Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: PRIVATE IT

Sichere Nutzung von Macs unter Apple OS X Mountain Lion

Ausgangslage

Viele nützliche und wichtige Dienstleistungen, wie Online-Banking, E-Commerce oder E-Government, werden heute über das Internet angeboten und genutzt. Auch in Zukunft wird sich die Anzahl der Online-Services noch weiter erhöhen. Hinzu kommt der verstärkte Einsatz mobiler Endgeräte, wie Smartphones und Tablets, mit denen diese Dienste auch unterwegs genutzt werden können. Personal Computer (PCs) mit verschiedenen Betriebssystemen, wie Apple Mac OS X, Microsoft Windows oder einer Linux-Variante, spielen derzeit jedoch noch die wichtigste Rolle.

Ziel

Die vorliegende BSI-Veröffentlichung bietet Hilfestellungen für die Konfiguration eines Macs unter dem Gesichtspunkt der Sicherheit. Sinnvoll ist dabei die Betrachtung des Lebenszyklus eines Rechners:

- Anschaffung des Systems
- Installation und erste Inbetriebnahme
- Regelmäßiger Betrieb
- Entsorgung des Systems

Mit wenigen Maßnahmen können Macs unter dem aktuellen Betriebssystem OS X Mountain Lion so abgesichert werden, dass eine weitgehend sichere Nutzung von Dienstleistungen über das Internet möglich ist.

Anschaffung des Systems

Bereits bei der Anschaffung des Systems gibt es wichtige Aspekte, die Sie für einen späteren sicheren Betrieb Ihres Macs beachten sollten.

Hardware und Betriebssystem

Achten Sie beim Kauf eines Macs auf möglichst aktuelle Hardware mit der jeweils neuesten Version des Betriebssystems, derzeit also OS X Mountain Lion. Bei einem Neukauf eines Macs ist dieses üblicherweise bereits vorinstalliert. Beim Kauf eines gebrauchten Macs achten Sie darauf, dass dieser von OS X Mountain Lion unterstützt wird. Welche Modelle hier infrage kommen, können Sie einer Übersichtstabelle[1] entnehmen, die Apple im Internet bereitstellt.

Falls der Mac nur über eine ältere Version des Betriebssystems (mindestens Mac OS X 10.6 „Snow Leopard“) verfügt, erwerben Sie über den im Betriebssystem integrierten Mac App Store eine Lizenz für OS X Mountain Lion.

Virenschutzprogramm

Die Installation eines separaten Virenschutzprogramms ist, basierend auf dem aktuellen Stand der Bedrohungslage durch Schadsoftware für Macs, unter OS X Mountain Lion nicht notwendig.

OS X Mountain Lion enthält einen einfachen integrierten Schutz gegen bekannte, Mac-spezifische Schadsoftware, der durch Apple in unregelmäßigen Abständen aktualisiert wird und standardmäßig bereits aktiviert ist. Sie können den Status dieser Funktion in den Systemeinstellungen unter dem Punkt *Sicherheit* | *Weitere Optionen...* überprüfen. Die Option *Liste für sichere Downloads automatisch aktualisieren* sollte aktiviert sein.

Zusätzlich enthält OS X Mountain Lion mit dem sogenannten „Gatekeeper“ eine Funktion, welche die Ausführung von Anwendungen kontrolliert. Standardmäßig erlaubt Gatekeeper nur die Ausführung von solchen Programmen, die entweder über den Mac App Store bezogen wurden oder die von Entwicklern stammen, welche von Apple verifiziert wurden. Das bedeutet keine Garantie dafür, dass diese Anwendungen in jedem Fall harmlos sind. Allerdings ist ihr Urheber identifizierbar und nachträglich manipulierte Programme können ebenfalls erkannt werden.

