Sicherheit für Macs

Mac User Group Stuttgart
18. Januar 2005

Christina Zeeh • info@tuxtina.de • http://tuxtina.de

Mac – wirklich sicherer?

- Standardinstallation ist relativ sicher (keine offenen Ports etc.)
- Unterstützung bewährter Unix-Sicherheitskonzepte (Mehrbenutzerbetrieb, Dateizugriffsrechte, ...)
- Nützliche Bordmittel
  - Keychain
  - File Vault, verschlüsselte Disk Images

Mac – wirklich sicherer?

- Ein sicheres Betriebssystem kann nicht alle Sicherheitsprobleme verhindern
- Jede Software enthält Fehler, mit zunehmender Verbreitung von Mac OS X steigt auch die Gefahr des Ausnutzens von Sicherheitslücken
- Ziele des Vortrags
  - Risiken erkennen
  - Risiken vermeiden

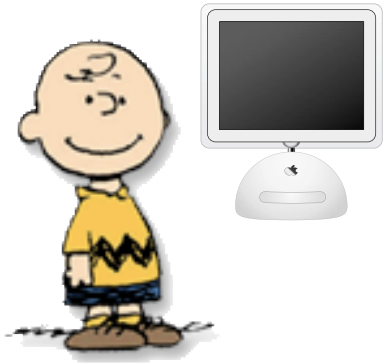
Mögliche Angreifer

Betrüger

Spammer

Skript-Kiddies

Datensammler



Virenschreiber

neugierige Mitbenutzer

Hacker

Dieb

Ex-LAP

Big Brother

Ex-Mitarbeiter

Angriffsziele

- Daten ausspionieren
  - Kreditkartennummern, Kontodaten etc.
  - Persönliche Informationen, Verhaltensprofile
- Daten verändern, löschen
- Rechnerzugriff
  - Spamversand
  - Ausgangsbasis für Angriffe
  - Lagerung illegaler Daten

Allgemeine Tipps (1)

- Vorsicht vor Anwendungen und Daten aus nicht-vertrauenswürdigen Quellen
  - Anwendungen haben beim Ausführen automatisch die Rechte des Benutzers
  - Daten können Sicherheitslücken (sog. Buffer-Overflows) zum Ausführen von Code ausnutzen
- Jede installierte Software, insbesondere mit Netzwerkfunktionalität, ist ein Risiko
  Nicht wahllos alles ausprobieren!

Allgemeine Tipps (2)

- Gesundes Misstrauen behalten
- Software aktuell halten
- Sorgfältige Benutzerverwaltung
- Backups machen
  - regelmäßig
  - überprüfen
  - sicher aufbewahren

Allgemeine Tipps (3)

- Gute Passwörter wählen
- Passwörter regelmäßig ändern
- Sicherheitsabfragen und Passwortabfragen beachten, im Zweifelsfall lieber ablehnen
- Passwörter niemals herausgeben
- Passwörter nicht aufschreiben (zumindest nicht in der nähe des Rechners), ggf. Keychain nutzen

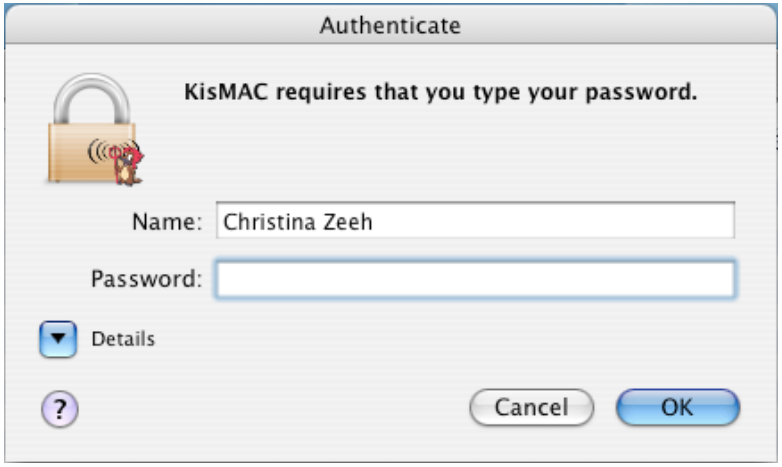
Macs sicher(er) konfigurieren

Mac sicher(er) konfigurieren

- Passworthinweis nicht verwenden
- Automatischen Login abschalten
- Bildschirmschoner und Schlafmodus mit Passwortschutz verwenden
- Unix-Philosophie: Wer physischen Zugriff auf den Rechner hat, hat ohnehin alle Rechte (Festplatte ausbauen), dennoch:
  - Single-User-Mode abschalten
  - Open-Firmware-Passwort verwenden

