blockieren gefährlicher MIME-Types mittels einer Blacklist konfiguriert? **[Variante 5.1.1 B]**

Authentifizierung

☐ Sind Benutzername und Kennwort zur Anmeldung am E-Mail-Server bei einer lokalen Speicherung verschlüsselt hinterlegt?

☐ Wird die Übermittlung der Authentifizierungsdaten abgelehnt, wenn keine Verschlüsselungsverfahren (also unverschlüsselt) oder kein geeigneter Verschlüsselungsalgorithmus vom E-Mail-Server verwendet wird?

S/MIME

☐ Wird für die Signierung von E-Mails das Nachrichtenaustauschformat „Clear Signed“ (auch als „Multipart-Signed“ bezeichnet) verwendet?

S/MIME und OpenPGP

☐ Werden starke Kryptoalgorithmen für Signatur und Verschlüsselung verwendet?

☐ Werden die Schlüssel mit entsprechender Länge generiert, damit eine sichere Signatur und Verschlüsselung möglich ist?

☐ Wird die Konfiguration von vertrauenswürdigen Herausgebern von Zertifikaten (z. B. Trustcenter) nur von zentraler Stelle ausgeführt, wie beispielsweise durch die Pflege einer Liste mit Zertifikaten vertrauenswürdiger Zertifizierungsstellen?

☐ Ist der private Schlüssel (S/MIME und OpenPGP) mittels eines Passwortes geschützt?

☐ Ist der private Schlüssel als „nicht exportierbar“ markiert?

Schutz vor Aktiven Inhalten

☐ Werden Aktiven Inhalte nicht ausgeführt? Das heißt:

- o Unterstützt das Produkt das Ausführen Aktiver Inhalte nicht? – **oder** –
- o Ist die Ausführung Aktiver Inhalte im E-Mail-Client deaktiviert? – **oder** –
- o Sofern der E-Mail-Client über einen Browser Aktive Inhalte ausführt: Ist die Ausführung Aktiver Inhalte im Browser generell deaktiviert?

HTML-E-Mail

☐ Werden HTML-E-Mails durch den E-Mail-Client sicher dargestellt?

- ☐ *Ist das Erstellen von E-Mails im HTML-Format ausgeschaltet und das Textformat gewählt?*
- ☐ *Werden empfangene E-Mails nur als Text angezeigt?*
- ☐ *Falls eine HTML-E-Mail durch die Darstellung als Text völlig unverständlich wird, besteht die Möglichkeit HTML-Strukturelemente anzuzeigen?*

☐ Ist das automatische Nachladen von „Inline Content“ wie Fotos ausgeschaltet?

☐ Ist die E-Mail-Client-Software so eingestellt, dass nicht nur Hyperlinks, sondern auch die tatsächliche URL oder nur diese angezeigt werden?

E-Mail-Vorschau

☐ Ist die Vorschaufunktionalität ausgeschaltet, sofern diese Aktive Inhalte ausführen kann?

Dateianhänge

☐ Ist die Software so konfiguriert, dass Dateianhänge vor dem Öffnen gespeichert und dann auf Schadprogramme geprüft werden?

☐ Ist das automatische Öffnen von Nachrichten außerhalb der Vorschau in der E-Mail-Client-Software ausgeschaltet (z. B. das automatische Öffnen der nächsten Nachricht nach dem Löschen einer Nachricht)?

☐ Ist das automatische Öffnen und Speichern von Dateianhängen ausgeschaltet?

☐ Ist der E-Mail-Client so konfiguriert, dass alle Dateiendungen angezeigt werden?

- o Ist dazu eine entsprechende Konfiguration des Betriebssystems[2] durchgeführt– **oder** –
- o Ist dazu eine entsprechende Konfiguration des E-Mail-Client-Programms durchgeführt?

☐ Ist ergänzend im E-Mail-Client eingestellt, dass ausführbare Dateianhänge (z. B. bat, vbx, chm, com usw.) blockiert/ausgeblendet werden?

☐ Ist für die Ermittlung von gefährlichen Dateianhängen eine Erkennung anhand des Dateityps und auf Basis des Magic-Byte konfiguriert?

Die folgende Frage ist nur dann zu beantworten, wenn die Funktion vom E-Mail-Client unterstützt wird:

☐ Ist eine Liste mit zugelassenen Dateianhängen eingerichtet (Whitelisting), damit nur explizit erlaubte Dateianhänge angezeigt werden?

