

Log Daten in der Praxis

Thomas Schreck

Corporate Technology Information & Communication

Definition Logdaten

Incident Response und Loganalyse

Loganalyse

Tools zur Loganalyse

Probleme

Standards

Sonstige Probleme

Was sind Logs ?

Ein **Log** ist ein Event, welcher zu irgendeiner Aktivität auf einen Informationssystem gehört.

Es gibt noch keine verbindliche Definition, MITRE definiert im Standard CEE (<http://cee.mitre.org>) Logdaten folgendermaßen:

“The collection of one or more log entries typically written to a local log file or sent across the network to a server via Syslog, SNMP, or a custom protocol. A log may also be referred to as an audit log or audit trail.”

Logdaten - Terms

- ▶ Events
Eine sichtbare Veränderung der Umgebung, welche über ein Zeitintervall anhält.
- ▶ Log Entry
Ein Eintrag, welcher Details zu einem oder mehreren Events zusammenführt
- ▶ Aggregation
Identifikation von zwei oder mehreren gleich Logeinträgen;
Deduplizierung
- ▶ Correlation
Assoziation von mehreren Events zu einer Gruppe

Incident Response

Incident Response (NIST Incident Response 800-61)

- ▶ Preparation
- ▶ Detection and Analysis
- ▶ Containment, Eradication, and Recovery
- ▶ Post-incident Activity

Logs im Incident Response

- ▶ Preparation
Monitoring von Logdateien
- ▶ Detection
Erkennung einer Infektion oder eines Angriff
- ▶ Analysis
Auswirkung der Infektion oder des Angriffs feststellen
- ▶ Containment, Eradication
Feststellung, wie Angreifer ins System gelangt ist; Forensik
- ▶ Recovery
Feststellung, wann Angriff feststand -> welches Backup
- ▶ Post-incident Activity
Hilfestellung für Management Report; Training von Administratoren

Log Analyse im Incident Response

Quelle von Logs:

- ▶ Betriebssystem (UNIX, Linux)
- ▶ Netzwerkgeräte (Firewalls, Switch)
- ▶ IDS/IPS
- ▶ Applikations Server (Tomcat, IBM Web Sphere)
- ▶ Datenbanken (MS SQL Server, Oracle)
- ▶ Anti-Virus Software

Logs im Incident Response - Aussagekraft

- ▶ Erste Einstufung der Auswirkung eines Angriffs
- ▶ Genauere Bestimmung, wo Schwachstelle ausgenutzt wurde
- ▶ Feststellung, ob andere Systeme befallen wurden

Tools für die Loganalyse

- ▶ Standard Unix Tools (grep, sed, etc.)
- ▶ Perl
- ▶ PyFlag <http://www.pyflag.net>
- ▶ Microsoft Windows Log Parser
- ▶ Microsoft Log Query (ab Vista, Windows 2003)
- ▶ Afterglow <http://afterglow.sourceforge.net> (Log Visualisierung)

Loganalyse in großen Infrastrukturen

Aufbewahrung von Logdateien

- ▶ Vorfälle werden erst Wochen später bekannt
- ▶ Compliance Richtlinien verlangen sichere Aufbewahrung

- ▶ Sinnvolle Zeiträume
 - ▶ Firewall in DMZ: 30 Tage
 - ▶ interne Server: 60 Tage
 - ▶ kritische Infrastruktur: 90 Tage
- ▶ Logdaten sollten desweiteren langfristig archiviert werden
- ▶ Verschlüsselte Aufbewahrung und Archivierung

Loganalyse in großen Infrastrukturen

Monitoring von Logdateien

- ▶ Logging sinnlos wenn Logdateien nicht ausgewertet werden
- ▶ Toolbasierte Auswertung sinnvoll
- ▶ Tools sollten Administrator benachrichtigen (per Email oder Anruf)

Loganalyse in großen Infrastrukturen

- ▶ Zentraler Logserver oft sinnvoll
- ▶ Logauswertung findet auf Logserver statt; Entlastung der Server
- ▶ Sicherstellung der sicheren Übertragung notwendig (z.B. durch Verwendung von TLS)
- ▶ einige Tools zur zentralen Logauswertung:
 - ▶ logcheck <http://www.logcheck.org>
 - ▶ swatch <http://swatch.sourceforge.org>

Fehlende Standards



```
<132>EvntSLog:6388: [AUF] Wed Oct 10 10:57:15 2001: newfoundland/Security (675) - "Pre-authent.  
ministrator User ID: %S-1-5-21-776561741-2052111302-1417001333-500 Service Name: krbtgt/LAB Pre  
Authentication Type: 0x2 Failure Code: 0x18 Client Address: 127.0.0.1 "
```



```
Apr 18 18:05:57 newhamphshire unix_chkpwd[10682]: password check failed for user (ts)
```



```
00:03:34:%SEC_LOGIN-4-LOGIN_FAILED:Login failed [user:ts] [Source:192.168.10.2] [localport:23]  
son:Invalid login] at 20:54:42 UTC Sat Apr 18 2009
```

Standards - MITRE CEE

- ▶ unterstützt von viele Unternehmen (Microsoft, Tenable) und U.S. Regierung

- ▶ Standardisierung von:
 - ▶ Common Event Taxonomy
 - ▶ Common Log Syntax
 - ▶ Common Log Transport
 - ▶ Common Event Log Recommendations

Standards - IETF / XDAS

- ▶ IETF Syslog Working Group
 - ▶ RFC 5424 verbessert Syslog um strukturierte Eventdaten
 - ▶ RFC 5425 beschreibt den Transport von Syslog Nachrichten über TLS
 - ▶ RFC 5426 beschreibt den Transport über UDP
- ▶ XDAS - X/OPEN Distributed Audit Standard
 - ▶ offene Arbeitsgruppe mit Herstellern und Benutzerorganisationen
 - ▶ Zusammenarbeit mit CEE

Weitere Probleme von Logdaten

- ▶ steigende Menge von Logdaten
- ▶ Logdateien werden nur kurzzeitig aufbewahrt
- ▶ Loglevel oft unterschiedlich eingestellt

Zusammenfassung

- ▶ Logdatenasuwertung enorm wichtig für Incident Handling
- ▶ Gibt immer noch Probleme
- ▶ Mögliche Hilfe durch Standardisierung
- ▶ Logdaten-Analyse als notwendiger Forschungsgegenstand

Contact

Thomas Schreck

Siemens AG

Corporate Technology Information & Communication

Corporate Technology

Telephone: +49 (89) 636 411 65

E-mail: t.schreck@siemens.com