



E-Mail-Sicherheit





Übersicht

- Gefahren bei der Nutzung von Elektronischer Post
 - Spam
 - Hoax
 - Malware
 - Unerlaubter Zugriff auf das Postfach
 - Abfangen oder Mitlesen der Email
- Sichere Elektronische Post
 - Versende- und Empfangsmechanismus
 - Verschlüsselung und Authentizität



Unerwünschte elektronische Post SPAM

- Vergleichbar mit der täglichen Werbung im realen Briefkasten
- Spam-Mails transportieren
 - Links zu Internetangeboten, evtl. kostenpflichtige Inhalte
 - Macroviiren
 - Spyware



Tipps zur Vermeidung von Spam-Mails 1/2

- Benutzen Sie Ihre E-Mail nur sparsam im Internet
 - E-Mail nicht in News oder Web-Foren (z.B. Schlumpf Fanpage oder oder) benutzen. Wenn nötig, für solche Zwecke ein Benutzerkonto bei einem Freemailer eröffnen und nutzen. Der Trend zur Weg-Werf-Zweit-Email!
 - E-Mail nicht direkt auf Internetseiten bekannt geben.
 - Für geschäftliche Erstkontakte ein eigenständiges Benutzerkonto (z.B. info@ihredomain.de) nutzen, das gegebenenfalls umbenannt werden kann.
 - Bei der Internet-Firmenpräsentation E-Mail nicht in Form von ich@meinedomain.de, sondern das AT-Zeichen (@) ersetzen. Beispiel ich<>meinedomain.de oder als Grafik darstellen

