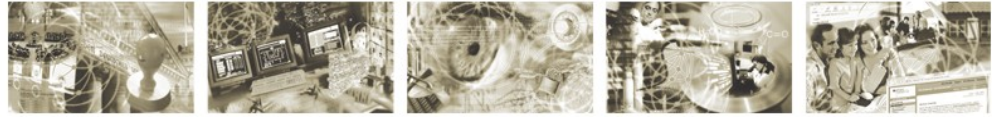




Bundesamt
für Sicherheit in der
Informationstechnik



Sicherer Betrieb von E-Mail-Servern (ISi-Mail-Server)

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

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 finden Sie auf den Internet-Seiten des BSI.

<http://www.bsi.bund.de> oder <http://www.isi-reihe.de>

Bundesamt für Sicherheit in der Informationstechnik

ISi-Projektgruppe

Postfach 20 03 63

53133 Bonn

Tel. +49 (0) 228 99 9582-0

E-Mail: isi@bsi.bund.de

Internet: <http://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2009

Inhaltsverzeichnis

1 Leitlinie zum sicheren Betrieb von E-Mail-Servern.....	5
1.1 Management Summary.....	5
1.2 Einführung und Überblick.....	6
1.2.1 SMTP-Proxy.....	6
1.2.2 Spam-Filter.....	6
1.2.3 Content-Filter.....	6
1.3 Wesentliche Ergebnisse der Gefährdungsanalyse.....	7
1.3.1 Eindringen.....	7
1.3.2 Täuschen, Fälschen und Betrügen.....	7
1.3.3 Entwenden und Ausspähen.....	8
1.3.4 Verhindern und Zerstören.....	8
1.4 Sichere E-Mail-Server-Architektur.....	9
1.4.1 Application Level Gateway.....	9
1.4.2 ALG/SMTP-Proxy.....	9
1.4.3 Content-Filter.....	10
1.4.4 E-Mail-Server.....	10
1.4.5 Virtuelle Poststelle.....	10
1.5 Fazit.....	12
2 Glossar.....	13
3 Stichwort- und Abkürzungsverzeichnis.....	17
4 Literaturverzeichnis.....	19

1 Leitlinie zum sicheren Betrieb von E-Mail-Servern

Elektronische Post (E-Mail) ist heute ein wichtiger Bestandteil der Kommunikationskultur und ersetzt zunehmend den traditionellen Briefverkehr. Sie bietet die Möglichkeit, Informationen schnell, effizient und kostengünstig auszutauschen. Allerdings sind mit der Nutzung von E-Mail über ein unsicheres Netz, wie beispielsweise dem Internet, auch erhebliche Gefahren verbunden.

Die vorliegende Leitlinie zum „Sicheren Betrieb von E-Mail-Servern“ ist Bestandteil des Moduls [ISi-Mail-Server] der BSI-Schriftenreihe zur Internet-Sicherheit (ISi-Reihe). Sie fasst die wesentlichen Ergebnisse der zugehörigen Studie zusammen. Der Fokus liegt dabei auf Gefährdungen und Empfehlungen, die für E-Mail-Server spezifisch sind. Informationen zur sicheren Nutzung von E-Mail finden sich im Modul [ISi-Mail-Client].

1.1 Management Summary

E-Mails sind als Kommunikationsmittel aus Unternehmen und Behörden heute kaum noch wegzudenken. Bei der Nutzung von E-Mails über das Internet bestehen jedoch eine Reihe von Gefährdungen, die insbesondere die Integrität und Vertraulichkeit von Nachrichten, die Authentizität der Absender und die Verfügbarkeit des E-Mail-Dienstes selbst betreffen.

Ein Angreifer, der Zugriff auf den Netzverkehr hat, kann sämtliche unverschlüsselten E-Mails mitlesen. Dabei kann er auch in den Besitz sensibler Informationen gelangen. Schutz vor dem Ausspähen sensibler Daten kann eine Verschlüsselung der E-Mail-Kommunikation bieten. Ein verwandtes Thema sind digitale Signaturen. Werden E-Mails nicht signiert, so ist es für den Angreifer sogar möglich, E-Mails zu fälschen, d. h. deren Inhalt unbemerkt zu ändern oder neue Nachrichten mit einer falschen Identität zu erstellen und somit beispielsweise Bestellungen auszulösen oder Rufschädigung zu betreiben.

Eine weitere 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 des E-Mail-Dienstes führen. Schadprogramme, die per E-Mail verschickt werden, stellen normalerweise keine direkte Gefährdung des E-Mail-Servers dar, sondern vielmehr der Benutzer und ihrer E-Mail-Clients. Sie sollten dennoch an dieser Stelle berücksichtigt werden, da der E-Mail-Server als zentrale Komponente effiziente Schutzmechanismen umsetzen kann.

