Norbert Pohlmann

Bedrohungen und Herausforderungen des E-Mail-Dienstes

Die Sicherheitsrisiken des E-Mail-Dienstes im Internet

Der E-Mail-Dienst ist eine elastische Anwendung, in der diskrete Medien, die zeitunabhängig sind, wie Text und Grafik, ausgetauscht werden. Der E-Mail-Dienst ist einer der am weitesten verbreiteten und meist genutzten Dienste des Internets. Der E-Mail Verkehr macht 12% der Bandbreite im Backbone international agierender IP-Carrier aus. Pro Monat werden mehrere Billion (10^{12}) E-Mails weltweit ausgetauscht. Obwohl die E-Mail-Anwendung nicht als verlässlicher Dienst konzipiert wurde, wird sie heutzutage häufig als Mittel zur einfachen und professionellen nachrichtenbasierten Kommunikation im Internet eingesetzt.

1 Einleitung

Die Vorteile der E-Mail-Anwendung sind sehr klar zu erkennen: Jeder kann damit umgehen, weil die Handhabung sehr einfach ist. Die E-Mails werden innerhalb weniger Sekunden weltweit übertragen und jeder kann immer mit Hilfe von Mail-Boxen erreicht werden. Die Inhalte und Anhänge der E-Mails können sofort weiter verwendet werden, es tritt kein Medienbruch auf. Die E-Mail Anwendung ist sehr kostengünstig, da i.d.R. keine extra Gebühren für den Austausch der E-Mail bezahlt werden müssen.

Der E-Mail Dienst ist für die vernetzte Informations- und Wissensgesellschaft inzwischen eine nicht mehr wegzudenkende Anwendung.

Aber der E-Mail-Dienst erfüllt zurzeit nicht die gängigen Anforderungen an die IT-Sicherheit. Der E-Mail-Dienst basiert auf den Komponenten E-Mail-User-Agent (UA – Outlook, Thunderbird, …) und dem Mail-Transfer-Agenten (MTA – E-Mail-Server). Als Protokolle werden SMTP für den Austausch der E-Mail vom UA zum MTA und zwischen den MTAs verwendet sowie POP3 und IMAP für den Abruf der E-Mail aus den Mail-Boxen. Diese Komponenten und Protokolle bieten von sich aus keinerlei bzw. nur unzureichende Sicherheitsmechanismen, mit Hilfe derer Vertraulichkeit, Integrität und Verbindlichkeit der Nachrichtenübermittlung realisierbar wären.

Doch genau diese Aspekte sind grundlegend für eine verlässliche, sichere Anwendung des E-Mail-Dienstes. Ohne einen sicheren E-Mail-Dienst ist der Einsatz von E-Mail, z.B. in elektronischen Geschäftsprozessen sehr risikoreich, da z.B. im Falle von Vertragsabschlüssen per E-Mail zum Schutz aller Parteien ein vertraulicher, integrer und verbindlicher Kommunikationskanal unabdingbare Voraussetzung ist.

Wir müssen zurzeit feststellen, dass Spam, Viren, Phishing-Mails und andere Schwachstellen wie schlecht konfiguriert und betriebene E-Mail-Server, unzureichende Nutzung von Verschlüsselung und digitaler Signatur sowie nicht-aufgeklärte Mitarbeiter ein ernsthaftes Problem mit hohem Schadenspotential und ein sehr hohes Sicherheitsrisiko für jeden einzelnen, die Unternehmen und für die Gesellschaft dar stellen!

2 E-Mail-Infrastruktur

Im Folgenden soll die E-Mail-Infrastruktur zum besseren Verständnis der E-Mail-Anwendung dargestellt werden. Generell sind unterschiedlichste E-Mail-Server Installationen hinsichtlich Aufbau, Struktur und Funktionalität der E-Mail Infrastruktur denkbar. Zur näheren Verdeutlichung sind einige exemplarische Beispiele, die eine E-Mail-Infrastruktur eines E-Mail Service Providers und der Aufbau einer typischen E-Mail Installation eines kleinen oder mittelständischen Unternehmens mit einem SMTP Proxy, dargestellt.

2.1 E-Mail-Infrastruktur eines E-Mail Service Providers

Der Mail User Agent (Outlook, Thunderbird, …) auf unserem Computer (PC, Notebook, SmartPhone, …) interagiert prinzipiell mit Smarthost (spezieller Mail-Server), um eine E-Mail zu versenden und mit einem Mailbox-Server (Mail-Server mit E-Mail-Boxen), um E-Mail abrufen zu können. Account- und Identi-

Prof. Dr. Norbert Pohlmann

ist seit 2003 Informatikprofessor für Verteilte Systeme und Informationssicherheit im Fachbereich Informatik und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen. Außerdem ist er Vorstandsvorsitzender des IT-Sicherheitsverbandes TeleTrusT.
E-Mail: norbert.pohlmann@internet-sicherheit.de

Abbildung 1 | Typische Mail-Infrastruktur bei E-Mail-Providern, Großunternehmen oder Hochschulen

