



Bundesamt
für Sicherheit in der
Informationstechnik



Sichere Nutzung von E-Mail mit Lotus Notes 8.0

BSI-Checkliste zur Notes-8.0-Sicherheit (ISi-Check)

Version 1.0

Vervielfältigung und Verbreitung

Bitte beachten Sie, dass das Werk einschließlich aller Teile urheberrechtlich geschützt ist.

Erlaubt sind die Vervielfältigung und Verbreitung zu nicht-kommerziellen Zwecken, insbesondere zu Zwecken der Ausbildung, Schulung, Information oder hausinternen Bekanntmachung, sofern sie unter Hinweis auf die ISi-Reihe des BSI als Quelle erfolgen.

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>

© Bundesamt für Sicherheit in der Informationstechnik 2009

Inhaltsverzeichnis

1 Einleitung.....	5
1.1 Funktion der Checkliste.....	5
1.2 Benutzung der Checklisten.....	5
2 Konzeption.....	7
2.1 Client-PCs.....	7
3 Auswahl sicherer Komponenten.....	8
3.1 E-Mail-Client-Software/Plug-Ins.....	8
4 Konfiguration.....	9
4.1 E-Mail-Client-Software.....	9
5 Grundvorgaben für den sicheren Betrieb.....	12
6 Literaturverzeichnis.....	13

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 Lotus Notes 8.0 (im weiteren Dokument als „Notes“ bezeichnet) im Kontext des ISi-Mail-Client-Moduls. Die zur Zeit der Entstehung dieser Studie verfügbare stabile Version von Lotus Notes 8 diente als Basis für die folgende Checkliste. Es handelte sich dabei um Lotus Notes 8.0.1 in deutscher Sprache. Allgemeine Grundschutzmaßnahmen, die nicht spezifisch für die Verwendung von Notes 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 Prüfaspkte 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 Notes 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 Prüfaspkten 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 dieser Phase bereits abgeschlossen sein sollte, bevor der E-Mail-Client konfiguriert wird, behandelt diese produktspezifische Checkliste die Konzeption nicht erneut im Detail.

2.1 Client-PCs

- Wird verhindert, dass die vom Administrator getroffenen Einstellungen von Benutzern verändert werden können (siehe auch „Einsatz von Policy Documents“ im Kapitel 4.1 auf Seite 11)?

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 E-Mail-Client konfiguriert wird, behandelt diese Checkliste nur Komponenten, die beim Einsatz von Notes 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 eine sichere Komponente zur Verschlüsselung von E-Mails mittels S/MIME ausgewählt?
 - Entspricht die in Notes enthaltene Komponente zur Nutzung von S/MIME den Anforderungen einer sichere Verschlüsselung mittels des Standards S/MIME? – **oder** –
 - Wurde ein Programm oder Plug-In ausgewählt, 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, 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 Lotus Notes 8 diene als Basis für die folgende Checkliste. Es handelte sich dabei um Lotus Notes 8.0.1 in deutscher Sprache unter Windows/XP (SP3).

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 Lotus Notes sind folgende Prüfaspekte zu berücksichtigen.

Allgemein

- Ist das Versenden von automatischen Lesebestätigungen deaktiviert? (Die Deaktivierung der Lesebestätigung muss im Lotus Domino Designer mittels einer Funktion konfiguriert werden. Weitere Informationen können unter <http://www.ibm.com/developerworks/lotus/library/ls-BlockRetRec/index.html> abgerufen werden.)
- Ist als Antwortadresse eine externe Adresse konfiguriert? Beispiel: name@firma.de. (*Datei* → *Arbeitsumgebungen* → *Arbeitsumgebungen verwalten...* → *<Name Arbeitsumgebung>* → *Bearbeiten...* → *Internet-Mailadresse*)?
- Ist die automatische Weiterleitung von E-Mails deaktiviert? (In *Werkzeuge* → *Regeln* → *Neue Regel* dürfen keine automatischen Weiterleitungen konfiguriert sein.)
- [hohe Vertraulichkeit]** Werden lokal gespeicherte E-Mails verschlüsselt? **[Variante 5.3.4 A]** (*Datei* → *Sicherheit* → *Benutzersicherheit* → *Notes Daten* → *Notes Datenbanken* → *Lokal verschlüsseln mit: Starker Verschlüsselung*.)

S/MIME

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

- Ist S/MIME konfiguriert? (*Datei* → *Sicherheit* → *Benutzersicherheit...* → *Mail* → *Option für Mail im Internetstil* → *MIME-Format zum Senden von Mail* → *MIME-Format (in dieser Arbeitsumgebung) zum Senden von Mail an Internetadressen verwenden* aktiviert.)