Das Modul ISi-Mail-Server stellt eine sichere Grundarchitektur für den normalen Schutzbedarf vor, mit der alle relevanten Gegenmaßnahmen abgedeckt sind. Um diese Architektur flexibel an die Größe der Infrastruktur und individuellen Schutzanforderungen anpassen zu können, stellt die Studie zusätzlich erweiterte oder alternative Maßnahmen vor. Auch einem erhöhten Schutzbedarf kann so Rechnung getragen werden.

Die Grundarchitektur besteht aus einem SMTP-Proxy, einem Content-Filter, dem E-Mail-Server an sich und optional aus einer virtuellen Poststelle. Der SMTP-Proxy und der Content-Filter dienen der Erkennung und Filterung von Spam und Schadprogrammen. Mittels einer virtuellen Poststelle lassen sich die Verschlüsselung und Signierung von Nachrichten an einer zentralen Komponente realisieren.

1.2 Einführung und Überblick

E-Mail-Server bieten Funktionen zum Empfangen, Versenden, Speichern und Weiterleiten von E-Mails. Um Nutzern diese Funktionen bereitzustellen, wird in der Regel jedem Nutzer ein Postfach zugeteilt, in dem eingehende Nachrichten abgelegt werden. Ferner kann ein Nutzer mittels des E-Mail-Clients über sein Postfach selbst Nachrichten erstellen und versenden. Der Zugang zu einem Postfach erfolgt meist über die Protokolle POP3 oder IMAP. Um den Zugang zu diesen Postfächern abzusichern, müssen sich die Nutzer am E-Mail-Server authentisieren. Dies erfolgt üblicherweise über Benutzername und Passwort.

Sowohl die Zahl unerwünschter E-Mails (sog. Spam) als auch die Anzahl mit Schadprogrammen behafteter E-Mails ist im Laufe der Jahre enorm gestiegen. Um diesen Trends zu begegnen werden E-Mail-Server mit zusätzlichen Filtern erweitert. Diese Filter werden üblicherweise auf getrennten Komponenten bzw. mit spezialisierter Software umgesetzt. Im Folgenden werden mehrere Filter-techniken und -typen beschrieben.

1.2.1 SMTP-Proxy

Ein SMTP-Proxy vermittelt den E-Mail-Verkehr zwischen externem und internem E-Mail-Server und ist somit die erste Prüfinstanz für eingehende E-Mails (z. B. aus dem Internet). Er nimmt E-Mails entgegen und kann untersuchen, ob sie gefährliche oder unerwünschte SMTP-Protokollelemente enthalten, bevor er sie weiterleitet. E-Mails, die nicht SMTP-konform sind, können direkt am SMTP-Proxy verworfen werden. Diese Maßnahme hilft auch gegen unerwünschte E-Mails, da beim Versenden von Spam häufig das SMTP-Protokoll verletzt wird. Eine derzeit sehr effiziente Maßnahme zur Reduzierung unerwünschter E-Mails ist, E-Mails von unbekanntem E-Mail-Server zuerst abzulehnen und erst bei der zweiten Zustellung anzunehmen¹. Hintergrund dieser Technik ist, dass Spam-versendende Systeme zumeist nur einmal versuchen eine E-Mail zuzustellen.

1.2.2 Spam-Filter

Spam-Filter dienen zum Erkennen von unerwünschten E-Mails und untersuchen diese auf einzelne markante Wörter, bestimmte Phrasen, bekannte Prüfsummen, verdächtige Verweise oder auch in Anhängen versteckten Spam.

Bei der Spam-Filterung wird folgendermaßen vorgegangen: E-Mails werden der Reihe nach auf verschiedene Spam-Merkmale geprüft. Bei jeder Prüfung wird der E-Mail eine Punktzahl zugeordnet, die angibt, inwieweit die jeweilige Prüfung den Spam-Verdacht erhärtet. Übersteigt die Summe der Punktzahlen aus allen Prüfungen einen Schwellenwert, so gilt die E-Mail als Spam und wird entsprechend gekennzeichnet oder aussortiert.

1.2.3 Content-Filter

Content-Filter untersuchen den Inhalt einer E-Mail auf nicht erwünschte Inhalte wie beispielsweise Schadprogramme, Phishing, Aktive Inhalte oder gefährliche Dateianhänge. So erkannte E-Mails können danach geändert (z. B. Löschen eines gefährlichen Dateianhangs), in einen vorgesehenen Quarantäne-Bereich verschoben, oder sogar komplett gelöscht werden. Benutzer oder Administratoren können über die vorgenommenen Aktionen über E-Mail informiert werden. Häufig wird die Funktion des Spam-Filters und Content-Filters auf einem gemeinsamen Server realisiert, um Kosten zu reduzieren.

¹ Diese Methode wird Greylisting genannt.