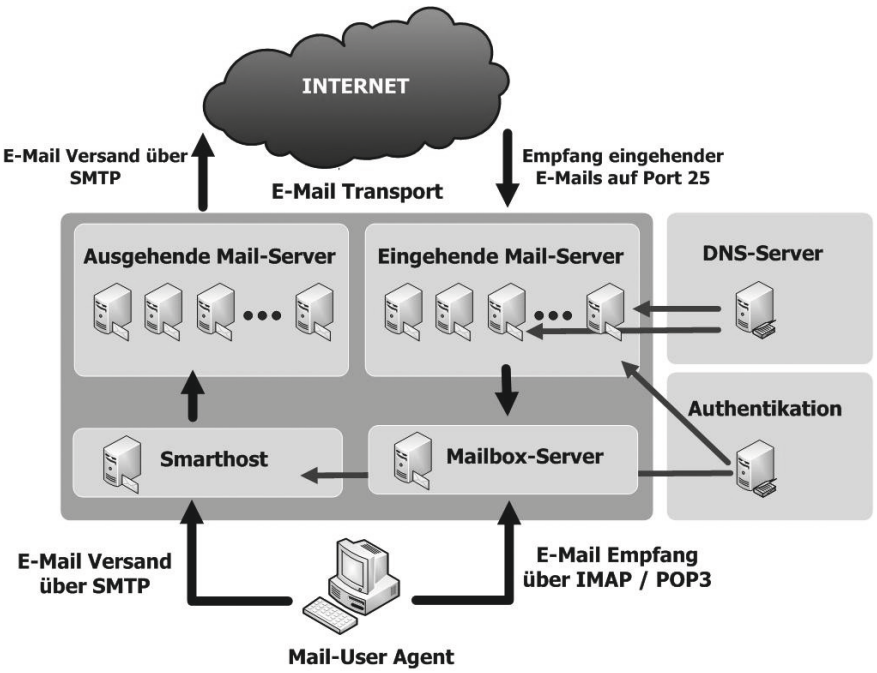
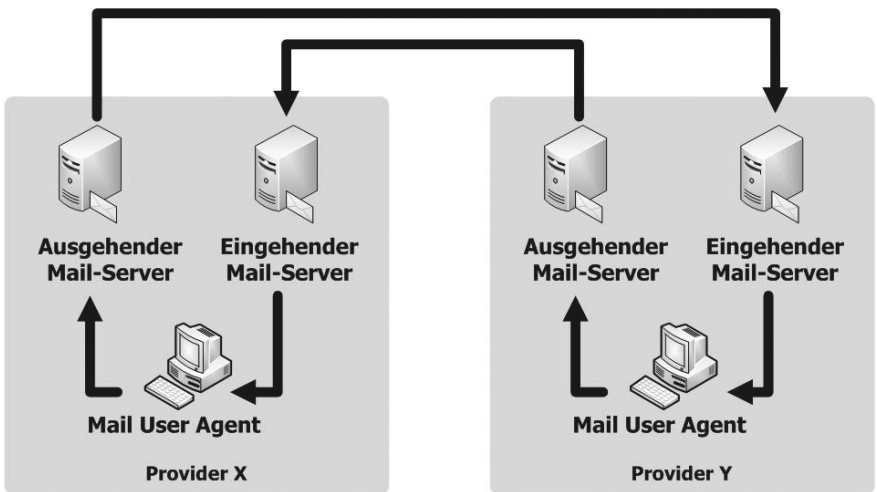


Abbildung 2 | Prinzip des E-Mail-Versandes zwischen zwei E-Mail-Service-Providern



ty-Management mit Authentikation wird i.d.R. über einen Verzeichnisdienst realisiert. In den DNS-Servern zeigen MX RRs mit verschiedenen Prioritäten auf „Eingehende Mail-Server" (Mail-Ins) des Providers. Damit weiß der „Ausgehende Mail-Server" (Mail-Out) eines Senders, zu welchem Mail-Server einer Domäne (…@abc.de) er die E-Mail senden soll. Um die Verfügbarkeit groß zu halten und den Performance-Ansprüchen zu genügen, arbeiten mehrere Mail-Server parallel. Große E-Mail Service Provider arbeiten mit mehreren hundert Mail-Servern und weiteren dazugehörigen Servern, um ihre Dienste anbieten zu können.

2.2 Ablauf des E-Mail-Versandes

Prinzipiell versendet der Provider X (E-Mail-Provider oder Unternehmen) über einen „Ausgehenden Mail-Server" (Mail-Out) ausgehende E-Mails mit Empfängern bei Provider Y an den „Eingehenden Mail-Server" (Mail-In) von Provider Y. Das heißt, E-Mails werden immer von Mail-Servern an andere Mail-Server gesendet. Ausnahme ist nur der Versand der Mail User-Agenten an die „internen"-Mail-Server (Ausgehender Mail-Server).

2.3 E-Mail-Infrastruktur eines kleinen oder mittelständischen Unternehmens mit einem SMTP Proxy

In Unternehmen werden oft Firewalls mit SMTP-Proxy verwendet, um den „Internen Mail-Server" gegen Angriffe von außen aus dem Internet zu schützen. Oft betreiben kleinere Unternehmen nur einen E-Mail-Server. Dennoch ist eine richtige Konfiguration für die Vertrauenswürdigkeit des Unternehmens und der gesamten E-Mail-Infrastruktur wichtig.

2.4 Die E-Mail-Infrastruktur des Internets

Laut einer durchgeführten Messung mit Hilfe einer Zustandsanalayse der SMTP-Ports aller erreichbaren Mail-Server/Proxys, kann abgeschätzt werden, dass die weltweite E-Mail-Infrastruktur im Internet ungefähr 2,4 Millionen Mail-Server weltweit bereit stellt [1].

All diese Mail-Server im Internet müssen richtig konfiguriert und betrieben werden, damit die E-Mail-Anwendung zuverlässig und vertrauenswürdig funktionieren kann. Leider wird diese Aufgabe im Internet nicht koordiniert. Jeder Betreiber eines E-Mail-Servers ist selbst für richtige Konfiguration und Betrieb verantwortlich.