Es wird empfohlen, Gatekeeper in der Standardkonfiguration zu betreiben. Möchten Sie bewusst eine Anwendung aus einer verlässlichen Quelle starten, bei der Gatekeeper die Ausführung nicht zulässt, können Sie dies über *CTRL+Klick* bzw. *Rechtsklick* und *Öffnen* tun. Gatekeeper merkt sich die Anwendung anschließend als vertrauenswürdig. Dieses Verfahren ist beispielsweise bei manchen Programmen notwendig, die vor der Veröffentlichung von OS X Mountain Lion erstellt wurden. Auch bestimmte Anwendungen aus dem Open-Source-Bereich, wie etwa OpenOffice, sind unter Umständen noch nicht für den Einsatz mit Gatekeeper vorbereitet. Prüfen Sie daher stets die Quelle und bevorzugen Sie die jeweilige Hersteller-Webseite für den Download der Anwendung.

Backups

Um Sicherungskopien sowohl des Systems als auch Ihrer Daten zu erstellen, können Sie die in OS X Mountain Lion eingebaute Funktionalität „Time Machine"[2] verwenden. Der Kauf einer gesonderten Backup-Software ist für OS X Mountain Lion im privaten Umfeld üblicherweise nicht erforderlich.

Beschaffen Sie beim Kauf des Macs für die Erstellung von Backups mittels Time Machine eine zusätzliche externe Festplatte mit ausreichend großem Speicherplatz (Richtwert: mindestens die doppelte Größe der internen Festplatte).

Anwendungen

Zur Darstellung von PDF-Dateien sowie vieler anderer Dokumenten- und Medienformate verfügt OS X

1 http://www.apple.com/de/osx/specs/
2 http://www.apple.com/de/macosx/apps/#timemachine

Mountain Lion bereits über eingebaute Funktionalitäten, wie die Anwendung „Vorschau“ oder die Funktion „QuickLook“. Prüfen Sie im Einzelfall, ob Sie eine zusätzliche Anwendung zur Darstellung ihrer Dateien benötigen oder ob die bereits vorhandenen Möglichkeiten ausreichend sind. Je weniger zusätzliche Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche des Systems.

Bei allen zusätzlichen Anwendungsprogrammen, die Sie etwa zur Bearbeitung von Fotos oder zum Komponieren und Abspielen von Musik nutzen, sollten Sie darauf achten, dass die Produkte mit einer Funktion zur automatischen Aktualisierung ausgestattet sind. In der Regel lässt sich dies unter dem Menüpunkt *Einstellungen* in der jeweiligen Software überprüfen und konfigurieren. Updates sollten idealerweise ohne Ihr Zutun automatisch im Hintergrund installiert werden. Verbreiteter sind Aktualisierungsfunktionen, die Sie bei verfügbaren Updates benachrichtigen. Die Installation sollten Sie stets zeitnah durchführen. Für die im Folgenden beispielhaft genannten Produkte aus dem Bereich Bürosoftware gibt es solche Aktualisierungsmechanismen, die standardmäßig nach der Installation bereits aktiviert sind:

- kostenlos: LibreOffice (http://www.libreoffice.org)
- kostenpflichtig: Apple iWork (http://www.apple.com/de/iwork/)
- kostenpflichtig: Microsoft Office für Mac (http://www.microsoft.com/germany/mac)

Installation und erste Inbetriebnahme

Einen wichtigen Grundstein für die Systemsicherheit Ihres Macs können Sie bereits bei der Installation und ersten Inbetriebnahme des Rechners legen.

Installation aller vorhandenen Sicherheitsaktualisierungen

Üblicherweise ist OS X Mountain Lion im Auslieferungszustand eines neu erworbenen Macs bereits vorinstalliert. Ist dies – etwa bei einem Gebrauchtgerät – nicht der Fall, so führen Sie zunächst eine vollständige Neuinstallation von OS X Mountain Lion durch.

Um das Sicherheitsniveau des Macs zu halten, ist es erforderlich, stets alle Sicherheitsaktualisierungen nach deren Erscheinen zu installieren. Die automatische Softwareaktualisierung von OS X Mountain Lion ist in den Mac App Store integriert und im Auslieferungszustand bereits aktiviert. Sie sucht täglich nach Aktualisierungen für das Betriebssystem, alle Anwendungen von Apple sowie alle Drittanbieter-Anwendungen, die über den App Store auf dem Mac installiert wurden.

