Mit Sicherheit ein gutes Gefühl

von Dieter Schütze

Sicherheit im Allgemeinen

In den meisten Fällen geht es um die Sicherheit der eigenen Daten, jedoch ist meine persönliche Meinung, dass auch die Daten Anderer geschützt werden sollten. Um gleich eins vorweg zu nehmen, eine absolute Sicherheit gibt es nicht und wird es auch nie geben. Da dieses Thema sehr weitreichend ist, kann nachfolgend nicht auf alles eingegangen werden. So dient dieser erste Artikel lediglich als grober Überblick. Auch werden Server in diesem Artikel außen vor gelassen, da diese einen viel umfangreicheren Schutz benötigen.

Wo fängt die Sicherheit an ?

Eigentlich ganz einfach, sie fängt immer bei uns selber an. Es ist natürlich äußerst bequem, alles einfach als root oder Administrator machen zu können. Viele Umsteiger zu Linux/Unix-Systemen tun sich äußerst schwer mit der Tatsache, nicht mehr einfach so alles via Mausklick durchführen zu können, zumal sie vorher meistens mit Administrationsrechten unterwegs waren. Dass dies keine Option sein sollte, zeigt ein kleines Beispiel aus dem alltäglichen Leben. Niemand würde heutzutage seine Haustür offen stehen lassen, wenn das Haus verlassen wird. Aber wäre es nicht äußerst bequem, keinen Schlüssel mehr herauszukramen und einfach so ins Haus zu gehen?

Genau so muss ein System betrachtet werden, welches am Netzwerk (auch Internet) hängt oder von mehreren Personen verwendet wird. Ein Rechner oder Netzwerk, das mit dem Internet verbunden ist, wird heutzutage spätestens nach 10 Minuten einigen Angriffen ausgesetzt sein.

Es ist absolut unbedeutend, welches System benutzt wird, die Grundlagen zur Sicherheit sind überall die Gleichen, nur die Möglichkeiten zur Absicherung unterscheiden sich gravierend. Dank Systemen mit offenem Quellcode (z.B. Linux) lernen so langsam auch andere kommerzielle Systeme, den Anwendern mehr Schutz zu bieten. Diesen Anwendern hingegen wird es nicht entgangen sein, dass mehr Schutz auch mehr Aktionen ihrerseits erfordern und dadurch unbequem wirken.

Wie sicher sind denn die Systeme ?

Die Systeme sind zumeist unsicher, es sei denn, man entscheidet sich für diverse spezialisierte Distributionen, die nur auf Sicherheit ausgelegt sind. Damit würde aber kein normaler Anwender oder Einsteiger zurecht kommen und somit sind natürlich Abstriche bei der Sicherheit zu machen. Es muss aber ganz klar unterschieden werden, welche Sicherheit gemeint ist. Den meisten Anwendern werden Unsicherheiten, die nur lokal auszunutzen sind, nicht so wichtig sein.
In einer Firma sind auch diese Sicherheitslöcher enorm wichtig, da je nach Größe der Firma die meisten Angriffe (ungewollte, aber auch gewollte) von innen kommen.
Da in Firmennetzwerken aber der System- und Netzwerkadministrator für die Sicherheit zuständig ist, interessiert das den Anwender dort nur wenig.

Gegen die verbreiteten typischen Viren, die auf Windows basierten Systeme ausgerichtet sind, sind die Linux Systeme selber sicher. Das liegt zum einen daran, dass es derzeit so gut wie keine Viren für Linux gibt und zum anderen, dass es durch den Systemaufbau (Rechteverteilung, Dateisystem usw.) um einiges schwieriger ist, effektive Viren für diese Systeme zu schreiben.

Es gibt aber dennoch genug Angriffsmöglichkeiten, die es abzuwehren gilt. Der Vorteil von Linux basierten Systemen ist, dass man diese sehr sicher machen kann. Allerdings gilt auch hier: Inwieweit das Ganze abgesichert werden soll und muss, hängt von der Benutzung des Systems ab. Man sollte abwägen zwischen der Benutzbarkeit eines Systems und der Sicherheit, die für die benutzten Anwendungen erforderlich ist. Oder anders ausgedrückt, je bequemer der Anwender sein will, desto unsicherer wird das System.

