Bundesamt
für Sicherheit in der
Informationstechnik

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

BSI-Leitlinie zur Internet-Sicherheit (ISi-L)

Version 1.0

Vervielfältigung und Verbreitung

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 Leitlinie zur sicheren Nutzung von E-Mail

E-Mail ist neben dem Web einer der meist genutzten Internet-Dienste. Die Verwendung elektronischer Post ermöglicht einen einfachen, schnellen und kostengünstigen Austausch von Informationen und ersetzt zunehmend den traditionellen Briefverkehr. Allerdings birgt der Gebrauch von E-Mail über ein nicht vertrauenswürdiges Netz, wie beispielsweise dem Internet, auch erhebliche Gefahren, insbesondere in Bezug auf die Integrität und die Vertraulichkeit von Nachrichten.

Das Modul ISi-Mail-Client der BSI-Schriftenreihe zum Thema Internet-Sicherheit beschreibt die Grundlagen und Gefährdungen in Zusammenhang mit E-Mail und gibt entsprechende Sicherheitsempfehlungen. Die vorliegende Leitlinie fokussiert dabei auf die „Sichere Nutzung von E-Mail“ und basiert in erster Linie auf der Studie [ISi-Mail-Client]. Der „Sichere Betrieb von E-Mail-Servern“ wird in [ISi-Mail-Server] betrachtet.

1.1 Management Summary

In letzter Zeit erregten zahlreiche Meldungen über Schadprogramme, Phishing und Spam große Aufmerksamkeit. Jedes dieser Schlagwörter bezeichnet eine Gefährdung, die sich mit der Nutzung von E-Mail in Verbindung bringen lässt. So verbreiten sich beispielsweise Schadprogramme wie Viren, Würmer und Trojanische Pferde unter anderem über E-Mails. Der Zweck dieser Schadprogramme ist meist die Kompromittierung von Systemen oder Angriffe auf die Vertraulichkeit von Daten. Dazu werden häufig E-Mails mit gefälschtem Absender verschickt, die Schadcode oder einen Verweis auf eine präparierte Web-Seite mit Schadcode enthalten.

Eine andere Gefährdung stellen unerwünschte E-Mails (sog. Spam) dar. Ein übermäßig hohes Spam-Aufkommen kann unter Umständen zur Überlastung von E-Mail-Servern und damit zum Verlust der Verfügbarkeit führen. Aber auch für den einzelnen Benutzer kann Spam zum Problem werden. So ist die Erkennung von erwünschten E-Mails in einer großen Flut von Spam oft sehr zeitintensiv und kann zu Beeinträchtigungen im Arbeitsbetrieb führen.

Die vorliegende Leitlinie gibt eine Zusammenfassung der Empfehlungen aus der Studie „Sichere Nutzung von E-Mail“ [ISi-Mail-Client]. Diese Studie beschreibt wie bestehenden Gefährdungen bei normalem Schutzbedarf mit geeigneten Maßnahmen begegnet werden kann. Diese Maßnahmen beziehen sich dabei auf eine sichere Architektur des E-Mail-Clients, eine geschützte Anbindung an den E-Mail-Server und einen sicheren Austausch von Informationen zwischen den einzelnen Kommunikationspartnern. Zudem werden Varianten aufgezeigt, die auch einen höheren Schutzbedarf abdecken können.

In der vorgeschlagenen Architektur wird die eigentliche E-Mail-Client-Software durch weitere Komponenten für verschiedene Sicherheitsüberprüfungen ergänzt:

- ein Virenschutzprogramm, das eingehende und ausgehende E-Mails auf Schadprogramme prüft,
- eine Anti-Spam-Software, die unerwünschte E-Mails erkennt und aussortiert,
- eine Anti-Phishing-Software, die Angriffe abwehrt, bei denen der Benutzer mittels gefälschter E-Mails dazu verführt wird, vertrauliche oder persönliche Daten preiszugeben, und
- eine Personal Firewall, die alle eingehenden und ausgehenden Verbindungen filtert.

Darüber hinaus wird empfohlen eine E-Mail-Richtline zu erstellen, die beschreibt wie sich Benutzer bei der Nutzung von E-Mail zu verhalten haben. Beispielsweise sollten Dateianhänge nicht unbedacht geöffnet werden, um einer Infizierung mit Schadprogrammen vorzubeugen.

Die Anbindung der E-Mail-Clients an den E-Mail-Server sollte über standardisierter Protokolle erfolgen, die mittels SSL/TLS (Secure Socket Layer/Transport Layer Security) zusätzlich mit Authentisierung und Verschlüsselung gesichert werden sollten.

Schließlich sollten für den sicheren Austausch von Informationen zwischen den einzelnen Kommunikationspartnern Verfahren zur Verschlüsselung und Signierung von E-Mails genutzt werden.

