Anleitung zum Anschluss eines mod_security Sensors an das Frühwarnsystem der Deutschen Telekom AG

Deutsche Telekom AG

Version 1.2
Stand 14.11.2012
Status Final

Öffentlich

Impressum

Herausgeber

Deutsche Telekom AG
Vorstandsbereich Datenschutz, Recht und Compliance
Friedrich-Ebert-Allee 140, 53113 Bonn
Deutschland

Version	Stand	Status
1.2	14.11.2012	Final

Fachlicher Ansprechpartner

Deutsche Telekom AG

Rainer Schmidt
T-Online Allee 1
64295 Darmstadt
Email: cert@telekom.de

Zusammenfassung

Dieses Dokument beschreibt die erforderlichen Konfigurationsschritte, um einen mod_security Sensor (Web Applikation Firewall) mit dem zentralen Early Warning System der Deutschen Telekom AG zu verbinden.

Die zum Betrieb notwendigen Scripte und Konfigurationsdateien sind als Download verfügbar.

Inhaltsverzeichnis

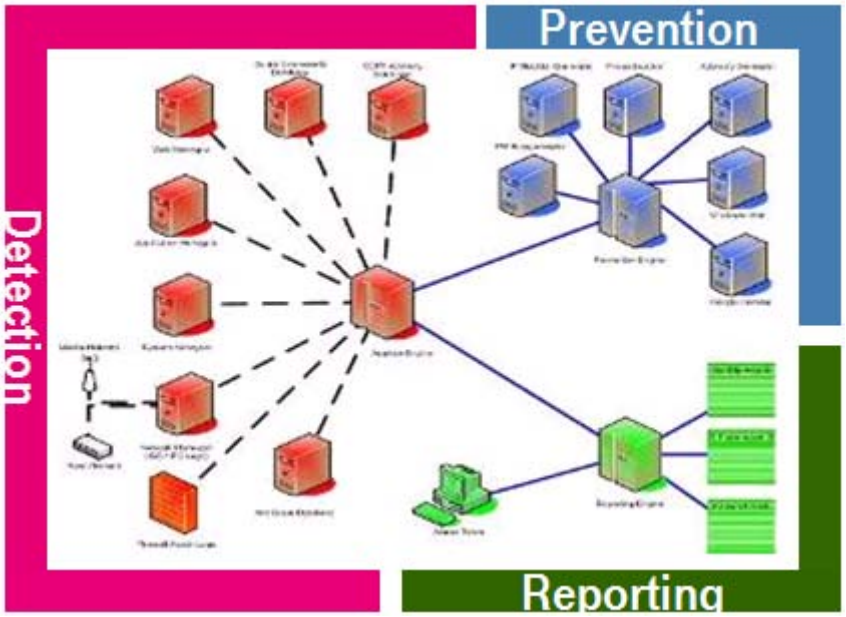
1. Einleitung

Die Deutsche Telekom AG betreibt seit dem Jahr 2010 diverse Honeypots, die in ein zentrales System zur Datenaufbereitung, Datenanalyse und Reporting die jeweiligen Informationen einliefern. Das zentrale System wird im folgenden Text als „Early Warning System“ kurz EWS bezeichnet.
Ein einzelner Honeypot wird im folgenden Text als Peer oder auch als Sensor bezeichnet.

Dieses Dokument beschreibt, wie eine „mod security“ basierte Web Applikation Firewall konfiguriert wird, um als Peer Daten an das EWS zur Auswertung senden zu können.

1.1 Das System im Überblick

Im EWS werden die Daten aller angeschlossenen Peers verdichtet und filterbasiert ausgewertet. Das System unterteilt sich in die drei dargestellten Modulbereiche:



Erkennung / Detection:
Der Modulbereich Detection umfasst alle Peers der Frühwarnung und logisch auch die Komponente, die alle eingehenden Alarmmeldungen entgegennimmt. Diese Komponente ist als Teil des EWS zu sehen.

Prävention / Prevention:
Dieser Modulbereich ist zuständig für das automatisierte Aufbereiten und Bereitstellen u.a. von IP-Blacklisten und einer Malware Ausleitung zu dem Analyseportal Virustotal.

Bei Virustotal handelt es sich um einen frei zugänglichen Dienst, der beliebige Dateien automatisch auf Virenbefall überprüft und die übermittelten Dateien an die angeschlossenen Antivirusfirmen versendet..
Bei der Überprüfung werden mehr als dreißig verschiedene Antiviruslösungen verwendet, so dass eine hohe Verbreitung von neuer, ggf. unbekannter Malware unter den Antivirusfirmen sichergestellt ist.

