Sicherer am Mac

Warum OS X sicherer als Windows ist

A. Stile ©2011

letztes Update: 24.08.11

Sicherheit ohne Aufwand

- OS X bietet ein mehrschichtiges System von Mechanismen zum Schutz vor gefährlicher Malware, ohne dass man etwas dazu tun muss:
  - Sandboxing: Diese Technologie legt fest, welche Aktionen die Programme auf dem Mac ausführen, auf welche Dateien sie zugreifen und welche anderen Programme sie öffnen dürfen. Dies hindert somit Hackern das System mit Schadprogrammen zu infizieren.
  - Quarantäne: OS X kann heruntergeladene Dateien unter Quarantäne stellen. Sie sorgt dafür, dass beim Aufruf solcher Dateien geprüft wird, ob sie ausführbare Programme enthalten. Tricks, die ein heruntergeladenes Programm zum Beispiel als Musikdatei tarnen, fliegen nun auf, weil das Betriebssytem den Benutzer darüber informiert, dass es sich tatsächlich um ein ausführbares Programm handelt.
  - Antiphishing: Safari erkennt betrügerische Webseiten und schützt den Benutzer. Wenn eine verdächtige Webseite besucht wird, wird diese deaktiviert und Safari weist einem darauf hin, dass die Seite suspekt ist.
  - Library Randomisation: Diese willkürliche Nutzung von Bibliotheken verhindert, dass bösartige Befehle ihre Ziele finden, sowie die Funktion zur Verhinderung der Code-ausführung ("Execute Disable"), die den Arbeitsspeicher des Mac vor Attacken schützt.
  - Address-Space Layout Randomisation: Speicherschutz vor Angriffen, sowohl für 32- als auch 64-Bit Programmen.
- OS X überprüft beim Aufstarten alle System-Erweiterungen und Programme nach Kompatibilitätsproblemen. Werden solche gefunden, legt das Betriebssystem sie zur Seite und informiert den Benutzer darüber.

Scheinargument „Marktanteil“ (1)

- Apple ist längst nicht mehr der Exot, für den es sich nicht lohnen würde Schadprogramme zu schreiben!

- Wenn der Verbreitungsgrad eines Systems eine Rolle für die Sicherheit spielen würde, dann müsste der Apache Webserver deutlich mehr Sicherheitsprobleme haben als der Microsoft Internet Information Server - was statistisch widerlegt ist! - Ebenso müsste es für das iPhone schon massenweise Schadprogramme geben.

- Bis dato konnten keine sich global ausbreitende Viren oder Würmer für OS X nachgewiesen werden. Intego, ein Antiviren-Hersteller, meldete 2009 für OS X nur 2 Malware, die der Nutzer durch illegale Programme über Tauschbörsen beziehen und selbst installieren musste, damit sie Schaden anrichten konnten. Bei allen anderen Meldungen handelte es sich um Prototypen und Machbarkeitsstudien („Proof Of Concepts“).

Scheinargument „Marktanteil“ (2)

- Windows zeichnet sich durch die schlichte Offenheit an Schnittstellen für Dritte aus (Programmiersprachen, einfache Zugriffe auf die Systemebenen, usw.). Das half der Verbreitung von Windows. Es half aber auch, Windows so anfällig zu machen wie kein anderes System. Wer alle Türen offen hält, bekommt eben auch ungebetene Gäste zu Besuch.

- Je leichter ein System angreifbar ist, desto öfter ist es Ziel von Attacken. Ein unsicheres Betriebssystem wird als leichtes Opfer immer einem sichereren vorgezogen!

Von jedem UNIX das Beste

- In OS X findet man viele gute Konzepte wieder, die es in irgendeinem anderen UNIX gibt!
- OS X hat eine quell-offene Grundlage, die „Darwin“ heißt und verwendet einige Sicherheitstechniken, die BSD (Berkeley Software Distribution) auszeichnen:
  - Prozess-Trennung: In UNIX sind sowohl Prozesse als auch Dateien unterschiedlicher Nutzer sauber und sicher voneinander getrennt. Insbesondere laufen alle Prozesse aus Prinzip mit möglichst minimalen Berechtigungen.
  - Zugriffsbeschränkung auf Datei-Ebene: UNIX verwendet mindestens Zugriffsrechte auf Datei-Ebene. Kontrollsteuerungen wie ACLs werden bei UNIX zusätzlich zur Verfeinerung der Zugriffsrechte eingesetzt.