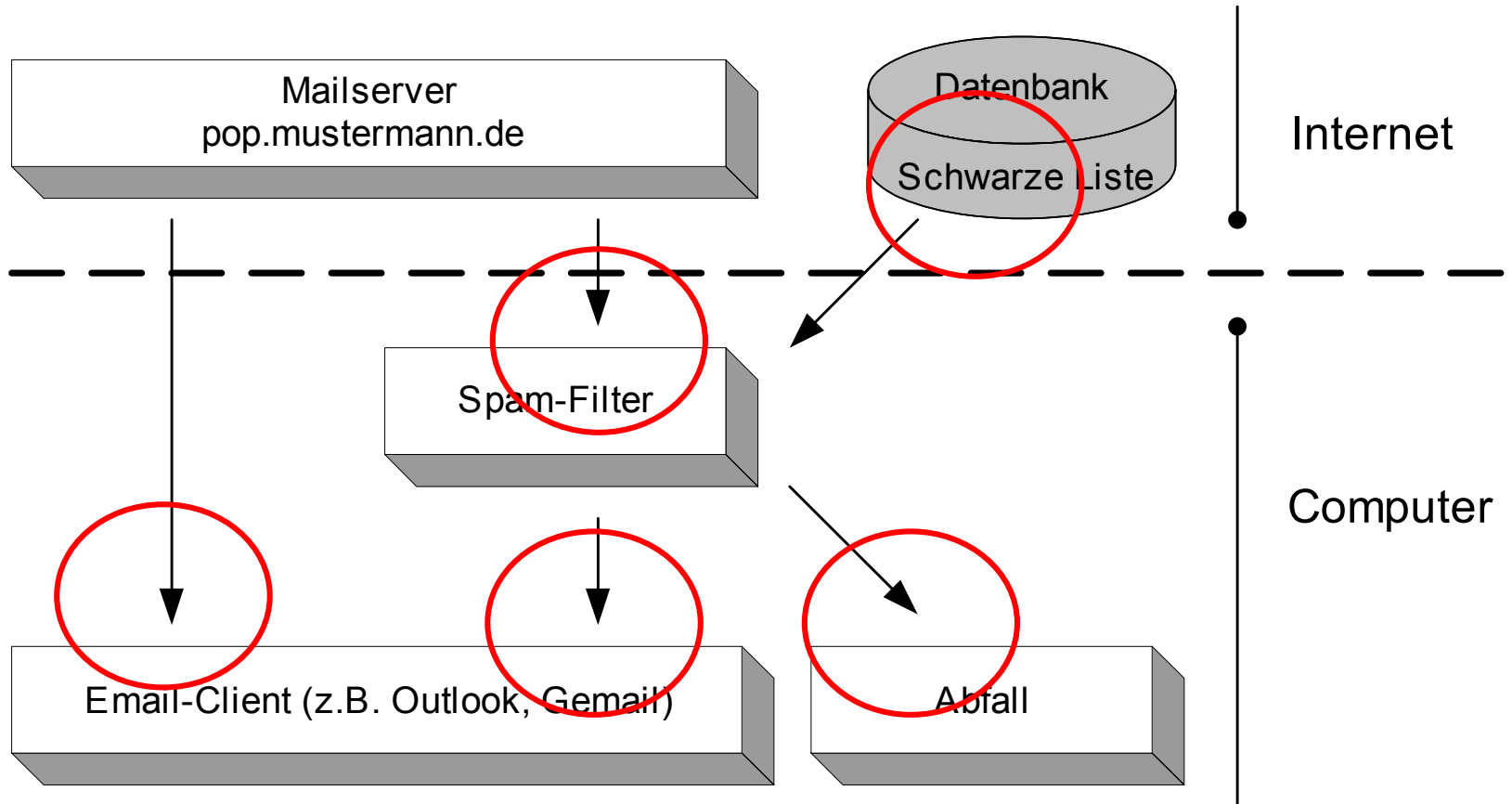


Tipps zur Vermeidung von Spam-Mails 2/2

- Freemail-Benutzerkonten stehen häufiger unter Beschuss von Spammails. Die Verwendung von einer eigenen Domain (z.B. anja@mustermann.de) mindert Spam und wirkt professioneller
- Niemals auf einen Link, den die Spam-Mail enthält, klicken. Meist ist die angezeigte Adresse des Links nicht die Tatsächliche.
- Niemals den Spam-Sender benachrichtigen, dass man von ihn keine Mail möchte



Spam-Filter





Möglichkeiten von Spam-Filtern

- Wahl eines Mail-Provider, der Spam-Filter mit anbietet (z.B. strato.de)
- Anti-Spam-Software für Heimanwender/Desktop
 - z.B. Opensource Spampal
<http://spampal.spxs.net/> Preis: 0€
(Nachteil: unterstützt nicht direkt TSL-Verschlüsselung)
 - z.B. Symantec Anti Spam 2004
<http://www.symantec.com/> Preis: ca. 40 €
- Anti Spam Filter für eigenen Mailserver z.B.
 - <http://www.networkassociates.com/>
<http://de.trendmicro-europe.com/>



Falschmeldungen engl. Hoax

- Ist eine E-Mail, die von einer vermeintlichen vertrauenswürdigen Person an Sie gerichtet ist
- Es wird versucht mit dieser Falschmeldung eine Aktion bei Ihnen auszulösen
 - Beispiel
Sender: info@antivirenhersteller
Betr. Neuer Virus im Umlauf
Sehr geehrte Kunden Bitte installieren Sie folgendes Programm, um ihr System zu schützen.....



Tipps

- Softwarehersteller verschicken keine Programme per E-Mail
- Klicken Sie nicht auf den Link in solchen E-Mails, da meist der angezeigte Text nicht mit der tatsächlichen Adresse (URL) übereinstimmt
- Niemals Passwörter bekannt geben oder sie auf Wunsch einer E-Mail ändern.
- Mahnungen kommen immer noch per Post!
- Kritische Änderungen, Aufforderung oder dergleichen werden auch heute noch **per Brief** mitgeteilt
- bei Unklarheit - zum Telefon greifen!
- Weitergehende Informationen auf www.hoax-info.de



Die Geschichte von Viren, Würmer, Trojanischen Pferden und Spyware

- Viren
 - sind Programme, die sich an Dateien anhängen
- Würmer
 - sind eigenständige Programme, die sich selbst verbreiten
- Makroviren
 - sind Skripte, die z.B. durch den E-Mail-Client ausgeführt werden
- Trojanische Pferde
 - sind Programme, die zunächst nützlich aussehen, aber im verborgenen böartige Funktionen haben
- Spyware
 - sind Programme, die Ihr System belauschen