Festlegung des Zeichencodes

☐ Sind in der E-Mail-Client-Software die Zeichensätze 7-Bit ASCII, UTF-8, ISO 8859-1 (Latin-1) und ISO-8859-15 konfiguriert?

Kommunikation mit dem E-Mail-Server

☐ Sind sichere Protokolle zur Kommunikation des E-Mail-Clients mit dem E-Mail-Server konfiguriert?

- o Werden die Protokolle POP3/IMAP und SMTP über TLS verwendet? – **oder** –
- o Werden andere proprietäre Protokolle (z. B. MAPI) verwendet?

☐ Ist der E-Mail-Client entsprechend konfiguriert, sodass E-Mail-Protokolle mit einer schwachen oder ohne Verschlüsselung nicht verwendet werden können (wie z. B. SSLv2)?

Kommunikation mit dem Verzeichnisserver

☐ Erfolgt die Anbindung an den Verzeichnisserver mit dem Protokoll LDAP?

☐ Ist für die Authentifizierung des E-Mail-Clients am Verzeichnisserver die verschlüsselte Übermittlung von Benutzername und Kennwort konfiguriert?

☐ Ist auf dem LDAP-Proxy hinterlegt, auf welchem Verzeichnisserver das Zertifikat eines bestimmten Empfängers abrufbar ist?

2 Unter Windows muss z. B. der Explorer konfiguriert werden, damit auch bekannte Dateiendungen angezeigt werden.

4.2 Virenschutzprogramm

Für das Virenschutzprogramm sind folgende Prüfaspekte zu berücksichtigen.

- ☐ Erfolgt die Aktualisierung der Virenschutz-Signaturen automatisch und regelmäßig?
- ☐ Werden eingehende E-Mails unmittelbar auf Viren, Würmer, Trojanische Pferde, Spyware und Adware geprüft?
- ☐ Ist die Protokollierung bei allen Prüfungen aktiviert?
- ☐ Ist die Virenprüfung bei Zugriff auf Dateien aktiviert?
- ☐ Werden verschlüsselte Nachrichten und Dateien zuerst entschlüsselt und danach unmittelbar auf Schadprogramme geprüft?
- ☐ Werden E-Mails beim Empfang und vor dem Versand geprüft?
  - ☐ *Ist das Virenschutzprogramm bei der Übertragung mit POP3, IMAP und SMTP über TLS integriert?*

4.3 Anti-Phishing-Software

Für die Anti-Phishing-Software sind folgende Prüfaspekte zu berücksichtigen.

- ☐ Werden eingehende E-Mails unmittelbar auf Phishing-Merkmale geprüft?
- ☐ Werden Phishing-E-Mails protokolliert?
- ☐ Ist die automatische Aktualisierung der Phishing-Datenbank, in der die Adressen betrügerischer Webseiten eingetragen sind, eingeschaltet?
- ☐ Ist die automatische Aktualisierung der Prüfsummen von Phishing-Merkmalen eingeschaltet?
- ☐ Ist die automatische Aktualisierung der URL Blacklist eingeschaltet?

4.4 Anti-Spam-Software

Für die optionale Anti-Spam-Software sind folgende Prüfaspekte zu berücksichtigen.

- ☐ Werden E-Mails, die als Spam markiert sind, geeignet behandelt?
  - ☐ *Ist ein separater Quarantäne-Ordner eingerichtet?*
  - ☐ *Sind Filterregeln eingerichtet, die Spam-markierte E-Mails in den Quarantäne-Ordner verschieben?*
  - ☐ *Ist der Zugriff auf den Quarantäne-Ordner so konfiguriert, dass fälschlicherweise als Spam-markierte E-Mails wieder zurückgeschoben werden können?*
- ☐ Ist die automatische Aktualisierung der statistischen Datenbank zur Erkennung von Spam aktiviert?
- ☐ Ist die Software so konfiguriert, dass E-Mails von einem Absender, der beim Benutzer im Adressbuch steht, nicht als Spam markiert werden?
- ☐ Ist eine Protokollierung über eingehende Spam E-Mails aktiviert?

4.5 Personal Firewall

Für die Personal Firewall sind folgende Prüfaspekte zu berücksichtigen.

☐ Werden Zugriffe von außen, bis auf definierte Ausnahmen, auf den Client-Rechner blockiert? Eine zulässige Ausnahme ist der Fernwartungszugang für Rechner, die zentral administriert werden.

☐ Erfolgt der Datenverkehr nach außen nur über vordefinierte Ports und mit vordefinierten Programmen?