Mehrbenutzerbetrieb & Netzwerk

- UNIX ist für den Betrieb mit vielen gleichzeitigen Benutzern und als Netzwerk entworfen worden.
- Erst mit NT von 1998 wurde Mehrbenutzerbetrieb auf Windows möglich, mit ein paar Sicherheits-Einschränkungen:
  - Administrator ungleich System: Unter OS X ist ein Administrator nicht gleichmächtig mit dem System. Auf Systemverzeichnisse hat nur das System („root“) Schreibrechte! Bei Windows hingegen hat der Administrator vollumfängliche Rechte auf das System.
  - Passwortschutz: Wenn man unter Windows einen Benutzer anlegt, dann gibt es kein Eingabefeld für die Festlegung eines Passwortes. Jeder Benutzer ist erst mal ohne Passwort (trotz Benutzerkontensteuerung).
  - Access Control List (ACL): Auf beiden Systemen gibt es ACLs, die u.a. Ausführungsrechte für Benutzer regeln. Allerdings sind ACLs wegen ihrer Komplexität für Fehl-konfigurationen anfällig. Um abwärts-kompatibel zu sein, erlaubt Windows diese zu ignorieren.

Windows Broken By Design

- Windows ist "broken by design", weil es folgende Architekturfehler beinhaltet:
  - Monolithische Architektur: Windows hat zuviele Funktionen in den Betriebssystem-Kern integriert, die in eine höhere Schicht gehören (beispielsweise Internet Explorer und Grafik-Routinen). Diese unsaubere Trennung verhilft Schadprogrammen leichter zu System-rechten. Und ein Fehler in einem Programm wirkt sich leichter auf andere Programme und das System aus.
  - Remote Procedure Calls (RPCs): Windows ermöglicht Funktionsaufrufe über das Netzwerk. Dies kann aber zu unkontrollierten Aufrufen missbraucht werden. Weil Windows und seine Programme jedoch auf RPCs angewiesen sind, kann man sie nicht abschalten. Dieses Problem versucht man zu lösen, indem man zusätzliche Firewall-Regeln dazwischen schaltet, die schwer zu verwalten sind.
  - Unkontrollierte Anwendungs-Nachrichten: Mit dem „Windows Messaging System“ besteht die Möglichkeit, dass sich Programme ohne Authentifizierung gegenseitige Anweisungen zuschicken können. Der Absender bleibt verborgen.

Mit dem Internet Explorer surfen (1)

- Wer mit dem Internet Explorer (IE) von Microsoft surft, der muss sich zunächst mit über 30 Sicherheitseinstellungen auseinandersetzen (nota bene: der IE-Sicherheitsleitfaden umfasst mehr als 60 Seiten). Der Grossteil ist alles andere als selbst erklärend. Safari von Apple bringt überraschenderweise nur 6 sicherheitsrelevante Einstellungen mit. Schaut man nun genauer auf die IE-Einstellungen, so stellt man fest, dass sehr viele Einstellungen eigentlich vom System übernommen werden sollten und nicht in die Hände des Benutzers gehören. Es wird jedoch bei vielen Einstellungen empfohlen auf "Eingabeaufforderung" zu setzen, d.h. der Anwender soll gefragt werden und selber entscheiden. Dies kann nicht gut funktionieren und zeugt von einer schlechten Sicherheitsarchitektur! Beispiele dazu:
  - Sicherheitszonen: Als privaten Benutzer sollte man nur die Zone für "Internet" einstellen. Die Sicherheitseinstellungen für die anderen drei Zonen kommen normalerweise nicht zur Anwendung. Hier muss man seriöse und unseriöse Internetseiten zuvor in eigene Listen des IEs eintragen. Da man unseriöse Seiten erst einmal kennen muss, um sie sperren zu lassen, ist die Verwendung der Listen auch kaum praktikabel. Eine aufwendige Arbeit, die nur Netz-Administratoren zumutbar ist!

