Seminararbeit

Service und Security-Monitoring

Seminar: Aufbereitung und Auswertung komplexer Daten

Martin Steinbach
Juni 2018

universität Rostock

Exzerpt

Servicemonitoring ist eine wichtige Voraussetzung um eine zuverlässige IT-Infrastruktur zu betreiben. Monitoring ist auch geeigent 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 Servicemonitoring auch gleichzeitig Securitymonitoring 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 Lösungen im Bereich der Passiven-Überwachung vorgestellt.

Inhaltsverzeichnis

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 erfasste 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 Zugriffsrechte[1] 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.

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?

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

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.

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 Industriekonzern. 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.

1.2.1 Gremien

1.3 Formen der 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).

Abbildungsverzeichnis