1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

Die in den folgenden Abschnitten beschriebenen Angriffe können sowohl den E-Mail-Dienst selbst als auch die Benutzer bedrohen. Maßnahmen zum Schutz der Benutzer können häufig auch auf den E-Mail-Servern sinnvoll realisiert werden. Daher werden bei der Realisierung des E-Mail-Dienstes auch Maßnahmen betrachtet, um den E-Mail-Client zu schützen. Die Gefährdungen lassen sich grundsätzlich in vier Kategorien unterteilen:

- 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

Die erste Kategorie von Bedrohungen besteht darin, dass ein Angreifer versucht, in einen E-Mail-Server oder E-Mail-Client einzudringen. Ist es einem Angreifer gelungen den E-Mail-Server oder E-Mail-Client zu kompromittieren, so befindet er sich im internen Netz und kann von dort aus weitere Systeme angreifen. Ziel eines solchen Angriffes ist es meist, Sicherheitsgrundwerte, wie beispielsweise die Vertraulichkeit von E-Mails, zu beeinträchtigen.

Um in den E-Mail-Server oder E-Mail-Client einzudringen, kann ein Angreifer versuchen Sicherheitslücken in der verwendeten Software auszunutzen. Entsprechende Angriffe erfolgen entweder manuell oder automatisiert. Häufig sind von diesen Angriffen die E-Mail-Clients betroffen, z. B. bei automatisierten Angriffen durch Würmer. In beiden Fällen nutzt der Angreifer Software-Schwachstellen aus. Im Falle von Würmern kann auch eine fehlerhafte Konfiguration das Eindringen begünstigen, wenn z. B. veraltete Virenschutz-Signaturen dazu führen, dass neue Schadprogramme nicht erkannt werden.

Eine typische Schwachstelle bei der Realisierung eines E-Mail-Dienstes ist das ungeprüfte Weiterleiten von E-Mails aus dem Internet in das interne Netz. So können beispielsweise mit Schadprogrammen behaftete Dateianhänge zu den E-Mail-Clients gelangen. Auch über Aktive Inhalte in E-Mails ist eine Infektion des E-Mail-Client-Systems mit Schadprogrammen möglich.

1.3.2 Täuschen, Fälschen und Betrügen

Ein Angriff dieser Kategorie zielt typischerweise auf die Nutzer von E-Mail-Diensten und betrifft somit eher die Client-Seite. Der E-Mail-Server ist insofern von dieser Art Angriffe betroffen, als dass er eine zentrale Komponente zu deren Abwehr darstellt.

Bei der Kommunikation zwischen zwei E-Mail-Servern besteht die Gefahr, dass die Angaben zu Absender oder sendendem E-Mail-Server gefälscht werden. Schäden entstehen dabei nicht direkt auf dem E-Mail-Server, sondern erst beim Empfänger, wenn dieser die in dieser E-Mail enthaltenen Informationen als authentisch und verbindlich ansieht. Ein Angreifer könnte auf diese Weise beispielsweise im Namen einer anderen Person oder Organisation eine Bestellung auslösen oder in deren Namen falsche Aussagen verbreiten, um dem Ruf dieser Person bzw. Organisation zu schaden.

Ein Angreifer kann Inhalte von unsignierten E-Mails ändern. Dies kann durch Zugriff auf einen E-Mail-Server oder auch durch Manipulation des DNS-Dienstes erfolgen. Letztere Methode erlaubt es, E-Mails auf einen eigenen E-Mail-Server umzuleiten, abzuändern und wieder weiterzuleiten.

1.3.3 Entwenden und Ausspähen

Eine der größten Gefahren bei der Nutzung von E-Mail ist, dass vertrauliche Nachrichten unerlaubt mitgelesen werden. Ein Angreifer hat prinzipiell mehrere Möglichkeiten vertrauliche E-Mails auszuspähen. Zum einen kann er den Netzverkehr abhören und somit auch unverschlüsselte E-Mails mitlesen, zum anderen kann er aber auch versuchen, sich Zugang zu den Postfächern auf dem E-Mail-Server zu verschaffen, und die dort gespeicherten Nachrichten zu lesen. Eine Möglichkeit den Zugang zu einem Postfach zu erlangen ist das Ausnutzen eines schwachen Benutzer-Passwortes. Ein Angreifer kann auch die Verteilerlisten auf dem E-Mail-Server so manipulieren, dass er eine Kopie aller E-Mails an diese Verteilerlisten erhält.

Doch nicht nur die E-Mails selber, sondern auch E-Mail-Adressen sollten vor Ausspähung geschützt werden. Spammer sind sehr daran interessiert, möglichst viele gültige E-Mail-Adressen einer Domäne zu ermitteln. Ein schlecht konfigurierter E-Mail-Server kann in Form von Statusberichten einem Angreifer die benötigten Informationen liefern.

1.3.4 Verhindern und Zerstören

Neben der Integrität und der Vertraulichkeit von E-Mails ist auch die Verfügbarkeit des E-Mail-Dienstes ein wichtiger Sicherheitsaspekt. Ein Verlust der Verfügbarkeit bedeutet, dass keine neuen E-Mails mehr versendet oder empfangen werden können und gegebenenfalls sogar auf dem E-Mail-Server gespeicherte Nachrichten nicht mehr abgerufen werden können. In vielen Fällen ist die alltägliche Arbeit damit sehr eingeschränkt oder nicht durchführbar.

