Einen sicheren Laptop mit Ubuntu einrichten

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

Chemnitzer Linux-Tage



Über Mich



Über Mich

- Geek, Nerd, Hacker seit knapp 20 Jahren
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



Inhaltsverzeichnis

1 Einführung

2 Laptop-Hardware

3 Ubuntu einrichten



Bedrohungslage

- Schadsoftware greift Rechner an
- mobile Rechner gehen verloren oder werden gestohlen
- Manipulationen einfach möglich bei physischer Kontrolle
- Daten abschöpfen im Hotel
- Trojaner aufspielen bei »Zollkontrolle«
- sensible Daten schützen



Warum Linux?

- kostenlos, frei, offen
- Open Source - Backdoors verstecken schwierig
- Unix-Sicherheitsmodell
- gute Hardwareunterstützung
- vielfältige Software verfügbar



Warum Ubuntu?

- Ubuntu recht einfach nutzbar
- unterstützt von Canonical
- viele Anwendungen verfügbar
- 2 Releases pro Jahr (.04 und .10)
- LTS mit 5 Jahren Laufzeit (16.04., 14.04, 12.04)
- Alternate Install/Server existiert



Bedrohungsszenario

- Abwägung Aufwand und Kosten vs. Bedrohung und Sicherheit
- Was bedroht mich?
- Risikoanalyse!
- Grundlage der Journalistenschulung für Syrien



Inhaltsverzeichnis

1 Einführung

2 Laptop-Hardware

3 Ubuntu einrichten



Hardware

- professionelle Laptops mit ordentlichem BIOS/UEFI
- Lenovo Thinkpad, Dell Latitude, HP Elitebook
- Thinkpad-BIOS besonders geschützt
- BIOS: User, Admin und Festplattenpasswort setzen
- gebrauchten Wegwerflaptop/Netbook
- z.B. Lapstore
- Hardwaremanipulationen existieren - Rechner nicht aus den Augen lassen



Hardware

- SSD: Samsung 850 Pro 1TB
- SSD: Samsung 850 Evo 1TB
- SSHD: Seagate ST1000LM015 1TB ab 95 Euro
- Hardwareverschlüsselung in AES
- immer aktiviert
- Festplattenpasswort im BIOS setzen
- cf: OPAL TCG



Hardware



Inhaltsverzeichnis

1 Einführung

2 Laptop-Hardware

3 Ubuntu einrichten



Ubuntu Download

- `http://www.ubuntu.com/download/server`
- Ubuntu Server 16.04 LTS
- Minimal-Installation
- Anwendungen per Internet nachinstallieren
- Installation per CD/DVD oder USB-Stick
- nur Ubuntu auf Platte sehr einfach
- Dualboot komplexer, nicht empfohlen



VERSCHLÜSSELUNG

- Verschlüsselung der gesamten Festplatte (LVM LUKS)
- Verschlüsselung von user durch ecryptfs
- Verschlüsselung beliebiger Verzeichnisse durch encfs
- Verschlüsselung einzelner Dateien durch mcrypt, OpenSSL oder GnuPG
- sicheres Passwort!
  min. 12 Zeichen, Groß/Kleinbuchstaben, Ziffern, Sonderzeichen, keine Wörter aus dem Wörterbuch



VERSCHLÜSSELUNG

- Verschlüsselung der gesamten Festplatte (LVM LUKS)
- Verschlüsselung von user durch ecryptfs
- Verschlüsselung beliebiger Verzeichnisse durch encfs
- Verschlüsselung einzelner Dateien durch mcrypt, OpenSSL oder GnuPG
- sicheres Passwort!
  min. 12 Zeichen, Groß/Kleinbuchstaben, Ziffern, Sonderzeichen, keine Wörter aus dem Wörterbuch



Verschlüsselung

- Partitionierung: /boot (1GB), Swap (RAM), / (Rest)
- 3 Partitionen
- /boot unverschlüsselt, beinhaltet Startsystem
- / wird per LVM und dm-crypt verschlüsselt
- Swap ist Auslagerungsspeicher, wird verschlüsselt mit Zufallspasswort oder ggf. weggelassen



VERSCHLÜSSELUNG

- `Geführt - gesamte Platte mit verschlüsseltem LVM`
- `Manuell`
- `http://wiki.ubuntuusers.de/System_verschlüsseln/Alternate_Installation`
- `/` kann kaum mehr manipuliert werden, `/boot` schon
- `/boot` auf USB-Stick verschieben
- kann auch für USB-Sticks oder USB-Platten eingesetzt



VERSCHLÜSSELUNG

- eCryptFS: verschlüsselt das Benutzerverzeichnis (`/home/stefan/`)
- verschlüsselt im Dateisystem, Passwort automatisch aus User-Passwort abgeleitet
- wird automatisch bei der Installation mit eingerichtet
- Nutzung transparent
- schützt aber nur Nutzerdateien, nicht Systemdateien



VERSCHLÜSSELUNG

- encfs: verschlüsselt ein beliebiges Verzeichnis
- verschlüsselt im Dateisystem, Passwort muss übergeben werden
- muss nachinstalliert werden (apt-get -y install encfs)
- kann beliebig ineinander gestapelt werden
- Nutzung z.B. in Cloud ggf. ohne `.encfs6.xml`



