

SEMINARARBEIT

Service und Security-Monitoring

Seminar:
Aufbereitung und Auswertung komplexer Daten

Martin Steinbach
Juni 2018

**Universität
Rostock**



Traditio et Innovatio

UNIVERSITÄT ROSTOCK

Exzerpt

Service-Monitoring ist eine wichtige Voraussetzung, um eine zuverlässige IT-Infrastruktur zu betreiben. Monitoring ist auch geeignet, um IT-Sicherheitskritische Ereignisse zu identifizieren und adäquat auf diese zu reagieren. Die vorliegende Arbeit bietet eine Einführung in die Thematik der Dienstüberwachung und stellt die beiden Überwachungsformen Aktive- und Passive-Überwachung vor. Es wird zudem die Frage geklärt, warum Service-Monitoring auch gleichzeitig Security-Monitoring ist. Anschließend wird anhand eines existierenden Prototypen aufgezeigt, wie eine Korrelation von Ereignissen in Cloud-Umgebungen realisiert werden kann. In Abschnitt vier wird kurz auf eine schon verfügbare Lösung im Bereich der Passiven-Überwachung vorgestellt.

Inhaltsverzeichnis

1	Einführung	3
1.1	Service monitoring und Security monitoring	3
1.2	Motive	4
1.2.1	Behörden mit Überwachungsauftrag	5
1.3	Überwachungsformen	5
1.3.1	Aktive Überwachung	5
1.3.2	Passive Überwachung	6
2	Logkorrelation in Cloud-Umgebungen	8
3	Weitere Lösungen zur passiven Überwachung	9
4	Ausblick	10
5	Fazit	11

1 Einführung

In diesem Kapitel wird anhand der IT-Sicherheitsziele aufgezeigt, dass man unter dem Servicemonitoring auch immer den Begriff Securitymonitoring verstehen kann. Auch soll darauf hingewiesen werden, dass der Ausdruck Überwachung im ganzen Dokument mit der Bedeutung: Aufsicht oder Monitoring belegt wird um eine klare Abgrenzung zur zweiten Bedeutung: Observation, Beschattung (engl. surveillance) zu erlangen.

1.1 Servicemonitoring und Securitymonitoring

Die Überwachung von Diensten ist mittlerweile ein integraler Bestandteil der Infrastruktur jedes IT-Diensteanbieters geworden. Neben der einfachen Erfassung und der (z.B. grafischen) Aufarbeitung dieser Messgrößen, werden die erfassten Daten zunehmend analysiert und es wird versucht Muster zu erkennen. Dieser Vorgang wird auch als *BigData* bezeichnet. Diese Daten werden auch verstärkt zur Sicherheitsanalyse herangezogen. Daher stellt sich die Frage, ob Securitymonitoring äquivalent zum Servicemonitoring-Begriff ist. Um es vorweg zunehmen, ja, denn es kommt ausschließlich auf die Fragestellung an, die ich mit den erfassten Daten klären möchte. Im Folgenden werden die drei Hauptziele der IT-Sicherheit aufgeschlüsselt und in Beziehung mit dem Servicemonitoring gebracht.

Vertraulichkeit

Das Ziel der Vertraulichkeit sagt aus, dass der Zugriff auf Daten ausschließlich von autorisierten Nutzern erfolgen darf, egal in welchem Modus. Erreicht wird das Ziel zum Beispiel durch Zugriffsrechte¹ und vor allem durch Verschlüsselung.

Die Frage, ob sich Vertraulichkeit überwachen lässt, ist nur teilweise beantwortbar. Stellt man sich ein System vor auf dem ein nicht autorisierter Nutzer Zugriff auf Informationen erlangt, so ist dies messbar und es ist möglich eine Meldung zu generieren (z.B. eine Log-Meldung oder eine Nachricht an Verantwortliche). Wird jedoch ein autorisiertes Konto durch einen nicht autorisierten Nutzer kompromittiert, gestaltet sich die Entdeckung dieses Ereignisses schwieriger. Ob es sich in diesem Fall um einen erlaubten Zugriff des tatsächlichen Nutzers oder einen nicht erlaubten Zugriff handelt kann nur unter der Zuhilfenahme weiterer Information geklärt werden, zum Beispiel könnte die Quelle (Kapitel 3), von der aus sich der Nutzer Zugriff verschafft hat, miteinbezogen werden. Auch die Korrelation mit Zeitdaten, an denen sich der zugriffsberechtigte Nutzer einloggt, können zur Klärung hinzugezogen werden.

