Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Nutzung von E-Mail mit Microsoft Outlook 2007

BSI-Checkliste zur Outlook 2007-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....5
1.1 Funktion der Checklisten....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....14
6 Literaturverzeichnis....15

1 Einleitung

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

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 dieser Checkliste beschränken sich auf produktspezifische Empfehlungen für den E-Mail-Client Microsoft Outlook 2007 (im weiteren Dokument als „Outlook“ bezeichnet) im Kontext des ISi-Mail-Client-Moduls. Die zur Zeit der Entstehung dieser Studie verfügbare stabile Version von Outlook 2007 in deutscher Sprache diente als Basis für die folgende Checkliste. Allgemeine Grundschutzmaßnahmen, die nicht spezifisch für die Verwendung von Outlook sind, werden von den Fragen nicht erfasst. Solche grundlegenden Empfehlungen sind in der allgemeinen Checkliste (ISi-Check zu ISi-Mail-Client) und den BSI-IT-Grundschutzkatalogen [ITGSK] zu entnehmen. Die IT-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 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 Anwender bei der Konfiguration von Outlook 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-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 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

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 im Detail.

2.1 Client-PCs

☐ Wird verhindert, dass die vom Administrator getroffenen Einstellungen von Benutzern verändert werden können (siehe auch „Einsatz von Gruppenrichtlinien“ im Kapitel 4.1 auf Seite 13)?

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 Outlook 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?

- o Entspricht die in Outlook enthaltene Komponente zur Nutzung von S/MIME den Anforderungen einer sichere Verschlüsselung mittels des Standards S/MIME? – **oder** –
- o 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.

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 Microsoft Outlook 2007 sind folgende Prüfaspekte zu berücksichtigen.

Allgemein

☐ Ist der automatische Zugriff von anderen Programmen – außer der E-Mail-Client-Software selbst – auf das Adressbuch über den E-Mail-Client ausgeschaltet? *(Für Windows Systeme sollten die Registrierung angepasst und die Registrierungsschlüssel PromptOOMAddressBookAccess und PromptOOMAddressInformationAccess auf den Wert „0“ gesetzt werden, damit der Zugriff automatisch verweigert wird. Weitere Informationen sind auf der Microsoft Webseite unter http://support.microsoft.com/kb/926512 zu finden.)*

☐ Ist das Senden einer E-Mail durch ein Fremdprogramm mittels des Outlook Object Models ausgeschaltet? *(Für Windows Systeme sollte die Registrierung angepasst und der Registrierungsschlüssel PromptOOMSend auf den Wert „0“ gesetzt werden, damit das Senden einer E-Mail durch ein Fremdprogramm automatisch verweigert wird. Weitere Informationen sind auf der Microsoft Webseite unter http://support.microsoft.com/kb/926512 zu finden.)*

☐ Ist das Versenden von automatischen Lesebestätigungen deaktiviert? (*Extras → Optionen → Einstellungen → E-Mail-Optionen... → Verlaufoptionen... → Immer eine Antwort senden [deaktiviert] sowie Nie eine Antwort senden [aktiviert]*.)

☐ Ist als Antwortadresse eine externe Adresse konfiguriert (z. B. name@firma.de)

- ☐ *Bei der Anbindung des E-Mail-Clients an den Mail-Server über SMTP und POP3/IMAP: Extras → Kontoeinstellungen... → E-Mail → Konto wählen → Ändern... → E-Mail-Adresse*?– **oder** –
- ☐ *Bei der Anbindung des E-Mail-Clients an einen Microsoft Exchange Server:* Die Antwortadresse wird nicht in Outlook, sondern im Active Directory in der Kontokonfiguration des Benutzers unter General/E-Mail eingestellt.

☐ Ist die automatische Weiterleitung von E-Mails deaktiviert? (In *Extras → Regeln und Benachrichtigungen* dürfen keine Regeln konfiguriert sein, die eingehende E-Mails automatisch

an eine (externe) E-Mail-Adresse weiterleiten. Bei der Einbindung von Outlook in einen Exchange Server kann die automatische Weiterleitung von E-Mails auch serverseitig unterbunden werden, siehe [ISi-Check-Ex2003] und [ISi-Check-Ex2007].)

