Security Intelligence als Säule des modernen Datenschutzes

White Paper
der Experton Group AG

November 2014

Copyright

Die vorliegende Analyse wurde von der Experton Group, im Auftrag von LogRhythm, erstellt. Trotz der gewissenhaften und mit größter Sorgfalt ermittelten Informationen und Daten kann für deren Vollständigkeit und Richtigkeit keine Garantie übernommen werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

Inhalt

1 Management Summary

Im Rahmen ihrer Analysen des Security-Marktes in Deutschland hat sich die Experton Group eine Vielzahl von Lösungen angesehen, die sicherheitsrelevante Informationen sammeln, auswerten und Maßnahmen der Angriffsabwehr initiieren können.

Darunter sind SIEM-Anwendungen (Security Informationen and Event Management), diejenigen Lösungen, die Sicherheitsinformationen mittels Big-Data-Analyse in nahezu Echtzeit auswerten und damit die kritische Zeitspanne zwischen Angriff, Angriffserkennung und Abwehr drastisch verkürzen. Durch die schnelle Erkennung von Attacken und möglicher Datenlecks trägt eine solche Security Intelligence Lösung maßgeblich zur Verbesserung der Datensicherheit bei.

Ein Fokus der Experton Group-Analysen lag dabei auch auf der datenschutzgerechten Auswertung der Nutzerdaten, da Security Intelligence in jeder Hinsicht ein Vorteil für den Datenschutz sein soll und auch sein kann.

Dieses White Paper stellt Ergebnisse aus diesen Untersuchungen dar und beleuchtet dabei, wie die Security Intelligence Plattform von LogRhythm den Datenschutz wesentlich fördern kann und damit eine zentrale Forderung des deutschsprachigen Marktes an Informationssicherheit erfüllt.

Die Experton Group stellt im Ergebnis der vorliegenden Untersuchung fest, dass die Security Intelligence Plattform von LogRhythm

- den Datenschutz und die Datensicherheit fördert, indem die Datenschutzkontrolle deutlich unterstützt wird und mögliche Datenpannen in wesentlich kürzerer Zeit erkannt und in ihren Auswirkungen minimiert werden können, und
- spezielle Datenschutzfunktionen (Data Masking, Administratorkontrolle, Case Management) aufweist, die es ermöglichen, die für die Risikobewertung und Gefährdungserkennung wichtigen Nutzungsdaten so auszuwerten, dass ohne entsprechende Berechtigung kein Personenbezug zu den sicherheitsrelevanten Informationen mehr hergestellt werden kann. Erst im konkreten Verdachtsfall findet die Identifizierung der konkreten Nutzer statt, wie es der deutsche Datenschutz vorsieht.

Ismaning, im November 2014

Oliver Schonschek, Research Fellow

Experton Group AG

2 Security Intelligence ist Grundlage eines guten Datenschutzes

Gerade für Unternehmen im deutschsprachigen Raum hat der Schutz personenbezogener Daten eine hohe Priorität. Für die Optimierung von Datenschutz und Datensicherheit ist es allerdings wichtig, zu verstehen, dass die dafür notwendige Sammlung und Analyse sicherheitsrelevanter Nutzerdaten kein Risiko für den Datenschutz darstellt, sondern vielmehr eine wesentliche Grundlage des modernen Datenschutzes ist.

Der Schutz personenbezogener Daten erfordert ein hohes Maß an Transparenz in der Datenverarbeitung. Bei der Datenschutzkontrolle müssen Benutzeranmeldungen und Datenzugriffe nachvollzogen werden können. Die sogenannte Eingabekontrolle als Forderung des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) verlangt, dass festgestellt werden kann, **welcher Nutzer bestimmte Daten angelegt, geändert oder gelöscht hat.** Die Datensicherheit kann nicht zuverlässig gewährleistet werden, wenn eine fehlende Verschlüsselung oder ein ausbleibendes Backup nicht auf Geräteebene und damit meist auch auf Nutzerebene protokolliert und gemeldet wird.

Eine Security Intelligence Plattform wie die von LogRhythm sorgt für diese notwendige Transparenz. Sie bildet mit ihren Analysen und Berichten die Basis der erforderlichen Datenschutznachweise und Dokumentationen, die die geplante EU-Datenschutz-Grundverordnung in einem eigenen Artikel ausdrücklich fordern wird.

Security Intelligence Plattformen sind auch elementar zur Erkennung und Vermeidung von Datenverlust und ungewolltem Datenabfluss (Data Loss Prevention). Die integrierte Überwachung von Datenzugriffen dient der Eingabekontrolle und dem Schutz der Datenintegrität.

Die Alarmierung bei Angriffen und Datenpannen durch die Security Intelligence Plattform ist zudem eine Basis für die gesetzlich vorgeschriebene Meldung von Sicherheitsvorfällen, die unter bestimmten Umständen nach § 42a BDSG erfolgen muss. Ohne Security Intelligence werden Unternehmen komplexe Angriffe wie Advanced Persistent Threats (APT) viel zu spät erkennen, um den möglichen Schaden minimieren und den gesetzlichen Meldepflichten nachkommen zu können.