¹Unabhängig von der Umsetzungsstrategie, wie z.B. Mandatory Access Control (MAC) oder Discretionary Access Control (DAC)

Verfügbarkeit

Ob ein Dienst Verfügbar ist, wird dadurch geklärt, ob der Zugriff auf Informationen innerhalb eines gewissen Zeitraums erfolgreich ist.

Die Verfügbarkeit gleicht damit auch der grundlegenden Fragestellung des Servicemonitorings. Ist ein gewisser Dienst erreichbar und ist dessen Abarbeitungsgeschwindigkeit in einem vorgegebenem Rahmen?

Integrität

Integrität wird erreicht, wenn eine Änderung der Daten nicht unbemerkt geschieht. Es soll somit ein Indikator für die Veränderung existieren. Um dieses Ziel zu erreichen werden Verfahren wie digitale Signatur und Hashes verwendet.

Auch das Ziel der Integrität lässt sich kontrollieren, dazu finden die selben Maßnahmen Verwendung wie in der IT-Sicherheit. Es lassen sich zum Beispiel auf regelmäßiger Basis Daten prüfen, von denen man vorher mit einem kryptografisch sicheren Verfahren ein Hash errechnet hat. Ändert sich die Hashsumme, ohne das ein Zugriff auf die Daten genehmigt wurde, ist dies ein Integritätsverlust.

Zusammengefasst ist Monitoring von IT-Infrastruktur immer auch gleich Securitymonitoring. Mithilfe eines lückenlos ausgerollten Monitorings ist es demnach möglich zu Beweisen zu welchem Zeitpunkt ein gewisser Dienst welchen Zustand hatte.

1.2 Motive

Der Grund warum eine dauerhafte Überwachung von Infrastruktur und den darauf aufbauenden Diensten keine Option sondern obligatorisch sein sollte, ist recht simpel zu erörtern. Allein die in [1, 461] berichteten Zahlen sprechen für sich. 90 % aller Firmen waren schon Cyberattacken ausgesetzt, 80 % davon haben dadurch erhebliche finanzielle Einbußen erlitten. Aktuell werden innerhalb eines Jahres 86 % der großen nordamerikanischen Unternehmen Opfer von Cyberattacken und der Diebstahl des geistigen Eigentums hat sich in den Jahren 2011-2015 verdoppelt.

Auch der aktuelle, jährlich veröffentlichte Lagebericht zur nationalen IT-Sicherheit des Bundesamtes für Sicherheit in Informationstechnik (BSI) [2, 12] berichtet von einer Cyberattacke auf eine großen deutschen Industriekonzerne. Etwa zwei Monate konnten unbemerkt Daten aus weltweit verteilten Standorten in Richtung Südostasien abfließen bevor der Vorfall detektiert wurde. Aus den Empfehlungen des BSI lässt sich schließen, dass neben einer ungünstigen Netzwerksegmentierung auch mangelhaftes Monitoring der Grund für die späte Erkennung war. In diesem Zusammenhang ist auch der Angriff auf den Deutschen Bundestag im Jahr 2015 erwähnenswert, da auch in diesem Fall einige Wochen lang unbemerkt Daten abfließen konnten und das Ziel hoheitliches war, Technologietransfer und finanzielle Absichten also eine untergeordnete Rolle gespielt haben.

1.2.1 Behörden mit Überwachungsauftrag

Aufgrund der zuvor dargestellten Gründe, wurden in den letzten Jahren eine Reihe an neuen Behörden in der Bundesrepublik Deutschland gegründet, deren Auftrag die Überwachung (Monitoring) wichtiger Infrastrukturen innerhalb der Grenzen der Bundesrepublik ist. Zum Einen das Nationale Cyber-Abwehrzentrum (NCAZ) [3] mit Sitz in Bonn. Die Aufgabe des NCAZ ist die Koordinierung von Abwehrmaßnahmen und Informationskonsolidierung über den Aufbau von rein ziviler Infrastruktur über mehrere Behörden hinweg. Das Nationale IT-Lagezentrum [4] überwacht hingegen aktiv die Regierungsnetze und erstellt monatliche Lageberichte. Auf militärischer Seite übernimmt der Bundeswehr-Organisationsbereich Cyber- und Informationsraum (CIR) diese Aufgabe.