Mit dem Internet Explorer surfen (2)

- Benutzerauthentifizierung: Es wird empfohlen die entsprechende Option auf "Nach Benutzername und Kennwort fragen" zu setzen. Denn wenn man sich auf einer Internetseite anmeldet, sollten Name und Passwort prinzipiell selbst eingetippt werden. Dies darum weil solche Anmeldedaten vom IE nicht verschlüsselt abgelegt und somit leichter ausgespäht werden können. Safari hingegen legt solche Anmeldedaten verschlüsselt in die Schlüsselbundverwaltung des Betriebssystems ab. Hier kann man nur per Admin-Passwort zugreifen. Ausserdem stehen die Anmeldedaten jedem Browser zur Verfügung.
- Dömanengrenzen: Der Punkt "Auf Datenquellen über Domänengrenzen hinweg zugreifen" kann eigentlich auf "Aktivieren" gesetzt werden. Es ist nämlich ganz normal, dass im Internet auf Daten von anderen Webseiten zugegriffen wird. Warum dies also als Einstellungsoption anbieten?

OS X Sicherheitsgaranten (1)

- Vorneweg: Kein System ist zu 100% immun gegen Bedrohungen! Das grösste Risiko bildet der Benutzer selbst durch fahrlässiges Handeln:
  - Verwendung von unsicheren Passwörtern oder unbedachte Weitergabe bei Phishing-Emails
  - Inaktive Bildschirmsperre beim Verlassen des Arbeitsplatzes
  - keine Software-Updates einspielen
  - unverschlüsseltes WLAN

- Die Installation von Programmen erfordert unter OS X Administrations-rechte (keine Systemrechte). Man kann damit keine Systemdateien ändern. Auf Windows kann jedoch jedes Installations-Programm beliebig tief im Betriebssystem Dateien ablegen, durch den Benutzer unkontrolliert!

- Eine ausführbare Datei, die vom Internet runtergeladen wurde, wird beim ersten Aufruf dem Benutzer zur Identifizierung vorgelegt. Damit wird verhindert, dass eine solche Datei unbemerkt im Hintergrund aufgerufen wird.

OS X Sicherheitsgaranten (2)

- OS X hat zwei Firewalls, die auf unterschiedlichen Protokoll-Ebenen arbeiten. Beide können gleichzeitig betrieben werden und ermöglichen zusammen eine umfassende Regelung:
  - System-Firewall: Diese Firewall schirmt die interne Dienste gegenüber dem Netzwerk und Internet ab. Diese Dienste (z.B. Internet-Sharing) müssen unter der System-Einstellung „Freigabe“ explizit freigegeben werden und können dann mit der Anwendungs-Firewall auf Applikations-Ebene nochmals justiert werden.
  - Anwendungs-Firewall: Diese muss in der System-Einstellung „Sicherheit“ aktiviert werden. Sie soll dem normalen Benutzer, dem Port-Nummern nichts sagen, eine Möglichkeit geben, überhaupt Einstellungen machen und verstehen zu können. Eine Filterung von Ports würde auch nicht immer nützen, da einige Programme ihre Ports wechseln.
- OS X stellt einen „Schlüsselbund“ zur Verfügung, mit dem sowohl Zertifikate als auch Kennwörter für Websites, Server, Netzwerke, Programme, Email-Accounts, Notizen, Volumes und verschlüsselte Ordner verwaltet werden können.

OS X Sicherheitsgaranten (3)

- Im Falle eines Stromausfalls startet OS X eine laufende Installation erneut, wenn der Strom wieder da ist. Dabei gehen keine Daten verloren!

- Die im Betriebssystem integrierte Backup-Funktion „Time Machine“ reduziert das Risiko von Datenverlust auf äusserst komfortable und sichere Weise, und sie ist kostenlos!

- Um vertrauliche Dateien sicher abzulegen, bietet OS X die Möglichkeit einer verschlüsselten Disk- Image. Es ist empfehlenswert das dazugehörige Passwort nicht in den Schlüsselbund abzulegen.

- Mit der Kindersicherung können Eltern Regeln für ihre Kinder festlegen - beispielsweise wie lange sie den Mac benutzen, welche Webseiten sie besuchen und mit welchen Personen sie chatten dürfen.