Wie eine Security Intelligence Plattform bei der Erkennung von Angriffsversuchen konkret hilft, zeigt zum Beispiel die „User Behavior Anomaly Detection“, die LogRhythm bietet:

- Viele Attacken beginnen mit dem Diebstahl von Zugangsdaten. Die Angreifer spähen zum Beispiel Benutzernamen und Passwort eines legitimen Nutzers aus und missbrauchen dessen Identität und Systemberechtigungen für ihre weiteren digitalen Beutezüge.
- Die Erkennung eines solchen Angriffs mit herkömmlichen Mittel der IT-Sicherheit ist durch den Identitätsmissbrauch sehr schwierig. Da sich der Datendieb mit der Identität eines legitimen Nutzers anmeldet, reicht die normale Zugangs- und Zugriffskontrolle nicht aus.
- Dies fällt nur auf, wenn man sich die Aktivitäten des angeblich legitimen Nutzers genauer ansieht, denn hier gibt es meist deutliche Abweichungen zu den sonst üblichen Nutzeraktivitäten, zum Beispiel Zugriffe auf Daten in einer ungewöhnlich hohen Anzahl.
- Eine Security Intelligence Lösung kann das ungewöhnliche Nutzerhalten aufdecken, indem die herkömmlichen Aktivitäten eines Nutzers ausgewertet und mit den jeweils neuen Aktionen des Nutzers verglichen werden. Abweichungen ab einem bestimmten Grad können als Alarmzeichen für einen Identitätsmissbrauch und Angriff gewertet werden.

Die Analyse des Nutzerverhaltens hilft somit bei der Erkennung von Identitäts- und Datendiebstahl. Mit einer Auswertung auf Nutzerebene wird allerdings ein weiterer Bereich des Datenschutzes berührt.

Wie das nächste Kapitel zeigt, sollten Security Intelligence Lösungen deshalb spezielle Datenschutzfunktionen aufweisen.

3 Datenschutz-Vorgaben für Security Intelligence Lösungen

Sicherheitsrelevante Informationen stammen von einer Vielzahl von Datenquellen, seien es Server, Endgeräte, Betriebssysteme, Anwendungen, Cloud-Dienste oder auch spezielle IT-Sicherheitslösungen wie Firewall und Anti-Malware-Lösungen. Alleine schon diese Vielfalt macht deutlich, dass Sicherheitsinformationen einen großen Datenumfang annehmen können und ein Beispiel für Big Data sind.

Mit den Sicherheitsinformationen können Nutzerdaten verbunden sein, die unter die Vorgaben des Datenschutzes fallen. Das Bundesdatenschutzgesetz (BDSG) geht in den nachfolgend dargestellten Paragraphen speziell auf diesen Fall ein:

Besondere Zweckbindung (§ 31 BDSG)

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

Gerade IT- und Sicherheitsadministratoren sind theoretisch in der Lage, sicherheitsrelevante Protokolle zu anderen Zwecken auszuwerten, zum Beispiel für sogenannte Verhaltens- und Leistungskontrollen oder für eine anlasslose Mitarbeiterüberwachung (Screening). Solche Kontrollen unterliegen aber den Vorgaben des Datenschutzes und der Mitbestimmung durch die Interessenvertretung im Unternehmen oder in der Behörde.

Aus Sicht des Datenschutzes benötigen SIEM-Lösungen und Lösungen für Security Intelligence deshalb geeignete Funktionen, um die missbräuchliche Auswertung von Nutzerdaten zu verhindern. Entsprechende Maßnahmen sind die Administratorkontrolle (Vier-Augen-Prinzip, Trennung der Aufgaben von Administratoren), eine Beschränkung der Auswertungen und Protokollzugriffe auf konkrete Anlässe (Case Management) sowie Verfahren der Datensparsamkeit und Datenvermeidung, insbesondere die Anonymisierung und Pseudonymisierung der Nutzerdaten innerhalb der Sicherheitsinformationen. Die Aufdeckung der konkreten Nutzeridentität muss dem konkreten, begründeten Verdachtsfall vorbehalten sein - so will es der Datenschutz (§ 32 Abs. 1 BDSG).

Das Beispiel der Security Intelligence Plattform von LogRhythm zeigt, dass die Analyse sicherheitsrelevanter Nutzungsdaten sehr gut mit den in Deutschland geltenden Datenschutzvorgaben in Übereinstimmung gebracht werden können.

1. LogRhythm bietet Funktionen zur **Datenmaskierung** (Data Masking) für personenbezogene Daten innerhalb von Sicherheitsinformationen. Nutzerdaten werden automatisch in den Sicherheitsprotokollen erkannt und durch Pseudonyme ersetzt, die erst im konkreten Verdachtsfall und mit entsprechenden Berechtigungen einer Person zugeordnet werden können.