1.3 Überwachungsformen

Es lassen sich zwei verschiedene Überwachungsformen identifizieren die im Folgenden vorgestellt werden.

1.3.1 Aktive Überwachung

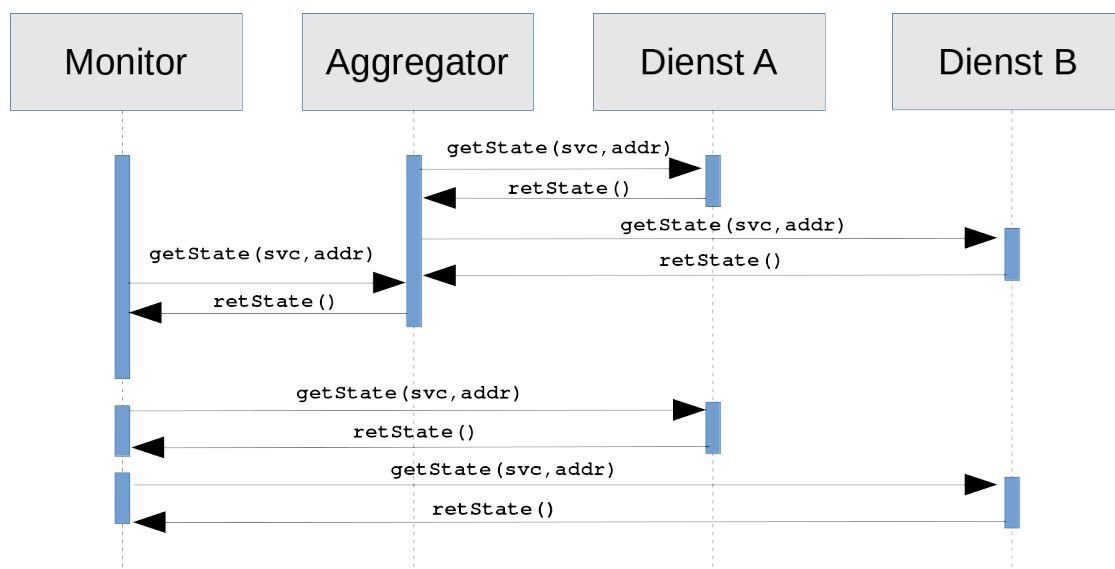


Abbildung 1.1: Sequenzdiagramm: Aktive Überwachung

Obiges Sequenzdiagramm zeigt schematisch den Ablauf aktiver Überwachung. *Monitor* ist die zentrale Instanz auf der alle zu überwachenden Informationen gesammelt, aufbereitet und ausgegeben werden. Jedoch muss der *Monitor* nicht alle Information sammeln, es können auch hierarchisch untergeordnete *Aggregatoren* existieren, welche ebenfalls Informationen von verschiedenen Diensten erheben. Diese *Aggregatoren* können aus Leistungsgründen vor einen *Monitor* geschaltet werden, um die Anzahl an abzufragenden Diensten für den *Monitor* zu verringern. In diesem Fall bereitet bereits der *Aggregator* die Daten auf und der *Monitor* fragt nur noch die schon konsolidierten Informationen ab. Aber auch Segmentierungen von Infrastruktur können diesen Aufbau notwendig machen, wenn z.B. *Monitor* *Dienst A* und *Dienst B* nicht direkt erreichen kann oder darf. Zur Klassifizierung von Ereignissen werden in Überwachungslösungen² oft verschiedene Status verwendet, dies dient hauptsächlich zum schnelleren Verständnis

²zum Beispiel: Nagios, Icinga

für die auswertende Person. Aus diesem Grund wurden in Abbildung 1.1 die Bezeichnungen für der Abfragefunktionen `getState()` und `reState()` gewählt. Mögliche Status für die Rückgabe sind folgende:

Statusbezeichnung	Statusbeschreibung
OK	Dienst läuft innerhalb normaler Parameter.
WARNING	Die (zuvor definierte) Warnschwelle wurde überschritten.
CRITICAL	Die kritische Schwelle wurde überschritten oder es gab einen Timeout.
UNKNOWN	Ein undefinierter Wert wurde an <i>Monitor</i> übermittelt.