Tipps zur Schadensbegrenzung

- Öffnen Sie nur E-Mails mit bekannten Absendern **und** sinnvoller Betreffzeile
- Benutzen Sie ein E-Mail-Programm mit den für Sie nur nötigen Funktionen oder schränken Sie diese ein
- Die Verwendung von Antivirenprogrammen ist **notwendig**
- Regelmäßiges Updaten der Virensoftware ist **absolut notwendig**

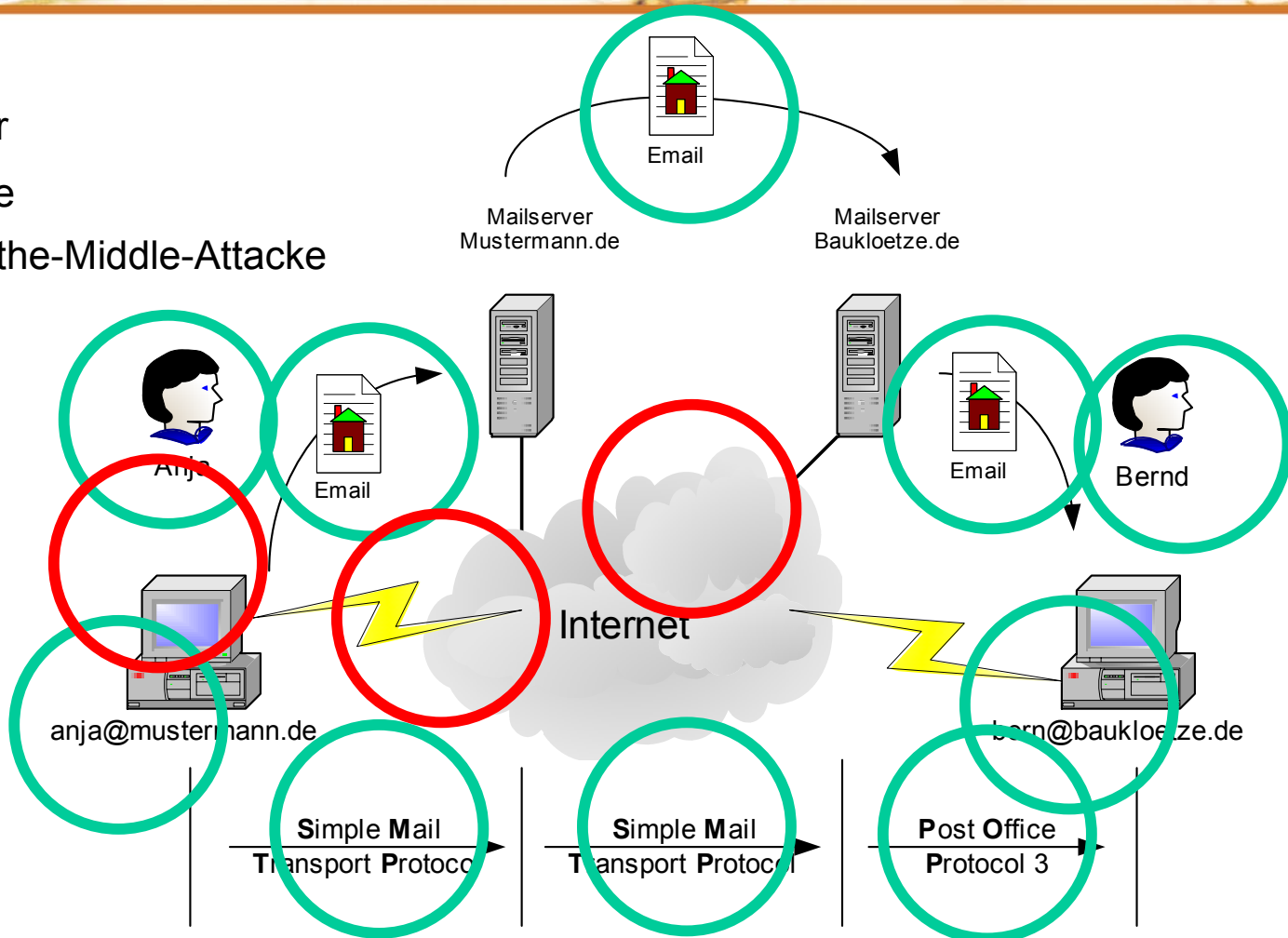


Grundlage E-Mail-Transport

Vom Sender zum Empfänger

Gefahren

- z.B. Trojaner
- z.B. Spyware
- z.B. Man-in-the-Middle-Attacke





Tipps für die Kommunikation.

- Verwendung von TSL (SSL) Verschlüsselung zum Schutz von Benutzernamen (Kontonamen) und Passwörtern beim POP3, SMTP und IMAP Protokoll
- Verschlüsselung (SSL/TSL) an dieser Stelle schützt **nicht vor Malware**, wie Trojaner, Spyware usw....
Die Antivirensoftware ist trotzdem notwendig
- Verwendung von separatem Passwort, das nur für das Mail-Konto verwendet wird.
- Falls es nur die Möglichkeit „POP über SSL“ und „SMTP unverschlüsselt“ gibt, so ist die Option „vor versenden POP-Abfragen“ die sicherste Methode



Vertraulichkeit, Integrität und Authentizität



Was macht einen Brief aus?

- Das Schreiben ist in einem Briefumschlag verpackt und ungeöffnet.
- Der Absender ist mit seiner vollständiger Adresse genannt, so dass ich prüfen kann wer mir schreibt.
- Den Text des Schreibens kann ich auf Veränderungen, wie Streichen, Überschreiben oder Manipulieren, prüfen.
- Der Verantwortliche für das Schreiben bestätigt mir die Richtigkeit mit seiner Unterschrift, die ich bei Bedarf später prüfen kann



Was macht eine E-Mail aus?

- Die E-Mail wird unverpackt, für jeden lesbar, durch die Netzwerke transportiert.