☐ **[hoher Schutzbedarf]** Werden lokal gespeicherte E-Mails verschlüsselt? **[Variante 5.3.4 A]**

☐ *Wird bei der Benutzung von Offline Dateien (bei der Benutzung von Exchange oder .pst-Dateien) diese Datei verschlüsselt[1]?*

☐ Ist das automatische Herunterladen von Schriftarten im Internet Explorer deaktiviert, um die Ausführung von Programmen von entfernten Standorten (Remote) zu verhindern? (*Im Internet Explorer: Extras →Internetoptionen → Sicherheit → Zoneneinstellungen → Stufe anpassen... → Download → Schriftartdownload → Deaktivieren.*)

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[2]? (*Extras → Vertrauensstellungscenter → E-Mail-Sicherheit → Einstellungen → Signaturzertifikat: Auswählen...* und *Verschlüsselungszertifikat: Auswählen.*)

☐ Ist S/MIME konfiguriert? (*Extras → Vertrauensstellungscenter → E-Mail-Sicherheit → Einstellungen → Kryptografieformat → S/MIME.)*

☐ Ist als Hashalgorithmus für die digitale Signatur SHA1 ausgewählt? (*Extras → Vertrauensstellungscenter → E-Mail-Sicherheit → Einstellungen → Hashalgorithmus: SHA1.)*

☐ Ist als Verschlüsselungsalgorithmus 3DES[3] oder AES (nur ab Windows Vista) ausgewählt? (*Extras → Vertrauensstellungscenter → E-Mail-Sicherheit → Einstellungen → Verschlüsselungsalgorithmus: 3DES* oder *AES.)*

☐ Werden signierte Nachrichten als Klartext gesendet (*clear signed*)? (*Extras → Vertrauensstellungscenter → E-Mail-Sicherheit → Signierte Nachrichten als Klartext senden.*)

☐ Ist der private Schlüssel (S/MIME und OpenPGP) mittels eines Passwortes geschützt und als „nicht exportierbar“ markiert? *(*In Windows XP sollte beim Importieren einer PKCS#12-Datei folgende Vorgehensweise gewählt werden: Doppelklick auf das *Zertifikat → Weiter → Weiter → <Kennwort der PKCS#12-Datei eingeben>, „Hohe Sicherheit für den privaten Schlüssel aktivieren“ [aktiviert] und „Schlüssel als exportierbar markieren“ [deaktiviert] → Weiter → Weiter → Fertigstellen → „Sicherheitsstufe...“ → Hoch → Weiter → <Kennwort eingeben> → Fertigstellen).*

Schutz vor Aktiven Inhalten

☐ Ist das Ausführen von Aktiven Inhalten über die Browsereinstellungen des E-Mail-Clients ausgeschaltet? (*Im Internet Explorer: Extras → Optionen → Sicherheit → Zoneneinstellungen... → Standardstufe → Hoch*)?

1 Für hohen Schutzbedarf reicht es nicht aus, die in Outlook verfügbare Verschlüsselung zu benutzen, sondern es sollten externe Programme mit starken Verschlüsselungsalgorithmen wie z. B. AES benutzt werden.

2 Für die Konfiguration der Zertifikate in Outlook ist es notwendig erst einen Zertifikatsantrag zu generieren und die Zertifikate auf dem System zu installieren.

3 In Windows XP stehen keine starken Verschlüsselungsalgorithmen wie AES zur Verfügung. Stärkere Verschlüsselungsalgorithmen wie AES sind nur mittels Plug-Ins realisierbar. Dies hat aber Folgen für die Interoperabilität mit Nachrichtenempfängern, die dieses Plug-In nicht benutzen.