Macs sicher(er) konfigurieren

- Eingabe des Admin-Passworts gibt einer Anwendung sämtliche Rechte auf dem Computer
- Im Zweifel nicht eingeben



Macs sicher(er) konfigurieren

- Dateizugriffsrechte
  - Mac OS X hat im Lieferzustand Dateizugriffsrechte, die das Ausspähen von Daten ermöglichen können
  - Softwareinstallationen erfolgen manchmal mit unsicheren Dateizugriffsrechten (für alle schreibbare Programme und Verzeichnisse)

Exkurs: Dateizugriffsrechte

- “Everything is a file in Unix” (Dateien, Verzeichnisse, usw.)
- Jede Datei ist einem Besitzer und einer Gruppe zugeordnet
- Zugriffsrechte
  - Lesen
  - Schreiben
  - Ausführen
- Rechte können für Besitzer, Gruppe und “Andere” getrennt festgelegt werden

Macs sicher(er) konfigurieren

- Dateizugriffsrechte Homeverzeichnis
  - alle Benutzer können lesen
  - Lese- und/oder Ausführrechte entfernen
  - Vorsicht! Ausführrechte sind für Public- und Sites-Verzeichnisse nötig
- Global schreibbare Dateien und Verzeichnisse
  - Ursache: Softwareinstallationen, Benutzerfehler
  - Vorsicht! Manche Software braucht diese Zugriffsrechte!

Keychain

- Verschlüsselte Speicherung von Passwörtern und beliebigen Notizen, Zertifikatsverwaltung
- Keychains sind durch Passwort geschützt
- Zugriffserlaubnis pro Anwendung
  - Warn-Dialoge durchlesen, ggf. ablehnen
- Keychain sicherer machen:
  - anderes Passwort wählen
  - automatisches Locking aktivieren
  - ggf. unterschiedliche Keychains nutzen

Schutz vor Angreifern mit physischem Zugriff

Angriff mit physischem Zugriff

- Einziger “echter” Schutz: Verschlüsselung der Daten auf der Festplatte
  - File Vault oder verschlüsselte Disk Images
  - ggf. Einsatz von PGP/GPG o.ä.
- Schutz des Open-Firmware-Passworts bei öffentlich zugänglichen Arbeitsplätzen durch Verhinderung des Zugriffs auf RAM-Steckplätze
- Kensington-Schlösser bieten nur sehr primitiven Schutz vor Wegtragen!

File Vault

- Verschlüsselung des kompletten Homeverzeichnisses
- Einrichten braucht Zeit und Plattenplatz
- Verringert die Zugriffsgeschwindigkeiten
- Abhilfe: Nur die wichtigsten Daten im Home, Rest ausserhalb und mit Links an die erwarteten Stellen im Home einbinden

Verschlüsselte Disk Images

- Umgekehrte Vorgehensweise: Nur wichtige Daten in verschlüsselten Disk Images, diese mit Links an den erwarteten Stellen im Home einbinden
- Homeverzeichnis an sich bleibt unverschlüsselt
- Mounten der Disk Images ist nicht so komfortabel

Sicherheit im Internet
Netzwerksicherheit

Sicherheit im Internet

- Schutz vor Einbruch ins System
- Schutz vor Datensammlern
- Schutz zu übertragender Daten
  - Emails
  - Online-Banking, Einkaufen, ...
  - Chat, Telefonie, ...

Einbruch ins System

- Einbruchsmöglichkeiten
  - Login mit ausspioniertem Benutzernamen und Passwort (Voraussetzung: Remote-Login möglich)
  - Sicherheitslücken in laufenden Diensten (z.B. durch Buffer Overflows)
  - “Ausbruch” – bösartige Software auf dem Rechner öffnet Zugriff von außen

Abhilfe Einbruch

- Dienste nur aktivieren wenn unbedingt nötig
- Nur sichere Dienste verwenden
- Remote-Login: gute Passwörter usw.
- Softwareupdates einspielen
- Nur vertrauenswürdige Software verwenden
- Firewall – am besten auf getrenntem Rechner (z.B. AirPort Basisstation, DSL-Router o.ä.)

