Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT IM UNTERNEHMEN

Sichere Nutzung von PCs unter Ubuntu

Empfehlungen für kleine Unternehmen und Selbstständige

1 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 Microsoft Windows, Apple Mac OS X oder einer Linux-Variante spielen derzeit jedoch noch die wichtigste Rolle.

2 Ziel

Die vorliegende BSI-Empfehlung zur Cyber-Sicherheit bietet Hilfestellungen für die sichere Konfiguration eines PCs unter der Linux-Distribution Ubuntu. Sinnvoll ist dabei die Betrachtung des Lebenszyklus eines solchen Linux-Systems:

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

Mit wenigen Maßnahmen kann ein PC unter dem Linux-Betriebssystem Ubuntu so abgesichert werden, dass eine weitgehend sichere Nutzung von Dienstleistungen über das Internet möglich ist.

Beachten Sie zusätzlich auch das Dokument „Sichere private Nutzung des Internets“, ebenfalls aus der Reihe „BSI-Empfehlungen zur Cyber-Sicherheit“.

3 Anschaffung des Systems

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

3.1 Hardware und Betriebssystem

Achten Sie beim Kauf des PCs auf möglichst aktuelle PC-Hardware. Diese sollte zudem für einen reibungslosen Betrieb mit Ubuntu geeignet sein. Eine Übersicht von Systemen verschiedener Hersteller, deren Eignung geprüft wurde, finden Sie auf der Internetseite

von Ubuntu[1]. Falls Sie PC-Hardware ohne eine vorinstallierte Version von Ubuntu erwerben, sollten Sie die neueste Version von Ubuntu herunterladen[2] und installieren. Dabei können Sie sich zur Vermeidung häufiger Wechsel auf neue Betriebssystemversionen auch für eine sogenannte *LTS-Version* von Ubuntu (Long-Term Support) entscheiden, die Ihnen eine Langzeitunterstützung über fünf Jahre mit Updates und Sicherheitsaktualisierungen garantiert.

3.2 Virenschutzprogramm

Die Installation eines Virenschutzprogramms ist, basierend auf dem aktuellen Stand der Bedrohungslage in Bezug auf Schadsoftware für Linux, unter Ubuntu nicht notwendig.

3.3 Backups

Um Sicherungskopien Ihrer Daten zu erstellen, können Sie das in Ubuntu über die Dash-Startseite bereitgestellte Werkzeug *Datensicherung* verwenden. Diese Backups können Sie entweder in einem Online-Speicher im Internet ablegen oder auf einem externen Speichermedium wie einer USB-Festplatte. Der Vorteil eines eigenen Speichermediums liegt in der vollen Kontrolle über Ihre Daten, die Sie bei einer Sicherung über einen Internetdienst zum Teil aufgeben.

Der Einsatz einer gesonderten Backup-Software ist für Ubuntu im Allgemeinen nicht erforderlich. Im geschäftlichen Einsatz von Ubuntu ist gegebenenfalls zu prüfen, ob ein professionelles Sicherungssystem eingesetzt werden sollte, welches spezifische Anforderungen – beispielsweise an Revisionssicherheit, Reporting oder Disaster Recovery – gewährleisten kann.

3.4 Anwendungen

Orientiert an Ihrem individuellen Bedarf werden Sie mit der Zeit verschiedene Anwendungsprogramme nutzen, die bei einer Installation von Ubuntu standardmäßig bereits vorhanden sind oder darüber hinaus auch neue Software hinzufügen. Dabei sollten Sie stets Software bevorzugen, die über das Ubuntu Software-Center zur Verfügung gestellt wird. So ist insbesondere auch die automatische Aktualisierung im späteren Betrieb gewährleistet. Darüber hinaus sind Software-Pakete aus dieser Quelle mit Prüfsummen versehen, um zu vermeiden, dass manipulierte Programme installiert werden.

Zur Bearbeitung von Texten, Tabellen oder Präsentationen ist in Ubuntu die kostenlose Bürosoftware *LibreOffice* enthalten, sodass hier keine zusätzliche Installation erforderlich ist.

Zur Darstellung von PDF-Dateien sowie vieler anderer Dokumenten- und Medienformate verfügt Ubuntu bereits über eingebaute Funktionalitäten wie die Anwendung *Dokumentenbetrachter*. 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 Sicherheitsaktualisierungen vom Software-Hersteller auch tatsächlich automatisch installiert werden, ohne dass Sie bei den einzelnen Aktualisierungen aktiv werden müssen. Am einfachsten ist dies über das integrierte Paketverwaltungssystem von Ubuntu möglich. Bei Verwendung von Software aus dem Ubuntu Software-Center sind automatische Updates gewährleistet. Daher sollten Sie sich auf Anwendungen aus dieser Quelle beschränken, wenn Ihnen zu anderen Programmen keine Informationen vorliegen oder Sie unsicher sind, wie sich diese verhalten.