Beispiel

- Kunde1 | Kunde2 | Kunde3 | Buchhaltung jeweils mit encfs
- verschlüsseltes /home/stefan mit eCryptFS
- Festplattenverschlüsselung LVM
- hardwareverschlüsselte SSD/SSHD



EXTERNE DATENTRÄGER

- USB-Stick oder SD-Karte verschlüsseln
- Dateisystem mit LUKS
- Verzeichnisse mit encfs
- sensible Daten auslagern
- SD-Karte im Portemonnaie mitführen



Live-Systeme

- starten von CD/DVD oder USB-Stick
- fassen Festplatte nicht an
- können ständig mitgeführt werden
- TAILS: https://tails.boum.org/download/index.de.html
- Porteus / Porteus Kiosk



Dateien verschlüsseln

- mcrypt, GnuPG, OpenSSL
- GnuPG hat standardisiertes Format
- portabel und austauschbar: Linux, *BSD, OS X, Windows
- OpenSSL recht weit verbreitet
- Dateien in tar-Ball packen, verschlüsseln und im Internet ablegen
- Nach der Einreise auf Laptop ziehen
- vor Ausreise wieder löschen



Datensicherung

- Backups! Backups! Backups!
- Offline, Offsite, Archiv!
- Verschlüsseln
- `tar cpf Backup-`date +%y%m%d%H%M`.tar /home/.ecryptfs/stefan/`



Manipulationen erkennen

- Fingerabdruck des Systems erstellen
- AIDE automatisiert dies
- Datenbank von /boot erstellen und vergleichen
- `/etc /bin /sbin /usr/bin /usr/sbin`
- Nach jedem Update aktualisieren
- Prüfung nicht im Live-System sondern via CD/Stick



Manipulationen erkennen

- chkrootkit: Scannt nach Anzeichen von Rootkits
- clamav: freier Virenscanner
- regelmäßige Scans sinnvoll, aber von Live-CD/Stick
- können nicht alle Schadsoftware erkennen



Anwendungen

- so wenig wie möglich installieren
- regelmäßig updates einspielen - sofort
- LibreOffice als Ersatz für MS Office
- nach Möglichkeit vermeiden
- Desktop Environments (KDE, Gnome, LXDE etc.) meiden



VPN

- Virtual Private Network - verschlüsselt Verbindung zwischen Laptop und Server
- Server zu Hause oder im Unternehmensnetz
- Laptop kann auf Unternehmensserver etc. zugreifen
- Server einfach einrichten z.B. Raspberry PI mit Raspbian, PC mit Ubuntu oder Hardwarelösung (Fritzbox, ASUS)
- Miet-Lösungen
- sichert Verbindungen ins Internet ab
- umgeht Zensurmaßnahmen im Internet
- eventuell verboten und geblockt
- Updates möglichst bei VPN-Verbindung einspielen



Anonymität im Internet



Anonymität

- Internetverbindungen zurückverfolgbar
- TOR anonymisiert diese durch kaskadierende Proxys
- Tor Browser Bundle
- Whonix: Virtuelle Maschine
- TAILS: USB-Stick oder Virtuelle Maschine



Browser

- zentrales Einfallstor für Schadsoftware
- Chromium derzeit am sichersten, AdBlocker installieren (μBlock),
- Midori ist klein und schnell
- auf Flash, Java und Javascript möglichst verzichten (uMatrix, FlashBlock)
- ggf. mehrere Browser einsetzen
- einfaches absichern mit FireJail



NextCloud

- NextCloud: eigenen Cloud-Server aufsetzen
- kann z.B. Google auf Android ersetzen, iOS App verfügbar
- Kalender, Aufgaben, Adressbuch, Dokumentenverwaltung etc.
- Keine Auslieferung der Daten an Google, Apple, Dropbox und Co.
- Betrieb mittels VPN zusätzlich absichern



Virtuelle Maschinen

- VirtualBox `https://www.virtualbox.org/`
- Open Source, Virtuelle Maschine
- Linux, Windows, Android, FreeBSD, NetBSD ...
- virtuelle Maschinen voneinander abgrenzen



AppArmor

- Kernelmodul, steuert Zugriffsrechte der Prozesse
- automatisch installiert
- Profile für bekannte Programme existieren und werden automatisch eingerichtet
- eigene Profile können erstellt werden
- sichert insbesondere komplexe Programme (Thunderbird, Evolution)




yubico
yubico
fido

U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass



U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass



Web.de unterstützt U2F nicht

- OATH-HOTP im Yubikey Personalization Tool einrichten, Secret Key generieren
- KeePass installieren und einrichten, Plugin OtpKeyProv installieren, Secret Key hinterlegen
- sicheres Passwort für Keepass vergeben
- Zufallspasswort (256HEX Bit) generieren und bei Web.de eintragen

  `09137f0ac6627f9e94e2af2342d2610bf20ff0ee929114d27b3629e3823e11ea`
- KeePass mit dem Webbrowser via Plugin verbinden
- KeePass-Datenbank mit Passwort und Token entschlüsseln, Browser holt User/Passwort für Web.de via Plugin aus DB.



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher