Alexander Kern, Matrikelnummer: 43524, INB08, IT-Sicherheit-Projekt

Inhaltsverzeichnis

1 Phasenmodell

1.1. Planung und Konzeption

1.1. 1. Definition des Einsatzzwecks:

privater Server für eigene Zwecke, Nutzen für Familienmitglieder und Freunde im Rahmen des Möglichen und mit mittlerem Aufwand

1.1.2. Festlegung von Einsatzszenarien:

- Es braucht jemand Webspace, dann werden alle Strukturen erstellt und freigeschaltet, damit die betreffende Person Zugriff hat. Ggf. wird über eine Aufwandsentschädigung verhandelt.
- Es braucht jemand Speicherplatz im Internet zur Datensicherung.
- Es braucht jemand einen Instant-Messaging-Account
- Es braucht jemand eine E-Mail-Adresse mit Monitoringfunktionen und Abschottung von Administratoren großer Unternehmen
- Es braucht jemand Zugriff zur Datenbank mit festgelegten Rechten
- Es braucht eine vertrauenswürdige Person SSH Zugriff, um das System seinen Wünschen anzupassen
- Es braucht jemand einen entfernten Linux-Desktop-Zugriff über VNC
- Es braucht jemand einen Game-Server, wie z.B. Quake 3 oder Operation Flashpoint unter Linux
- Es braucht jemand eine Monitoringfunktion, die gescriptet werden muss
- Es braucht jemand Zugang zur Gruppen-Telefonie-Software Ventrilo
- Es braucht jemand die Funktion nur vollständige Downloads zu messen (Log-Auswertungs-Monitoring-Script)
- Alle Datenaustauschverfahren versagen oder sind ungeeignet, dann lässt sich der ftp und http des Servers nutzen. (Schon oft verwendet)

1.1.3. Abwägung Risikopotential

Das Risikopotential ist relativ hoch bzw. eigentlich normal, da alle Dienste auf einem Computer installiert sind und gestartet sind. Weiterhin sind private Daten gespeichert. Sollte sich ein Angreifer diese beschaffen, dann sind verschiedene Folgeschäden schwer abzuschätzen. Sollte nur Dienst, der durch die Firewall freigeschaltet ist mittels eines Exploits gehackt werden, dann ist es möglich dass Tür und Tor offen steht zu allen Daten. Es sind jedoch viele Dienste freigeschaltet, weshalb es eine größere Angriffsfläche gibt. Der Server steht im Internet und nicht in einem Intranet, wodurch jeder aus der gesamten Welt angreifen könnte. Jedoch müsste der Server vielleicht Aufmerksamkeit erregen, dass sich ein Hacker auf ihn stürzen würde, aber auch das ist nicht unbedingt erforderlich dafür.

Ein Worst-Case (1.) (Löschen) wäre es, wenn alle Daten verloren gehen. Das wäre keine so schlimme Katastrophe, denn das würde nur bedeuten, dass es einen Großen Aufwand gibt, alles wieder herzustellen. Ein E-Mail-Nutzer müsste sich z.B. alle Passwörter, die im E-Mail-Konto gespeichert worden sind, neu besorgen.

Worst-Case 2: (Ausspähen) Schlimmer wäre es, wenn ein Hacker sich Zugang zu diesen Passwörtern verschaffen würde, um einen Identitätsdiebstahl zu begehen. Weiterhin könnten Jabber-Messenger-Chats ausgelesen werden, sollten diese nicht verschlüsselt stattfinden. Das Gefahrenpotential davon hängt ganz individuell von der jeweiligen Diskussion im Chat ab.

Worst-Case 3: (Manipulation) Die Informationen von E-Mails könnten manipuliert werden, bevor sie gelesen worden sind. Der Zutrittspunkt eines Hackers könnte öffentlich gemacht

werden, so dass weitere Hacker ihr Unwesen treiben und das Gefahrenpotential besser ausgeschöpft werden könnte. Automatisierte Spionagesoftware, die sich versteckt, könnte installiert werden.

Der Server ließe sich missbrauchen, als Basis um von diesem Punkt aus Hackerangriffe auf andere Systeme zu starten, wodurch sich der Betreiber unter Umständen strafbar machen könnte. Ein Finanzieller Schaden könnte die Folge sein.

Der Server könnte als Spamschleuder missbraucht werden.

Auf dem Server könnten Beweise für einen kriminellen Akt einer Mafia gespeichert werden von einem Hacker. Sollte die Mafia davon etwas erfahren durch den Hacker, müsste der Betreiber des Servers unter Umständen um sein Leben und das Leben seiner Familie und Freunde fürchten.

