**BI-S**

Business Integration & Security

**Notes**

|  |  |
| --- | --- |
| Project / Meeting: | Osiris 2.0 |
| Main topic: | Beschreibung Syslog Server |
| Date: | Donnerstag, 20. Februar 2014 |
| Writer: | Jochen Platzgummer |
| Revision: | 1 |
| File location: | documento2 |

## Funktionsweise des Syslog Server

Osiris 2.0 fungiert als zentraler Syslog Server für alle Geräte im Netzwerk, welche in der Lage sind, Syslog Meldungen an Osiris 2.0 zu versenden.

Auf dem Syslog Server müssen die Netzwerke aus welchen Meldungen empfangen werden dürfen, konfiguriert werden.

Auf folgenden Ports werden Syslog Meldungen empfangen:

* 514 UDP
* 514 TCP

Der Syslog Server verarbeitet die empfangenen Meldungen und gibt diese an 2 verschiedene Ausgabekanäle:

* MySQL Datenbank: die Meldungen der letzten 30 Tage werden in einer Datenbank abgelegt und können dadurch besser den berechtigten Benutzern angezeigt werden
* Logfiles: alle Meldungen werden in Logfiles geschrieben. Pro Gerät und Tag wird jeweils ein eigenes Logfile erstellt. Die Logfiles sind in einer Verzeichnisstruktur abgelegt, die folgende Struktur aufweist: <YYYMM>/<YYYYMMDD>/<YYYYMMDD-HOSTNAME-IP>.log. Die Logfiles werden standardmäßig für 180 Tage in dieser Struktur aufbewahrt und dann gelöscht. Diese Retention Time kann an den Kunden angepasst werden.

## Digitale Signatur

Jeden Tag um 0:05 Uhr werden automatisch alle generierten Logfiles des Vortages digital Signiert. Dafür wird GPG ([www.gpg.org](http://www.gpg.org)) verwendet, welches alle Dateien einzeln mit dem privaten Schlüssel signiert und für jede Syslog Datei eine Signaturdatei erstellt. Die digitale Signatur wird mit einer Schlüssellänge von 4096 Bit berechnet.

Es ist nicht möglich, ohne den privaten Key und dessen Passwort die digitale Signatur neu zu berechnen.

Der gesamte Vorgang der digitalen Signierung wird in einer Logdatei festgehalten und kann überprüft werden.

## Prüfung der digitalen Signatur

Das System prüft automatisch mehrmals täglich für alle vorhandenen Logfiles, ob diese noch mit der digitalen Signatur übereinstimmen. Das Logfile und das Signatur File werden mit dem Public Key überprüft und das Ergebnis wiederum in ein Logfile geschrieben, das zur Kontrolle eingesehen werden kann.

Im Monitoring Modul von Osiris 2.0 ist ein Check eingebaut, der automatisch eine Benachrichtigung versendet, sofern die digitale Signatur eines Logfiles nicht mehr mit dem Inhalt des Logfiles übereinstimmt.

Ebenso besteht die Möglichkeit, die digitale Signatur eines Logfile mit einem GPG Frontend manuell zu prüfen (z.B. GPG4win). Der Public Key ist auf dem System abgelegt und frei zugänglich.

## Sicherheit der Logfiles

Die Logfiles werden standardmäßig auf eine Festplatte von Osiris 2.0 geschrieben. Diese Logfiles sind über ein Windows-Share über SAMBA freigegeben. Um auf dieses Share zuzugreifen, werden ein Benutzername und ein Password benötigt, wobei die Freigabe nur READONLY verfügbar ist. Dieses Password kann vom Kunden verändert angepasst werden.

Die Windows-Freigabe kann vom Kunden verwendet werden, um:

* Tägliche Backups der Logfiles und digitalen Signaturen zu erstellen
* Logfiles manuell zu überprüfen
* Den Inhalt der Logfiles zu analysieren

Es besteht keine Möglichkeit, über die Windows-Freigabe höhere Rechte als READONLY zu erlangen.

Optional besteht die Möglichkeit, die Logfiles auf einen WORM-Datenträger zu schreiben, sofern eine solche Hardware vorhanden ist.