

Zusammenfassung

Die zunehmende Nutzung des Internets als Mittel sowohl privater als auch beruflicher Kommunikation macht die E-Mail zum universellen Kommunikationsmittel. Heute laufen viele Beziehungen privater oder geschäftlicher Natur oder mit dem Staat weitgehend über die Verwendung dieses Kommunikationsmittels. Die E-Mail ist in unserer heutigen Gesellschaft praktisch zu einem Kommunikationsstandard geworden.

Der Breitbandanschluss (DSL oder über Kabel-TV) verstärkt das Phänomen der weit verbreiteten E-Mail-Verwendung noch. Dank dieser Leistungssteigerung können heute problemlos mehrere Megabyte grosse Anhänge jeglicher Art (Textdateien, Programme, Musikdateien) verschickt werden.

Inhalt

- 1 Was ist eine E-Mail? →
- 2 Wie funktionieren E-Mails? →
- 3 Welches sind die mit der Verwendung von E-Mails verbundenen Risiken? →
- 4 Wie kann man sich schützen? →



1 Was ist eine E-Mail?

Eine E-Mail ist eine Nachricht, die über dazwischenliegende E-Mail-Server oder -Relays von einer Mailbox zu einer anderen übertragen wird. Konkret ist eine E-Mail ein Strom von Daten, die so strukturiert sind, dass die E-Mail-Server sie interpretieren und in die Mailbox des Empfängers befördern können.

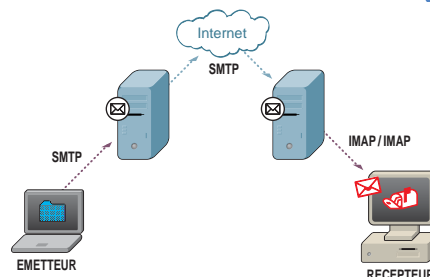
Eine E-Mail enthält folgende Elemente:

- die E-Mail-Adresse des oder der Hauptempfänger(s);
- die E-Mail-Adresse des Absenders der Nachricht;
- einen Inhalt (Message Body), der den Text der Nachricht enthält, und häufig auch angehängte Dateien;
- im Unterschied zur konventionellen Post enthält eine E-Mail ausserdem einen Betreff, anhand dessen sich die Nachricht identifizieren lässt;
- weitere Informationen für die Zustellung der Nachricht, ähnlich wie ein Poststempel (Datum, Uhrzeit, Liste der Server, über die die Nachricht weitergeleitet wurde usw.).

2 Wie funktionieren E-Mails?

Wie bereits erwähnt, ist eine E-Mail ein Datenstrom, der von einem Absender über dazwischenliegende E-Mail-Server oder -Relays an einen Empfänger übertragen wird. Das folgende Schema illustriert diesen Ablauf:

Wie dieses Schema zeigt, werden bei den Send- und Empfangsvorgängen mehrere Kommunikationsprotokolle verwendet.



Bekanntlich ist ein Protokoll eine Form der Kommunikation, die zwischen zwei Organisationen festgelegt wird und es ihnen erlaubt, Informationen auszutauschen. Es handelt sich dabei um nicht mehr und nicht weniger als eine gemeinsame Sprache, die zwei Organisationen (in der Regel ein Client und ein Server) verwenden, um eine bestimmte Aufgabe, hier den Versand einer E-Mail, durchführen zu können.

Die Tabelle rechts zeigt eine Übersicht über die diversen Protokolle, die im Rahmen des Versands und des Empfangs von E-Mails verwendet werden:

Die beschriebene Funktion erfordert die Verwendung eines E-Mail-Clients, d. h. eines Programms, das E-Mails lesen, schreiben, versenden und empfangen kann (z. B. Outlook, Outlook Express, Eudora).

Eine andere sehr beliebte Methode zur E-Mail-Verwendung ist Webmail. Dabei wird der E-Mail-Client durch einen einfachen Internet-Browser (z. B. Opera oder Internet Explorer) ersetzt. Der Zugriff des Clients auf den E-Mail-Server erfolgt über eine speziell dafür konzipierte Website (z. B. <http://webmail.pt.lu/> oder <http://mail.yahoo.com/>).