Die automatische Softwareaktualisierung benachrichtigt Sie, wenn Aktualisierungen verfügbar sind, und bietet sie zur Installation an. Führen Sie die Installation zeitnah durch.

Aktivieren Sie die Option *Systemdateien und Sicherheits-Updates installieren* in den *Systemeinstellungen* unter dem Punkt *Softwareaktualisierung*, um sicherheitsrelevante Aktualisierungen ohne Ihr Zutun installieren zu lassen.

Bei der ersten Inbetriebnahme sollten Sie alle zu diesem Zeitpunkt von Apple über die automatische Softwareaktualisierung angebotenen Software-Aktualisierungen unmittelbar herunterladen und installieren.

Benutzerkonten und Inhaltefilter

Das bei der Erstkonfiguration von OS X Mountain Lion angelegte Benutzerkonto (von Apple „Computer-Account“ genannt) ist ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Achten Sie darauf, dass nur solche Anwender administrative Aufgaben auf dem System wahrnehmen dürfen, die diese Funktionalität auch benötigen und beherrschen. Legen Sie für die tägliche Verwendung des Macs auf jeden Fall zusätzlich ein Standard-Benutzerkonto an. Sollte der Mac von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto anlegen.

Verwenden Sie neben dem Standard-Benutzerkonto, welches Sie für die tägliche Arbeit verwenden, ein zu-

sätzliches Benutzerkonto, um transaktionsbezogene Aktivitäten wie Online-Banking durchzuführen oder um kritische Daten online zu versenden.

Für einfache Benutzerkonten erlaubt OS X Mountain Lion die Aktivierung der Inhaltefilter-Funktion „Kindersicherung". Diese kann dazu genutzt werden, beispielsweise den Zugriff auf Anwendungen und Webseiten einzuschränken oder Nutzungszeiten für das Benutzerkonto festzulegen.

Verschlüsselung der Festplatte

Falls es sich bei Ihrem Mac um ein Notebook handelt, das Sie auch unterwegs nutzen, sollten Sie unbedingt die Festplatte verschlüsseln, um Daten bei Verlust oder Diebstahl des Geräts zu schützen. Wenn Sie einen Desktop-Mac besitzen, ist abzuwägen, ob ein möglicher Leistungsverlust Ihres Systems aufgrund der Verschlüsselung in einem angemessenen Verhältnis zum Schutz Ihrer Daten vor dem Zugriff unbefugter Dritter steht.

Das Betriebssystem OS X Mountain Lion verfügt über die eingebaute Festplattenverschlüsselung „FileVault". Diese ist zur Verschlüsselung Ihrer Daten ausreichend, die Anschaffung einer separaten Verschlüsselungs-Software ist nicht erforderlich. Wenn Sie Ihre Daten mit FileVault verschlüsselt haben, können Sie darauf nur mittels Eingabe des Passworts Ihres Benutzerkontos zugreifen. Wählen Sie daher ein sicheres Passwort, welches Sie sich gut einprägen können. Schreiben Sie sich dieses Passwort zusätzlich auf und bewahren Sie den Zettel räumlich getrennt von Ihrem Mac an einem sicheren Ort auf. Hinweise zur Erstellung eines sicheren Passworts finden Sie bei „BSI für Bürger[3]".