Reporting:

Eine der Hauptaufgaben des Reportingmoduls ist das Benachrichtigen der als Partner angeschlossenen Abuse[1] Einheiten, sobald die eingestellten Kriterien für einen Alarm erfüllt wurden. Des Weiteren ermöglicht das Reportingmodul die webbasierte Generierung von Lang- und Echtzeit Statistiken zur Sicherheitslage im Internet.

[1] Abuse: Als Abuse Einheit wird die Meldestelle eines Providers bezeichnet, an die sich Dritte bei Verdacht auf Missbrauch von Internetdiensten und Zugangsdaten / Kennungen wenden können.

2 Peer Setup

2.1 mod_security Installationsüberblick

Um die „mod_security“ Web Applikation Firewall als Peer zu integrieren, muss als Vorbereitung das „mod_security2“ Apache Modul Ihrer jeweiligen Distribution installiert werden und die hier beschriebenen Konfigurationsschritte ausgeführt werden.

Ferner ist sicher zu stellen, dass ein SFTP Client auf Ihrem System für die Übertragung der Logdateien installiert ist. Den für die Übertragung (SFTP Login) zu verwendenden Usernamen teilt Ihnen Ihr EWS Ansprechpartner der Deutschen Telekom AG mit. Abschließend ist für die SFTP Übertragung der mod_security Logfiles zum EWS ein SSH-Key Paar (RSA2, 2048 Bit Schlüssellänge) zu erzeugen. Der erzeugte Private Key muss in das Verzeichnis „/opt/app/apache2/etc/private/MOD_SEC_KEY“ kopiert werden, da dieser beim Verbindungsaufbau gemäß der hier vorgeschlagenen Konfiguration dort erwartet wird. Der Public Key hingegen ist an Ihren EWS Ansprechpartner der Deutschen Telekom AG zur Einrichtung auf der zentralen Serverseite zu übergeben.

Anmerkung:
Alle hier beschriebenen Scripte sind unter http://www.sicherheitstacho.eu/download/mod_security/ hinterlegt.

2.1.1 Vorbereitung

Die folgenden Abschnitte basieren beispielhaft auf einer Suse Linux SLES11 Distribution. Das Modul mod_security ist als Suse Paket im SLES11-SDK-SP1-Pool enthalten. Grundsätzlich ist das mod_security Modul ab der Version 2.3 verwendbar. Um zu überprüfen, ob das Modul bereits auf Ihrem Client System installiert ist, kann z.B. mit dem RPM Tool zypper die installierten Pakete abgefragt werden.

Des Weiteren wird das Modul unique_id verwendet, um eine eindeutige Bezeichnung für jede Anfrage bereitzustellen.

Installierte Pakete können unter Suse Linux SLES mit folgendem Befehl abgefragt werden:

zypper lr

Nachfolgend beispielhaft die Ausgabe eines Suse Linux SLES11 System (SP1):

zypper se -s apache2-mod_security2

Loading repository data...
Reading installed packages...

S	Name	Type	Version	Arch	Repository
i	apache2-mod_security2	package	2.5.6-2.10.1	x86_64	SLES11-SDK-SP1-Pool

2.2 mod_security Konfiguration

2.2.1 Verzeichnis(se) anlegen

```
mkdir /etc/apache2/mod_security
chmod 750 /etc/apache2/mod_security
chown root:root /etc/apache2/mod_security

mkdir /var/log/mod_security
chmod 750 /var/log/mod_security
chown www-data:adm /var/log/mod_security
```

2.2.2 Modul(e) aktivieren

```
a2enmod unique_id
a2enmod mod-security
```

In der Webserver Konfigurationsdatei (/etc/apache2/httpd.conf)
(alternativ in /etc/apache2/conf.d/security) ist folgender Abschnitt einzufügen:

```
<IfModule security2_module>
   Include mod_security/*.conf
   Include mod_security/base_rules/*.conf
</IfModule>
```

2.2.3 Ruleset vorbereiten

Im Verzeichnis /etc/apache2/mod_security ist das durch die Deutschen Telekom AG vorgegebene Ruleset mod_security_conf.tgz zu entpacken.

```
cd /etc/apache2/mod_security
tar -xzvf mod_security_conf.tgz
```

Nach dem Entpacken des TAR Files ist die Installation des Moduls abgeschlossen und wird mit einem Restart des Apache Webserver aktiviert.

Restart:

```
apache2ctl restart
```

Nach dem Absenden des Restartbefehls ist die „done“ Meldung abzuwarten.