1.2 Einführung und Überblick

Der Gebrauch eines E-Mail-Programms ist für viele Benutzer Routine. Allerdings bieten aktuelle Programme meist eine sehr umfangreiche Funktionspalette, die sich auf den ersten Blick nicht vollständig erschließt. Dabei kann der Funktionsumfang bei Programmen verschiedener Anbieter stark variieren. Dieser Abschnitt fasst die wesentlichen Funktionen zusammen.

Funktionen eines E-Mail-Clients

Zu den grundlegenden Funktionen eines E-Mail-Clients gehören das Abrufen und Anzeigen sowie das Erstellen und Versenden von Nachrichten. Darüber hinaus verfügen viele E-Mail-Clients über zusätzliche Funktionen wie z. B. ein Adressbuch, ein Vorschaufenster oder die Verwendung von Lesebestätigungen.

Eine weitere übliche Funktion ist die Darstellung von HTML-Nachrichten. Im Regelfall werden E-Mails im Textformat erstellt und versendet. Zur strukturierten Darstellung von Inhalten wie Texten, Bildern und Hyperlinks kann jedoch auch das HTML-Format verwendet werden. Um solche Inhalte korrekt anzeigen zu können, werden viele E-Mail-Clients mit ähnlichen Funktionen wie Browser ausgestattet. Dadurch ergeben sich prinzipiell auch die gleichen Sicherheitsprobleme wie bei Browsern. So können HTML-E-Mails beispielsweise Aktive Inhalte enthalten. Solche Aktiven Inhalte sind in den HTML-Code eingebettete Programme (z. B. JavaScript), die auf dem Rechner des Benutzers ausgeführt werden und somit einen möglichen Angriffspunkt bilden.

Auch Funktionen zur Signierung und Verschlüsselung von Nachrichten gehören heute bei vielen E-Mail-Clients zum Standard. Hier stehen häufig die Verfahren S/MIME oder OpenPGP zur Verfügung. Entsprechende Funktionen können entweder direkt im E-Mail-Client integriert sein oder durch Zusatzsoftware (sog. Plug-Ins) implementiert werden. Voraussetzung für die Nutzung von digitalen Signaturen und Verschlüsselung ist ein entsprechendes Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel. Bei S/MIME ist zusätzlich ein Zertifikat erforderlich, das von einer Zertifizierungsstelle (Trustcenter) ausgestellt wird. Bei OpenPGP entfällt diese Zertifizierungsstelle und wird durch gegenseitiges Benutzervertrauen, das sogenannte „Web of Trust“, ersetzt (siehe Abschnitt 1.4.3).

1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

Nachdem im vorherigen Abschnitt die wesentlichen Funktionen von E-Mail-Clients behandelt wurden, werden nun die Gefährdungen bei der Nutzung von E-Mail dargestellt. Diese Gefährdungen lassen sich in vier Kategorien einteilen, die im Folgenden näher beschrieben werden:

- Eindringen (sog. „Hacking“)
- Täuschen, Fälschen und Betrügen (Angriffe auf die Integrität und Authentizität)
- Ausspähen und Entwenden (Angriffe auf die Vertraulichkeit)
- Verhindern und Zerstören (Angriffe auf die Verfügbarkeit)

1.3.1 Eindringen und Übernehmen

Bedrohungen dieser Kategorie entstehen, wenn ein Angreifer versucht auf das System des Benutzers zuzugreifen und dieses unter seine Kontrolle zu bringen. Mögliche Ansatzpunkte für einen Angriff sind Schwachstellen in der verwendeten Software (z. B. dem E-Mail-Client). Das Bekanntwerden von Software-Schwachstellen ist keine Seltenheit und fester Bestandteil des IT-Alltags. Viele Hersteller sind jedoch bemüht, aufgedeckten Schwachstellen in ihrer Software mit entsprechenden Maßnahmen (Patches) schnellstmöglich zu begegnen. Dennoch bleiben Schwachstellen, für die noch keine Patches verfügbar sind, ein Risiko.

Ein weiteres Risiko dieser Kategorie stellen Schadprogramme wie Viren oder Würmern dar. Beide verbreiten sich u. a. über E-Mails. Während Würmer aktiv versuchen über bekannte Schwachstellen in Systeme einzudringen, müssen Viren vom Benutzer ausgeführt werden, um ihre Schadfunktion zu aktivieren. Sie nutzen daher eine Schwachstelle im Benutzerverhalten aus.

Die Bedrohungen durch Eindringen und Übernehmen können durch Konfigurations- und Wartungsfehler vergrößert werden, wenn beispielsweise ungepatchte Software oder veraltete Virenschutz-Signaturen eingesetzt werden.

1.3.2 Täuschen, Fälschen und Betrügen

Typische Beispiele für Bedrohungen dieser Kategorie sind Trojanische Pferde, Spoofing und Phishing. Trojanische Pferde sind Programme, die dem Benutzer nützlich erscheinen, aber im Hintergrund zusätzliche Funktionen ausführen. Solche Funktionen können beispielsweise das Ausspähen von Passwörtern oder das Installieren unerwünschter Software sein. Ähnlich wie Viren und Würmer werden Trojanische Pferde häufig über E-Mails verbreitet.