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?* (*Extras → Optionen... → E-Mail-Format → Verfassen im Nachrichtenformat: Nur-Text.*)
- ☐ *Werden empfangene E-Mails nur als Text angezeigt?* (*Extras → Vertrauenstellungscenter → E-Mail-Sicherheit → Standardnachrichten im Nur-Text-Format lesen.)*
- ☐ *Werden empfangene signierte E-Mails nur als Text angezeigt?* (*Extras → Vertrauenstellungscenter → E-Mail-Sicherheit → Digital signierte Nachrichten im Nur-Text-Format lesen [aktiviert].)*
- ☐ *Falls eine HTML-E-Mail durch die Darstellung als Text völlig unverständlich wird, besteht die Möglichkeit, den Text leserlich anzuzeigen* (Wichtig: diese Option sollte nur gewählt werden, sofern Aktive Inhalte deaktiviert wurden. In diesem Fall wird innerhalb der betreffenden E-Mail die Bemerkung „Diese Nachricht wurde zum Nur-Text-Format konvertiert“ angezeigt. Das Kontextmenü dieser Bemerkung bietet die Option *„Als HTML anzeigen“)?*

☐ Ist das automatische Nachladen von „Inline Content“ wie Fotos ausgeschaltet? (*Extras → Vertrauenstellungscenter → Automatischer Download → Bilder in HTML-Nachrichten oder RSS-Elementen nicht automatisch herunterladen [aktiviert]. Ferner sollten die fünf weiteren Unterpunkte deaktiviert werden.*)

Dateianhänge

☐ 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? Für Windows Systeme gibt es drei Möglichkeiten diese Anforderung umzusetzen:

- In der lokalen Registry (mittels des Registrierungsschlüssels AddWarningFileTypes, siehe http://support.microsoft.com/kb/259228/[4]) – **oder** –
- Mittels einer Gruppenrichtlinie. (In der Office Resource Kit sind Policy Templates enthalten. Nach der Installation des Outlook 2007 Templates kann mittels der Richtlinie „Allow access to e-mail attachments“ eine Liste mit Anlagen konfiguriert werden, so dass in Outlook erst nach Abfrage und Bestätigung der Anhang geöffnet wird, siehe http://technet.microsoft.com/en-us/library/cc178961.aspx.) – **oder** –
- Mittels des Outlook Security Templates. (Die Sicherheitseinstellungen können mit dem Outlook Formular „Outlook Security Template“ geändert werden. Anhand „Level 2 File Extensions“ können die Datei-Typen konfiguriert werden, die erst nach einer Bestätigung gestartet werden, siehe http://technet.microsoft.com/en-us/library/cc179095.aspx.)

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

- ☐ *Ist dazu eine entsprechende Konfiguration des Betriebssystems durchgeführt?* (*Windows-Explorer: Extras → Ordneroptionen → Ansicht → Erweiterungen bei bekannten Datentypen ausblenden [deaktiviert].)*

☐ Wurde für den E-Mail-Client eingestellt, dass ausführbare Dateianhänge (z. B. bat, vbx, chm, com usw.) blockiert/ausgeblendet werden? Für Windows Systeme gibt es drei Möglichkeiten

4 Der Knowledge Base Artikel beschreibt die Einstellungen für Outlook 2000. Für Outlook 2007 muss der Registrierungsschlüssel in HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\ erzeugt werden.

diese Anforderung umzusetzen:

- In der lokalen Registry (mittels des Registrierungsschlüssels „Level1Add“, siehe http://support.microsoft.com/kb/926512/) – **oder** –
- Mittels einer Gruppenrichtlinie. (In der Office Resource Kit sind Policy Templates enthalten. Nach die Installation des Outlook 2007 Templates kann mittels der Richtlinie „Add file extensions to block as level 1“ eine Liste mit Anlagen konfiguriert werden, die von Outlook ausgeblendet werden, siehe http://technet.microsoft.com/en-us/library/cc179095.aspx.) – **oder** –
- Anhand des Outlook Security Templates. (Die Sicherheitseinstellungen können mit dem Outlook Formular „Outlook Security Template“ geändert werden. Anhand „Level 1 File Extensions“ können die Datei-Typen konfiguriert werden, die von Outlook ausgeblendet werden, siehe http://office.microsoft.com/en-us/ork2003/HA011402931033.aspx.)

☐ Ist die Anlagenvorschau deaktiviert? *(Extras → Vertrauensstellungscenter → Anlagenbehandlung → Anlagenvorschau deaktivieren [aktiviert].)*

Festlegung des Zeichencodes

☐ Sind im E-Mail-Client die 8-Bit Zeichencodes UTF-8 und ISO 8859-1 (Latin-1) konfiguriert? (*Extras → Optionen... → E-Mail-Format → Internationale Optionen → Bevorzugte Codierung für ausgehende Nachrichten → Unicode (UTF-8) oder Westeuropäisch (ISO) und „Codierung ausgehender Nachrichten automatisch wählen“ [aktiviert]*.)