Bei Verlust Ihres persönlichen Passworts können Sie nur noch auf Ihre Daten zugreifen, wenn Sie einen Wiederherstellungsschlüssel haben. Notieren Sie sich daher auch den von FileVault bei der Aktivierung angezeigten Wiederherstellungsschlüssel und bewahren Sie ihn ebenfalls an einem sicheren Ort auf. FileVault bietet zusätzlich an, den Wiederherstellungsschlüssel verschlüsselt bei Apple zu hinterlegen. Entscheiden Sie, ob dies – abhängig von der Art Ihrer Daten – für Sie akzeptabel ist. Vor allem im privaten Umfeld ist der Verlust Ihrer Daten durch einen verlorenen Wiederherstellungsschlüssel oftmals gravierender als der theoretische Fall, dass ein Unbefugter Zugriff auf den bei Apple hinterlegten Schlüssel erlangt. Im Zuge der Speicherung des Schlüssels auf den Apple-Servern müssen Sie Sicherheitsfragen und dazu passende Antworten festlegen. Wählen Sie hier Sicherheitsfragen mit entsprechenden Antworten, die ausschließlich Ihnen bekannt sind.

Die Verschlüsselung durch FileVault erfolgt im Hintergrund. Sie können also nach der Aktivierung von FileVault normal weiterarbeiten.

Personal Firewall

OS X Mountain Lion besitzt eine integrierte Personal Firewall, die im Auslieferungszustand jedoch nicht aktiviert ist. Starten Sie daher die Firewall in den Systemeinstellungen unter dem Punkt Sicherheit. Die Installation einer zusätzlichen Firewall ist nicht erforderlich, da das System durch die eingebaute Firewall hinreichend gegen Angriffe über das Netz geschützt wird und zudem standardmäßig von OS X Mountain Lion keine aktivierten Netzwerkdienste wie Dateifreigaben oder Fernwartungsmöglichkeiten bereitgestellt werden. Aktivieren Sie solche Dienste nur, wenn Sie diese tatsächlich benötigen und sicher konfigurieren können.

3 https://www.bsi-fuer-buerger.de/Passwoerter

Internet-Browser

Ihr Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten im Internet und stellt somit eins der beliebtesten Ziele für Cyber-Angriffe dar. Verwenden Sie daher möglichst einen Browser mit Sandbox-Technologie. Unter OS X Mountain Lion sind dies:

- Apple Safari (im Betriebssystem integriert)
- Google Chrome (https://www.google.com/chrome)

Vorteilhaft sind bei Google Chrome die kurzen Update-Intervalle sowie die Funktion zur automatischen Aktualisierung, die auch den integrierten Adobe Flash Player umfasst. Dadurch wird auch der Adobe Flash Player stets auf dem neuesten Stand gehalten. Wenn Sie ausschließlich Google Chrome verwenden, sollten Sie einen eventuell zusätzlich installierten Adobe Flash Player von Ihrem Mac entfernen.

Aktivieren Sie zudem den im Browser integrierten Filter zum Schutz vor Phishing und gefährlichen Websites. Bei Chrome finden Sie die entsprechende Option unter *Einstellungen* | *Erweiterte Einstellungen anzeigen...* | *Datenschutz*, bei Safari unter *Einstellungen* | *Sicherheit*.

Durch den Einsatz eines dieser Browser in Verbindung mit den anderen aufgeführten Maßnahmen können Sie das Risiko eines erfolgreichen IT-Angriffs stark reduzieren.

E-Mail

Für die weitgehend sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. Viele E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (HTTPS) zum Postfach zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren. Achten Sie darauf, dass die Verschlüsselung nicht nur für den Login-Vorgang, sondern während der gesamten Webmail-Nutzung aktiviert ist.

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen aktuellen und verbreiteten E-Mail-Client auswählen und diesen sicher konfigurieren, wie zum Beispiel:

- Apple Mail (im Betriebssystem integriert)
- Thunderbird (http://mozilla.org/de/thunderbird)

Hilfestellungen zur Konfiguration finden Sie auf den Webseiten der Anbieter:

- Apple Mail (http://www.apple.com/de/support/mail/)
- Thunderbird (http://support.mozillamessaging.com/de/home)

Auch bei der Nutzung von E-Mail-Programmen ist auf die Verwendung verschlüsselter Übertragungsprotokolle (POP3S, IMAPS, SMTPS) zu achten.