1 http://www.ubuntu.com/certification
2 http://www.ubuntu.com/download

4 Installation und erste Inbetriebnahme

Einen wichtigen Grundstein für die Systemsicherheit Ihres Systems können Sie bereits bei der Installation und ersten Inbetriebnahme von Ubuntu legen, wenn Sie folgende Punkte beachten.

4.1 Installation aller vorhandenen Sicherheitsaktualisierungen

Sofern Sie keine Hardware mit einem vorinstallierten Ubuntu einsetzen, können Sie eine Neuinstallation des Systems in wenigen Schritten selbst vornehmen. Installationsmedien erhalten Sie dabei über die Internetseiten von Ubuntu. Es ist einerseits möglich, Ubuntu als einziges Betriebssystem auf Ihrer PC-Hardware zu installieren, andererseits können Sie es aber auch parallel zu einem bereits vorhandenen Betriebssystem wie z. B. Microsoft Windows einrichten. Während des Installationsprozesses werden Ihnen die für einen solchen Parallelbetrieb relevanten Hinweise gegeben.

Bei einer Neuinstallation von Ubuntu sollten Sie das System mit dem Internet verbinden und die Option *Aktualisierungen während der Installation herunterladen* aktivieren. Bei der ersten Inbetriebnahme eines bereits vorinstallierten Ubuntu-Systems sollten Sie dieses ebenfalls mit dem Internet verbinden und die vom Betriebssystem angebotenen Softwareaktualisierungen herunterladen und installieren.

Um das Sicherheitsniveau von Ubuntu zu halten, ist es erforderlich, stets alle Sicherheitsaktualisierungen nach der Veröffentlichung zu installieren. Die automatische Softwareaktualisierung von Ubuntu ist im Auslieferungszustand bereits aktiviert und deckt sämtliche vorinstallierte Software sowie alle Anwendungen ab, die über das Ubuntu Software-Center hinzugefügt wurden.

Das Suchintervall für neue Updates ist in den Einstellungen der Aktualisierungsverwaltung auf *Täglich* voreingestellt. Hier sollten Sie nicht auf längere Zeiträume wechseln. Damit vorhandene Updates automatisch installiert werden, ohne dass Sie sich weiter darum kümmern müssen, sollten Sie zudem in den Einstellungen der Aktualisierungsverwaltung die Option *Wenn Sicherheitsaktualisierungen vorhanden sind* auf *Automatisch herunterladen und installieren* ändern.

Achten Sie bei der Installation von Drittanbieter-Software darauf, dass auch diese ebenfalls automatische Aktualisierungen vornimmt. Am besten ist dies durch Integration in die Paketverwaltung von Ubuntu möglich.

4.2 Benutzerkonten

Das bei der Erstkonfiguration von Ubuntu angelegte Benutzerkonto ist gleichzeitig auch 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 auf jeden Fall ein zusätzliches einfaches Benutzerkonto an. Sollte Ubuntu von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto anlegen.

Verwenden Sie neben Ihrem normalen Benutzerkonto, welches Sie für die tägliche Arbeit verwenden, ein zusätzliches Benutzerkonto, um transaktionsbezogene Aktivitäten wie Online-Banking durchzuführen oder um kritische Daten online zu versenden.

4.3 Verschlüsselung der Festplatte

Falls es sich bei Ihrem Ubuntu-System 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-PC 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.

Wenn Sie Ihre Daten verschlüsseln möchten, dann sollten Sie bei der Installation von Ubuntu die Option *Meine persönlichen Daten verschlüsseln* auswählen. Gleiches gilt beim Anlegen zusätzlicher Benutzerkonten, deren Daten ebenfalls verschlüsselt werden sollten. Zur Entschlüsselung Ihrer Daten im Falle eines Verlusts des Passworts zeigt Ihnen Ubuntu dann einmalig eine zusätzliche *Passphrase* an, die Sie notieren und räumlich getrennt von Ihrem Rechner an einem sicheren Ort aufbewahren sollten.

Neben der Verschlüsselung Ihrer Daten können Sie auch das komplette System einschließlich Ihres Datenverzeichnisses auf der Festplatte verschlüsseln. Bei einer aktuellen Ubuntu-Version wählen Sie hierzu die Option *Die neue Ubuntu-Installation zur Sicherheit verschlüsseln* während des Installationsvorgangs aus und folgen den angezeigten Hinweisen. Zur vollständig verschlüsselten Installation der derzeitigen Version 12.04 mit Langzeitunterstützung durch den Hersteller (LTS) müssen Sie eine sogenannte Alternate-Installation durchführen[3]. Alternativ dazu können Sie bei der LTS-Version beispielsweise auch das kostenlose Produkt *VeraCrypt*[4] verwenden, dessen Einsatz auf den Internetseiten der Ubuntu-Community[5] im Detail beschrieben wird. Erstellen Sie während des Verschlüsselungsvorgangs unbedingt eine "Rescue Disk". Diese hilft, wenn Probleme beim Entschlüsseln der Festplatte auftreten sollten.