Außerirdische könnten ……. (ok, war nur Spaß)
´

Worst-Case 4: (außerhalb vom Server). Im Root-Ssh-Einlog-Prozess könnte ein Hardware- oder Software-Keylogger die Eingabe des Passwortes abfangen, wodurch voller Zugriff für einen Fremden gewährleistet werden würde.

1.1.4. Dokumentation der Einsatz-Entscheidung

Der Betreiber des Servers hat sich dafür entschieden alle Potentiale der Nutzbarkeit auszuschöpfen, die für ihn, seine Freunde und seine Familie nützlich sind, da er die Wahrscheinlichkeiten für große Gefahren als sehr gering einschätzt und die mittleren Gefahren vertretbar sind.

1.1.5. Erstellung des Sicherheitskonzepts

folgt später

1.1.6. Festlegung von Richtlinien für den Einsatz:

wird basierend auf dem Sicherheitskonzept formuliert, folgt später.

1.2. Beschaffung

1.2.1. Festlegung der Anforderungen an zu beschaffende Produkte:

sicher, stabil, einfach und zeitsparend konfigurierbar, kostenlos, vielseitig konfigurierbar, gut bewertet durch Referenzquellen, möglichst schon in den Paketquellen der Distribution enthalten, ausgereift, modular, hoher Kompatibilitäts-Grad, standard-treu, Reichhaltigkeit an Features ohne Sicherheitsvernachlässigung (nahezu unmöglich)

1.2.2. Auswahl der geeigneten Produkte

Angeschafft wurde ein Root-V-Server, alle nötige Sicherheitssoftware ist vorinstalliert oder kostenlos nach-installierbar. Sicherheitsaspekt:

- Antivirensoftware
- Firewall-System
- Spamfilter
- Audit und Logging liefern die Dienste mit
- Alle Pakete des RPM-Systems zu nennen wäre jetzt zu viel
- Plesk und PowerPannel Webinterface für den Server (vorinstalliert)

1.3. Umsetzung

1.3.1. Konzeption und Durchführung des Testbetriebs

Der Vserver arbeitet schon seit 3 Jahren problemlos. Testbetrieb war nicht erforderlich, da der erhöhte Aufwand dadurch nicht gerechtfertigt ist, weil der Betreiber keine kommerziellen Absichten hegt.

1.3.2. Installation und Konfiguration entsprechend Sicherheitsrichtlinie

Alle Dienste haben aktiviertes Logging mit ausreichendem Grad an Logging. Eine Software, die das Logging bzw. Auditing analysiert bzw. besser lesbar macht wird vorgesehen. Bietet der jeweilige Dienst Verschlüsselung an, so wird die Architektur dafür genutzt und aufgesetzt. Bietet der Dienst dies nicht, so wird sich ggf. nach einem vergleichbaren Dienst umgeschaut, der dies unterstützt. Speziell für den sensibelsten Dienste, der E-Mail-Server-Architektur werden mehrere Bücher gekauft, weil das Potential für Sicherheitsfehler hier sehr groß ist. Vor der Installation werden noch Sicherheits-News im Internet durchgelesen, die von aktuellen Sicherheitslücken berichten. Ggf. wird der Dienst ausgesetzt oder es wird nach Alternativen gesucht. Häufigkeiten von Sicherheitslücken und Geschwindigkeit der Schließung derer werden im Netz analysiert und Berichte darüber werden gelesen; alles im Rahmen der Installation und Konfiguration. Es werden nicht die allerneuesten Softwarepakete installiert, sondern die neuesten sicheren Pakete, d.h. Nicht Version x.x.0 sondern z.B. x.x.9. Vor Inbetriebnahme werden Sicherheitsupdates durchgeführt. Die Firewall muss auch vor Inbetriebnahme auf die Policy Deny gestellt werden, egal ob alle Ports schon freigeschaltet wurden sind und der Stateful-Filter eingerichtet ist.