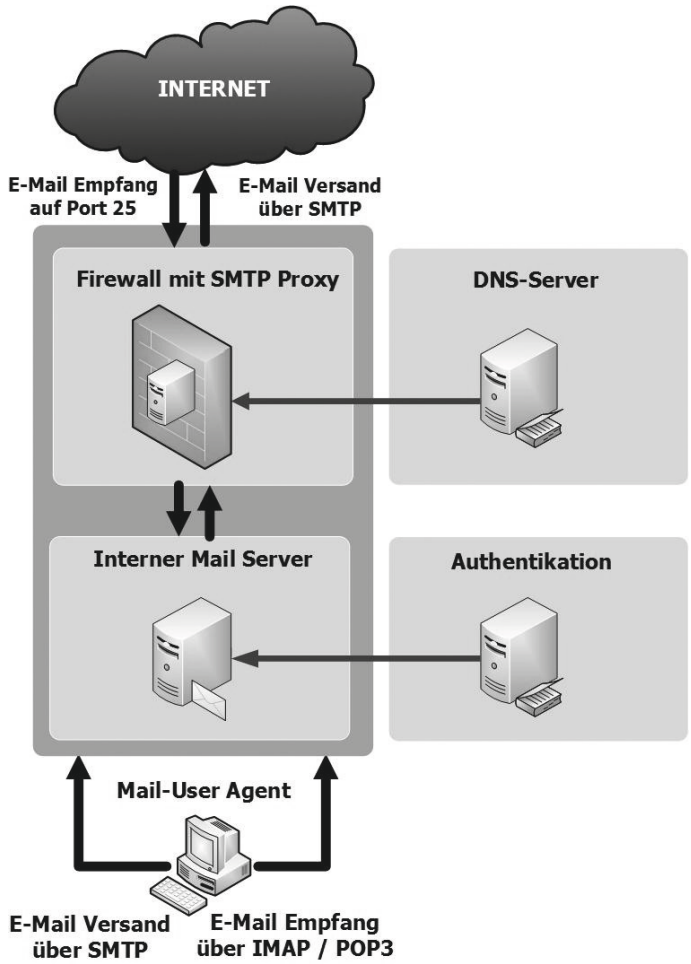
3 Anforderungen an Mail-Server

Die Mail-Server von E-Mail-Providern und Unternehmen müssen sehr gut konfiguriert sein und betrieben werden, damit die E-Mail-Infrastruktur im Ganzen vertrauenswürdig ihre Dienste tun kann. Dabei haben die E-Mail-Provider i.d.R. Experten, die diese Aufgabenstellungen umsetzen sollten. Problematischer ist dieser Bereich bei Unternehmen und hier insbesondere bei kleinen Unternehmen, die über keine besonderen Experten für die Aufgabenstellungen verfügen.

Hier einige Anforderungen an die Mail-Server:

- Umsetzung eines sicheren und robusten Aufbaus von E-Mail-Server zum Schutz von Angriffen.
- In einem eingehenden Mail-Server sollte sofort in Echtzeit nach Spam/Malware gesucht werden! Dazu müssen Anti-Spam und Anti-Malware Produkte oder

Abbildung 3 | Gängige E-Mail Infrastruktur kleiner und mittelständischer Unternehmen



Dienstleistungen optimal in die E-Mail-Infrastruktur eingebunden werden.

- Der erste Mail-Server (Mail-Proxy) muss direkte nichtexistente Empfänger blocken, damit solche E-Mails nicht die eigene E-Mail-Infrastruktur belasten! Einige größere und verteilte E-Mail-Infrastrukturen haben hier Probleme, weil die Informationen von erreichbaren Empfängern nicht zentral zu Verfügung stehen.
- Klares Konzept und Umsetzung von Delivery Status Notification (DSN) Message, Non Delivery Notifications (NDN) oder Bounce. Dies ist wichtig, damit der positive Empfang oder die Ablehnung von E-Mails implizit oder explizit für den Sender nachvollziehbar ist.
- Auch BackUp- oder Parallele-Mail-Server müssen kontinuierlich optimal konfiguriert sein, damit sie nicht für Angriffe genutzt werden können.
- Das Abrufen von E-Mails sollte grundsätzlich nur verschlüsselt erlaubt sein. Abruf-Protokolle gibt es auch mit Transportverschlüsselung (TSL, SSL), wie IMAPS, POP3S.
- Mail-Server müssen RFC-konform konfiguriert und betrieben werden. Das Problem ist aber, dass sich leider nicht alle an die Standards halten. Oft herrscht die Angst, dass wichtige E-Mails ablehnt werden müssen. Auch guten E-Mail-Experten fehlt häufig der Überblick über alle Abhängigkeiten und Besonderheiten, die mit den verschiedenen Konfigurationsmöglichkeiten einhergehen. Selbst sehr große Hersteller halten sich nicht an RFCs. Bei ordentlich konfigurierten Mail-Servern würde ein Großteil an Spam gar nicht erst auftreten/verbreitet!
- Auch die saubere DNS-Verwaltung und die Nutzung von klaren Hostnamen sind elementar wichtig für eine stabile und verifizierbare E-Mail-Infrastruktur!
- Klares und überprüfbares Account- und Identity-Management, um missbräuchliche Verwendungen zu unterbinden.
- Auch die Archivierung ist für Unternehmen notwendig, um die Geschäftsprozesse, die den E-Mail-Dienst nutzen, im Nachhinein verifizieren zu können. Auch hier gibt es sehr viele unterschiedliche Aspekte und Anforderungen, die berücksichtigt und umgesetzt werden müssen.
- Usw.

Für alle diese notwendigen Aufgaben sind Experten für E-Mail-Server notwendig. Leider sind aber sehr viele Mail-Server unzureichend konfiguriert, sodass viele Prüfungen, die einen verlässlicheren Dienst ermöglichen würden, zurzeit nicht flächendeckend und damit nicht automatisierbar möglich sind.

Diese ganze Situation sorgt dafür, dass die weltweite E-Mail-Infrastruktur zurzeit nicht optimal vertrauenswürdig gewährleistet werden kann!

▸ **Hinweis:**
Mit dem Deutschen DE-Mail-Gesetz wird zum ersten Mal ein E-Mail-Dienst mit definierten Eigenschaften reglementiert und mit Hilfe einer notwendigen Evaluation auch verifizierbar gemacht. Es ist bedauerlich, dass die globale Internet-Gemeinde es nicht geschafft hat, selbstorganisiert einen verlässlichen E-Mail-Dienst zu etablieren, der international genutzt werden kann.

4 Generelle Probleme des E-Mail-Dienstes

Der Basis-E-Mail-Dienst hat einige generelle Probleme oder Herausforderungen, die bei der Nutzung grundsätzlich betrachtet werden müssen.

4.1 Weltweit kann uns jeder E-Mails senden!

Für die E-Mails, die wir empfangen wollen, ist das eine sehr gute Eigenschaft!

Für die E-Mails, die wir nicht empfangen wollen (E-Mails mit Werbung, politischen Inhalten, kriminellen Absichten, …) hat sich das Wort „Spam“ etabliert. Es gibt aber auch E-Mails, die uns einen di-

rekten Schaden zufügen sollen. Das sind E-Mails mit Viren, Würmen, Trojanern oder auch Pishing E-Mails. Alle E-Mails, die wir nicht empfangen wollen, stellen ein großes Problem für die E-Mail-Anwendung dar, insbesondere weil die eigene E-Mail-Infrastruktur das Senden nicht verhindern und der Sender nicht eindeutig verifiziert werden kann.

Spam-E-Mails

Laut einer Studie der ENISA [3] ist der Spam-Anteil größer als 95 % in der E-Mail-Infrastruktur. Bei den Benutzern kommen zwar durch intelligente Filtermechanismen nicht mehr so viele Spams in den E-Mail-Postfächern an, aber das Aufkommen ist immer noch hoch und produziert einen sehr großen Schaden, weil 95 % der E-Mail-Infrastruktur für nicht-gewollte E-Mails vorgehalten werden muss. Leider sind die E-Mail-Provider nicht so sehr an gemeinsamen und internationalen Lösungen des Spam-Problems interessiert, weil sie mit ihren eigenen Anti-Spam-Lösungen auch Geld verdienen!

E-Mail-Anhänge

E-Mail-Anhänge können und werden dazu missbraucht, beim Empfänger Schadcode (Malware) auf den Computer zu schleusen. Dies kann z.B. in Form einer Datei im E-Mail-Anhang geschehen, die der Benutzer erst selbst ausführen muss, damit der Schadcode ausgeführt wird. Oder der Dateianhang nutzt direkt eine Sicherheitslücke in dem benutzten E-Mail Programm, das die erhaltene E-Mail in einem bestimmten Format darstellt. Eine weitere Möglichkeit, Schadcode über E-Mail einzuschleusen ist das Verlinken aus der E-Mail heraus auf eine kompromittierte Webseite. Solche E-Mails sind oftmals personalisiert und werden deshalb vom Benutzer als vertrauenswürdig eingestuft. Aber durch das Anklicken eines Links auf eine kompromittierte Webseite gelangt das Schadprogramm auf den Computer und wird infiziert. Aus diesem Grund müssen geeignete Anti-Malware-Systeme in die E-Mail-Infrastruktur eingebunden werden.

4.2 Eine E-Mail ist wie eine Postkarte!

Es wird vom E-Mail-Dienst keine Vertraulichkeit garantiert! Passworte, Kreditkartennummern und weitere Bankdaten sowie vertrauliche Informationen, werden im Klartext übertragen und stellen so ein großes Risiko dar! Die Möglichkeiten, eine E-Mail abzugreifen sind sehr hoch. In einigen Ländern werden alle E-Mails analysiert, um z.B. an das Knowhow von Firmen andere Länder zu kommen.

Wir wissen von Untersuchungen und Befragungen, dass zurzeit weniger als 4 % alle E-Mail verschlüsselt werden. Wir wissen aber auch, dass mindestens 43 % der E-Mails in Business-Prozessen verwendet werden [3]. Aus diesem Grund sollten den Mitarbeitern im Unternehmen E-Mail-Verschlüsselungstechnologien zur Verfügung gestellt werden, damit die E-Mails gegen unberechtigte Einsichtnahme geschützt werden. Die Mitarbeiter müssen aber wissen, wie und - ganz wichtig - wann diese Verschlüsselungstechnologien für vertrauliche E-Mails verwendet werden sollen.

E-Mail-Verschlüsselung

Bis auf einige isolierte PGP- und S/MIME-Inseln, gibt es in der Praxis zurzeit kaum fundierte Konzepte für unternehmensweite und übergreifende E-Mail-Verschlüsselungslösungen. Die Ursachen für die geringe Nutzung, sind neben dem Unwissen über die Risiken, die hohen Kosten für die E-Mail-Verschlüsselungsinfrastruktur durch Clientsoftware, Token, Lesegeräte, Rollout, Helpdesk, Zertifikatsmanagement, usw. [4].

End-to-End Verschlüsselungslösungen

End-to-End Verschlüsselungslösungen für E-Mails haben sich in der Praxis kaum durchgesetzt. Neben den hohen Kosten und aufwendiger Administration kranken die End-to-End-Lösungen an den folgenden Problemfeldern:

- Interoperabilitätsprobleme, insbesondere bei unternehmensübergreifender und produktübergreifende Verschlüsselung
- Message-Recovery-Problematik
- Vertreter-Regeln
- Malware-Problematik in E-Mail-Anhängen

End-to-End Konzepte sind individuelle Konzepte, d.h. sie benötigen so viele Schlüssel wie Mitarbeiter im Unternehmen sind. Scheidet ein Mitarbeiter aus dem Unternehmen aus, muss gewährleistet sein, dass berechtigte Personen, die an diesen Mitarbeiter gerichteten oder von ihm bereits erhaltenen E-Mails, lesen und beantworten können. Die Schlüssel der Mitarbeiter müssen bei diesen Konzepten entweder an zentraler Stelle hinterlegt werden, oder jede E-Mail muss zusätzlich mit einem „Hauptschlüssel“ - also doppelt - verschlüsselt werden. Die gleiche Problematik gilt für die Vertretung bei Abwesenheit des Mitarbeiters. Bei der Prüfung verschlüsselter Mail-Anhänge auf Malwarebefall wären aufwendige Umverschlüsselungen erforderlich, da Anti-Malware-Programme nur im Klartext die Anhänge analysieren können. Hier müssen dann auf dem Computer besondere Anti-Malware-Maßnahmen getroffen werden, um nach der Entschlüsselung die Anhänge auf Malwarebefall zu untersuchen.

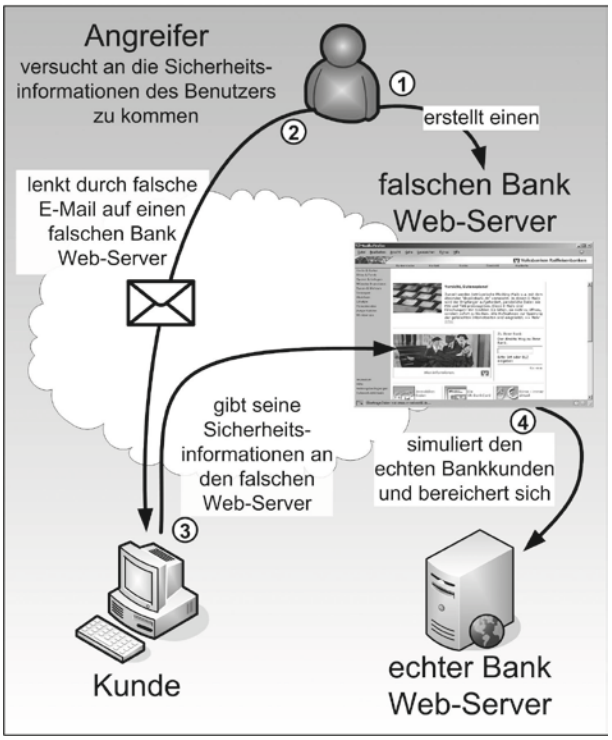
Gateway E-Mail-Sicherheitslösungen

Bei dem Gateway-Ansatz befindet sich ein E-Mail-Gateway mit Sicherheitsfunktionen an zentraler Stelle im Netzwerk. Diese E-Mail-Sicherheits-Gateways entschlüsselt und verifiziert eingehende E-Mails und sind in der Lage, hinausgehenden E-Mail-Verkehr zu verschlüsseln und zu signieren. Durch die zentrale Positionierung bietet das E-Mail-Sicherheits-Gateway Vertraulichkeit (Verschlüsselung), Integrität und Verbindlichkeit (Signatur) für den gesamten E-Mail-Verkehr. Auf der Gegenseite kann ebenfalls ein E-Mail-Sicherheits-Gateway stehen oder eine entsprechende Client-Software, um die Sicherheitsfunktionen zu realisieren. Steht keine dieser Komponenten auf der Gegenseite zur Verfügung, können solche E-Mail-Sicherheits-Gateways verschlüsselte, selbstextrahierende Dateien zuschicken, die mittels Passphrase wieder entschlüsselt werden können. Da bei dem Gateway-Ansatz die Entschlüsselung zentral im E-Mail-Sicherheits-Gateway durchgeführt wird, kann eine Vertreterregelung sowie die zentrale Überprüfung der E-Mail-Anhänge sehr einfach realisiert werden.

4.3 Fehlende Nachweisbarkeit

Der Absender einer E-Mail und die Echtheit des Inhaltes einer E-Mail können nicht verifiziert werden, das heißt, wir können nicht eindeutig feststellen, ob die E-Mail während der Übertragung mani-

Abbildung 1 | Phishing-Angriff, Beispiel: Emissionshandel



puliert wurde. Außerdem können Sender und Empfänger nicht sicher sein, mit wem sie E-Mails austauschen.

Die Gewissheit, dass eine E-Mail angekommen ist (Bestellungen, usw.) hängt von der Qualität von E-Mail-Servern anderer ab, auf die der Sender keinen Einfluss hat (vertraglich, rechtlich, …). Die Verbindlichkeit einer Bestellung durch eine E-Mail (Zimmer, Tagungsräume, usw.) ist nicht zweifelsfrei möglich, da der Sender jede E-Mail-Adresse annehmen kann.