Wovor muss ich mich schützen ?

Nun, das kommt darauf an, wie der Rechner genutzt wird und welche Dienste aktiviert sind.
Hier mal ein paar mögliche Sicherheitsaspekte:

Emails mit so genannten Phishing-Versuchen sind auch für Linux relevant.

Beispiel: Eine Email mit ein paar wichtigen Links, auf die einfach ohne zu überlegen draufgeklickt wird und welche zu einer gefälschten Seite verweisen. Diese kann so gut gestaltet sein, dass sie vom Original nicht zu unterscheiden ist. Wenn wir dann ein mögliches Kennwort zu einem Zugang (z.B. zu eBay oder zu einem Geldinstitut) eingeben, haben wir schon verloren. Auch sollte man Anwender, welche mit virenanfälligen Systemen arbeiten, vor Email-Viren schützen. Damit hilft man gleichzeitig, die Verbreitung von Viren zu verhindern.

Böswillige Server

Im Prinzip das Gleiche wie mit Phishing-Emails oder wir vertippen uns mit der Internetadresse, ohne es zu bemerken. Auch wenn wir mit einem Mediaplayer unsere Lieblings-CD anhören und das Inhaltsverzeichnis von einem Server aus dem Internet beziehen, ist Vorsicht geboten. Es gab in der Vergangenheit Sicherheitslücken in diesen Playern, die fatale Folgen haben konnten, wenn wir uns mit einem nicht vertrauenswürdigen Server verbunden hatten.

Ein Mail Transport Agent

(MTA, z.B. postfix), der als Mailrelay missbraucht wird.
Er ist einfach zu installieren und sehr leistungsfähig, was den Transport von Emails angeht.
Deshalb muss ein offenes Relay unter allen Umständen unterbunden werden. Ein offenes Relay bedeutet, das jemand Fremdes über den eigenen MTA Emails in die ganze Welt versenden kann. Linuxsysteme werden wegen Ihrer Leistungsfähigkeit gerne als Massenmailversender benutzt.

Aber nicht nur durch einen MTA kann man als Relay missbraucht werden, es geht auch viel einfacher. Ein erfolgreicher Angriff auf den sshd-Dienst oder eine Sicherheitslücke in einer Anwendung, bei dem ein Angreifer beliebigen Code ausführen kann, genügt schon.

Einen MTA braucht dieser dann nicht, da er seinen eigenen Maildienst implementieren kann. Meistens merken das die betroffenen Personen erst, nachdem schon tausende Emails versendet wurden (Linux ist ein leistungsfähiges System). Der Schaden kann beträchtlich sein, zumal dies auch strafrechtlich verfolgt werden kann.

Offene Ports

Sind durch geeignete Maßnahmen zu schützen, entweder durch eine Begrenzung des Dienstes oder durch eine Firewall. Hierbei sollten durch die Firewall auch die ausgehenden Ports begrenzt werden, so kann ein eingeschleustes Tool sich nicht einfach über irgendeinen Port mit der Außenwelt verbinden.

Rootkits.

Ist ein Angriff erst einmal gelungen, so würden viele Angreifer auch gerne ein so genanntes Rootkit einschleusen. Ein Rootkit hilft dem Angreifer, auch in Zukunft immer vollen Zugriff auf das System zu haben. Rootkits ersetzen Teile des Systems mit eigenen Tools, welche sich in das System integrieren. Als Beispiele seien hier ps, top, passwd oder route zu nennen, die dem Anwender nach erfolgreicher Installation nur seine normalen Ausgaben anzeigen und die vom Angreifer getätigten Veränderungen verbergen.

Viren für Windows.

Wenn auf dem Rechner beide Systeme installiert sind und die Partitionen eingebunden oder das Windowssystem auf die gleichen Partitionen wie Linux Zugriff hat, so sollte man sich auch davor schützen.