Ein Angriff, der darauf abzielt den Zugriff auf eine Ressource der E-Mail-Architektur zu verhindern, wird als Denial-of-Service-Angriffe (DoS) bezeichnet. Ein Angreifer versucht dabei Server zu überlasten oder gar zum Absturz zu bringen. Um entsprechende Lasten zu generieren, basieren solche Angriffe häufig auf einem ferngesteuerten, koordinierten Angriff auf das Zielsystem, der von einer sehr großen Zahl von Rechnern ausgeht. Dies wird als Distributed-Denial-of-Service (DDoS) bezeichnet. In diesem Falle erfolgen die Angriffe überwiegend über sogenannte Botnetze. Bei einem Botnetz steuert ein Angreifer eine Vielzahl von Rechnern, die ohne das Wissen des Anwenders übernommen und ferngesteuert werden.

Der Angreifer kann mittels eines Botnetzes innerhalb kurzer Zeit eine große Menge Spam-E-Mails versenden und so E-Mail-Server überlasten. Weiterhin können Konfigurationsfehler auf dem E-Mail-Server dazu führen, dass unberechtigte Benutzer E-Mails an Verteilerlisten senden können, wodurch es einem Angreifer möglich ist, große Mengen Spam-E-Mails zu generieren.

Das Vertrauen der Anwender in den E-Mail-Dienst kann durch den Verlust von E-Mails beeinträchtigt werden, insbesondere dann, wenn er bei der Nichtzustellung von E-Mails keine entsprechende Fehlermeldung erhält.

Eine Gefährdung stellen E-Mail-Server dar, die es wegen einer fehlerhaften Konfiguration erlauben, E-Mails für beliebige Domänen weiterzuleiten. Man spricht dann von sogenannten „Open Relays“. In diesem Fall kann der Angreifer den E-Mail-Server dazu verwenden in fremden Namen Spam zu versenden. Neben einer missbräuchlichen Nutzung besteht die Gefahr, dass der eigene E-Mail-Server in einer sogenannten Blacklist, also einer Liste potentieller Spam-Versender, eingetragen wird. Damit kann das betroffene Unternehmen keine E-Mails mehr an Unternehmen versenden, die zur Reduzierung von Spam E-Mails diese Blacklist verwenden.

1.4 Sichere E-Mail-Server-Architektur

Die Empfehlungen für einen sicheren Betrieb von E-Mail-Servern basieren auf einer sicheren E-Mail-Server-Architektur (vgl. Abbildung 1.1). Diese Architektur ist gemäß der allgemeinen Grundarchitektur aus dem Modul „Sichere Anbindung lokaler Netze an das Internet“ [ISi-LANA] in die Zonen „internes Netz“ und „Sicherheits-Gateway“ unterteilt.

Im Vergleich zur allgemeinen Grundarchitektur aus [ISi-LANA] ist zusätzlich zu dem Application Level Gateway (ALG) noch ein weiteres ALG mit SMTP-Proxy hinzugekommen. An dieses neue ALG ist der Content-Filter angeschlossen. Wichtig ist, dass sämtlicher Verkehr in das und aus dem internen Netz über ein ALG geleitet wird. Der E-Mail-Server selbst befindet sich zusammen mit den E-Mail-Clients im internen Netz. Die einzelnen Komponenten der Grundarchitektur werden im Folgenden näher erläutert.