Digitale Signatur

Mit Hilfe einer digitalen Signatur auf der Basis von Public-Key-Verfahren kann eine E-Mail signiert werden und damit ist eine gesetzliche Verbindlichkeit von E-Mails realisierbar.

Zwar werden laut Untersuchungen im Schnitt 6 % aller E-Mails digital signiert, im Finanzbereich sogar bis zu 17 %, aber verifizieren können i.d.R. wieder nur 4 %, die über ein etabliertes Public-Key-Management verfügen.

Hier brauchen wir auf der Geschäftsebene Sicherheitsfunktionen, z.B. durch die Bestätigung des Empfangs auf der Anwendungsebene oder auf der Infrastrukturebene, wie bei DE-Mail vorgesehen.

Zeitstempeldienste

Signaturen sind durch die Einbindung so genannter Zeitstempeldienste erweiterbar. Die Zeitstempelfunktionalität bedeutet jedoch mehr als nur ein elektronischer „Post-Eingangsstempel". Ein Zeitstempel ist der eindeutige Beleg darüber, wann ein Dokument in einer bestimmten Form vorgelegen hat. Sobald an dem digital „zeitgestempelten" Dokument Veränderungen vorgenommen werden, sind diese nachprüfbar. E-Mail-Korrespondenz und Archivierungssysteme profitieren durch Zeitstempelfunktionaliäten. Zeitstempeldienste erlauben den Nachweis der Authentizität und Integrität von Daten zu einem bestimmten Zeitpunkt. Ereignisse wie zum Beispiel der Eingang von Bestellungen, Online-Auktionsgeboten oder Online-Brokerage-Aktivitäten werden mittels des Time-Stamping-Systems mit einer offiziellen Zeitangabe versehen.

5 Phishing (Password Fishing)

Im Folgenden wird ein Phishing-Angriff am Beispiel eines Angriffes auf Bankkunden dargestellt. Um an die Benutzerdaten des Bankkunden zu kommen, wendet der Phisher einige Tricks an (Abbildung 2). Als erstes erstellt er einen falschen Bank-Web-Server, der vom Erscheinungsbild her dem echten Bankserver täuschend ähnelt. Als zweites sendet er hunderttausende gefälschter Bank-E-Mails, die aussehen, als wären sie von der echten Bank, an potentielle Kunden. Diese gefälschten Bank-E-Mails fordert den Bankkunden auf, wichtige und notwendige Aktionen auf den falschen Bank-Web-Server durchzuführen. Fällt ein Empfänger auf die falsche Bank-E-Mail herein und folgt dem falschen Link, so gelangt dieser auf einen falschen Bank-Web-Server. Dabei geben meist sogar die Links auf den ersten Blick nur wenig Grund zur Annahme, dass es sich dabei um eine Fälschung handeln könnte. Die Schwierigkeit besteht also im Wesentlichen darin, dass es für den Kunden nicht sofort ersichtlich ist, dass diese E-Mail gefälscht ist und nicht von seiner Bank versendet wurde.

Im dritten Schritt werden dem Opfer dann seine Sicherheitsinformationen auf dem falschen Bank-Web-Server entlockt. Sowohl die gefälschte E-Mail als auch die gefälschte Webseite wirken wie die der echten Bank. Neben falschen Bank-E-Mails werden weitere Techniken verwendet, um die Kunden auf falsche Web-Server zu leiten. Darunter befinden sich z.B. etwa falsche Werbebanner oder falsche Suchmaschineneinträge. Im vierten Schritt nutzt dann der Angreifer die Sicherheitsinformationen, um sich gegenüber dem echten Bank-Server als Kunde zu präsentieren und unberechtigt Geld auf sein Konto zu transferieren [5].

Die Mitarbeiter in Unternehmen, die für den Emissionshandel verantwortlich waren, sind auf intelligente Phishing-E-Mail hereingefallen! Dieser Angriff hat Schäden in Millionen höhe verursacht. Die Mitarbeiten der Unternehmen hätten geschult werden müssen, damit diese Angriffe nicht erfolgreich durchgeführt werden können.

6 Mitarbeiter müssen die Gefahren der E-Mail-Anwendung kennen, sonst schaden sie der eigenen Firma!

Damit die E-Mail-Anwendung vertrauenswürdige genutzt werden kann, können einige Kompetenzen für Mitarbeiter hilfreich sein.

6.1 Verhaltensregeln beim E-Mail-Austausch (E-Mail-Policy)

Die Kommunikation via E-Mail ist im privaten und beruflichen Leben für viele bereits selbstverständlich geworden. Der richtige Umgang mit der E-Mail-Anwendung ist jedoch noch nicht optimal etabliert. Aus diesem Grund werden einige Verhaltensregeln beschrieben, die für alle Beteiligten bei der richtigen Umsetzung hilfreich sind und als E-Mail-Policy eingehalten werden sollten. Diese Regeln helfen auch, die Vertrauenswürdigkeit von E-Mails besser einschätzen zu können und damit Schäden zu vermeiden.