Unter Spoofing versteht man das Manipulieren oder Fälschen von E-Mails. Aufgrund fehlender Authentisierungsmechanismen bei der Übertragung von E-Mails ist es einem Angreifer beispielsweise möglich Nachrichten mit beliebigen Absenderadressen zu verschicken. Somit kann er gefälschte Informationen unter fremdem Namen versenden. Dieses kann zu Schäden führen, wenn der Empfänger die erhaltenen Informationen als authentisch und verbindlich ansieht. Häufig enthalten solche gefälschten E-Mails Schadcode in Dateianhängen oder Verweise auf präparierte Web-Seiten. Sofern der Benutzer dem Verweis folgt, wird dadurch Schadcode heruntergeladen (Drive-By-Download) oder er wird dazu verleitet vertrauliche Daten preiszugeben (Phishing).

1.3.3 Entwenden und Ausspähen

In diese Kategorie fallen insbesondere Angriffe auf die Vertraulichkeit von Informationen. Mögliche Ziele solcher Angriffe sind u. a. E-Mail-Inhalte und Benutzerdaten. E-Mail-Inhalte sind häufig ein leichtes Ziel, da E-Mails in der Regel unverschlüsselt übertragen werden. Dadurch ist es einem Angreifer möglich Nachrichten mitzulesen, sofern er den Netzverkehr abhören kann. Alternativ kann ein Angreifer auch versuchen sich Zugang zu einem E-Mail-Konto auf dem E-Mail-Server zu verschaffen. Eine mögliche Schwachstelle, die einen solchen Angriff ermöglicht, sind schwache Passwörter.

Eine Variante zum Ausspähen von Benutzerdaten sind Spyware bzw. Adware. Unter Spyware werden im Allgemeinen Programme gefasst, welche die Tätigkeiten eines Benutzers ausspionieren. Bei Adware handelt es sich um Programme, die zusätzlich zur eigentlichen Funktion noch Werbung einblendet. Dieses dient ähnlich wie beim Phishing meist dazu, den Benutzer auf bestimmte Web-Seiten zu locken.

Es sind jedoch nicht ausschließlich Nachrichten und Benutzerdaten für Angreifer interessant. So liefern Lesebestätigungen oder Web-Bugs z. B. wertvolle Informationen für Spammer. Web-Bugs sind in E-Mails eingebettete Objekte, die beim Betrachten der E-Mail von einem Server nachgeladen werden und dabei Informationen an diesen Server übermitteln. Die hierbei ausgenutzte Schwachstelle ist eine fehlerhafte bzw. unzureichende Konfiguration des E-Mail-Programms.

1.3.4 Verhindern und Zerstören

Verfügbarkeit ist neben Integrität und Vertraulichkeit ein wichtiger Aspekt der IT-Sicherheit. Angriffe auf die Verfügbarkeit des E-Mail-Dienstes richtet sich typischerweise gegen E-Mail-Server (siehe auch [ISi-Mail-Server]). Es bestehen aber auch Bedrohungen für den einzelnen Client. So kann beispielsweise ein erhöhtes Spam-Aufkommen den Arbeitsbetrieb erheblich stören. Aufgrund unzureichender Datensicherung oder Verhaltensfehler im Betrieb kann es auch zum Verlust von E-Mails kommen. Dieses ist als ernsthafte Gefährdung zu sehen, da es für den Arbeitsbetrieb oft notwendig ist auch auf bereits gelesene E-Mails erneut zuzugreifen.

1.4 Wesentliche Lösungen und Empfehlungen

Die Empfehlungen für eine sichere Nutzung von E-Mail gliedern sich in Empfehlungen für eine sichere Architektur des E-Mail-Clients, für eine sichere Anbindung der E-Mail-Clients an den E-Mail-Server und für einen sicheren Austausch von Informationen zwischen den Kommunikationspartnern. Die in diesem Abschnitt beschriebenen Lösungen und Empfehlungen dienen zum Schutz von Authentizität, Integrität, Vertraulichkeit und Verfügbarkeit bei normalen Schutzbedarf.

1.4.1 Sichere Architektur des E-Mail-Clients

Für den Schutz des E-Mail-Clients wird die in Abbildung 1.1 gezeigte Architektur empfohlen. Diese besteht aus den Komponenten E-Mail-Client-Software, Anti-Phishing, Anti-Spam, Virenschutzprogramm und Personal Firewall. Die einzelnen Komponenten werden im Folgenden kurz beschrieben. Anschließend erfolgt eine Betrachtung der Sicherheitsprüfungen bei ein- und ausgehenden E-Mails.