Verzichten Sie zudem auf die Darstellung und Erzeugung von E-Mails im HTML-Format. Die Anzeige von externen Inhalten – beispielsweise Bilder in HTML-E-Mails – sollten Sie deaktivieren, da diese ein zusätzliches Einfallstor zur Ausführung von Schadcode auf Ihrem Rechner darstellen.

Java-Laufzeitumgebung

Einige Anwendungen benötigen unter Umständen die Java-Laufzeitumgebung[4], die nicht in einer Standard-Installation von OS X Mountain Lion enthalten ist. Um die Angriffsfläche Ihres Systems zu reduzieren, sollten Sie Java nur dann installieren, wenn Ihre Anwendungsprogramme diese Laufzeitumgebung tatsächlich benötigen. Beim Start einer entsprechenden Anwendung weist OS X Mountain Lion auf das Fehlen von Java hin und bietet einen automatischen Download einer von Apple bereitgestellten Version von Java 6 an. Nach der Installation wird diese über die im Betriebssystem integrierte Software-

4 http://java.com/de

aktualisierung automatisch auf einem aktuellen Stand gehalten. Für ein manuell installiertes Java 7 der Firma Oracle können die Updates über die „Systemeinstellungen“ von OS X Mountain Lion konfiguriert werden.

Wenn Sie die Java-Laufzeitumgebung installieren müssen, sollten Sie trotzdem die Java-Unterstützung in den Einstellungen Ihres Webbrowsers abschalten. Sie können Java dann fallweise aktivieren, wenn es von einer vertrauenswürdigen Website benötigt wird. Alternativ können Sie das Dienstprogramm „Java-Einstellungen“ verwenden, um Java systemweit ein- und auszuschalten.

Erzeugung eines Datenträgers zur Systemreparatur

Macs mit OS X Mountain Lion werden ohne ein Installationsmedium für das Betriebssystem ausgeliefert. Mit der vorinstallierten Funktion OS X Wiederherstellung können Sie jedoch im Falle eines Defekts oder Absturzes Wartungsarbeiten oder eine Neuinstallation durchführen. Nähere Informationen zur Nutzung stellt Apple im Internet bereit[5].

Ebenfalls sind auf der oben genannten Apple-Webseite Informationen darüber zu finden, wie Sie für den Fall eines Festplattendefekts ein externes Wiederherstellungsmedium erstellen können.

Regelmäßiger Betrieb

Beachten Sie im täglichen Umgang mit Ihrem Mac die folgenden Ratschläge für einen sicheren Betrieb.

Sicherheitsaktualisierungen

Wenn Sie während der Installation eingestellt haben, dass sowohl das Betriebssystem als auch alle installierten Anwendungen automatische Updates durchführen, dann achten Sie auf entsprechende Hinweise im laufenden Betrieb.

In manchen Fällen werden Sie aufgefordert, die Installation von Updates zu bestätigen. Dies trifft etwa auf die integrierte Softwareaktualisierung von OS X Mountain Lion zu. Andere Softwareprodukte, wie beispielsweise der Browser Google Chrome, installieren die Updates selbsttätig und ohne eine weitere Nachfrage.

Backups

Bei einem defekten System ist die Gefahr eines unwiederbringlichen Verlusts Ihrer Daten sehr hoch. Regelmäßige Datensicherungen (Backups) auf externen Speichermedien, wie externen Festplatten, DVDs oder USB-Sticks, bieten Abhilfe.

Die integrierte Backup-Funktion „Time Machine“ von OS X Mountain Lion sichert das Betriebssystem und Ihre Daten kontinuierlich im Hintergrund auf eine für diesen Zweck eingerichtete externe Festplatte. Ist diese nicht dauerhaft mit dem Mac verbunden, sollten Sie mindestens einmal wöchentlich ein Backup Ihrer Daten anfertigen. Bedenken Sie stets, dass Sie im Ernstfall alle Daten verlieren können, die im Zeitraum nach der letzten Sicherung erstellt wurden.