PROTOKOLLE | BESCHREIBUNG

PROTOKOLLE	BESCHREIBUNG
SMTP	SIMPLE MAIL TRANSFER PROTOCOL Versand der E-Mail vom Absender zum Server und Übermittlung von Server zu Server.
POP3	POST OFFICE PROTOCOL E-Mail-Empfangsprotokoll. Das älteste und am häufigsten verwendete Empfangsprotokoll.
IMAP4	INTERNET MESSAGE ACCESS PROTOCOL Mit POP3 vergleichbares Empfangsprotokoll. Ein Protokoll neueren Datums, das neue Funktionen aufweist. Diese Funktionen haben keinen besonders grossen Nutzen für die User, daher findet IMAP4 keine grosse Verwendung.



3

Welches sind die mit der Verwendung von E-Mails verbundenen Risiken?

Eine E-Mail stellt gewisse Risiken für die Anwender dar und ist anfällig für zahlreiche Übergriffe. Aufgrund der starken E-Mail-Verwendung sind diese Risiken entsprechend stark verbreitet und bedrohen fast alle User. Die wichtigsten Risiken für die E-Mail-Anwender sind:

► Würmer und Viren

Ein Virus ist ein Programm (oder Teil eines Programms) - auch ausführbarer Code genannt -, das sich verbreitet, indem es sich an diverse Dateien oder andere Programme anhängt, Computer infiziert und sich ohne Wissen der User von einem Gerät zum anderen verbreitet. Ein Virus aktiviert sich nur, wenn ein User aktiv den Code ausführt, in den er integriert ist.

Ein Wurm ist ein Programm, das dem eines Virus ähnelt. Ein Wurm benötigt jedoch im Gegensatz zum Virus nicht die Mitwirkung des Menschen, um einen Computer zu infizieren. Er verfügt über einen Automatismus, der es ihm ermöglicht, seinen Code automatisch auszugeben und in der Folge neu zu infizierende Ziele zu suchen.

Durch die direkte Integration des aktiven Codes in bestimmte E-Mail-Clients sowie durch neue Viren-Kodierungstechniken können Viren heute aktiv werden, ohne dass ein Anhang geöffnet wird.

▶ Untergrabung von Vertraulichkeit und Integrität

Die Entwickler der E-Mail-Protokolle haben nicht berücksichtigt, dass Vertraulichkeit und Integrität der ausgetauschten Daten gewährleistet sein müssen: Alle E-Mails werden standardmässig in Klartext im Internet versandt, und jeder, der auf die E-Mail auf ihrem Weg zum Empfänger Zugriff hat, kann den Inhalt lesen und kopieren. Darüber hinaus ist die Integrität der Nachricht nicht geschützt, und es lässt sich leicht eine E-Mail mit einer falschen Absenderadresse versenden (Identitätsdiebstahl).

Die Zugangsdaten des Users zu seiner Mailbox (Username und Passwort) sind ebenfalls für jeden lesbar, der sie abfangen oder darauf zugreifen kann.

▶ Trojanische Pferde

Ein **Trojaner** ist ein Programm oder ein Teil eines Programms (auch ausführbarer Code genannt), das den Anschein erweckt, harmlos zu sein, in Wirklichkeit jedoch ähnlich wie ein Virus den Zweck hat, einen Computer ohne Wissen der Anwender zu infizieren.

Im Unterschied zu einem Virus oder einem Wurm reproduziert sich ein Trojaner nicht. Er verbreitet sich auch nicht weiter. Er kann jedoch in bestimmten Fällen eine ebenso zerstörerische Wirkung haben.

Die E-Mail ist ein beliebtes Mittel, um einen Trojaner zu aktivieren und auf einem Zielrechner zu installieren.

▶ Spyware

Spyware ist ein Programm, das Informationen über den Anwender oder über seine Gewohnheiten ohne dessen Erlaubnis über das Internet insbesondere an Werbekunden übermittelt. Spyware wird in erster Linie über Websites und manchmal per E-Mail übertragen.