1.3.3. Schulung und Sensibilisierung aller Betroffenen

Alle Benutzer des Ventrilo-Gruppen-Telefonie-Programms werden angewiesen sichere Passwörter zu verwenden. des weiteren wird ein weitere Ventrilo-Administrator eingesetzt, falls der Chef des Vservers nicht anwesend ist, dass es dann noch jemanden gibt. FTP-, SSH-, E-Mail-Nutzer sind Linux-User. Sie werden auch angewiesen sichere Passwörter zu verwenden und das Passwort nicht an dritte weiter-zu-reichen. Sollte der Chef des Vservers einem User für eine Periode einem User SSH-Zugang verschaffen, so wird dieser dazu angewiesen nur Software zu installieren, die vorher abgesprochen wurde. Jabber-Messenger-User werden angewiesen möglichst immer TLS aktiviert zu haben in ihrem Client. FTP-User wird es verboten SSH zu verwenden und SSH-Usern wird es verboten FTP zu verwenden. SFTP,FTPS und SSH ist gesichert und kann mit einem User-Account verwendet werden, weil die Daten nicht getrennt gelagert werden müssen und somit sicher sind. Webserver-Nutzer sind dazu aufgefordert ihre Websoftware immer auf den neuesten Stand zu halten, wobei PHP-Sicherheitslücken nur ein eingeschränktes

Risiko darstellen. E-Mail-System-Nutzer werden aufgefordert keine Spam-E-mails zu versenden, damit der E-Mail-Server nicht in eine Blacklist gerät von einem Blacklist-E-Mail-Dienst im Internet. Alle Anwender werden darauf geschult, was überhaupt ein sicheres Passwort ausmacht. Der Betreiber des Vservers schult sich selbst über das Thema IT-Sicherheit. Die Nutzer des Servers werden darüber belehrt, dass der Administrator des Servers die E-Mails lesen kann, wenn er das wollte. Dies dient ihrer Sicherheit, das zu wissen. Sie werden weiterhin darüber Informiert, dass man E-Mail z.B. mit Enigmail verschlüsseln kann. Die Strafandrohung sich nicht an die vorgegeben Richtlinien zu halten ist es sich eine Standpauke vom Administrator anhören zu müssen.

1.4. Betrieb

1.4.1. Sicherheitsmaßnahmen für den laufenden Betrieb

Alle Dienste sind auf ein gerechtfertigtes Maß an Logging eingestellt. Eine Logging-Auswertungs-Software wird in regelmäßigen Abständen verwendet, um die Aktionen nachzuvollziehen. Eine Monitoringsoftware über ein Webinterface und Scripte steuerbar nimmt weitere Daten auf. Daten sind dabei wann sich jemand in welchen Dienst einloggt und ausloggt und wer z.B. in den Jabber-Messenger-Dienst oder als Linux-User oder in den Gruppen-Telefonie-Server Ventrilo. Durch das Monitoring können auch Ausfälle dokumentiert werden und Download-Häufigkeiten analysiert werden, Netzwerkaktivitäten überwacht werden und theoretisch sogar das Wetter dokumentiert werden oder die CPU-Temperatur etc. Mit einem Cronjob und einem Bashscript wurde es realisiert, dass regelmäßige Backups durchgeführt werden, mit dem die Daten verschlüsselt, komprimiert und in gleichgroße Stücke gekapselt werden und alles in einer Pipeline in einem Ruck auf einem FTP-Server geladen wird. Da hierbei mehrfach gepiped wird, kann der Vorgang deutlich beschleunigt werden und verbraucht weniger Ressourcen. Der Betreiber des Vservers wird durch den Hoster ständig per E-Mail informiert, wann Systemausfälle zu erwarten sind. Dazu ist es erforderlich, die E-Mails oft zu kontrollieren. Der Kontostand auf dem Girokonto wird oft überprüft damit genug Deckung für die Finanzierung des Servers da ist, damit der Hoster des Servers diesen nicht abschaltet. Es werden in größerem Abstand auch weitere Backups gesichert auf den Rechner auf dem der SSH Client verwendet wird. Somit hat man auch ein geographisch verteiltes Backup. Bei Ausfallerscheinungen wird der Vserver-Administrator per SMS darüber benachrichtigt. In größeren Abständen wird auch über das angebotene Webinterface des Hosters ein Image erstellt und gesichert.

1.4.2. Kontinuierliche Pflege und Weiterentwicklung

Ein automatisches Backup ist eingerichtet. Es wird regelmäßig nach Viren gescannt. Vieles wurde schon genannt im vorigen Abschnitt „Sicherheitsmaßnahmen für den laufenden Betrieb“. Bisher war es unnötig weitere Software zu installieren. Es wird auf speziellen Nachrichtenportalen und auf den Seiten der Dienst-Programmierer regelmäßig überprüft ob Sicherheitslücken bekannt sind, und darauf entsprechend reagiert auf dem Vserver. Es wird überprüft, ob die Sicherheits-Cronjobs wie vorgesehen arbeiten. Logdateien werden ausgewertet. Die Häufigkeit der Login-Versuche wird überwacht. Der Trafficverbrauch wird überwacht, damit festgestellt werden kann, ob ein Hacker mit dem Server Spam versendet.