2.2.4 mod_security Logfiles

Um die Angriffe auf das konfigurierte System aufzuzeichnen, ist es erforderlich, die relevanten Logfiles des Moduls zu konfigurieren. Hierzu ist mit einem Texteditor die Datei mod_security.conf zu öffnen und die Einträge entsprechend dem folgenden Beispiel anzupassen. Hierbei ist auf umgebungsspezifische Verzeichnisstrukturen zu achten.

```
SecDebugLog /var/opt/mod_security/log/debug.log
SecDebugLogLevel 1
SecAuditEngine relevantonly
SecAuditLog /var/opt/mod_security/log/audit.log
SecAuditLogParts ABCFHZ
SecAuditLogType concurrent
SecAuditLogStorageDir /var/opt/mod_security/log
```

2.2.5 mod_security Ausleitung

Die Ausleitung der mod_security Logdaten an das EWS erfolgt per SFTP (ggf. ist hierfür ein separater User einzurichten, der nur für diesen Zweck benutzt wird). Hierzu wird durch einen Cronjob in regelmäßigen Abständen vom Client eine SFTP Verbindung aufgebaut, um die Logdaten zu übertragen. Auf der Clientseite ist ein Script zu erstellen, welches die Vorbereitungen für die Übertragung automatisiert ausführt.

2.2.6 Anlegen des Script zum Rotieren (copy truncate) sowie zum Übertragen der Logfiles (Ausleitung)

In einem beliebigen Verzeichnis ist ein Startscript für das Rotieren und die Übertragung der Logfiles zu erstellen. Ein Vorschlag hierfür wäre:

/opt/app/apache2/bin/sftp_mod_security_logs.sh

Der Befehl

```
touch /opt/app/apache2/bin/sftp_mod_security_logs.sh
```

erstellt die entsprechende Datei.

In die durch den touch Befehl erstellte Datei ist der nachfolgende Scriptvorschlag hinein zu kopieren. Sollten andere Dateinamen und/oder Verzeichnisse gewählt werden, ist in dem Scriptvorschlag darauf zu achten, dass die Anpassungen hier übernommen werden.

```
##############################################################################

#! /bin/bash
HOSTNAME=`hostname`
LDIR=/var/opt/mod_security/log
if [ "$1" = "" ] ; then
HDATUM=`date -d 'now -5 min' '+%Y%m%d-%H' `
DATUM=`date -d 'now -5 min' '+%Y%m%d' `
GESTERN=`date -d 'now -1 day' '+%Y%m%d'`
else
DATUM=$1
fi
if [ -d /var/opt/mod_security/log ] ; then
cd /var/opt/mod_security/log
else
```

```
exit 1
fi
TGZNAME="${HDATUM}_${HOSTNAME}.tgz"
cp audit.log audit-${HDATUM}.log
> audit.log
cp debug.log debug-${HDATUM}.log
> debug.log
tar -czf $TGZNAME ${DATUM}/${HDATUM}* audit-${HDATUM}.log debug-
${HDATUM}.log
KEYFILE=/opt/app/apache2/etc/private/MOD_SEC_KEY
ZIEL='Muster-Peer.de@80.153.226.137:incoming'
PORT=37022
echo -e "put $TGZNAME" | sftp -b - -o Port=$PORT -o IdentityFile=${KEYFILE} ${ZIEL}
> /dev/null 2>&1
#rm $TGZNAME
rm -rf ${DATUM}/${HDATUM}* audit-${HDATUM}.log debug-${HDATUM}.log
rm -rf ${GESTERN}
#############################################################################
```

Nach dem Erstellen des Ausleitungsscripts ist es für eine automatisierte Übertragung erforderlich, einen entsprechenden Cronjob zu erstellen, der das Ausleitungsscript ansteuert.

2.2.7 Ausleitungs Cronjob

Im Verzeichnis /etc/cron.d/ ist die Datei mod_security anzulegen.

```
touch /etc/cron.d/mod_security
```

Anschließend ist die durch den touch Befehl angelegte Datei mit einem Texteditor zu öffnen und durch den folgenden Eintrag fertig zu stellen.

```
01 * * * * root /opt/app/apache2/bin/sftp_mod_security_logs.sh > /dev/null 2>&1
```

Alternativ hierzu ist das Anlegen des Cronjobs auch über den Befehl crontab –e (als root User) möglich.

Der mod_security Cronjob steuert jetzt automatisiert zu jeder vollen Stunde die Rotation und die Ausleitung der Logfiles an das zentrale EWS.

In den ersten Tagen nach Inbetriebnahme des Modules sollte die Logfilegröße beobachtet werden.

3 Linkverzeichnis

http://www.apache.org
http://www.modsecurity.org/
http://de.wikipedia.org/wiki/Malware
http://www.virustotal.com/
http://www.sicherheitstacho.eu/download/sftp_mod_security_logs.sh
http://www.sicherheitstacho.eu/download/mod_security.cron
http://www.sicherheitstacho.eu/download/mod_security_conf.tgz