☐ Werden Angriffsversuche auf den E-Mail-Client von der Personal Firewall protokolliert und mindestens folgende Informationen aufgezeichnet: IP-Adresse (Source/Destination), Port, Dienst und Zeit/Datum[3]?

☐ Kann die vom Administrator festgelegte Reihenfolge zur Abarbeitung der Filterregeln nicht vom Benutzer verändert werden?

☐ Sind die von POP3S/IMAPS, SMTPS, HTTP/HTTPS, LDAP oder evtl. von proprietären Protokollen genutzten Ports freigeschaltet und Abfragen bzw. Abrufe über die Ports möglich?

3 Hierbei müssen geltende Gesetze und Vorschriften wie beispielsweise das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG) und Datenschutzbestimmungen betrachtet werden.

5 Betrieb

Die Checklisten zum sicheren Betrieb sind vor allem für Administratoren bestimmt, die eine sichere E-Mail-Client-Architektur betreiben wollen.

Die Anforderungen an den sicheren Betrieb der E-Mail-Client-Architektur setzen einen sicheren Betrieb der zugrunde liegenden IT-Systeme voraus. Darüber hinaus sind allgemeine IT-Grundschutzmaßnahmen umzusetzen [ITGSK].

5.1 Übergreifende Aspekte

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

☐ Werden die E-Mail-Richtlinien regelmäßig auf ihren Aktualisierungsbedarf hin geprüft?

☐ **[hoher Schutzbedarf]** Werden Systeme, die nicht den aktuellsten Stand der Virenschutzprogramme einsetzen, nicht in das lokale Netz eingebunden? **[Variante 5.1.3 A]**

☐ **[hoher Schutzbedarf]** Werden nur gepatchte Systeme in das lokale Netz eingebunden? **[Variante 5.1.8 A]**

☐ **[hoher Schutzbedarf]** Wird eine „12x7“-Überwachung von Exploits durchgeführt? **[Variante 5.1.8 B]**

☐ **[hohe Vertraulichkeit]** Werden Verschlusssachen mittels zugelassener Produkte verschlüsselt? **[Variante 5.3.3 C]**

5.2 E-Mail-Client-Software

Für die E-Mail-Client-Software sind folgende Kontrollfragen zu berücksichtigen.

☐ Werden Patches regelmäßig installiert?

☐ Sind Verfahren etabliert, wie auf Schwachstellen ohne verfügbare Patches zu reagieren ist?

☐ Ist eine (zentrale) E-Mail-Adresse eingerichtet, an die sicherheitsrelevante Vorkommnisse zu melden sind (z. B. mail_abuse@organisation.de)?

☐ Erfolgt eine umgehende Aktualisierung (Erweiterung) der Blacklist bei Bekanntwerden „schädlicher“ Dateianhänge?

5.3 Virenschutzprogramm

Für das Virenschutzprogramm sind folgende Kontrollfragen zu berücksichtigen.

☐ Erfolgt eine kontinuierliche Aktualisierung der Virenschutz-Signaturen?

☐ Wird eine periodische Überprüfung und Aktualisierung der Scan-Engine durchgeführt, damit neue Erkennungsmuster-Dateien eingespielt werden können?

☐ Wird bei Bedarf (z. B. bei Verdacht einer Infektion des PC mit Viren) eine Prüfung auf Schadprogramme durch den Anwender selbst (*on-demand*) durchgeführt?

☐ Erfolgt eine kontinuierliche Überwachung der Logdateien und Fehlermeldungen des Virenschutzprogramms?

5.4 Anti-Phishing-Software

Für die Anti-Phishing-Software sind folgende Kontrollfragen zu berücksichtigen.

☐ Erfolgt eine kontinuierliche Überwachung der Logdateien und Fehlermeldungen der Anti-Phishing-Software?

5.5 Anti-Spam-Software

Für die optionale Anti-Spam-Software sind folgende Kontrollfragen zu berücksichtigen.

☐ Wird eine regelmäßige Überprüfung der Quarantäne-Ordner auf *false positives* und deren Behebung durchgeführt?

☐ Erfolgt eine kontinuierliche Überwachung der Logdateien und Fehlermeldungen der Anti-Spam-Software?

5.6 Personal Firewall

Für die Personal Firewall sind folgende Kontrollfragen zu berücksichtigen.

☐ Werden aktuelle Sicherheitswarnungen verfolgt und unverzüglich sicherheitsrelevante Updates und Patches nach vorherigem Test eingespielt?

☐ Erfolgt eine kontinuierliche Überwachung der Logdateien und Fehlermeldungen der Personal Firewall?

6 Literaturverzeichnis

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

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