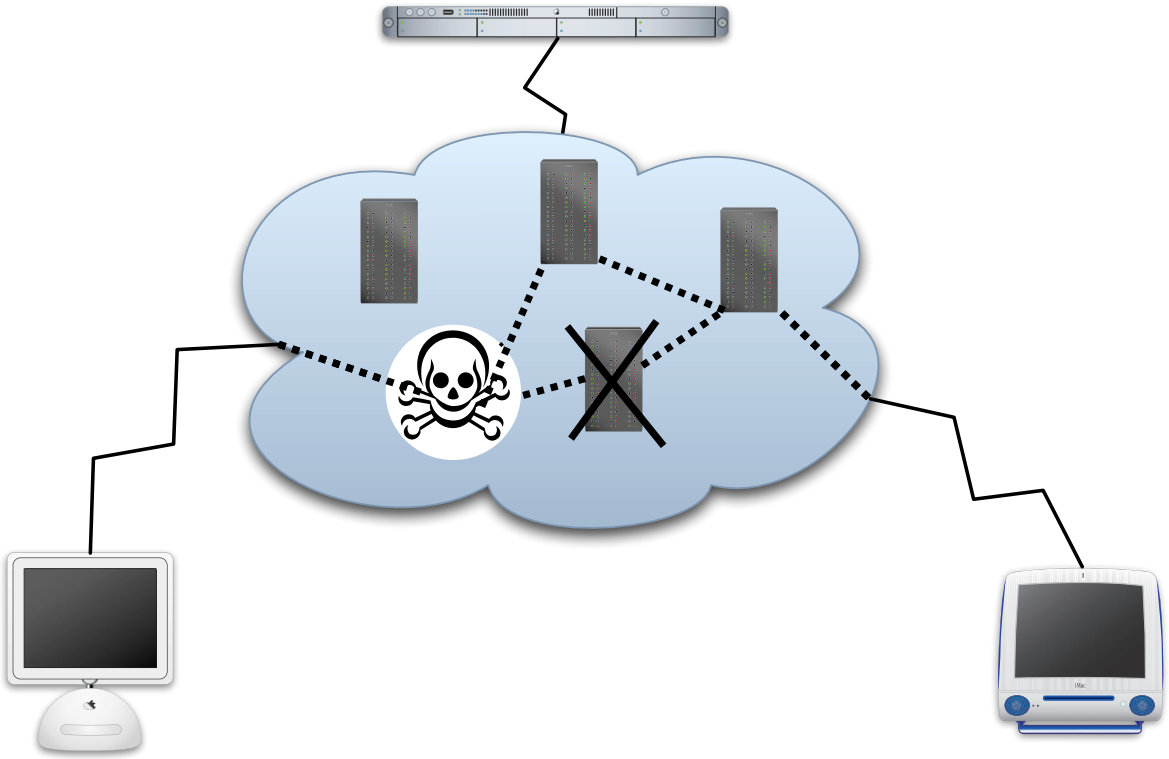
Lokale Firewalls

- Sharing Preferences
  - Firewall aktivieren
  - Internet Sharing ausschalten
- Filtern nach Anwendungen: Little Snitch
- Firewall kann auch von Hand (ipfw) oder mit Tools von Drittherstellern konfiguriert werden

Abhilfe Datensammler

- Nicht benötigte Cookies löschen / keine Cookies setzen lassen
- Persönliche Daten sparsam herausgeben
- In Emails Bilder nicht automatisch laden
- “Phone Home” verhindern
  - vertrauenswürdige Anwendungen
  - Einstellungsmöglichkeiten nutzen
  - ggf. Little Snitch o.ä. einsetzen

Aufbau des Internet



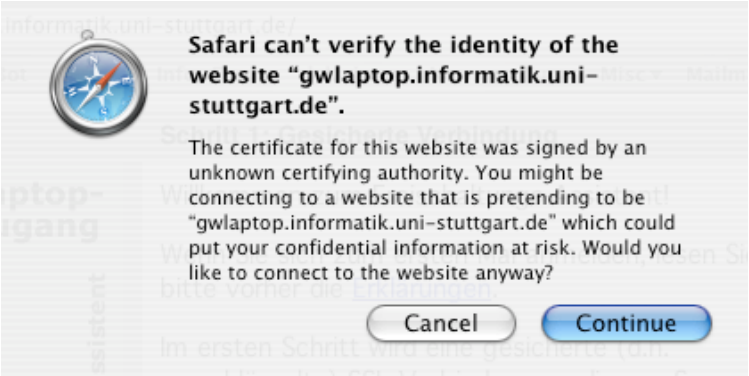
Schutz übertragener Daten

- Jeder Rechner, den die Datenpakete passieren, kann die übertragenen Daten (inkl. Passwörter) beliebig lesen, sammeln, analysieren, verändern
  - Admins
  - Hacker
  - Mitbenutzer (unverschlüsseltes WLAN, Hubs)
  - Big Brother :-)
- Abhilfe: Verschlüsselung + Authentifizierung