Tabelle 1.1: Statusübersicht

Mithilfe der Techniken zur aktiven Überwachung lassen sich zwei Klassen überwachbarer Dienste identifizieren: Die Betriebssystemabhängigen und die Betriebssystemunabhängigen Dienste.

Dienst / Entität	Beispiel
Betriebssystemabhängig	
Auslastung	wie viel CPU-Zeit benötigt ein bestimmter Prozess/das ganze System
Speicher	Speicherauslastung des Systems/ Belegung persistenter Speicher
Prozesse	läuft ein bestimmter Prozess/ wie viele Prozesse eines Namens laufen
Datendurchsatz	wie viele Bytes passieren ein Interface, Anzahl an <i>paket-drops, rejects</i>
Audit	wurden Zugriffsregeln verletzt/ welcher Nutzer hat auf Datei X zugegriffen
Betriebssystemunabhängig	
ICMP	Netzwerkschnittstelle/ System erreichbar, <i>round trip time</i>
TCP/UDP	ist bestimmter <i>port</i> erreichbar
Anwendungsprotokolle	Login möglich / Referenzdaten abrufbar / Rückgabewerte Testroutinen
SNMP	Abfrage beliebiger Kenngrößen

Tabelle 1.2: Beispiele für aktive Überwachung

1.3.2 Passive Überwachung

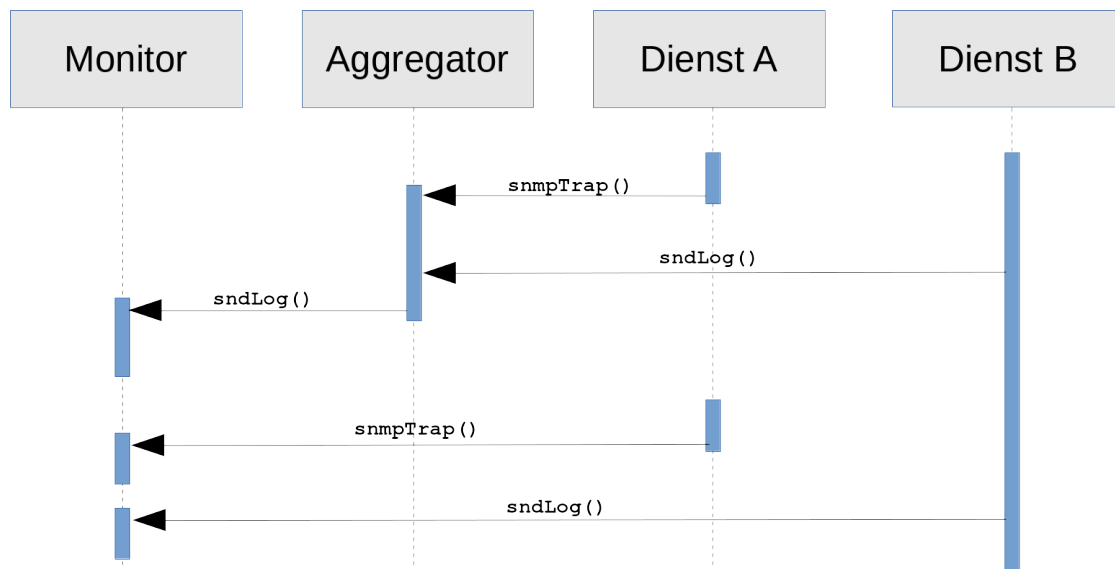


Abbildung 1.2: Passive Überwachung

2 Logkorrelation in Cloud-Umgebungen

3 Weitere Lösungen zur passiven Überwachung

4 Ausblick

5 Fazit

Literaturverzeichnis

- [1] Guillermo Francia, Levent Ertaul, Luis Hernandez Encinas, and Eman El-Sheikh. *Computer and Network Security Essentials*. Springer, 2017.
- [2] Bundesamt für Sicherheit in der Informationstechnik (BSI). Die lage der it-sicherheit in deutschland 2017. Technical report, Bundesamt für Sicherheit in der Informationstechnik (BSI).
- [3] Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html. 03.06.2018.
- [4] Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Lagezentrum/itlagezentrum_node.html. 03.06.2018.

Abbildungsverzeichnis

1.1	Sequenzdiagramm: Aktive Überwachung	5
1.2	Passive Überwachung	7