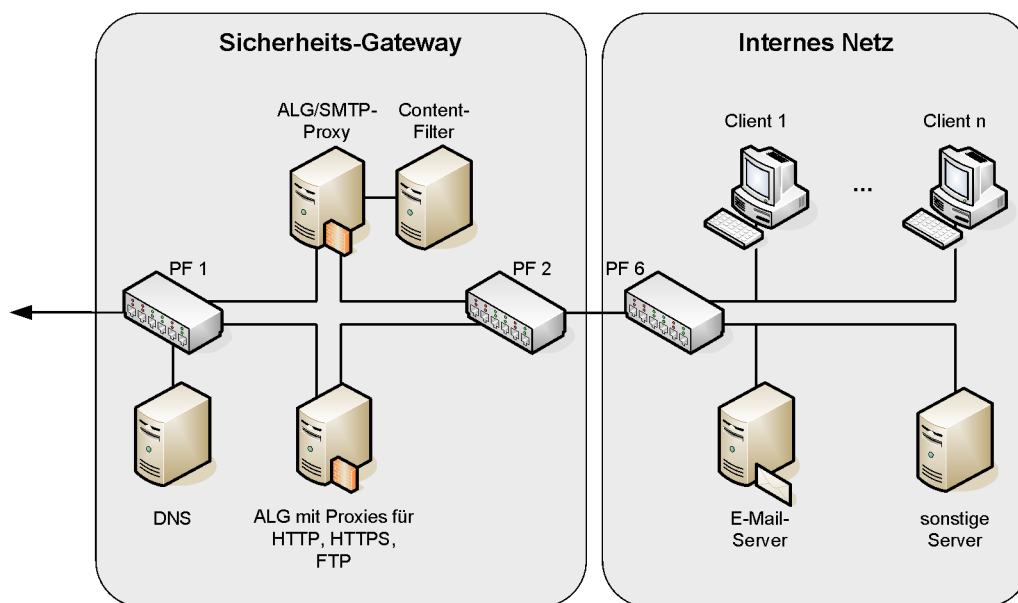


Abbildung 1.1: Sichere E-Mail-Server-Architektur

1.4.1 Application Level Gateway

Das ALG dient zur Überprüfung und Filterung des Netzverkehrs, insbesondere HTTP und HTTPS. Für die E-Mail Kommunikation wird dieses ALG nicht genutzt. Stattdessen wurde als zusätzliche Komponente ein ALG/SMTP-Proxy hinzugefügt. Somit haben Sicherheits- und Verfügbarkeitsprobleme des SMTP-Dienstes keine Auswirkungen auf die übrigen Dienste wie beispielsweise der Nutzung von Web-Angeboten.

1.4.2 ALG/SMTP-Proxy

Das ALG mit SMTP-Proxy nimmt E-Mails aus dem Internet entgegen und unterbricht damit die direkte Kommunikation zwischen Quelle (dem Sender) und Ziel (dem internen E-Mail-Server). Der SMTP-Proxy überprüft E-Mails auf Einhaltung der Protokoll-Merkmale und übergibt sie anschließend an den angeschlossenen Content-Filter, der die E-Mails auf nicht erwünschte Inhalte und Schadprogramme überprüft.

Nach erfolgreicher Überprüfung werden die E-Mails an den E-Mail-Server im internen Netz weitergeleitet. Das Vorgehen beim Versenden von E-Mails aus dem internen Netz verläuft analog dazu. Zusätzlich zu den Prüfungen auf Protokoll-Merkmale und Inhalte sollten folgende Maßnahmen für eingehende E-Mails umgesetzt werden:

- E-Mails an nicht existierende Empfänger oder interne Verteilerlisten werden blockiert.
- E-Mails von unbekanntem E-Mail-Servern werden zunächst abgelehnt und erst nach dem zweiten Versuch, die E-Mails abzuliefern, angenommen (Greylisting).

1.4.3 Content-Filter

Die Komponente Content-Filter überprüft E-Mails auf nicht erwünschte Inhalte und Schadprogramme. Alle E-Mails werden mit mindestens einem Virenschutzprogramm geprüft. Da Schadprogramme meist in Dateianhängen verschickt werden, sollten nur zugelassene Typen von Dateianhängen weitergeleitet werden. Damit können auch Schadprogramme abgewehrt werden, die vom Virenschutzprogramm noch nicht erkannt wurden. Des Weiteren erfolgen auch Prüfungen der E-Mails auf Phishing-Merkmale sowie Aktive Inhalte.

Zusätzlich werden E-Mails auch auf Spam-Merkmale geprüft. Da über eine Inhaltsprüfung keine eindeutige Feststellung möglich ist, wird jeder E-Mail bei Prüfungen auf Spam-Kriterien eine Bewertungszahl zugewiesen, anhand der eine E-Mail als Spam-E-Mail eingestuft und gekennzeichnet wird.

1.4.4 E-Mail-Server

Der E-Mail-Server bietet die in Abschnitt 1.2 beschriebenen Funktionen zur Steuerung und Verwaltung von E-Mails. Er befindet sich im internen Netz und ist nur über die Paketfilter PF1 und PF2 sowie das ALG mit SMTP-Proxy vom Internet aus zu erreichen. Von den E-Mail-Clients im internen Netz ist er durch den Paketfilter PF6 abgeschirmt.

Es wird empfohlen, auf dem E-Mail-Server zusätzlich ein Virenschutzprogramm zu installieren, um auch interne E-Mails auf Schadprogramme prüfen zu können. Das Virenschutzprogramm sollte sowohl einen Abgleich mit Virenschutz-Signaturen als auch eine heuristische Prüfung bieten.

1.4.5 Virtuelle Poststelle

Um die Vertraulichkeit und Integrität/Authentizität von Nachrichteninhalten zu schützen, sollten E-Mails verschlüsselt bzw. signiert werden. Dies kann entweder dezentral auf den E-Mail-Clients erfolgen (z. B. mittels S/MIME oder OpenPGP, siehe auch [ISi-Mail-Client]) oder zentral an einer virtuellen Poststelle (VPS).