Sicheres Surfen (1)

- HTTPS ist die sichere Variante von HTTP
  - Einsatz z.B. bei Banken, Online-Shopping, ...
  - Verschlüsselte Verbindung zum Webserver
  - Authentifizierung mit Zertifikaten
- Zertifikatsvergabe durch Organisationen (CAs), OS X hat Liste vertrauenswürdiger CAs
- Zertifikate, die nicht von einer dieser CAs unterschrieben sind, verursachen eine Fehlermeldung

Sicheres Surfen (2)



- Leider bietet Safari keine Möglichkeit, die Zertifikatsinformationen anzuzeigen
- Im Zweifelsfall ablehnen!
- Vertrauenswürdige Zertifikate können ggf. in `/System/Library/Keychains/X509Anchors.keychain` importiert werden

Email – Gefahren

- Emails und Passwörter für Email-Postfächer werden im Klartext verschickt
  - Admins, Hacker, Mitbenutzer, Big Brother usw. können alles mitlesen, verändern und löschen
- Absenderadressen sind fälschbar
  - Social Engineering, Phishing
- Unsichere Mailprogramme und Anwenderfehler sind weitere Gefahren

Sichere Email (1)

- Verhinderung unberechtigten Zugriffs auf Email-Postfächer
  - Verwendung sicherer Zugriffsprotokolle (POP3/SSL statt POP3, IMAP/SSL statt IMAP)
  - Wird von Mail unterstützt, aber leider nur von wenigen Anbietern
  - Notlösung: Passwörter häufig ändern, nicht in unsicheren Netzen verwenden

Sichere Email (2)

- Verhinderung des Mitlesens von Email
  - Verschlüsselung
- Authentifizierung von Absendern
  - Elektronische Unterschrift
- Lösungen
  - S/MIME
  - Pretty Good Privacy (PGP) bzw. GPG

S/MIME

- Keine zusätzliche Software nötig
- Zertifikat erforderlich (wie bei HTTPS)
  - erhältlich bei einer CA (Certificate Authority)
  - z.B. Verisign, Web.de, TC Trust Center
- OS X vertraut standardmäßig auch weniger sicheren Zertifikatsklassen => “signed” im Mailprogramm bedeutet relativ wenig

PGP/GPG (1)

- Vertrauen entsteht durch ein “Web of Trust” gegenseitiger Unterschriften
- Schlüsselpaar bestehend aus geheimem Teil (Private Key) und öffentlichem Teil (Public Key)
- Unterschreiben mit privatem Schlüssel
- Verschlüsseln mit öffentlichem Schlüssel des Empfängers
- Komfortable Integration in Mail durch GPGMail oder PGP Desktop

PGP/GPG (2)

- GPG (GNU Privacy Guard) ist freie Software
- Schlüsselgenerierung erfolgt auf dem eigenen, vertrauenswürdigen Rechner
- Privater Schlüssel bleibt immer beim Besitzer
- Kann auch zum Verschlüsseln beliebiger Dateien oder für verschlüsseltes Instant Messaging (z.B. mit Fire) verwendet werden
- Mehr Informationen? inf.misc Vortrag am 26. Januar um 14 Uhr in V38.01

Datensammler

- Unnötige Cookies gelegentlich löschen
- Automatisches Laden von Bildern in Mail abschalten (wegen Spammern, neugierigen Absendern)
- Konfigurationsoptionen nutzen (z.B. im RealPlayer)
- “Nach Hause telefonieren” von Anwendungen kann z.B. durch Verwendung von Little Snitch unterbunden werden

Wireless

- AirPort / WLAN
  - Stärkstmögliche Verschlüsselung aktivieren
    - Schlüssel regelmässig ändern
  - Reichweite verringern
- Bluetooth
  - Sichtbarkeit abschalten
  - Verschlüsselung aktivieren
  - Datentransfers nicht automatisch akzeptieren

Viren

Viren

- Es sind derzeit keine echten Mac OS X Viren in freier Wildbahn bekannt
- Antivirenprogramme verursachen für viele Anwender unter Mac OS X mehr Ärger, als dass sie nutzen

Weiterführende Informationen

- Securing Mac OS X
  http://www.csse.uwa.edu.au/~pd
- Apple Mac OS X v10.3.x Security Configuration Guide
  http://www.nsa.gov/snac/os/applemac/osx_client_final_v_1_1.pdf
- Securing Mac OS X
  http://www.corsaire.com/white-papers/
- GPG Mail
  http://www.sente.ch/software