SerNet

Auf den Elch gekommen: Logfile-Analyse mit ELK-Server

Fast jedes Programm schreibt sie und fast jeder Admin wäre ohne sie bei der Fehleranalyse aufgeschmissen: die Logfiles. Diese Dateien enthalten viele nützlich Informationen, die normalerweise je nach Bedarf manuell und aufwändig auf dem jeweiligen System ausgewertet werden müssen. Schneller und komfortabler wäre es, die Dateien zentral auf einem Server zu sammeln. Fertige Filter vereinfachen zusätzlich die Analyse.

Mit relativ geringem Aufwand lässt sich eine solche Logfile-Analyse mittels eines ELK-Servers umsetzen, der zudem das Debugging via Unix-Logfiles erleichtert. Der ELK-Server dient dazu, Daten von beliebigen Quellen zu sammeln, zu analysieren, zu durchsuchen und zu visualisieren. Die drei ELK-Komponenten – Elasticsearch, Logstash und Kibana – sind Open-Source-Produkte. Der Zugriff erfolgt in Echtzeit.

Jedes der ELK-Komponenten hat seine eigene Aufgabe und arbeitet dabei eng mit den anderen Komponenten zusammen:

- Logstash sammelt alle benötigten Logfiles und bietet die Möglichkeit über Filterregeln zu entscheiden, ob eine Logzeile benötigt und gespeichert wird oder nicht.
- Elasticsearch ermöglicht die Speicherung der Daten und bietet eine Suche an.
- Kibana bedient die Endnutzer mit grafischen Auswertung der Logs über eine Weboberfläche.

Auf der Gegenseite kommt der Logstash-Forwarder zum Einsatz: Er schiebt die Logs von den anderen Servern direkt in das Logstash auf dem ELK-Server.

Der Vortrag zeigt die Einrichtung eines ELK-Servers in einer DMZ, bestehend aus einem sernet.PORTAL, mit einer OpenBSD Firewall, einem Apache Webserver und einem sernet.GATE das eine iptables-Firewall zur Verfügung stellt.

Anschauliche Schritte führen durch die Grundkonfiguration bis hin zum Erstellen eigener Filter. Standardmäßig ist der ELK-Server darauf ausgelegt Logfiles von Webserver auszuwerten. Dieser Vortrag geht darüber hinaus und zeigt, wie sich mit eigenen Filtern das Setup erweitern lässt, so dass auch verschiedene Firewall-Logs ausgewertet werden können. Dafür habe ich Filterkriterien wie Quell- und Ziel-IP-Adresse und Quell- und Ziel-Ports ergänzt.

Der Sicherheitsaspekt kommt natürlich ebenfalls nicht zu kurz. Ein kurzer Ausflug in die Welt der Zertifikate zeigt wie sich der ELK-Server mithilfe eines Openssl-Zertifikats den anderen Servern gegenüber identifiziert. Der Webserver wird intern über eine passwortgeschütze Seite erreichbar gemacht.Über diese Webseite können individuelle Filter zusammengeklickt und dargestellt werden.
Mithilfe einer aufgezeichneten Browser-Session zeigt der Vortag 'live', an welchen Stellen ein fertig eingerichteter ELK-Server hilfreich ist und wo er an seine Grenzen stößt. Z.B. können schnell IP-Adressen identifiziert werden, die Aufmerksamkeit verlangen, oder Logdaten über eine längere Zeitspanne überwacht werden.
Doch ein Rundum-Paket ist der ELK-Server leider nicht: Er bietet etwa kein Monitoring in dem Sinne, dass automatisch Alarm auslöst, wenn Unregelmäßigkeiten auftreten.

Zum Schluss ist noch Zeit für neue Anregungen. Was könnte man verbessern? Lassen sich auch Windows-Logfiles mit einem ELK-Server auswerten? Welche Log-Informationen können noch Interessant sein?