Eine VPS wird beispielsweise für die gesicherte Kommunikation zwischen Verwaltungsbehörden und ihren Kommunikationspartnern wie Bürgern, Wirtschaftsunternehmen oder anderen Behörden eingesetzt. Der Einsatz einer VPS erlaubt es, ein Regelwerk zu definieren wie der Einsatz von Verschlüsselung und Signatur grundsätzlich gehandhabt werden soll. Damit kann beispielsweise festgelegt werden, dass zu bestimmten Empfängern E-Mails grundsätzlich verschlüsselt und signiert versendet werden.

Abbildung 1.2 zeigt, wie die sichere E-Mail-Server Architektur aus Abbildung 1.1 beim optionalen Einsatz einer VPS erweitert werden sollte. Diese zusätzlichen Komponenten werden im Folgenden kurz erläutert:

- VPS-Server beim Absender, der an den ALG/SMTP-Proxy angeschlossen wird.
- Optionaler VPS-Server beim Empfänger. Alternativ zu einer VPS können Empfänger auch E-Mails mit entsprechenden E-Mail-Clients (z.B. mit S/MIME-Funktionalität) lesen.
- Externe Verzeichnis-Server, welche die Zertifikate für die Verschlüsselung bereitstellen.
- Externe Server für die Gültigkeitsprüfung von Zertifikaten mittels OCSP² und CRL³.

Die VPS übernimmt bei einer E-Mail-Kommunikation die Verschlüsselung von ausgehenden Nachrichten und die Entschlüsselung von eingehenden Nachrichten. Bei eingehenden Nachrichten werden digitale Signaturen und/oder Zeitstempel geprüft sowie bei ausgehenden Nachrichten digitale Signaturen und/oder Zeitstempel erstellt.

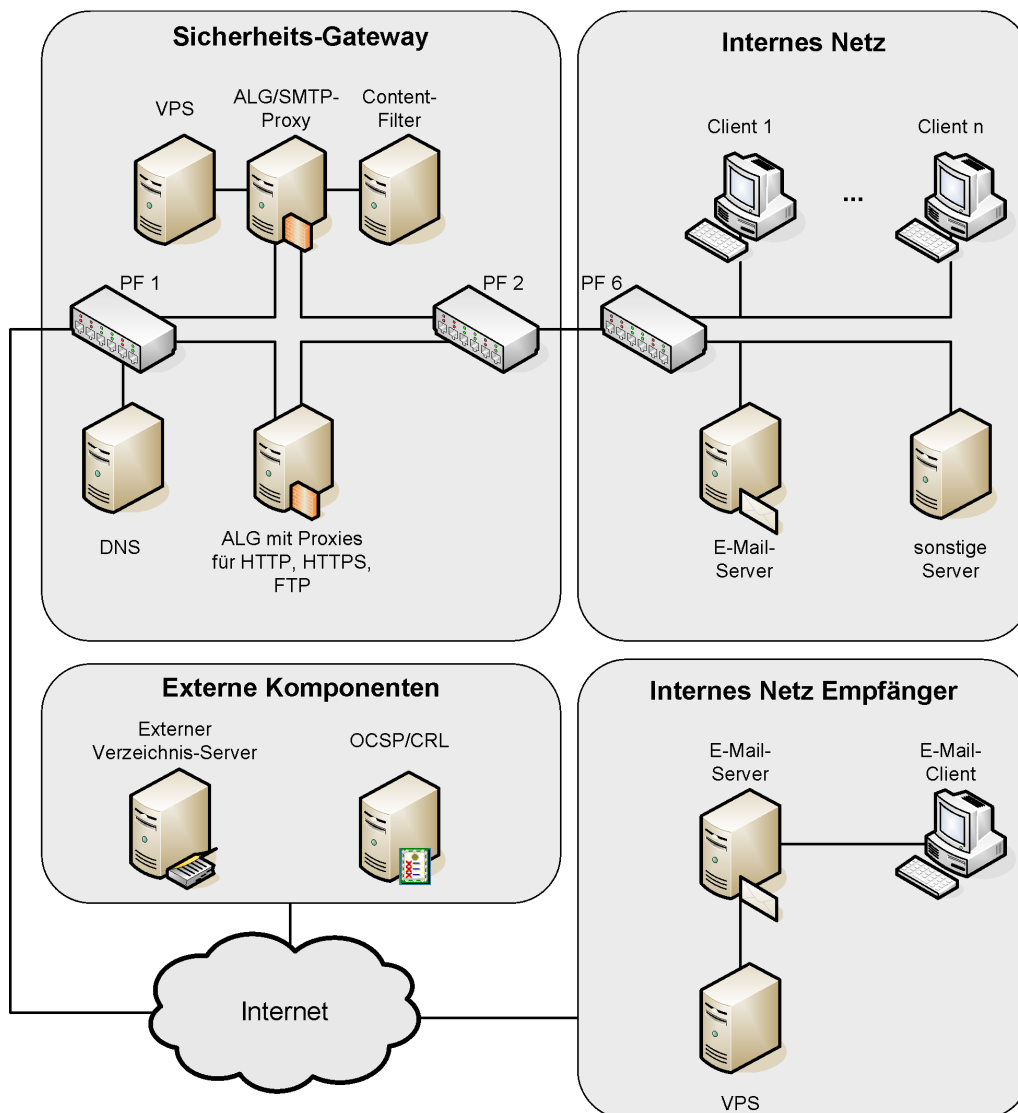


Abbildung 1.2: Sichere E-Mail-Server-Architektur mit Virtueller Poststelle

² Online Certificate Status Protocol

³ Certificate Revocation List

1.5 Fazit

E-Mails ermöglichen eine schnelle und kostengünstige Kommunikation. Bei einer Verwendung über nicht-vertrauenswürdige Netze, wie beispielsweise dem Internet, bestehen jedoch zahlreiche Gefährdungen. Diese Gefährdungen beziehen sich sowohl auf die Integrität und Vertraulichkeit von Nachrichten als auch auf die Verfügbarkeit des E-Mail-Dienstes.

Die in dieser Leitlinie vorgestellte E-Mail-Server-Architektur dient dazu, möglichen Gefährdungen für die E-Mail-Kommunikation zu begegnen. Die Schnittstelle zum Internet bildet ein ALG mit SMTP-Proxy, der bereits erste Maßnahmen zur Gefahrenabwehr und auch Abwehrmechanismen gegen Spam beinhaltet. Einen weiteren Schutz bietet ein darauf folgender Content-Filter, der die im Unternehmen eingesetzten E-Mail-Clients durch Prüfung aller E-Mails auf Schadprogramme und unerwünschte Inhalte schützt. Auch auf dem E-Mail-Server im internen Netz sollte ein Virenschutzprogramm installiert sein, um so auch interne E-Mails prüfen zu können.

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

Zusammen mit der Studie zur sicheren Nutzung von E-Mail [ISi-Mail-Client] 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

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computer-Netze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzer-Kennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

ALG (Application Level Gateway [engl.])

Filterfunktionen oberhalb der Transportschicht werden von einem sogenannten Application Level Gateway übernommen, auch Sicherheits-Proxy genannt. Ein Proxy ist eine Art Stellvertreter für Dienste in Netzen. Er nimmt Daten an seinem Eingang entgegen und leitet sie nach einer Prüfung an den eigentlichen Dienst weiter. Mittels eines Proxys lassen sich Datenströme auf der Anwendungsschicht verwerfen, modifizieren oder gezielt weiterleiten. Implizit nehmen ALGs auch Funktionen auf den darunter liegenden Schichten des TCP/IP-Modells wahr. ALGs unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über das ALG hinweg nimmt das ALG die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt das ALG analog. Diese Kommunikationsform ermöglicht es dem ALG beispielsweise, bestimmte Protokollbefehle auf der Anwendungsschicht zu filtern. Das ALG kann zudem die strikte Einhaltung von Anwendungsprotokollen erzwingen, unerwünschte Anwendungsdaten aus den Datenpaketen entfernen (bzw. austauschen) oder Verbindungen anwendungsspezifisch protokollieren.

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.

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.

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.

CRL (Certificate Revocation List [engl.])

Eine Certificate-Revocation List (Zertifikatssperrliste) wird von Dienstleistern für digitale Zertifikate herausgegeben, um anzuzeigen, dass einzelne herausgegebene Zertifikate nicht länger gültig sind. Dies ist beispielsweise in Folge eines kompromittierten privaten Schlüssels notwendig.

DDoS (Distributed Denial of Service [engl.])

Ein koordinierter DoS-Angriff auf die Verfügbarkeit von IT mittels einer größeren Anzahl von angreifenden Systemen.

DNS (Domain Name System [engl.])

Das Domain Name System übersetzt alphanumerische Adressnamen (z. B. www.bsi.bund.de) in numerische Adressen (z. B. 194.95.177.86). Auch eine Übersetzung in die umgekehrte Richtung ist mit dem DNS möglich. Alphanumerische Namen für Rechner sind für die Benutzer einfach zu behalten und einzugeben. Da allerdings IPv4- und IPv6-Adressen in numerischer Form verlangen, ist eine Adressumsetzung durch das DNS notwendig.

DoS (Denial of Service [engl.])

Angriffe, mit dem Ziel, die Verfügbarkeit von IT zu schädigen.

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.

HTTP (Hypertext Transfer Protocol [engl.])

Das Hypertext Transfer Protocol dient zur Übertragung von Daten - meist Webseiten - zwischen einem HTTP-Server und einem HTTP-Client, also z. B. einem Browser. Die Daten werden über Uniform Resource Locators (URL) eindeutig bezeichnet. URLs werden meist in der Form Protokoll://Rechner/Pfad/Datei angegeben. Protokoll steht dabei für Protokolle der Anwendungsschicht, Rechner für den Namen oder die Adresse des Servers und der Pfad der Datei gibt den genauen Ort der Datei auf dem Server an. Ein Beispiel für eine URL ist <http://www.bsi.bund.de/fachthem/sinet/index.htm>

HTTPS (HTTP secure [engl.])