WLAN

Hat auch etwas mit der Bequemlichkeit der Anwender zu tun. Es ist schön, keine Kabel verwenden zu müssen, birgt aber weitere Gefahren und Sicherheitslöcher.
Die meisten WLAN-Zugänge sind immer noch absolut unsicher, da die normalen

Verschlüsselungsmethoden nicht ausreichen. Auch gilt es zu bedenken, dass sich ein WLAN-Zugang bei den meisten Anwendern im internen privaten Netzwerk befindet. So muss ein Angreifer nicht erst ins internen Netz vordringen, sondern ist bei einem erfolgreichen Angriff sofort drin. Der Nachbar oder das Auto mit Laptopbenutzer hört mit!
Wer einen offenen Accesspoint aus sozialer Nächstenliebe einrichten möchte, hat einigen Aufwand zu betreiben, um sich selber zu schützen.

Wie kann ich das System schützen ?

In diesem ersten Artikel für das dieses Magazin kann natürlich nicht auf alle Einzelheiten eingegangen werden. So werden nach und nach ein paar Tipps folgen, wie man was sicherer machen kann und/oder soll. Ein paar grundlegende Dinge sollen aber nachfolgend dargelegt werden.

Ein Rechner-Anwender Verhältnis ist immer ein aktives Verhältnis seitens des Anwenders. Es gibt keine Zaubersysteme, die dem Anwender alles abnehmen können, auch wenn es das eine oder andere System dem Anwender vorgaukeln möchte. Dies stufe ich persönlich als sehr gefährlich ein. Der Anwender (Besitzer des Systems) hat für die Sicherheit zu sorgen und muss diese auch permanent kontrollieren. Hierbei gibt es natürlich einige Tools, die dem Anwender das Leben in dieser Hinsicht vereinfachen. Als Beispiel sei der Artikel von tuxdriver mit dem Namen rootkithunter in diesem Magazin erwähnt. Die Sicherheit beginnt aber eigentlich schon viel früher.

Woher stammt die Distribution?
Wurde sie gekauft oder aus dem Internet heruntergeladen?
Ist die Downloadquelle vertrauenswürdig und wurde die Checksumme der Daten überprüft?
Vor dem Installieren sollten sich Einsteiger oder Umsteiger erst einmal informieren. Hierzu gibt es die Handbücher bei den gekauften Distributionen, die Dokumentationen im Internet und die Artikel auf MandrivaUser.de.

Bei der Installation kann auch die Sicherheitsstufe bestimmt werden, die im Normalfall sehr niedrig vorgewählt ist. Hier sollte zumindest „hoch“ ausgewählt werden.

Ein normaler Benutzer sollte jedoch nicht die höchste Sicherheitsstufe wählen, da er damit später überfordert wäre und unter Umständen keinen Zugang mehr zum eigenen System hätte. Wer die Möglichkeit hat, sollte auch eine Emailadresse angeben, um die Logs des Sicherheitssystems zu bekommen. Bei einer Verbindung mit dem Internet sollte auf alle Fälle die Firewall aktiviert sein. Wenn auch die via MCC (Mandriva Control Centrum) erstellte Firewall nicht auf alle Details eingehen kann, so bietet sie doch wenigstens einen grundlegenden Schutz. Grundsätzlich sollte immer als normaler Benutzer gearbeitet und nicht permanent die root-Rechte für alltägliche Dinge missbraucht werden. Dies wurde bei den meisten Distributionen gut gelöst, da der root-Zugang beim Anmelden zunächst einmal nicht sichtbar ist.

Als Virenschutz würde sich „clamav“ anbieten, was mit dem KDE Tool „klamav“ auch einfach zu bewerkstelligen ist. Im täglichen Betrieb sollten auch des Öfteren die Logdateien im Verzeichnis /var/log/ durchgeschaut werden. Da dort fast alles aufgezeichnet wird, können auch Angriffe erkannt werden. Zudem sind sie immer hilfreich bei einer Fehlersuche. Diese Logdateien können auch mit Hilfe des MCC durchsucht werden (unter System > Protokolldateien).