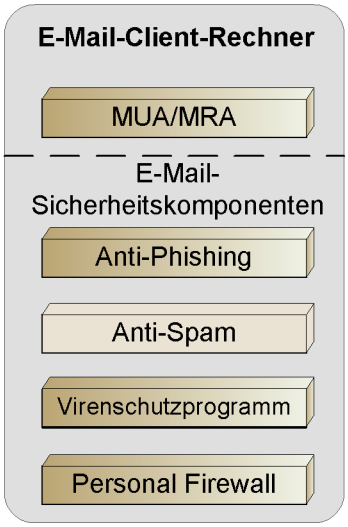

Abbildung 1.1.: Empfohlene Architekur für den E-Mail-Client

Die **E-Mail-Client-Software** dient sowohl zum Erstellen und Versenden als auch zum Empfangen und Anzeigen von Nachrichten. Zur sicheren Nutzung von E-Mail sollten folgende Aspekte beachtet werden:

- Vertrauliche oder persönliche Daten sollten stets verschlüsselt werden. E-Mails werden über das Internet normalerweise unverschlüsselt übertragen. Eine Verschlüsselung erfolgt nur über zusätzliche Maßnahmen. Dies kann dadurch erfolgen, dass der Benutzer selbst über die E-Mail-Client-Anwendung die Verschlüsselung mittels S/MIME oder OpenPGP anfordert. Alternativ ist die Verschlüsselung an einer zentralen Stelle mittels der sogenannten Virtuellen Poststelle (VPS) möglich. Der Einsatz der Virtuellen Poststelle wird in [ISi-Mail-Server] betrachtet.

- Bestimmte Dateianhänge (z. B. exe-, com-, vbs-Dateien) sollten blockiert werden. Nicht geblockte Anhänge sollten vor dem Öffnen auf Schadprogramme untersucht werden.
- Unerwartete Dateianhänge sollten prinzipiell nicht geöffnet werden. Dies gilt auch, wenn diese von bekannten Absendern stammen, da Absenderadressen gefälscht sein können.
- Bei einer E-Mail ohne digitale Signatur sind Absender und Inhalte beliebig fälschbar. Daher kann diesen Angaben nicht getraut werden.
- Nachrichten sollten stets als Text und nicht im HTML-Format angezeigt werden. Auch eine E-Mail-Vorschau sollte deaktiviert werden, wenn durch diese Aktive Inhalte ausgeführt werden könnten.

Die Komponente **Anti-Phishing** soll Angriffe ermitteln und vereiteln, die zum Ziel haben Benutzer mit gefälschten E-Mails zu verführen, vertrauliche oder persönliche Daten preiszugeben. Die hierbei verwendete Listen (z. B. mit Prüfsummen oder Verweisen auf bekannte Phishing-Seiten) sollten regelmäßig aktualisiert werden. Oftmals ist die Anti-Phishing-Funktion auch im Virenschutzprogramm integriert.

Die optionale Komponente **Anti-Spam** bietet Schutz gegen ungewünschte E-Mails. Hierzu kann die Spam-Filter-Funktion der E-Mail-Client-Software oder ein Spam-Filter in Form eines externen Programms verwendet werden. Einige Hersteller bieten Anti-Spam-Software auch als Teil des Virenschutzprogramms. Werden als Anti-Spam-Maßnahme Blacklists (Listen explizit geblockter Absender/Inhalte) bzw. Whitelists (Listen explizit erlaubter Absender/Inhalte) oder Signaturen verwendet, so sollten diese regelmäßig aktualisiert werden.

Viele Anti-Spam-Maßnahmen werden oftmals auf einem vorgeschalteten Spam-Filter-Server oder auf dem E-Mail-Server selbst durchgeführt. Auf diese Weise wird Spam entweder schon im Vorhinein in einen separaten Ordner verschoben oder gesondert gekennzeichnet. Gekennzeichneten Nachrichten können dann auf dem E-Mail-Client mittels einer Filterregel automatisch in einen dafür vorgesehenen Ordner verschoben werden.

Ein **Virenschutzprogramm** prüft eingehende und ausgehende E-Mails auf Schadprogramme und soll verhindern, dass Schadprogrammen auf dem E-Mail-Client ausgeführt werden oder vom Client verschickt werden. Es wird daher empfohlen einen E-Mail-Client zu verwenden, der die Möglichkeit zur Integration eines Virenschutzprogramms bietet. Um einen möglichst umfangreichen Schutz zu gewährleisten sollten aktuelle Virensignaturen verwendet und regelmäßig aktualisiert werden.

Die sichere E-Mail-Client-Architektur umfasst auch den Einsatz einer **Personal Firewall**. Es wird dringend empfohlen, alle von außen kommenden Zugriffe auf den Client-Rechner von der Personal Firewall prüfen zu lassen. Verbindungen in das Internet dürfen nur über definierte Ports initiiert werden.