4.4 Personal Firewall

Ubuntu bietet in seiner normalen Konfiguration keine Kommunikationsschnittstellen (genauer: keine Ports) nach außen an, die für Angriffe genutzt werden könnten. Daher ist der Einsatz einer Personal Firewall unter Ubuntu nicht erforderlich. Zur Absicherung des Einsatzes zusätzlicher Programme, die Ports nach außen öffnen, können Sie das Firewall-Werkzeug *Firestarter* über das Ubuntu Software-Center nachinstallieren. Dies ist jedoch eher für erfahrene Anwender zu empfehlen.

4.5 Internet-Browser

Ihr Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten im Internet und stellt somit eines der beliebtesten Ziele für Cyber-Angriffe dar. Verwenden Sie daher möglichst einen Browser mit fortgeschrittenen Sicherheitsfunktionen, der regelmäßig über Sicherheitsaktualisierungen auf den neuesten Stand gebracht wird, wie beispielsweise Google Chrome (https://www.google.com/chrome).

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*.

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

4.6 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.

3 http://wiki.ubuntuusers.de/System_verschl%C3%BCsseln/Alternate_Installation
4 https://www.veracrypt.fr/en/Downloads.html
5 https://wiki.ubuntuusers.de/VeraCrypt/

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen aktuellen E-Mail-Client auswählen und sicher konfigurieren. Bereits in Ubuntu vorhanden ist der E-Mail-Client *Thunderbird*. Hinweise zur Konfiguration von *Thunderbird* finden Sie auf den Internetseiten von Mozilla[6]. Insbesondere ist auch hier 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.

4.7 Java-Laufzeitumgebung

Einige Anwendungen benötigen unter Umständen die Java-Laufzeitumgebung[7]. Um die Angriffsfläche Ihres Systems zu reduzieren, sollten Sie Java nur dann installieren, wenn Ihre Anwendungsprogramme diese Laufzeitumgebung tatsächlich benötigen. Wenn Sie Java installieren müssen, schalten Sie es trotzdem standardmäßig in Ihrem Webbrowser ab. Sie können das Java-Plugin dann fallweise aktivieren, wenn es von einer vertrauenswürdigen Website benötigt wird.

5 Regelmäßiger Betrieb

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

5.1 Sicherheitsaktualisierungen

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

Standardmäßig werden Sie von Ubuntu dazu aufgefordert, die Installation von Updates stets zu bestätigen. Stellen Sie also wie weiter oben beschrieben sicher, dass in den Einstellungen der Aktualisierungsverwaltung die Option *Wenn Sicherheitsaktualisierungen vorhanden sind* auf den Wert *Automatisch herunterladen und installieren* konfiguriert ist.

5.2 Backups

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

Die integrierte Backup-Funktion *Datensicherung* von Ubuntu kann für regelmäßige Backups verwendet werden. Diese Funktion sollten Sie so konfigurieren, dass Ihre Daten kontinuierlich im Hintergrund auf dem für diesen Zweck eingerichteten externen Speichermedium gesichert werden. Ist dieses nicht dauerhaft mit Ubuntu 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.

5.3 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

6 http://support.mozillamessaging.com/de/home
7 http://java.com/de

jeweils unterschiedliche, nicht erratbare Passwörter. Um solche komplexen Passwörter handhaben zu können, sollten Sie Merkhilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes. Notieren Sie Ihre Passwörter zudem auf Zettel und bewahren Sie diese räumlich getrennt von Ihrem Rechner an einem sicheren Ort auf. Zudem können Sie den Passwortspeicher des Betriebssystems nutzen. Unter Ubuntu ist dies der *Schlüsselbund*. Hinweise zur Passwort-Sicherheit finden Sie bei „BSI für Bürger“[8].

5.4 Notfallmaßnahmen

Auch Linux-Systeme 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 Ihr E-Mail-Postfach einloggen.
- 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.

6 Entsorgung

Wenn Sie Ihr Ubuntu-System eines Tages entsorgen möchten, 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.

Vielmehr sollten Sie Ihren PC von einer in das DVD-/CD-ROM-Laufwerk eingelegten Live-CD (z. B. *Ubuntu LiveCD*[9]) starten, dann die Festplatte in das gestartete Live-System einbinden und schließlich in der Kommandozeile mit der Eingabe des folgenden Befehls löschen:

```
sudo dd bs=1M if=/dev/urandom of=/dev/GERAETENAME
```

Dabei steht der GERAETENAME für die Festplatte, die meistens mit "hda" oder "sda" bezeichnet wird, wenn es sich um die erste oder einzige Festplatte in dem System handelt. Informationen darüber, wie Sie herausfinden können, welcher GERAETENAME im obigen Befehl zu verwenden ist, finden Sie im Internet[10].

Sie können Ihre Festplatte alternativ auch mit VeraCrypt– siehe Kapitel *Verschlüsselung der Festplatte* – schützen und lediglich das Schlüsselmaterial vernichten.

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.

8 https://www.bsi-fuer-buerger.de/Passwoerter
9 http://www.ubuntu.com/download/ubuntu/download
10 http://wiki.ubuntuusers.de/Datenträger