Inhalt und Form der E-Mails

Jeder, der eine E-Mail schreibt, sollte sich genau überlegen, was er dem oder den anderen mitteilen möchte. Die Tatsache, dass eine E-Mail schnell verfasst ist und kein Porto kostet, ist kein Grund, andere mit Belanglosigkeiten zu bombardieren. Auch ist die Unkompliziertheit des Mediums kein Freibrief für formale Nachlässigkeit. Ein freundlicher Umgangston, korrekte Rechtschreibung, Anrede und Schlussformel sowie eine übersichtliche Struktur sollten in einer E-Mail ebenso selbstverständlich sein wie in einem „normalen" Brief. Dazu gehört auch, dass die Betreffzeile immer einen aussagekräftigen Hinweis auf den Inhalt der E-Mail enthält. Die Empfänger von E-Mails sollten vor dem Senden richtig eingeordnet werden, um Klarheit über den eigenen Anspruch an die Empfänger darzustellen.

- Das Feld „An" (To) gibt die E-Mail-Adresse von primären Empfängern an. Hier sollten nur die Empfänger eintragen werden, von denen eine Reaktion, eine Antwort, erwartet wird.
- Das Feld „Cc" (Carbon Copy = Durchschlag) gibt die E-Mail-Adressen der sekundären Empfänger an, die den Inhalt der E-Mail lediglich zur Kenntnis nehmen sollen. Bei der Zustellung wird zwischen primären und sekundären Empfängern nicht unterschieden.
- Das Feld „Bcc" (Blind Carbon Copy) hat die gleiche Bedeutung wie das Feld „Cc" – mit dem Unterschied, dass die Zeile „Bcc" in den Kopien, die an die verschiedenen Empfänger gesendet werden, nicht sichtbar ist. Das ermöglicht dem Sender, eine E-Mail an eine Gruppe von Empfängern zu schicken, ohne dass jeder die E-Mail-Adressen der anderen sieht. Dies ist eine sehr einfache Möglichkeit, E-Mail-Adressen zu schützen. Leider wird sie aber noch nicht von allen genutzt.

Die E-Mail-Antwort

Die E-Mail wird sehr schnell an den Empfänger ausgeliefert, der sich bemühen sollte, diese auch zügig zu beantworten. Im Geschäftsleben erwartet der Absender heute eine Antwort innerhalb eines Werktages. Wenn der Empfänger also weiß, dass er nicht so schnell reagieren kann, sollten er eine automatische Abwesenheitsnotiz versenden, die den Sender darüber informiert, dass der Empfänger nicht da ist und ab wann er wieder zu erreichen ist.

Außerdem sollte die Antworten-Funktion gewählt werden, damit der ursprüngliche Text wieder mit zurückgeschickt werden. So weiß der Empfänger auf einen Blick, worauf sich die Antwort bezieht. Dabei sollte der alte Text immer unten stehen und die Antwort oben. Geht eine E-Mail mehrfach hin und her, sollten sie zwischendurch neu angelegt werden, damit sie nicht unendlich lang wird.

Die E-Mail-Signatur

Die E-Mail-Signatur ist ein Text, der an das Ende einer E-Mail automatisiert oder explizit angehängt wird und Informationen über den Absender enthält. Sie ist in bestimmtem Kontext gesetzlich vorgeschrieben und erleichtert die Kontaktaufnahme, zum Beispiel im Falle einer telefonischen Rückfrage, zeigt die rechtliche Stellung des Absenders (bei Unternehmen gesetzlich vorgeschrieben) und hilft bei der Einschätzung der Vertrauenswürdigkeit des Absenders.

Vermeintlich vertrauenswürdige E-Mails

Wenn sich im E-Mail-Postfach eine E-Mail mit dem Absender eines guten Freundes befindet, wird diese automatisch schon als vertrauenswürdig eingestuft. Diese E-Mail verweist z.B. per Link auf eine interessante Seite im Internet. Aber auch diese E-Mail kommt gar nicht vom Freund, sondern von einem Angreifer. Wie aber kann das sein?

Der Absender kann bei E-Mails frei benannt werden – genau wie bei einer Postkarte. Das ist aus Betrügersicht natürlich eine hervorragende Grundlage für einen Angriff, nämlich mit E-Mails, die von einem vermeintlich vertrauenswürdigen Absender stammen und einen, auf den ersten Blick, interessanten Link beinhalten. Aus diesem Grund sollten die Empfänger von E-Mails niemals auf Links klicken, wenn sie nicht genau wissen, worum es sich dabei handelt. Der Link könnte beispielsweise auf eine infizierte Webseite leiten, wodurch Malware auf den Computer geladen wird. Mithilfe der Malware werden dann die Daten ausspioniert und/oder die Kontrolle über den Computer übernommen. Auch der Link ist letztlich nur ein Text, der frei eingegeben werden kann. Ohne eine Kontrolle kann der Nutzer sich deshalb nie sicher sein, ob der angegebene Link tatsächlich zu der angekündigten Webseite führt. Es gibt verschiedene Anhaltspunkte, anhand derer ein Nutzer drohende Gefahren erkennen und damit Schaden vermeiden kann [6].

Die Nutzer eines E-Mail-Dienstes sollten einer E-Mail keine Beachtung schenken, die eine seltsame Information enthält oder in einer Sprache geschrieben ist, die der Absender normalerweise nicht verwendet! Bei Unsicherheit hilft es, den Absender einfach anzurufen, der die E-Mail geschickt hat, und nachzufragen, was es damit auf sich hat. Die meisten Angriffsversuche lassen sich so bereits abwehren. Zudem ist es immer ratsam, das Ziel eines Links durch Darüberfahren mit der Maus zu überprüfen.