- Sind X.509v3 Zertifikate für die Verschlüsselung und die digitale Signatur konfiguriert? (Datei → Sicherheit → *Benutzersicherheit...* → Mail → Option für Mail im Internetstil → MIME-Format zum Senden von Mail → Zertifikatkonfiguration.)

Schutz vor Aktiven Inhalten

- Ist das Ausführen von Aktiven Inhalten über die Browsereinstellungen des E-Mail-Clients ausgeschaltet? (Datei → Sicherheit → *Benutzersicherheit...* → *Tätigkeiten anderer aufrufen*. Dabei unter *Workstation, Applets und JavaScript für die Kategorien -Default- und -No Signature-* alle Rechte deaktivieren. Außerdem unter Datei → *Arbeitsumgebungen* → *Arbeitsumgebungen verwalten...* → *<Name Arbeitsumgebung>* → *Bearbeiten...* → *Erweitert...* → *Netzwerkzugriff für nicht vertrauenswürdige Hosts: Java deaktivieren und Netzwerkzugriff für vertrauenswürdige Hosts: Java deaktivieren*. Ferner unter Datei → *Vorgaben...* → *Notes Client-Basiskonfiguration* → *Java-Applets aktivieren [deaktiviert], JavaScript aktivieren [deaktiviert] und Java-Zugriff von JavaScript aus aktivieren [deaktiviert]*.)

HTML-E-Mail

- Ist der E-Mail-Client hinreichend vor HTML-E-Mails geschützt?
- Ist als Format für Weiterleitungen und Antworten Nur-Text gewählt? (Datei → *Vorgaben* → Mail → Internet → *Internet Mail Format: Nur einfacher Text*.)
- Ist das automatische Nachladen von „Inline Content“ wie Fotos ausgeschaltet? (Datei → *Vorgaben* → Mail → Internet → *Sicherheit von Bilder* → *Keine Remote Bildern ohne meine Zustimmung anzeigen*.)

Festlegung des Zeichencodes

- Sind im E-Mail-Client die 8-Bit Zeichencodes UTF-8 und/oder ISO 8859-1 (Latin-1) konfiguriert? (Datei → *Vorgaben* → Mail → Internet → *Format für mehrsprachige Internet-Mail: Unicode (UTF-8) verwenden*.)

Kommunikation mit dem E-Mail-Server

- Sind für die Kommunikation mit einem E-Mail-Server sichere Protokolle konfiguriert?
- Ist für die Kommunikation mit dem POP3/IMAP-Server die Verschlüsselung via TLS oder SSL sowie die sichere Authentifizierung aktiviert? (Datei → *Vorgaben* → *Accounts* → *<Accountname>* → *Account bearbeiten...* → *Typ: IMAP online (SSL aktiviert) oder Typ: POP (SSL aktiviert)*.)
- Ist für die Kommunikation mit dem Postausgangsserver (SMTP) die Verschlüsselung via TLS oder SSL aktiviert? (Datei → *Vorgaben* → *Accounts* → *<Accountname>* → *Account bearbeiten...* → *Typ: SMTP (SSL aktiviert)*.)

Bei der Anbindung des E-Mail-Clients an einen Lotus Domino Server:

- Ist der Port für die Kommunikation mit den Notes Clients (NRPC) auf „verschlüsselt“ geschaltet? (In der *NOTES.INI* auf dem Server muss den Eintrag *TCPIP=TCP,0,15,0,,12320*, auf *TCPIP=TCP,0,15,0,45088* geändert werden. Hiermit ist die Kommunikation aller Notes Clients mit dem Server verschlüsselt, unabhängig davon, was auf den Clients konfiguriert ist.)

Kommunikation mit dem Verzeichnisserver

- Ist zur Anbindung von Verzeichnissen das Protokoll LDAP eingestellt? (*Datei* → *Vorgaben* → *Accounts* → *<Accountname>* → *Account bearbeiten...* → *Typ: LDAP.*)

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 das Verschieben von Spam-Nachrichten, in einen Quarantäne-Ordner konfiguriert? (*Werkzeuge* → *Regeln* → *Neue Regel* konfigurieren.)

Einsatz von Policy Documents

- Wurden die in dieser Checkliste vorgegebenen Einstellungen, soweit möglich, mit Hilfe von Policy Documents innerhalb eines Domino Servers konfiguriert, so dass Benutzer die Konfiguration nicht verändern können?

5 Grundvorgaben für den sicheren Betrieb

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

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-Grundschatzkataloge, 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/>