1.4.3. Änderungsmanagement

Änderungen sind nur erforderlich wenn Sicherheitslücken auftauchen oder neue Versionen von Software notwendig werden. In der Regel wird so vorgegangen, wie dies beim Einrichten des VServers war.

1.4.4. Organisation und Durchführung von Wartungsarbeiten

Der Server wird im laufenden Betrieb gewartet, da der Einsatzzweck es nicht rechtfertigt höheren Aufwand für Spiegelungen zu rechtfertigen. Wenn etwas schief geht, dann gibt es immer noch, die diversen Updates. Wenn eine gefährliche Änderung durchgeführt wird, dann wird ggf. vorher gespiegelt oder ein Backup durchgeführt. Ansonsten sind Wartungsarbeiten selten notwendig. Selten muss der Server neu gestartet werden. Einmal pro Jahr muss das Zertifikat des E-Mail-Servers gewechselt werden. Manchmal reicht der Speicherplatz nicht aus, und dann muss untersucht werden, wo sich Löschen lohnt.

1.4.5. Audit

Audits erfolgen selten, da der Aufwand für Audits nicht gerechtfertigt ist, da Ausfälle toleriert werden können. Die Nutzer des Ventrilo-Servers werden befragt, wen sie darauf einladen, damit der Betreiber des Servers einen Überblick hat. Weiterhin gibt es nur in Ausnahmefällen andere Server-Zuständige. Ansonsten gibt es nur einen Verantwortlichen für den Server. Also sind Audits nicht notwendig.

1.5. Aussonderung

Ggf. muss etwas gelöscht werden, wenn der Speicherplatz nicht ausreicht. Dazu wird eine Analyse durchgeführt, wo sich Löschen am ehesten lohnt. Ansonsten könnte auch Ein Serverupgrade durchgeführt werden, wodurch sich der Speicher automatisch erhöht, was vom Hoster durchgeführt wird. Ein Backup davor ist erforderlich. Mit einem Script über einen Cronjob über FTP werden regelmäßig alte Backups gelöscht. Dabei werden unwichtige große Datenbestände eher gelöscht und wichtige kleine Datenmengen werden länger aufbewahrt. So sind alte Konfigurationsdateien noch verfügbar. Man weiß ja nie. Datenträgerentsorgung übernimmt der Hoster. Änderungen an den Berechtigungen sind bisher nicht notwendig gewesen.

1.6. Notfallvorsorge

1.6.1. Konzeption und Organisation der Datensicherung

Die Datensicherung wurde in einem anderen Punkt schon ausführlich beschrieben. Zusammengefasst kann man sagen, dass die Daten dreifach gesichert werden und teilweise automatisiert. Kauf von Backupsoftware war nicht notwendig, da man mit einem kleinen Script große Möglichkeit aussschöpfen kann.

1.6.2. Nutzung von Redundanz zur Erhöhung der Verfügbarkeit

Redundanz gibt es beim Backup, was angebracht sein sollte. Spiegelserver gibt es nicht, da dies durch den Nutzen nicht gerechtfertigt ist. Jedoch existiert ein zweiter Server, da der alte schon 4 Jahre existiert und der neue einen deutlichen Preis-Leistungs-Vorteil darstellt. Migriert wurde schon. Jedoch gibt es für den alten Server eine 12-monatige

Restlaufzeit wegen dem Vertrag,

1.6.3. Umgang mit Sicherheitsvorfällen

Sollten alle Daten ausfallen, so wird das Image zurückgespielt. Sollte sich ein Konfigurationsfehler herausstellen, werden alte Konfigurationsdateien geladen. Sollte Spam durch einen Hacker versendet werden, so wird die Firewall entsprechend konfiguriert und es wird eine Analyse betrieben. Ggf. muss der Server abgeschaltet werden über das Webinterface. Es ist dann durchaus möglich, dass der Server neu aufgesetzt werden muss. Sollte dies der Fall sein, wird aus der Erfahrung gelernt und es werden die Sicherheitsvorkehrungen verschärft.