Protokoll zur sicheren Übertragung von HTML-Seiten im Internet. SSL/TLS dient dabei zur Absicherung der Client-Server-Kommunikation.

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.

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.

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.

Protokoll (engl. protocol)

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

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

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 E-Mail-Client zum Server (und die umgekehrte Richtung) kann SMTP genutzt werden.

Spam [engl.]

Gängige Bezeichnung für unverlangt zugesandte Werbepost per E-Mail.

TCP (Transmission Control Protocol [engl.])

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

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.

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.

Zeitstempel (engl. timestamp)

Elektronische Bescheinigung einer (vertrauenswürdigen) Stelle, dass ihr bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Es ist dabei im Allgemeinen nicht erforderlich, dass diese Stelle den Inhalt der Daten zur Kenntnis nimmt.

3 Stichwort- und Abkürzungsverzeichnis

Administrator.....	6, 13
ALG (Application-Level Gateway).....	9f., 12f., 16
Authentizität.....	5, 7, 10, 12
Bedrohung.....	7, 13, 15
Blacklist.....	8
Content.....	5f., 9f., 12
CRL (Certificate Revocation List).....	11, 14
Dateianhang.....	6f., 10
DDoS (Distributed Denial of Service).....	8, 14
DNS (Domain Name System).....	7, 14
DoS (Denial of Service).....	8, 14
E-Mail (Electronic Mail).....	1ff., 5ff., 15f., 20
Gefährdung.....	5, 7f., 12f.
DDoS (Distributed Denial of Service).....	8, 14
DoS (Denial of Service).....	8, 14
Hacking.....	7, 14
Phishing.....	6, 10, 15
Spam.....	5f., 8, 10, 12, 16
Gefährdungsanalyse.....	3, 7
Grundarchitektur.....	5, 9
Hacking.....	7, 14
HTTP (Hypertext Transfer Protocol).....	9, 14
HTTPS (HTTP secure).....	9, 14
IMAP (Internet Message Access Protocol).....	6
Integrität.....	5, 7f., 10, 12f.
IP (Internet Protocol).....	12ff.
ISi (Internet-Sicherheit).....	
ISi-L (ISi-Leitfaden).....	1
ISi-Reihe.....	2, 5
IT-Sicherheit.....	
Authentizität.....	5, 7, 10, 12
Integrität.....	5, 7f., 10, 12f.
Verfügbarkeit.....	5, 7f., 12ff.
Vertraulichkeit.....	5, 7f., 10, 12f., 16
MIME (Multipurpose Internet Mail Extensions).....	10, 12, 15
OCSP (Online Certificate Status Protocol).....	11
OpenPGP (Open Pretty Good Privacy).....	10, 12, 15
Paketfilter.....	10, 15f.
Passwort.....	6, 15
Phishing.....	6, 10, 15
POP3 (Post Office Protocol Version 3).....	6
Protokoll.....	
HTTP (Hypertext Transfer Protocol).....	9, 14
HTTPS (HTTP secure).....	9, 14
IP (Internet Protocol).....	12ff.
SMTP (Simple Mail Transfer Protocol).....	5f., 9f., 12, 15f.
TCP (Transmission Control Protocol).....	12ff.

Proxy.....	5f., 9f., 12f., 15
Prüfsumme.....	6
Schadprogramm.....	5ff., 9f., 12
Wurm.....	7, 16
Schutzbedarf.....	5, 15f.
Schwachstelle.....	7, 15
Sicherheits-Gateway.....	9, 16
ALG (Application-Level Gateway).....	9f., 12f., 16
Paketfilter.....	10, 15f.
Sicherheitsgrundwerte.....	7
SMTP (Simple Mail Transfer Protocol).....	5f., 9f., 12, 15f.
Spam.....	5f., 8, 10, 12, 16
TCP (Transmission Control Protocol).....	12ff.
Verfügbarkeit.....	5, 7f., 12ff.
Vertraulichkeit.....	5, 7f., 10, 12f., 16
Virenschutz.....	7, 10
Virenschutzprogramm.....	10, 12, 16
Virtuelle Poststelle.....	3, 10, 12, 16
Virus.....	7, 10, 12, 16
VPS (Virtuelle Poststelle).....	3, 10ff., 16
Wurm.....	7, 16
Zeitstempel.....	11, 16
Zertifikat.....	11, 14

4 Literaturverzeichnis

- [ISi-Mail-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Sicherer Betrieb von E-Mail-Servern, 2009, <http://www.bsi.bund.de/fachthem/sinet/>
- [ISi-Mail-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Sichere Nutzung von E-Mail, 2009, <http://www.bsi.bund.de/fachthem/sinet/>
- [ISi-LANA] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Sichere Anbindung lokaler Netze an das Internet, 2007, <http://www.bsi.bund.de/fachthem/sinet/>