Kommunikation mit dem E-Mail-Server

☐ Sind sichere Protokolle zur Integration eines E-Mail-Servers, mit dem der E-Mail-Client kommuniziert, konfiguriert?

- *Bei der Anbindung des E-Mail-Clients an den E-Mail-Server über SMTP und POP3/IMAP:*
  Ist ein verschlüsselter Verbindungstyp (SSL/TLS) sowohl für die Kommunikation mit dem Posteingangsserver (POP3/IMAP) als auch dem Postausgangsserver (SMTP) aktiviert? (*Extras → Kontoeinstellungen...→ E-Mail → <Konto wählen> → Ändern... → Weitere Einstellungen ...→ Erweitert → TLS [aktiviert]*.) – **oder** –
- *Bei der Anbindung des E-Mail-Clients an einen Microsoft Exchange Server:*
  Ist die Option „Daten zwischen Microsoft Outlook und Microsoft Exchange Server verschlüsseln“ aktiviert? (*Extras → Kontoeinstellungen... → E-Mail → Konto wählen → Ändern... → Weitere Einstellungen... → Sicherheit → Daten zwischen Microsoft Outlook und Microsoft Exchange verschlüsseln [aktiviert]*.)

Kommunikation mit dem Verzeichnisserver

☐ Ist zur Anbindung von Verzeichnisservern das Protokoll LDAP eingestellt (*Extras → Konteneinstellungen... → Adressbücher*)?

☐ Ist für die Authentifizierung des E-Mail-Clients am Verzeichnisserver die verschlüsselte Übermittlung von Benutzername und Kennwort aktiviert (*Extras → Kontoeinstellungen... → Adressbücher → Auswählen → Ändern → Gesicherte Kennwortautentifizierung (SPA) notwendig*) [aktiviert]?

Virenschutzprogramm

In Outlook 2007 können keine expliziten Einstellungen bezüglich der Integration von Virenschutzprogrammen vorgenommen werden.

☐ Ist im Virenschutzprogramm die Integration in Outlook konfiguriert?

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 aktiviert (*Extras → Optionen... → Einstellungen → Junk-E-Mail... → Optionen → Junk-E-Mail Schutz: Hoch [aktiviert]*)?

☐ Ist die Software so konfiguriert, dass E-Mails von einem Absender, der beim Benutzer im Adressbuch steht, nicht als Spam markiert werden (*Extras → Optionen... → Einstellungen → Junk-E-Mail... → Sichere Absender → Meine Kontakte sind auch vertrauenswürdige Absender [aktiviert]*)?

☐ Sind Filterregeln für Spam-markierte E-Mails aktiviert?

  ☐ *Werden Spam-markierte E-Mails in den Quarantäne-Ordner verschoben* (*Extras → Optionen... → Einstellungen → Junk-E-Mail... → Optionen → Als Junk-E-Mail identifizierte Nachrichten nicht in den Junk-E-Mail-Ordner verschieben, sondern endgültig löschen[deaktiviert]*)*?*

Einstellungen bezüglich Phishing

☐ Sind sicherheitskritische Hyperlinks und Funktionen von Phishingnachrichten deaktiviert (*Extras → Optionen... → Einstellungen → Junk-E-Mail... → Optionen → Hyperlinks und sonstige Funktionen in Phishingnachrichten deaktivieren [aktiviert]*)?

Einsatz von Gruppenrichtlinien

☐ Wurden die in dieser Checkliste vorgegebenen Einstellungen, soweit möglich, mit Hilfe von Gruppenrichtlinien konfiguriert, so dass Benutzer die Konfiguration nicht verändern können?

5 Grundvorgaben für den sicheren Betrieb

Im Betrieb unterscheidet sich Outlook 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-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-Check-Ex2003] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Konfiguration von Microsoft Exchange 2003, 2009, http://www.bsi.bund.de/fachthem/sinet/

[ISi-Check-Ex2007] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Konfiguration von Microsoft Exchange 2007, 2009, http://www.bsi.bund.de/fachthem/sinet/