Inhaltsverzeichnis

1 Schutzziele **2**

1.1 Anforderungen an das System (CIA Schutzziele) 2

1.1.1 Sicherheit - Confidentiality 2

1.1.2 Integrität - Integrity 2

1.1.3 Verlässlichkeit - Availability 2

2 Systemsetup **3**

2.1 Software 3

2.1.1 Authentifizierungssysteme 3

2.1.2 Firewall 3

2.2 Hardware 3

2.3 Betriebssystem 3

2.3.1 Ubuntu 3

2.3.2 Mint 4

2.3.3 SuSE 4

2.3.4 Debian 4

2.3.5 ArchLinux 4

2.3.6 Manjaro 5

2.3.7 Gentoo 5

2.3.8 Slackware 5

2.3.9 Fazit 5

3 Rechtemodellierung **6**

4 Kommunikationssicherheit **7**

4.1 E-mail 7

4.1.1 GPG 7

1 Schutzziele

Linux-Arbeitsfläche für Mitarbeiter einer Office-Umgebung.

1.1 Anforderungen an das System (CIA Schutzziele)

1.1.1 Sicherheit - Confidentiality

Sollte den neuesten Standard der Sicherheit entsprechen.

- Regelmäßige Sicherheitsupdates.
- Nach außen hin abgeriegelt sein (Interne Firewall).
- Abgesicherte Zugangspunkte für Mitarbeiter (Extern).
- Regelungen der Programmbenutzung. Nur Systemadministratoren sollten neue Programme dazu schalten können.
- Einschränkung der Webseitenbenutzung. Vermeidung von Pishing-Sites.
- Sicherheitsüberprüfung der ankommenden E-mails.

1.1.2 Integrität - Integrity

1.1.3 Verlässlichkeit - Availability

System sollte zuverlässlich sein.

- System sollte nicht instabil sein => Abstürze usw. vermeiden. => Keine Testing-Distributionen.
- Vermeidung von Hardware-Schäden. => Kostenfalle

2 Systemsetup

2.1 Software

2.1.1 Authentifizierungssysteme

Kerberos

AppArmor

SELinux

2.1.2 Firewall

iptables

iptables ist ein Paketfilter, der eingehende und ausgehende Pakete vom und zum Computer überwacht.

SuSEfirewall2

SuSEfirewall2 ist ein Skript, welches Regeln für iptables automatisch erstellt.

ufw

ufw ist ein einfaches Konsolen-Frontend für iptables.

2.2 Hardware

Davon ausgegangen wird, dass sowohl Laptops, als auch PCs (Personal Computers) im Office-Betrieb sind. Die Laptops sollten dabei mit nach Hause genommen werden können.

2.3 Betriebssystem

2.3.1 Ubuntu

Ubuntu ist eine von der Firma Canonical entwickelte auf Debian basierende Linux Distribution für den Desktop und Office Betrieb. Ubuntu eignet sich darin möglichst anfängerfreundlich zu sein. Ubuntu nutzt ein Bündel an vorinstallierter Software und man kann ganz ohne spezifische Linux Kenntnisse anfangen mit zu arbeiten.

Firewall

Ubuntu nutzt ufw.

Desktop

Ubuntu kommt in verschiedenen Ausführungen. Dabei sind das normale Ubuntu, welches auf Unity-Desktop von Canonical basiert, Kubuntu auf KDE-Basis und Xubuntu auf Xfce-Basis die bekanntesten.

2.3.2 Mint

Linux Mint ist ein Ableger von Ubuntu. Dabei versucht Mint nicht kommerziell zu sein und wird von einer großen Community weiterentwickelt.

Firewall

Linux Mint nutzt ufw und stellt der Einfachheit im Desktop das Programm Gufw zur Verfügung. Welches ufw per GUI verwalten lässt.

Desktop

Linux Mint nutzt MATE und das hauseigene Cinnamon als Desktops.

2.3.3 SuSE

2.3.4 Debian

Debian ist einer der beliebtesten von einer Community entwickelten Server Distributionen. Man kann Debian allerdings auch für den Desktop Betrieb verwenden. Es ist komplett Opensource und verfolgt das freie Software-Prinzip. Somit wird Debian als Betriebssystem nur mit nicht lizenzierter Software ausgeliefert. Debian kommt in 3 Varianten. Debian Stable, Testing und Sid. Debian Stable verspricht stabil zu sein und Software- und Kernelpakete müssen einen langen Testzyklus durchlaufen bevor sie in den Stable Zweig aufgenommen werden. Dies schadet natürlich der Aktualität der Pakete. Debian Testing nimmt Pakete vom Sid-Zweig auf, nachdem sie auf Stabilität getestet wurden, verspricht aber nicht fehlerfrei zu sein. Debian Sid kann unstabil werden, enthält aber die aktuellsten Pakete.

2.3.5 ArchLinux

ArchLinux ist eine von der Community entwickelten Rolling Release Distribution. Rolling Release heißt, dass es verspricht vom Kernel und der mitgelieferten Software immer auf den aktuellsten Stand zu sein. Aber die Installation von ArchLinux gestaltet sich als eher kompliziert und bedeutet recht viel Arbeit mit der Konsole. Somit ist es nicht

unbedingt für Einsteiger geeignet und ist auch nicht unbedingt immer 100 Prozent stabil oder fehlerfrei.

2.3.6 Manjaro

Manjaro baut auf ArchLinux auf und hat den Ziel ArchLinux für den Anwender so einfach wie möglich zu machen. Manjaro lässt sich mit einer Oberfläche installieren. Allerdings wartet Manjaro bei einem neuen Packet auf ArchLinux immer damit bis es getestet wurde ehe es selbst als Update einspielt. Damit hat Manjaro einen eher scheinbaren Rolling Release Status und ist auch nicht immer aktuell. Dies bedeutet aber auch, dass es um einiges sicherer und stabiler ist.

2.3.7 Gentoo

2.3.8 Slackware

2.3.9 Fazit

3 Rechtemodellierung

4 Kommunikationssicherheit

4.1 E-mail

E-mails sind heutzutage eines der wichtigsten Sicherheitsaspekte in der Systemsicherheit. Eine Menge von Hacking-Versuchen und das Einspielen von Schadsoftware entstehen durch den Austausch von E-mail. So ist es möglich seine Idendität per E-mail vorzutäuschen, einen Virus oder Trojaner im E-mail Anhang zu verschicken oder einen Mitarbeiter per Social Hacking zu einem Fehler zu verleiten, welcher ein Einfallstor in die Firma bietet.

4.1.1 GPG

Eines der bekanntesten Möglichkeiten ist es seine E-mails per GPG abzusichern. GPG hat ein Ende-zu-Ende Verschlüsselung Prinzip. Das heißt zwei Clients haben einen Private Key und einen Public Key. Beide tauschen untereinander ihren Public Key aus und verschlüsseln ihre Nachricht mit dem Public Key des jeweiligen Anderen. Nur derjenige der im Besitz des Private Key ist, kann dann die Nachricht wieder entschlüsseln. Dieses Verfahren gilt als so ziemlich die sicherste Methode sich vor Idenditätsbetrug und auch vorm Abfangen von Daten zu schützen. Denn falls eine E-mail abgefangen wird, kann derjenige, der sie abgefangen hat, nichts mit der Nachricht anfangen.