Ein- und ausgehende E-Mails

Bei eingehenden E-Mails werden alle genannten Komponenten aktiv. Die Personal Firewall prüft zunächst, ob die Verbindung zum E-Mail-Server für das Abrufen der Nachrichten erlaubt ist. Ist dies der Fall, lässt die Personal Firewall die E-Mails durch. Diese werden dann vom Virenschutzprogramm auf schädliche Programme geprüft. Anschließend prüft die Anti-Spam-Komponente, ob die E-Mails bekannte Spam-Kennzeichen enthalten und blockiert Spam-behaftete Nachrichten. Abschließend sortiert die Anti-Phishing-Komponente E-Mails mit typischen Phishing-Merkmalen aus. Nach diesen Prüfungen können nun die E-Mails durch die E-Mail-Client-Software geöffnet werden.

Analog wird bei ausgehenden Nachrichten vorgegangen. Dabei entfallen jedoch die Prüfungen auf Spam- und Phishing-Merkmale, da diese Prüfungen für ausgehende E-Mails häufig nicht unterstützt werden. Entsprechende Prüfungen werden aber in der Regel durch den E-Mail-Server vorgenommen (siehe auch [ISi-Mail-Server]). Die lokale Untersuchung durch das Virenschutzprogramm findet hingegen statt. Gegebenenfalls werden ausgehende Nachrichten noch digital signiert und/oder verschlüsselt. Anschließend prüft die Personal Firewall, ob die Verbindung zum E-Mail-Server erlaubt ist.

1.4.2 Sichere Anbindung an den E-Mail-Server

Neben einer sicheren Architektur des E-Mail-Clients ist auch dessen sichere Anbindung an den E-Mail-Server von Bedeutung. Oft wird auch ein Verzeichnisserver eingesetzt, um Kontaktdaten und Zertifikate zentral zu verwalten. Gemäß [ISi-LANA] befinden sich beide Server im internen Netz und sind über den Paketfilter PF6 mit den Clients und dem Sicherheits-Gateway verbunden (vgl. Abbildung 1.2). Im Folgenden werden Schutzmaßnahmen der Anbindungen an beide Server beschrieben.

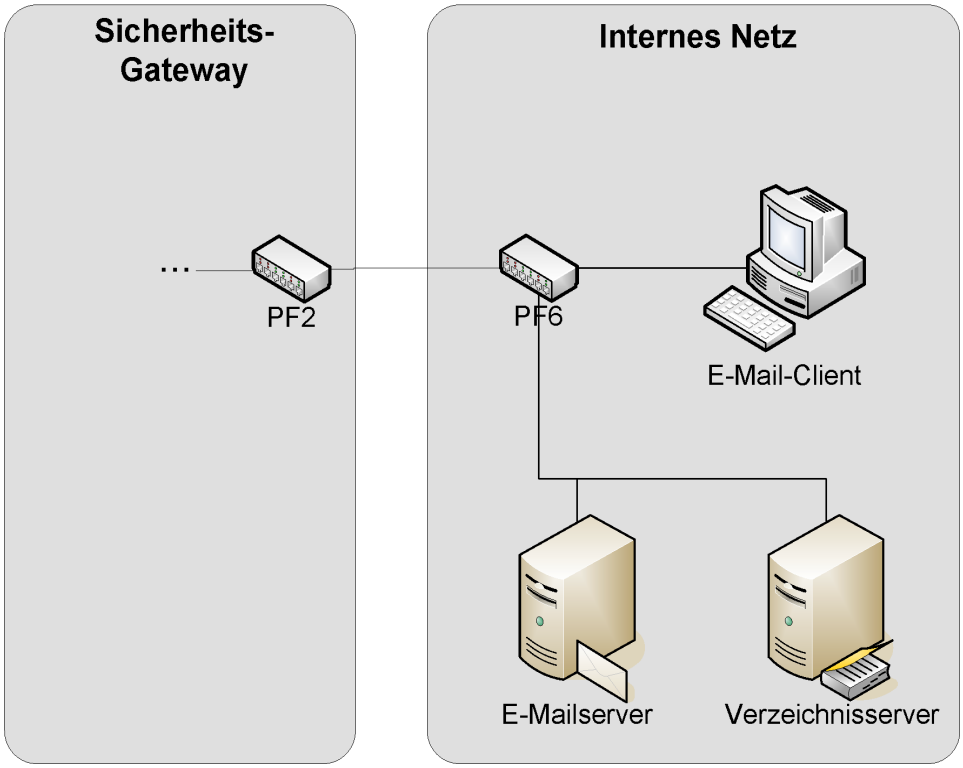

Abbildung 1.2.: Empfohlene Platzierung des E-Mail-Servers

E-Mail-Server

Nachrichten von externen E-Mail-Servern werden im Sicherheits-Gateway überprüft und dann an den internen E-Mail-Server weitergeleitet, wo die Nachrichten lokal gespeichert werden. Umgekehrt verschicken lokale E-Mail-Clients auch Nachrichten an interne oder externe Empfänger über den internen E-Mail-Server. E-Mails an externe Empfänger durchlaufen hierbei auch wieder das Sicherheits-Gateway.

Es wird empfohlen für die Kommunikation zwischen den E-Mail-Clients und dem E-Mail-Server standardisierte Protokolle wie SMTP, POP3 oder IMAP zu verwenden. Diese Protokolle sollten zusätzlich mit SSL/TLS abgesichert werden. Alternativ zu den genannten standardisierten Protokollen können E-Mail-Clients auch mit proprietären Protokollen wie z. B. Microsoft MAPI oder Lotus NRPC an den E-Mail-Server angebunden werden. Auch in diesem Fall sollte die Verbindung verschlüsselt werden.

Um das unerlaubte Verwenden des E-Mail-Servers zu vermeiden, sollten für die Authentisierung des E-Mail-Clients am E-Mail-Server mindestens Benutzername und Passwort verwendet werden. Es wird auch empfohlen den E-Mail-Client so zu konfigurieren, dass die Authentisierung automatisch abgelehnt wird, wenn nicht vorher eine verschlüsselte Verbindung mit einem starken Verschlüsselungsprotokoll aufgebaut worden ist, da sonst Kennwörter und Nachrichten unverschlüsselt im internen Netz übertragen werden.

Verzeichnisserver

Auf einem Verzeichnisserver werden Adressbücher und Zertifikate (für S/MIME oder OpenPGP) verwaltet. Zur Kommunikation zwischen den E-Mail-Clients und dem Verzeichnisserver sollte LDAP benutzt werden. Für die Authentisierung des E-Mail-Clients am Verzeichnisserver wird der Einsatz sicherer Authentisierungsmechanismen (z. B. SASL) empfohlen.

1.4.3 Sichere E-Mail-Kommunikation auf Anwendungsebene

Zur Absicherung der E-Mail-Kommunikation auf Anwendungsebene sollten E-Mails digital signiert und verschlüsselt werden. Signaturen dienen zur Sicherstellung der Integrität von Nachrichten und der Authentizität des Absenders, wohingegen Verschlüsselung zum Schutz der Vertraulichkeit verwendet wird. Sowohl zur Signierung als auch zur Verschlüsselung wird die Verwendung von S/MIME oder OpenPGP empfohlen. Alternativ ist auch die Verwendung einer Virtuellen Poststelle (VPS) denkbar.

Sichere Nutzung von S/MIME

S/MIME ist ein Standard für die digitale Signatur und Verschlüsselung von E-Mails, der auf symmetrischer sowie asymmetrischer Kryptografie mit privaten und öffentlichen Schlüsseln basiert.

S/MIME-Funktionen werden entweder direkt von der E-Mail-Client-Software angeboten oder können über ein Plug-In integriert werden. Um die korrekte Funktionsweise zu gewährleisten, wird bei S/MIME ein Zertifikat benötigt mit dem eine eindeutige Zuordnung zwischen einem öffentlichen Schlüssel und dessen Inhaber erfolgt. Solche Zertifikate werden von übergeordneten Zertifizierungsstellen (sog. Trustcenter) ausgestellt. Zertifikate können entweder in einem lokalen Speicher abgelegt sein oder von einem Verzeichnisserver abgerufen werden. Der Verzeichnisserver kann sich sowohl im internen Netz, als auch bei einem Trustcenter befinden.

Sichere Nutzung von OpenPGP

Ebenso wie S/MIME verwendet auch OpenPGP sowohl symmetrische als auch asymmetrische Kryptografie zur Erstellung digitaler Signaturen und zur Verschlüsselung. OpenPGP-Funktionen werden über ein Plug-In in einen E-Mail-Client integriert. Auch OpenPGP basiert auf Public-Key-Verfahren, bei dem Absender und Empfänger einen öffentlichen und privaten Schlüssel benötigen. Im Gegensatz zu S/MIME gibt es bei OpenPGP jedoch keine übergeordnete Stelle (Trustcenter) zur Ausgabe von Zertifikaten. Stattdessen bestätigen die OpenPGP-Benutzer sich gegenseitig die

Vertrauenswürdigkeit ihrer Schlüssel und bauen so eine Vertrauenskette auf (Aus „A vertraut B“ und „B vertraut C“ folgt auch „A vertraut C“). Diese Struktur wird als „Web of Trust“ bezeichnet.

Verwendung einer VPS

Anstatt jeden E-Mail-Client mit Schlüsseln und Zertifikaten auszustatten, kann auch eine zentrale Komponente zur Verschlüsselung und Signierung von Nachrichten verwendet werden. E-Mails aus dem internen Netz werden dabei unverschlüsselt an die VPS geschickt, wo sie dann mit einem allgemeinen Unternehmensschlüssel verschlüsselt werden. Eingehende E-Mails, die mit dem öffentlichen Unternehmensschlüssel verschlüsselt sind, werden an der VPS entschlüsselt und dann an den jeweiligen E-Mail-Client weitergeleitet.

Diese Vorgehensweise vereinfacht Aufbau und Wartung einer Schlüssel- und Zertifikats-Infrastruktur. Des Weiteren ermöglicht es auch die zentrale Überprüfung verschlüsselter E-Mails auf Schadprogramme und unerwünschte Inhalte, da keine Ende-zu-Ende-Verschlüsselung mehr besteht.

1.5 Fazit

Die Nutzung von E-Mails ermöglicht einen einfachen, schnellen und kostengünstigen Austausch von Informationen. Bei einer Verwendung zur externen Kommunikation über ein unsicheres Netz (wie beispielsweise das Internet) ergeben sich jedoch zahlreiche Bedrohungen für die Integrität, Vertraulichkeit und Verfügbarkeit.

In der Studie [ISi-Mail-Client], die diesem Dokument zu Grunde liegt, wurden Empfehlungen erarbeitet, um diesen Bedrohungen mit geeigneten Maßnahmen zu begegnen. Neben einer sorgfältigen Auswahl und Konfiguration der E-Mail-Client-Software sowie der sicheren Anbindung des E-Mail-Clients an den internen E-Mail-Server erhöhen zusätzliche Komponenten wie Virenschutzprogramm, Anti-Phishing-Software und Personal Firewall die Sicherheit wesentlich. Die Verwendung einer E-Mail-Richtlinie kann den Benutzer durch Hinweise zur Nutzung unterstützen.

Die Vertraulichkeit und die Integrität/Authentizität der E-Mail-Kommunikation kann über eine Realisierung auf dem E-Mail-Client mittels der offenen Standards S/MIME oder OpenPGP sichergestellt werden. Eine gute Alternative ist die in der Studie [ISi-Mail-Server] vorgestellte Lösung der Virtuelle Poststelle (VPS). Damit kann diese Aufgabe über einen zentralen Server ohne Änderungen an den E-Mail-Clients und ohne zusätzlichen Aufwand für den Benutzer realisiert werden.

Die Studie [ISi-Mail-Client] betrachtet in erster Linie Sicherheitsaspekte in Anwendungen und beschreibt entsprechende Schutzmaßnahmen. Zusammen mit der Studie zum sicheren Betrieb von E-Mail-Servern [ISi-Mail-Server] sowie der Absicherung der unteren drei Schichten des TCP/IP-Referenzmodells gemäß dem Modul „Sichere Anbindung von lokalen Netzen an das Internet“ [ISi-LANA] wird eine sichere Nutzung und Bereitstellung des Dienstes E-Mail ermöglicht.

2 Glossar

Angriff (engl. attack)

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Authentisierung (engl. authentication)

Unter einer Authentisierung versteht man die Vorlage eines Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Authentizität (engl. authenticity)

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Bedrohung (engl. threat)

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen bedrohen kann, wodurch dem Besitzer der Informationen ein Schaden entsteht.

Browser [engl.]

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (engl. Federal Office for Information Security)

Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern.

Client [engl.]

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme eines Servers zugreift.

Datensicherung (engl. backup)

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren. Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustands von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

Gefährdung

Eine Gefährdung ist eine Bedrohung, die konkret auf ein Objekt über eine Schwachstelle einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. So sind beispielsweise Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen. Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenbefallene Datei herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Typ Computer-Virus ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

Hacking [engl.]

Hacking bezeichnet im Kontext von Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein IT-System einzudringen, seine Schwächen offen zulegen und es gegebenenfalls - bei unethischem Hacking - zu übernehmen.

HTML (Hypertext Markup Language [engl.])

Für Web-Seiten verwendete Auszeichnungssprache, die von allen Browsern verstanden wird.

Hyperlink [engl.]

Kurz für Hypertext Link. Elektronischer Querverweis zwischen Dokumenten. Sind innerhalb von Textdokumenten meist farblich oder durch Unterstreichung hervorgehoben, verlinkte Dokumente lassen sich per einfachem Mausklick aufrufen.

Integrität (engl. integrity)

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von

Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Integrität ist ein Grundwert der IT-Sicherheit.

IP (Internet Protocol [engl.])

Verbindungsloses Protokoll der Internet-Schicht im TCP/IP-Referenzmodell. Ein IP-Header enthält in der Version IPv4 u. a. zwei 32-Bit-Nummern (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.

IT-Sicherheit (engl. IT Security)

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

JavaScript [engl.]

JavaScript ist eine Programmiersprache, die oft auf Webseiten eingesetzt wird. Mit ihr ist es z. B. möglich, Pop-Up-Fenster zu öffnen, Berechnungen durchzuführen oder Formulareingaben zu überprüfen. JavaScript ist Bestandteil aller neuen Browser. JavaScript zählt zu den Aktiven Inhalten.