Durch Mailinglisten oder studieren einiger Webseiten mit dem Thema Sicherheit sollte sich jeder über Systemverwundbarkeiten und andere Gefahren informieren, um umgehend das System zu aktualisieren oder Vorkehrungen zu treffen, um mögliche Gefahren abzuwehren.
Das System auf dem aktuellen Stand zu halten ist ebenfalls eine Grundvoraussetzung für jeden einigermaßen sicherheitsbewussten Anwender. Für Mandriva Linux gibt es einige Quellzweige, so z.B. main, update, contrib, jpackage und plf. Hierbei sollte der Anwender aber wissen, dass seitens Mandriva nur der main- und update-Zweig voll unterstützt wird. Dies bedeutet, dass nur für diese beiden Zweige die notwendigen Aktualisierungen gewährleistet sind. Um die Pakete aus all den anderen Zweigen (auch contrib oder jpackage) muss sich der Benutzer selber kümmern.
Dies kann mitunter eine sehr aufwendige Angelegenheit sein, da der Anwender/ Systemadministrator zumeist auf den jeweiligen Internetseiten nach Aktualisierungen Ausschau halten muss. Auf alle Fälle sollte der update-Zweig eingebunden sein und eine regelmäßige Aktualisierung durchgeführt werden.

Ein ebenfalls nützliches Tool von Mandriva ist „msec“ (Mandriva Security). Dieses Tool besteht aus einigen Scripten, die das System auf sicherheitsrelevante Dinge überprüfen. Konfigurieren lässt sich das Ganze „msec“ ebenfalls im MCC. Hierzu ist im MCC im Menü unter Einstellungen der Expertenmodus einzuschalten.
Dann können unter Sicherheit das Setzen der System-Sicherheitsstufe und auch die Feinabstimmungen der Sicherheitsrechte ausgewählt werden. Wer nicht über das MCC gehen möchte, kann dieses auch direkt als root in der Konsole durchführen. Es sind die Applikationen „draksec“ und „drakperm“. Leider läuft das Tool „msec“ standardmäßig nachts um 4:00 Uhr durch den Eintrag in der /etc/cron.daily/. Es kann aber jederzeit in der Konsole als root durch Eingabe von msec gestartet werden. Ich gehe jetzt nicht auf die Details dieser Tools ein, zumal die Hilfefunktion einige Erklärungen bietet. Sollten dennoch Unklarheiten vorhanden sein oder weitere Informationen benötigt werden, kann im Forum von MandrivaUser.de danach gefragt werden.

Mails sollten nur noch als Text versendet werden, da hierdurch die Gefahr versteckter Inhalte deutlich geringer ist. Zudem gibt es jetzt schon Unternehmen, die grundsätzlich alle HTML-formatierten Mails aus diesem Grund ablehnen. Die in Mails angegebenen Links sind aber trotzdem genau zu betrachten (siehe Phishing-Emails).

Ein anderes Thema sind regelmäßige Backups. Festplatten mit großer Kapazität sind heute enorm günstig, aber wo und wie werden die Daten gesichert? Schließlich kann auch die Festplatte mal das Zeitliche segnen und dann sind die Daten weg. Das Schöne an Linuxsystemen ist, dass man auch geöffnete oder gerade verwendete Dateien einfach sichern kann (alles ist nur eine Datei). So steht von dieser Seite im Unterschied zu anderen Systemen kein Hindernis im Weg, das komplette System zu sichern. Um nicht unnötige Dateien oder Anwendungen zu sichern, gilt wie bei allen Systemen: Ordnung erhält die Übersicht.

Ich hoffe dies war, - wenn auch nur ein kleiner allgemeiner Überblick - genug, um die Anwender für dieses Thema zu sensibilisieren.

Nützliche Links zu diesem Thema

http://MandrivaUser.de FAQ (deutsch)
http://MandrivaUser.de Artikel (deutsch)
http://MandrivaUser.de/ Forum (deutsch)
http://www1.mandrivalinux.com/de/fdoc.php3 (deutsch)
http://www.mandriva.com/security/advisories (englisch)
http://www.linux-mandrake.com/en/doc/82/en/ref.html/prog-msec.html (englisch)
http://www.securityfocus.com (englisch)
http://www.linuxsecurity.com/ (englisch)
http://www.heise.de/security/ (deutsch)
http://www.kernel.org (englisch)