BEISPIEL:

Keylogger ist ein Tool, das alle Tastenanschläge auf einem Computer aufzeichnet.

▶ Missbrauch und Fälschungen

Die Account- und Usernamen, die erforderlich sind, um auf einen E-Mail-Server zuzugreifen, werden in Klartext (ohne Verschlüsselung) über das Netz versandt. Böswillige, die bestimmte Kenntnisse und geeignete Tools besitzen, können den Netzverkehr abhören, die Kennungen wiederherstellen und anschliessend auf ein Konto zugreifen, das ihnen nicht gehört.

▶ Spam

Spam ist die absichtliche Überschwemmung eines E-Mail-Accounts durch den Versand unerwünschter E-Mails wie etwa Werbung. Bei dieser Technik des Versands unerwünschter Massen E-Mails wird besonders häufig die Absenderadresse gefälscht.

▶ Social engineering

Social Engineering ist eine nicht technische Manipulations- und Angriffsform, die darin besteht, die Arglosigkeit des Opfers auszunutzen, um sich persönliche Daten oder vertrauliche Informationen zu verschaffen.

➔ Beispiel 1:

Ein Angreifer gibt sich am Telefon als Bankmitarbeiter aus und versucht, eine Kreditkartennummer zu erhalten.

➔ Beispiel 2:

Ein Angreifer gibt sich als Netzwerkadministrator einer Firma aus, bei der angeblich ein Softwareproblem aufgetreten ist, und fragt nach dem persönlichen Passwort.

▶ Phishing

Phishing ist die Verknüpfung einer unerwünschten E-Mail (Spam) mit einer illegalen Website, die das Design einer legitimen Geschäfts-Website nachbildet und den Internetnutzer verleitet, dort seine persönlichen Daten, insbesondere die Bankdaten, einzugeben.

Diese falschen Websites bilden meist Websites grosser US-amerikanischer Banken nach. Aber auch zum Beispiel eBay und PayPal, das Zahlungssystem von eBay, werden von Online-Kriminellen missbraucht.

Phishing ist also eine Kombination aus Social Engineering und Identitätsdiebstahl.

4

Wie kann man sich schützen?

▶ Würmer, Viren und Trojanische Pferde

- ➔ Verwenden Sie auf Ihren Computer ein Virenschutzprogramm mit Firewall.
- ➔ Öffnen Sie keine E-Mails, Software, Programme oder anderen Dateien, deren Betreff oder Inhalt Ihnen ungewöhnlich oder verdächtig vorkommt.
- ➔ Installieren Sie sogenannte Patches, die in den meisten Fällen ebenfalls gegen eine Infektion und die Verbreitung von Würmern schützen.

▶ Preisgabe

Sind die per E-Mail zu übertragenden Daten vertraulich, ist ein Verschlüsselungsprogramm zu verwenden. Dadurch werden die Daten nur für den Empfänger lesbar. Mit diesen Programmen lassen sich entweder der gesamte Inhalt der E-Mail oder auch nur die Anhänge verschlüsseln.

▶ Missbrauch und Fälschungen

Die elektronische Signatur bietet Schutz gegen Identitätsdiebstahl (Usurpation) und -fälschung. Mit der digitalen Signatur einer E-Mail lassen sich die Integrität der E-Mail (vor Fälschung) und auch die Integrität des Absenders sicherstellen.

▶ Spam

Um sich gegen Spam zu schützen, gibt es nur wenige wirksame Mittel. Internetnutzer können jedoch sicherstellen, dass ihr Internet Service Provider (ISP) die bekannten Spams mit einem guten Filter blockiert. Es gibt Listen bekannter Spam-Versender. Diese Versender werden auf schwarze Listen gesetzt (auch Blacklist genannt). ISPs können Server, die auf dieser Liste stehen, daran hindern, E-Mails an einen ihrer Kunden zu schicken.

▶ Phishing

Das einzige Mittel, um sich gegen Phishing und Social Engineering zu schützen, besteht darin, niemals vertrauliche Informationen (Passwort, Kreditkartennummer usw.) zu versenden, ohne sich der Identität der Person, die danach fragt, ganz sicher zu sein.