- Unter dem Bereich für Datenschutz kann das Sammeln von Ortungsdienste, Diagnose- und Nutzungsdaten kontrolliert werden. Man kann auch festlegen, welche Programme auf Ortsdaten zugreifen dürfen. Wenn eine Applikation eine solche Position abfrägt, dann erscheint gleich ein entsprechendes Symbol in der Menüleiste.

OS X Sicherheitsgaranten (4)

- OS X ermöglicht zusätzlich folgende Sicherheits-Einstellungen:
  - Anmeldung: Die automatische Anmeldung beim System-Start kann über die System-Einstellungen kontrolliert werden. Ebenso ist es möglich zu definieren, ob nach dem Beenden des Ruhezustandes eine Authentifizierung erforderlich ist. Ausserdem müssen Änderungen an System-Einstellungen immer authentifiziert werden.
  - Virtueller Speicher: Informationen, die durch den virtuellen Speicher vom Arbeitsspeicher auf die Festplatte geschrieben wurden, können über eine System-Einstellung verschlüsselt werden.
  - Plattenverschlüsselung: Mit „FileVault“ kann der Benutzerordner geschützt werden, indem der Inhalt verschlüsselt wird. Die Dateien werden während des Betriebs automatisch verschlüsselt und entschlüsselt. Die Verschlüsselung wird über 2 Passwörter doppelt geschützt.
  - Zugriff auf gesicherte Netzwerke mit der integrierten VPN-Unterstützung
  - Verschlüsselungsstandards WEP, WPA und WPA2 für Internetzugriff
  - 802.1x-Standard zur Authentifizierung in Rechnernetzen
  - sicherer Zugriff zwischen Computern auf Befehlszeilen-Ebene mithilfe von OpenSSH
  - Überprüfung der Gültigkeit von Zertifikaten mit OCSP-Protokoll und über CRL-Liste
  - sichere Übertragung vertraulicher Informationen über das Internet mit SSL, z.B. Benutzer-informationen oder Kreditkartennummer (die Softwareaktualisierung verwendet ebenfalls SSL um eine sichere Übertragung der Daten zu gewährleisten)

OS X Sicherheitsgaranten (5)

- Wenn Dateien gelöscht werden, steht der Speicherplatz, den die Dateien belegten, wieder zur Verfügung. Solange dieser Bereich der Festplatte jedoch nicht mit neuen Daten überschrieben wird, lassen sich die gelöschten Informationen mithilfe von Programmen zum Lesen von Festplatten wiederherstellen. Wenn die Dateien, die in den Papierkorb gelegt werden, vertrauliche Daten enthalten, kann man diese Informationen mit dem Befehl "Papierkorb sicher entleeren" überschreiben, sodass sie nicht wiederhergestellt werden können.
- Das Inhaltsverzeichnis eines Volumes kann theoretisch durch einen Systemabsturz so beschädigt werden, dass das System Dateien nicht mehr findet. Deshalb verwendet OS X standardmäßig das „Journaling“, welches für alle Veränderungen am Inhalt eines Volumes protokolliert und bei einem Systemabsturz aus diesen Informationen den letzten funktionstüchtigen Zustand wiederherstellen kann.
- Hat man sein Admin-Passwort vergessen und kann sich nicht mehr am Rechner anmelden, lässt sich mit Hilfe der System-DVD oder über bestimmte UNIX-Befehle ein neues einrichten, ohne das alte angeben zu müssen. Will man dies unterbinden, so kann ein Firmware-Passwort angelegt oder die Plattenverschlüsselung FileVault aktiviert werden.

Quellen & weiterführende Dokumentation

- Apple: „Mac OS X Security Configuration Guides“
- Apple: „Firmware-Kennwortschutz in Mac OS X einrichten“
- Charles S Edge Jr.: „Enterprise Mac Security“
- National Security Agency: „Hardening Tips for MAC OS X 10.6 Snow Leopard“
- MacMark: „Sicherheit, Viren, Würmer und Trojaner“
- MacMacken: „10 x Mac OS X Sicherheit für Anfänger“
- MacTechNews: „Sicherheit beim Mac“
- MacMagazin: „Die Firewall von Snow Leopard“
- MacWelt: „Mac OS X Snow Leopard sichern“
- Steffen Hellmuth: „Der Mac im Unternehmen“