Kryptografie

Mathematisches Fachgebiet, das sich mit Methoden zum Schutz von Informationen befasst (u. a. mit Vertraulichkeit, Integrität und Authentizität von Daten).

MIME (Multipurpose Internet Mail Extensions [engl.])

Protokoll für die E-Mail-Kommunikation als Erweiterung zu SMTP. MIME ermöglicht die Übertragung von binären Dateien in E-Mails.

OpenPGP (Open Pretty Good Privacy [engl.])

Spezifikation für PGP-verwandte Verschlüsselungs- und Signatur-Software.

Paketfilter (engl. packet filter)

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr anhand spezieller Regeln filtern. Ihre Aufgabe ist es, Datenpakete anhand der Informationen in den Header-Daten der IP- und Transportschicht (z. B. Quell- und Ziel-Adresse, -Portnummer, TCP-Flags) weiterzuleiten oder zu verwerfen. Der Inhalt des Pakets bleibt dabei unberücksichtigt.

Passwort

Geheimes Kennwort, das Daten, Rechner, Programme u. a. vor unerlaubtem Zugriff schützt.

Patch [engl.]

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Software-Fehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Phishing [engl.]

Versuch von Betrügern, IT-Anwender irrezuführen und zur Herausgabe von Authentisierungsdaten zu bewegen. Dies wird in den meisten Fällen bei Online-Banking-Verfahren eingesetzt.

Plug-In [engl.]

Plug-Ins sind Zusatzmodule des Browsers, die erforderlich sind, um spezielle Multimedia-Fähigkeiten einzubinden und nutzen zu können.

Protokoll (engl. protocol)

Beschreibung (Spezifikation) des Datenformats für die Kommunikation zwischen elektronischen Geräten.

Prüfsumme (engl. checksum)

In der Informatik ist eine Prüfsumme eine einfache Maßnahme zur Gewährleistung von Datenintegrität bei der Datenübermittlung oder -speicherung.

Risiko (engl. risk)

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Schutzbedarf (engl. protection requirements)

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Schwachstelle (engl. vulnerability)

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Server [engl.]

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen

in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.

Sicherheits-Gateway

Ein Sicherheits-Gateway (oft auch Firewall genannt) gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Ein Sicherheits-Gateway für normalen Schutzbedarf besteht im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen Paketfilter und Application-Level Gateway (ALG) zu unterscheiden.

SMTP (Simple Mail Transfer Protocol [engl.])

Das Simple Mail Transfer Protocol legt fest, wie E-Mails zwischen Servern zu übertragen sind. Auch für den Transport von E-Mails vom Mail-Client zum Server (und die umgekehrte Richtung) kann SMTP genutzt werden.

Spam [engl.]

Gängige Bezeichnung für unverlangt zugesandte Werbepost per E-Mail.

Spoofing [engl.]

Spoofing (von to spoof, zu deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Spyware [engl.]

Software, die persönliche Daten des Benutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software oder an Dritte sendet.

SSL (Secure Sockets Layer [engl.])

Protokoll zur sicheren Kommunikation über das Internet, insbesondere zwischen Client und Server, basiert auf dem Verschlüsselungsalgorithmus RSA.

TCP (Transmission Control Protocol [engl.])

Verbindungsorientiertes Protokoll der Transportschicht im TCP/IP-Referenzmodell, welches auf IP aufsetzt.

TLS (Transport Layer Security [engl.])

Protokoll zur sicheren Datenübertragung über das Internet. Nachfolger von SSL.

Trojanisches Pferd (engl. trojan horse)

Programm, welches sich als nützliches Werkzeug tarnt, jedoch schädlichen Programmcode einschleust und im Verborgenen unerwünschte Aktionen ausführt.

Verfügbarkeit (engl. availability)

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets wie gewünscht zur Verfügung stehen. Verfügbarkeit ist ein Grundwert der IT-Sicherheit.

Verschlüsselung (engl. encryption)

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die Schlüssel genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartexts aus dem Geheimtext - wird Entschlüsselung genannt.

Vertraulichkeit (engl. confidentiality)

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit ist ein Grundwert der IT-Sicherheit.

Virenschutzprogramm

Ein Virenschutzprogramm ist eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Virus (engl. virus)

Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

VPS (Virtuelle Poststelle)

Die Virtuelle Poststelle des Bundes stellt als Basiskomponente "Datensicherheit" ein zentrales System für den Einsatz von Kryptografie zur Verfügung. Sie soll die sichere elektronische Kommunikation zwischen Behörden und externen Partnern auf Behördenseite praktisch erleichtern und unterstützen. Als Middleware wickelt sie kryptografische Operationen ab, die mit dem Einsatz elektronischer Signaturen und Verschlüsselung verbunden sind.

Wurm

Selbstständiges, sich selbst reproduzierendes Programm, das sich in einem System (vor allem in Netzen) ausbreitet.

3 Stichwort- und Abkürzungsverzeichnis

4 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/

[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/

[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/