2. Um mögliche Datenschutzverstöße durch besonders privilegierte Nutzer wie Sicherheitsadministratoren zu verhindern, sieht LogRhythm zudem **geteilte Rollen, Berechtigungen und Aufgaben** für die einzelnen Administratoren vor. Damit lässt sich das vom Datenschutz **geforderte Vier-Augen-Prinzip** technisch ohne großen Aufwand umsetzen.

3. Mit der Funktion **Case Management** ist es bei der Lösung von LogRhythm zudem möglich, die Auswertungen und Zugriffe auf die Sicherheitsprotokolle ganz konkret auf bestimmte Auffälligkeiten und Vorkommnisse zu beschränken. Ein Screening über alle Nutzerdaten hinweg ist somit weder notwendig noch ohne weiteres technisch möglich, wenn einem Administrator mittels Case Management nur bestimmte Fälle zur Untersuchung zugewiesen werden.

4 Analyse der Security Intelligence Plattform von LogRhythm

LogRhythm bietet mit seiner Security Intelligence Plattform eine leistungsstarke und außergewöhnliche Lösung zur Aufdeckung von Angriffen, insbesondere auch von den zunehmend auftretenden Advanced Persistent Threats (APT), die die Fähigkeiten zur Erkennung von Bedrohungen klassischer IT-Sicherheitslösungen deutlich übersteigt.

Zu den besonderen Funktionen der Security Intelligence Plattform von LogRhythm gehören:

- Überwachung der Dateiintegrität durch die Kontrolle von Zugriffen und Dateieigenschaften
- Möglichkeiten zur forensischen Datenanalyse, um Einbruchsversuche in IT-Systeme aufklären zu können
- Mustererkennung und Erkennung von Anomalien bei Nutzeraktivitäten, im Host- und Netzwerkverhalten, um bösartige Aktivitäten von normalen IT-Abläufen so genau wie möglich unterscheiden zu können
- Fähigkeit, große Datenmengen in kurzer Zeit zu analysieren (Big-Data-Analyse)
- Visuelle, sehr übersichtliche Darstellung der Berichte mit einem hohen Grad an Individualisierbarkeit
- Integrierte Funktionen zur automatisierten Reaktion auf erkannte Gefahren (SmartResponse)
- Integriertes Case Management bei der Bearbeitung von Sicherheitswarnungen, dadurch Trennung der Aufgaben und Berechtigungen von Sicherheitsadministratoren und Sicherheitsanalysten
- Unterstützung bei Einhaltung und entsprechender Dokumentation für zahlreiche Compliance-Vorgaben wie PCI, SOX, ISO27001

Die Security Intelligence Plattform von LogRhythm ist zudem Teil eines Threat Intelligence Ecosystems, einer Austauschplattform von Anbietern im Bereich Bedrohungsintelligenz (Threat Intelligence). Diese Plattform erweitert die bereits vorhandenen, sehr umfangreichen Datenquellen von LogRhythm zur Erkennung und Bewertung von Datenrisiken und Attacken.

Analyst-Statement (Oliver Schonschek, Experton Group Research Fellow)

Vorteile der LogRhythm-Lösung für Anwender

„Die Attacken auf die IT von Unternehmen und Behörden werden immer raffinierter. Herkömmliche Abwehrstrategien bieten hier schon lange keinen ausreichenden Schutz mehr. Mit intelligenten Sicherheitslösungen wie der Security Intelligence Plattform von LogRhythm lassen sich auch gut getarnte Angriffe erkennen, indem vielfältige Sicherheitsinformationen ausgewertet und Anomalien aufgespürt werden. Die Zeit zwischen einem Angriff und der Aufdeckung der Bedrohung kann durch Security Intelligence drastisch verkürzt werden. Dabei achtet die Lösung von LogRhythm darauf, dass Nutzerdaten dem strengen deutschen Datenschutz entsprechend behandelt und vor Missbrauch geschützt werden. Security Intelligence wird so zu einer tragenden Säule für den modernen Datenschutz.“

5 Über Experton Group

Experton Group ist ein führendes IT-Research- und Beratungsunternehmen. Mit europaweit 80 erfahrenen Advisors unterstützen wir mittelständische und große Anwenderunternehmen bei der strategischen Planung und Umsetzung ihrer IT-Strategien. Zudem unterstützt Experton Group IT-Anbieter in Strategie-, Marketing- und Wettbewerbsfragen.

http://www.experton-group.de/

Autor:

Oliver Schonschek (Lead) oliver.schonschek@experton-group.com

Version 1.0 (November 2014)

Impressum

Experton Group AG

Carl-Zeiss-Ring 4

D - 85737 Ismaning

Vorstand: Jürgen Brettel (Vorsitzender), Andreas Zilch

Aufsichtsratsvorsitzender: Wolfgang Stübich

Amtsgericht München HRB 158568

Bildquelle: Fotolia_44080741_M