- Den Absender kann man nicht überprüfen.
- Der Inhalt kann, da jeder mitliest, auch von jedem verändert worden sein.
- Die Unterschrift ist nicht vorhanden oder kann genau wie der Text verändert worden sein



Forderung, die für sicheren E-Mailverkehr gelten, sind:

- Integrität - Der gesamte Inhalt ist unverändert.
- Vertraulichkeit - Nur die Kommunikationspartner kennen den Inhalt
- Authentizität - Mein Gesprächspartner ist wirklich der, den er vorgibt
- Prüfwert, der eindeutig aus dem Text gewonnen wird. (Hash)
- Verschlüsselung der Daten (Symmetrische Verschlüsselung)
- Digitale Ausweise (Digitale Zertifikate und Asymmetrische Verschlüsselung)



Werkzeug für sichere E-Mail Kommunikation

- **PGP**
(*Pretty Good Privacy*)
 - arbeitet mit privaten und öffentlichen Schlüsseln
 - jeder Benutzer verwaltet sein privates Schlüsselbund der öffentlichen Schlüssel mit dem Gesprächspartner, mit dem er verschlüsselt kommunizieren möchte
 - wird als Zusatzsoftware installiert
- **S/Mime**
(*Secure Multipurpose Internet Mail Extension*)
 - arbeitet mit digitalen Zertifikaten
 - Eine Hierarchie mit verschiedenen Ebenen sorgt für die Echtheit der digitalen Zertifikate
 - Die Unterstützung ist in den gängigen E-Mail-Programmen eingebaut.



Fazit

- Mit der Verwendung von Antivirensoftware, Spam-Filtern und Signaturesoftware kann einiges an Sicherheit im Elektronischen Schriftverkehr erreicht werden.
- Ein umfassender Schutz ist allerdings nie erreichbar
- Die Schutzmaßnahmen müssen laufend auf dem aktuellsten Stand sein
- Es gilt: lieber ein mittelmäßiger Schutz, dessen Funktion man versteht, als **gar keinen!**