1.6.4. Erstellen eines Notfallplans

Es existiert kein Notfallplan. Die Schritte, die getätigt werden in einem Notfall sind nicht so viele, dass man sie sich nicht merken könnte oder man nicht aus seinem Erfahrungsschatz bedienen könnte. Sollte man etwas falsch machen, dann ist das auch keine Katastrophe, da der Server nur eine Art Hobby darstellt und in aller Regel eines Notfalls keine finanziellen Schäden entstehen werden. Das Sponsering könnte allerhöchtens aufhören, das Bekannte für den Server tätigen.

1.7. Datenschutz

Die Nutzer des Servers werden darüber informiert, dass wenn sie ihre abgesicherten Daten auf dem Server nicht extra verschlüsseln, der Administrator des Servers diese theoretisch lesen könnte. Der Administrator geht keine weiteren Verpflichtungen ein, die über das Gesetz hinausgehen, Datenschutz zu gewährleisten. Er tut jedoch was in seiner Macht liegt. Der Administrator blockiert nicht das informationelle Selbstbestimmungsrecht auf Integrität, Unversehrtheit und Privatsphäre für andere Nutzer auf seinem Server.

1.8. Kryptokonzept

Eine Public-Key-Infrastructure ist auf dem Server eingerichtet für das Backup-System. Das Passwort ist entsprechend groß gewählt worden, wie dies für asymmetrische Verfahren notwendig ist. Selbstsignierte Zertifikate werden für die SSL und TLS basierten Dienste bereit gestellt.

2. Ausgewählte Einzelbetrachtungen

2.1. Outsourcing

Sollte es erforderlich sein, Ressourcen zu benötigen die der Betreiber nur kurzfristig benötigt, so kann er einen Freund fragen, der wiederum einen kennt, der auch einen privaten Server betreibt.

2.2. Archivierung

Archivierung ist nicht notwendig. Für E-Mail-Archivierung ist der Nutzer verantwortlich. Ein spezieller Archivierungsdienst wird nicht bereit gestellt für Nutzer.

2.3. Höhere Gewalt

Um den Punkt „höhere Gewalt“ kümmert sich der Hoster, da dies in seinem Verantwortungsbereich liegt. Sollte höhere Gewalt beim Administrator wirken, so betrifft das den Server nicht. Im Notfall wurden geographisch entfernte Backups durchgeführt, die wieder eingespielt werden können.

2.4. Infrastruktur

Es gib einen Vserver, einen Backup-FTP-Server, einen neuen VServer bei einem anderen Anbieter/Hoster und es gibt einen Home-PC der diese fernsteuert.

2.5.. Rollen

Es gibt den Administrator und dessen Verwandte und Bekannte Nutzer des Servers und Sponsoren.

3. ausgewählte Dienste

3.1. E-Mail-Server-Umgebung

SMTP wurde grundsätzlich deaktiviert, da dies ein Risiko darstellt, dafür dass Hacker Spamemails versenden könnten. Die Nutzer sind dazu aufgefordert das Webinterface zu nutzen um E-Mails zu versenden. Es wird ein Spamfilter eingesetzt. IMAP ist für SSL oder TLS vorgesehen. Niemand kann von allein eine E-Mail-Adresse einrichten. Der Administrator ist dafür zuständig die E-Mail Adresse freizuschalten, was auch etwas Aufwand für ihn erfordert. (Linux User erstellen, leichte Änderungen an Konfigurationsdateien, Verzeichniserstellung, Konfig-Dateien von Userverzeichnisse bearbeiten). Es wurden Bücher gekauft wie man E-Mail-Server-Software-Zusammenstellungen am Besten konfiguriert, so dass nichts schief geht. Die Anzahl der E-Mails und deren Speicherverbrauch wird ordnerweise in einer Grafik gemonitored, was in einem Webinterface sichtbar ist.

3.2. Webserver

HTTS wurde eingerichtet für diverse Webinterfaces. Verzeichnisse und Domains wurden zugeordnet. PHP wurde nur dann freigeschaltet, wenn es für das Verzeichnis bzw. der Domain erforderlich ist. Der Port für die MySQL Datenbank wurde nicht in der Firewall freigeschaltet. Der Einsatzbereich des Servers ist für eine private Homepage, für ein nicht genutztes Forum, für selbst geschriebene Software und die selbst geschriebene Software von Freunden, zur Monitoring-Überwachung, für eine private Bildergalerie, für eine Internetpräsenz eines Marketing-Spezialisten. Eigene PHP-Scripte werden nicht eingesetzt, was ansonsten ein Sicherheitsrisiko darstellen könnte, jedoch wäre das keine Katastrophe, da die Verzeichnisse getrennt wurden pro Domain.