Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Nutzung von E-Mail mit KDE Kontact und KMail

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

Version 1.0

Vervielfältigung und Verbreitung

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände findet man 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

Die vorliegende Checkliste 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 Checkliste

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 dieser Checkliste beschränken sich auf produktspezifische Empfehlungen für den E-Mail-Client KDE Kontact und KMail (im weiteren Dokument als „Kontact“ bezeichnet) im Kontext des ISi-Mail-Client-Moduls. Die zur Zeit der Entstehung dieser Studie verfügbare stabile Version von Kontact und KMail diente als Basis für die folgende Checkliste. Es handelte sich dabei um Kontact 1.2.9 und KMail 1.9.9 in deutscher Sprache. Allgemeine Grundschutzmaßnahmen, die nicht spezifisch für die Verwendung von Kontact sind, werden von den Fragen nicht erfasst. Solche grundlegenden Empfehlungen sind in der allgemeinen Checkliste (ISi-Check zu ISi-Mail-Client) und den BSI-Grundschutzkatalogen [ITGSK] zu entnehmen. Die Grundschutzkataloge 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 die Nutzung von E-Mail. Nur ein kundiger Spezialist 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 Anwender bei der Konfiguration von Kontact die erforderlichen Maßnahmen und die dabei verfügbaren Varianten 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-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 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 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

Die Konzeptionsphase der sicheren Grundarchitektur erfolgt vor der Auswahl der sicheren Komponenten sowie vor der Konfiguration und dem Betrieb von E-Mail-Clients in einer E-Mail-Infrastruktur.

Da diese Phase bereits abgeschlossen sein sollte, bevor der E-Mail-Client konfiguriert wird, behandelt diese produktspezifische Checkliste die Konzeption nicht erneut.

3 Auswahl sicherer Komponenten

Auf die Konzeptionsphase folgt die Phase der Realisierung und Auswahl der sicheren Komponenten laut [ISi-E]. Da dieser Abschnitt bereits abgeschlossen sein sollte, bevor der Kontact konfiguriert wird, behandelt diese Checkliste nur Komponenten, die beim Einsatz von Kontact zusätzlich benötigt werden.

3.1 E-Mail-Client-Software/Plug-Ins

S/MIME

Die folgende Frage ist zu beantworten, wenn eine E-Mail-Verschlüsselung mittels S/MIME erfolgen soll.

☐ Wurde ein Programm oder Plug-In ausgewählt (z. B. gpgsm), mit dem eine sichere Verschlüsselung mittels des Standards S/MIME möglich ist?

OpenPGP

Die folgende Frage ist zu beantworten, wenn eine E-Mail-Verschlüsselung mittels des Standards OpenPGP erfolgen soll.

☐ Wurde ein Programm oder Plug-In ausgewählt (z. B. gpg), mit dem eine sichere Verschlüsselung mittels des Standards OpenPGP möglich ist?

4 Konfiguration

Nach der Beschaffung der benötigten Komponenten erfolgt deren Konfiguration durch die Administratoren. Der folgende Abschnitt enthält die für eine sichere Konfiguration zu berücksichtigenden Punkte.

Die zur Zeit der Entstehung dieser Studie verfügbare stabile Version von Kontact mit KMail diente als Basis für die folgende Checkliste. Es handelte sich dabei um Kontact 1.2.9 und KMail 1.9.9 in deutscher Sprache.

Optionen, die bereits in den Standardeinstellungen auf einen sicheren Wert vorkonfiguriert sind, werden von der Checkliste nicht immer explizit abgefragt. Bei bereits bestehenden Systemen sollte daher vor Anwendung der Checkliste die Konfiguration auf die Standardeinstellungen zurückgesetzt werden.

Die Reihenfolge der Menüpunkte in den Fragen entspricht genau der Bedienungsreihenfolge im E-Mail-Client. Die einzelnen Menü-Optionen bzw. -Ebenen sind dabei durch einen Rechtspfeil → voneinander getrennt.

Für nähere Informationen zu den angeführten Fragestellungen wird auf die BSI Studie [ISi-Mail-Client] verwiesen.

4.1 E-Mail-Client-Software

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

Allgemein

☐ Ist das Versenden von automatischen Lesebestätigungen deaktiviert? (*Einstellungen → KMail Einrichten → Sicherheit → Empfangs- und Lesebestätigungen → Versandregelung → Ignorieren* aktiviert.)

☐ Ist als Antwortadresse eine externe Adresse konfiguriert? Beispiel: name@firma.de. (*Einstellungen → KMailEinrichten → Identitäten →* <Identität wählen> *→ Ändern → Erweitert → Antwortadresse [Antwortadresse]*[1].)

☐ Ist sichergestellt, dass kein Filter für die Weiterleitung von E-Mails sorgt? (*Nachricht → Filter anlegen [keine Filter zum Weiterleiten konfiguriert]*.)

☐ **[hohe Vertraulichkeit]** Werden lokal gespeicherte E-Mails verschlüsselt[2]? **[Variante 5.3.4 A]**

Authentifizierung

☐ Werden lokal gespeicherte Benutzernamen und Kennwörter zur Anmeldung am E-Mail-Server verschlüsselt hinterlegt? (*Kontact unterstützt dazu KWallet, sofern dies installiert ist.*)

1 Dieses Feld muss nur ausgefüllt werden, wenn sich der Eintrag von der normalen Adresse (die für die Felder Name und E-Mail-Adresse auf der Karteikarte Allgemein verwendet wurde) unterscheidet, da Antworten standardmäßig immer an die Absenderadresse geschickt werden.

2 Kontact unterstützt keine Verschlüsselung von lokal gespeicherten E-Mails. Infolgedessen sollte ein externes Verschlüsselungsprogramm zur Verschlüsselung der entsprechenden Verzeichnisse oder der gesamten Festplatte mit starken Verschlüsselungsalgorithmen wie z. B. AES benutzt werden.

S/MIME

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

☐ Sind X.509v3 Zertifikate für die Verschlüsselung und die digitale Signatur konfiguriert? (*Einstellungen → KMail Einrichten → <Identität wählen> → Ändern → Kryptografie → S/MIME-Unterschriftzertifikat* und *S/MIME-Verschlüsselungszertifikat* konfigurieren.*)*

☐ Ist das Verifizieren von Zertifikaten konfiguriert? (*Einstellungen → KMail Einrichten → Sicherheit → S/MIME-Prüfung.* Hier kann entweder *Gültige Zertifikate unter Verwendung von CRLs* oder *Zertifikate online überprüfen (OCSP)* aktiviert werden.)

OpenPGP

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

☐ Sind OpenPGP-Schlüssel für die Verschlüsselung und die digitale Signatur konfiguriert? (*Einstellungen → KMail Einrichten → <Identität wählen> → Ändern → Kryptografie → OpenPGP-Signaturschlüssel* und *OpenPGP-Schlüssel zum Verschlüsseln* konfigurieren.*)*

HTML-E-Mail

☐ Ist der E-Mail-Client hinreichend vor HTML-E-Mails geschützt?

- ☐ *Ist das Erstellen von E-Mails im HTML-Format ausgeschaltet und das Textformat gewählt?* (*Neue Nachricht → Optionen → Formatierung HTML* deaktiviert.)
- ☐ *Werden empfangene E-Mails nur als Text angezeigt?* (*Einstellungen → KMailEinrichten → Sicherheit →Lesen → HTML-Nachrichten → HTML-Ansicht vor Klartext bevorzugen* deaktiviert.).
  Hinweis: Falls eine HTML-E-Mail durch die Darstellung als Text völlig unverständlich wird, besteht die Möglichkeit für den Benutzer eine einzelne E-Mail durch Markieren der E-Mail und Auswählen von „Ordner → HTML-Ansicht vor Klartext bevorzugen" als HTML anzuzeigen.Dazu erhält der Benutzer einen entsprechenden Warnhinweis.

☐ Ist das automatische Nachladen von „Inline Content" wie Fotos ausgeschaltet? (*Einstellungen → Kontact Einrichten → Sicherheit →Lesen → HTML-Nachrichten → Nachrichten dürfen externe Referenzen aus dem Internet laden* deaktiviert.)

Festlegung des Zeichencodes

☐ Sind im E-Mail-Client die 8-Bit Zeichencodes UTF-8 und ISO 8859-1 (Latin-1) konfiguriert? (*Neue Nachricht → Optionen → Kodierung festlegen → Unicode (UTF-8)* oder *Westeuropäisch (ISO 8859-1)* aktivieren.)

Kommunikation mit dem E-Mail-Server

☐ Sind für die Kommunikation mit dem E-Mail-Server sichere Protokolle konfiguriert?

- ☐ *Ist für die Kommunikation mit dem Postausgangsserver (SMTP) die Verschlüsselung via TLS oder SSL aktiviert?* (*Einstellungen → KMail Einrichten → Zugänge → Versand → <Ausgangspostfach auswählen> → Ändern → Sicherheit → Verschlüsselung → TLS oder SSL* aktiviert.)

☐ *Ist für die Kommunikation mit dem POP3/IMAP-Server die Verschlüsselung via TLS oder SSL sowie die sichere Authentifizierung aktiviert? (Einstellungen → KMail Einrichten → Zugänge → Empfang → <Eingangspostfach auswählen> → Ändern → Sicherheit → Verschlüsselung → TLS oder SSL für sicheres Abholen von Nachrichten benutzen* aktiviert*.)*

Kommunikation mit dem Verzeichnisserver

☐ Ist zur Anbindung von Verzeichnisservern das Protokoll LDAP eingestellt? (*Einstellungen → Kontact Einrichten → Kontakte→ LDAP Nachschlagefunktion* konfigurieren.)

☐ Ist für die Authentifizierung des E-Mail-Clients am Verzeichnisserver die verschlüsselte Übermittlung von Benutzername und Kennwort konfiguriert? (*Einstellungen → Kontact Einrichten → Kontakte→ LDAP Nachschlagefunktion → Sicherheit TLS aktivieren*)?

Einstellungen bezüglich Virenschutzprogramme

☐ Ist ein Virenschutzprogramm für das Konto konfiguriert? (*Extras → Anti-Virus Assistent* konfigurieren.)

☐ *Werden Nachrichten mit dem Virenschutzprogramm geprüft? (Extras → Anti-Virus Assistent → <Name Virenschutzprogramm> → Weiter → Nachrichten mit Anti-Virus-Programmen prüfen* aktiviert*.)*

☐ *Ist konfiguriert, dass Nachrichten, die mit Schadprogrammen behaftet sind, in einen Quarantäne-Ordner verschoben werden? (Extras → Anti-Virus Assistent → <Name Virenschutzprogramm> → Weiter → Erkannte Viren-Nachrichten in den ausgewählten Ordner verschieben* aktiviert*.)*

Einstellungen bezüglich Spam

Die Bearbeitung der Fragen dieses Abschnitts ist nur notwendig, wenn in der E-Mail-Client-Architektur eine Spam-Filter-Komponente vorgesehen ist.

☐ Ist der Spam-Filter für das Konto konfiguriert? (*Extras → Anti-Spam Assistent* konfigurieren.)

☐ *Ist das Verschieben von Spam-Nachrichten, in einen Quarantäne-Ordner konfiguriert? (Extras → Anti-Virus Assistent → <Name Spam-Filters> → Weiter → Erkannte unerwünschte Nachrichten verschieben nach* aktiviert*.)*

5 Grundvorgaben für den sicheren Betrieb

Im Betrieb unterscheidet sich Kontact kaum von anderen E-Mail-Clients. Aus diesem Grund sind lediglich die Anforderungen der allgemeinen Checkliste (ISi-Check zu ISi-Mail-Client) zu beachten.

6 Literaturverzeichnis

[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-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-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/