Eine aktuelle Studie der „Messaging Anti-Abuse Working Group" ergab, dass 57 Prozent der Befragten schon einmal Spam-Mails geöffnet oder einen darin enthaltenen Link angeklickt haben [7]. Das ist nicht nur ein persönliches Problem der Mitarbeiter. Das kann auch zur Gefahr für eine Firma werden. Ein Unternehmen braucht aufgeklärte Mitarbeiter, die die Gefahren kennen und sich und das Unternehmen schützen können.

6.2 Der richtige Umgang mit E-Mail-Adressen

Jeder sollte eine sehr große Zurückhaltung bei der Weitergabe der eigenen E-Mail-Adresse haben. E-Mail-Adressen sollten nur an Personen weitergegeben werden, die man kennt und/oder vertraut.

Jeder sollte eine E-Mail-Adresse für den geschäftlichen (privaten) Mailverkehr, und eine zweite (dritte, ...) Adresse für Newsletter-Abonnements, E-Commerce-

Transaktionen und sonstigen Web-Aktivitäten verwenden. Erstere E-Mail-Adresse erhalten die im vorherigen Punkt erwähnten Vertrauenspersonen, letztere Adresse erhalten alle anderen.

Ein weiteres Übel sind die sogenannten Harvester, die das Internet nach E-Mail-Adressen absuchen („crawlen") und diese sammeln, um anschließend Spam an sie zu versenden. Deshalb sollten E-Mail-Adressen entsprechend auf Webseiten schützt werden. Das gilt auch für Dokumente, die auf einer Webseite abrufbar sind, egal ob es sich dabei um Office-Dokumente, PDFs oder PowerPoint-Präsentationen handelt. Denn gerade in solchen Dokumenten befinden sich in der Regel personenorientierte E-Mail-Adressen. Es gibt verschiedene Gegenmaßnahmen, wie eine E-Mail-Adresse „verschleiert" dargestellt werden kann [8].

7 Den E-Mail-Dienst selber betreiben oder als Dienstleistung einkaufen?

Insbesondere für kleine und mittelständige Unternehmen stellt sich die Frage, ob sie in der Lage sind, den E-Mail-Dienst mit all seinen steigenden Anforderungen noch selber betreiben zu können. Durch die immer komplexeren Bedrohungen und steigenden gesetzlichen Anforderungen wird der Aufwand immer größer und damit sehr teuer.

Auf der anderen Seite werden die Anforderungen an einen geeigneten E-Mail Service Provider immer komplexer. Da der Provider alle wichtigen E-Mails für die Unternehmen behandelt, sind die Anforderungen an Vertrauenswürdigkeit außerordentlich hoch. Die Frage in der Zukunft wird sein: Können die E-Mail Service Providern diesen hohen Anforderungen genügen und sind die Unternehmen in der Lage, diese zu überprüfen? Anforderungen liegen im Bereich von Compliance-Anforderungen, Datenschutz und Vertraulichkeit für wichtige Unternehmenswerte und das über einen sehr langen Zeitraum.

8 Fazit

Die Sicherheitsrisiken des E-Mail-Dienstes im Internet sind zurzeit zu hoch.
Der E-Mail-Dienst bietet mit seinen Komponenten und Protokollen keine ausreichende vertrauliche, integere und verbindliche Kommunikation. Obwohl es Sicherheitslösungen für Verschlüsselung und digitale Signaturen gibt, sind diese heute nur punktuell im Einsatz. Auch Sicherheitslösungen gegen Spam und Malware sind vorhanden, bieten aber keinen 100%igen Schutz. Die Nutzer müssen gründlicher aufgeklärt werden, damit sie die E-Mail-Anwendungen angemessen nutzen können und nicht auf jeden Angriff herein fallen.

Damit der E-Mail-Dienst in Zukunft weiterhin positiv genutzt werden kann, müssen sehr viele Bedrohungen und Risiken durch die Technologiehersteller, die Betreiber von E-Mail-Infrastrukturen und die Nutzer der E-Mail-Anwendungen gemeinsam erkannt und verhindert werden. Hierbei scheint eine globale Lösung in Internet eine besondere Herausforderung zu sein, die aber für unsere internationale Gesellschaft unabdingbar sein wird.

Literatur:

[1] C. Dietrich, M. Niehues, N. Pohlmann: „Analyse der E-Mail-Infrastruktur - Hostzählung", iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 10/2007

[2] http://www.enisa.europa.eu/media/press-releases/prs-in-german/spam21012010de

[3] C. Dietrich, N. Pohlmann: „eMail-Verlässlichkeit – Verbreitung und Evaluation". In Proceedings der DACH Security Konferenz 2005, Hrsg.: Patrick Horster, syssec Verlag, 2005

[4] N. Pohlmann: „Die virtuelle Poststelle". In Proceedings des 8. BSI Kongress - IT-Sicherheit im verteilten Chaos, Hrsg.: Bundesamt für Sicherheit in der Informationstechnik, SecuMedia Verlag, 2003

[5] M. Hesse, N. Pohlmann: „Trickbetrügern auf der Spur: Wie man der Phishing-Welle entkommen kann", Bankinformation und Genossenschaftsforum, Deutscher Genossenschafts-Verlag, Wiesbaden, 01/2006

[6] M. Linnemann, N. Pohlmann: „Sicher im Internet: Tipps und Tricks für das digitale Leben", orell füssli Verlag, Zürich 2010

[7] http://www.maawg.org/system/files/2010_MAAWG-Consumer_Survey_Key_Findings.pdf

[8] S. Feld, N. Pohlmann: „E-Mail-Adress-Harvesting: Wie schütze ich mich vor dem E-Mail-Adress-Klau?", IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 02/2008