Passwörter

Der Zugang zu Online-Services im Internet erfolgt häufig mittels der Abfrage eines Benutzernamens und Passworts. Wenn Sie verschiedene Online-Dienste nutzen, verwenden Sie dafür jeweils unterschiedliche, nicht erratbare Passwörter. Um solche komplexen Passwörter besser behalten zu können, sollten Sie Merkhilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes. Notieren Sie Ihre Passwörter zudem auf Zetteln und bewahren Sie diese räumlich getrennt von Ihrem Rechner an einem sicheren Ort auf. Hin-

5 http://www.apple.com/de/macosx/recovery/

weise zur Passwort-Sicherheit finden Sie bei „BSI für Bürger“.

Die empfohlenen Browser Safari und Chrome besitzen integrierte Funktionen, mit denen Sie Kennwörter für besuchte Webseiten verwalten können. Beide verwenden dazu den in OS X Mountain Lion integrierten Zertifikats- und Passwort-Manager „Schlüsselbund“, auf den auch über das Dienstprogramm „Schlüsselbundverwaltung“ zugegriffen werden kann. Hier werden unter anderem auch alle Kennwörter gespeichert, die Sie etwa für den Zugriff auf WLANs verwenden. Standardmäßig wird der Schlüsselbund mit dem Anmeldepasswort des Benutzers vor einer unbefugten Einsichtnahme oder Verwendung der Passwörter geschützt. Zur Erhöhung der Sicherheit kann über das Dienstprogramm auch ein separates Kennwort für den Anmelde-Schlüsselbund vergeben werden.

Notfallmaßnahmen

Auch Macs können von Abstürzen oder Fehlfunktionen betroffen sein, die Auswirkungen auf Ihren Datenbestand oder die Nutzbarkeit Ihrer Anwendungen haben können. Bereiten Sie sich auf solche potenziellen Notfälle vor und überlegen Sie sich Ihre Reaktion in folgenden Situationen:

- Der Rechner startet nicht mehr.
- Sie können keine Verbindung mehr mit dem Internet herstellen.
- Sie können sich nicht mehr in Ihrem E-Mail-Postfach anmelden.
- Sie bemerken eine nicht von Ihnen vorgenommene Überweisung von Ihrem Bankkonto.

Wenn Sie das Gefühl haben, dass Sie in diesen Situationen unsicher reagieren werden oder keine angemessenen Antworten finden, suchen Sie sich schon jetzt einen vertrauenswürdigen Ansprechpartner, der Sie bei der Bewältigung unterstützen kann. Hierbei können Sie auch auf Angebote von Händlern oder Apple selbst zurückgreifen.

Entsorgung

Wenn Sie Ihren Mac eines Tages entsorgen möchten, dann sollten Sie sicherstellen, dass alle Daten auf der Festplatte vernichtet sind. Ein einfaches Löschen von Daten durch das Verschieben in den „Papierkorb“ ist hierfür nicht ausreichend.

Zur sicheren Löschung der Daten sollten Sie den Mac über die Funktion „OS X Wiederherstellung“ oder von einem externen Installationsmedium für OS X Mountain Lion starten und die Festplatte über das Festplatten-Dienstprogramm sicher löschen. Wählen Sie dazu Ihre Festplatte aus und bewegen Sie unter *Löschen* in den *Sicherheitsoptionen* den entsprechenden Regler nach rechts, um ein sicheres Löschen durchzuführen. Das einmalige Überschreiben aller Daten ist üblicherweise ausreichend. Mehrfaches Überschreiben kann die Sicherheit zusätzlich erhöhen, erfordert aber einen entsprechend größeren Zeitaufwand.

Um Ihre Festplatte alternativ unbrauchbar zu machen, können Sie diese ausbauen und physisch zerstören. Ein Verkauf einer gebrauchten Festplatte lohnt sich in den meisten Fällen nicht, wenn man den möglichen Erlös ins Verhältnis zum Wert Ihrer Daten setzt.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen IT-Themen. Kommentare und Hinweise können von Lesern an mail@bsi-fuer-buerger.de gesendet werden.