Notes zu Quellen

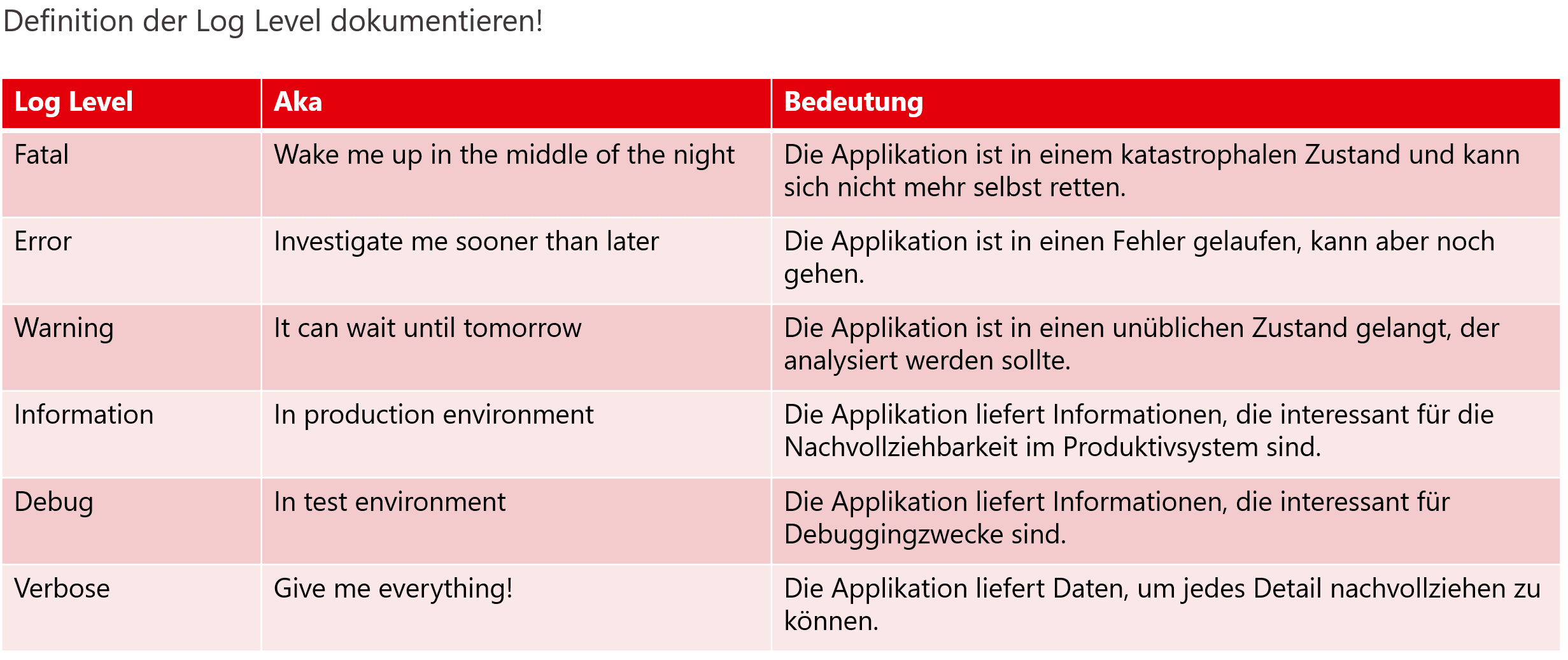
# Logging:

## Quelle: ip-insider

* Automatisches Protokollieren von Statusinformationen und Ereignissen
* Während Betrieb oder Ausführung von Systemen und Prozessen
* Fehlermeldungen, Systemnachrichten, Statusmeldungen, etc.
* In Logdateien sind Ergebnisse mit Zeitstempel und i.d.R. chronologisch
* Meist in Größe beschränkt, sodass nach gewisser Zeit überschrieben wird
* Log- und Event-Management hat die Aufgabe, die Log-Daten zu sammeln, aggregieren und speichern, sodass die Daten genutzt werden können, um Probleme zu identifizieren, Prozesse nachzuvollziehen, Systemleistung zu optimieren oder Cyberangriffe und andere Sicherheitsvorfälle zu erkennen und abzuwehren
* Teilweise gesetzlich verpflichtend Logs zu schreiben, bspw. Nachvollziehbarkeit von Transaktionen
* Sammeln der Logdaten erfolgt aktiv oder passiv: entweder Systeme senden Daten an Management oder Management holt sich Daten bei Systemen ab
* Standards und Protokolle: Syslog, SNMP (Simple Network Management Protocol), FTP (File Transfer Protocol) oder WMI (Windows Management Instrumentation)
* Aggregieren der Daten an zentraler Stelle, bspw. Datenbank
* Log-Management kümmert sich um langfristige Speicherung und Archivierung
* Event-Management stellt Funktionen zur Verfügung, zum Auswerten der Daten, bspw. Datenanalyse oder -suche
* Gesetzliche Anforderungen:
  + Finanzumfeld oder Gesundheitswesen ist Logging verpflichtend, um Compliance-Richtlinien zu erfüllen oder Nachvollziehbarkeit von Transaktionen sicherzustellen
  + Event-Management unterstützt: HIPAA (Health Insurance Portability and Accountability), SOX (Sarbanes-Oxley Act) oder DSGVO (Datenschutz-Grundverordnung)
* Softwarelösungen des Log-Management enthalten Komponenten zur Benutzeroberfläche für Analyse, Reporting und Visualisierung der Daten
* Durch Künstliche Intelligenz (KI) und Maschinelles Lernen (ML) können große Datenmengen automatisiert organisiert und intelligent ausgewertet werden
* SIEM (Security Information and Event Management): Lösung mit der sich sicherheitsrelevante Ereignisse, Sicherheitsvorfälle oder Anomalien innerhalb von IT-Umgebungen erkennen, beobachten und automatische Alarmierung und Abwehr ergreifen lassen
* SIEM-Lösungen liefern Überblick über die Sicherheitslage der IT und gewähren tiefe Einblicke in Aktivitäten der Systeme
* Vorteile:
  + liefert tiefe Einblicke in die Prozesse, Abläufe und in den Systemstatus der IT-Systeme und Netzwerke
  + verbessert die Observability der IT
  + stellt Funktionen bereit, mit denen sich Logdaten schnell durchsuchen lassen
  + ermöglicht umfangreiche Analysen der Logdaten
  + ermöglicht die Berichterstattung
  + hilft gesetzliche Vorgaben oder Compliance-Richtlinien einzuhalten
  + unterstützt beim Erkennen, Analysieren und Beheben von IT-Problemen
  + steigert die Sicherheit durch die Möglichkeit des Identifizierens, Nachvollziehens und Analysierens von Sicherheitsvorfällen
  + bildet die Basis für SIEM-Lösungen
  + verbessert die Reaktionsfähigkeit eines Unternehmens
  + stellt die Nachvollziehbarkeit von Transaktionen sicher
  + ermöglicht historische Analysen

## Quelle: ait gmbh

* in der Praxis bewährte Log-Anwendungen: Serilog, NLog und Log4net
* Protokollnachrichten sollten strukturiert sein, sodass in großen Protokollen besser nach Parametern filtern zu können
* Loglevel: wie dringend bzw wichtig ist eine Nachricht



* Wohin sollen Protokolle gespeichert werden
  + Console, Dateien, Event Log oder Datenbank
* Lokale Protokolle schwer auszuwerten

## Quelle: cheat sheet

* Logging sollte innerhalb einer Anwendung und im gesamten Portfolio einer Organisation einheitlich und konsistent sein und ggf. Industriestandards verwenden, um die protokollierten Ereignisse von verschiedenen Systemen vergleichbar und verwaltbar zu machen
* Application Logs
  + Identifizieren von Sicherheitsvorfällen
  + Überwachung von Richtlinienverstößen
  + Grundlagen festlegen
  + Unterstützung von Unbestreitbarkeitskontrollen (beachten Sie, dass die Eigenschaft Unbestreitbarkeit für Protokolle schwer zu erreichen ist, da ihre Vertrauenswürdigkeit oft nur darauf basiert, dass die Protokollpartei ordnungsgemäß geprüft wird, während Mechanismen wie digitale Signaturen hier schwer zu verwenden sind)
  + Bereitstellung von Informationen über Probleme und ungewöhnliche Bedingungen
  + Beitragen zusätzlicher anwendungsspezifischer Daten zur Untersuchung von Vorfällen, die in anderen Protokollquellen fehlen
  + Schutz vor der Identifizierung und Ausnutzung von Schwachstellen durch Angriffserkennung
* Andere Arten von Ereignissen:
  + Sicherheitsereignisse
  + Überwachung von Geschäftsprozessen, z. B. Abbruch von Verkaufsprozessen, Transaktionen, Verbindungen
  + Anti-Automatisierungsüberwachung
  + Audit-Trails, z. B. Hinzufügen, Ändern und Löschen von Daten, Datenexport
  + Leistungsüberwachung, zB Datenladezeit, Seiten-Timeouts
  + Compliance-Überwachung
  + Daten für spätere Auskunftsanfragen, z. B. Auskunft über betroffene Personen, Informationsfreiheit, Rechtsstreitigkeiten, polizeiliche und andere behördliche Ermittlungen
  + Gesetzlich sanktioniertes Abfangen von Daten, z. B. Abhören auf Anwendungsebene
  + Andere geschäftsspezifische Anforderungen
* Bspw PCIDSS-Auditprotokolle enthalten chronologische Aufzeichnungen von Aktivitäten
  + Ermöglicht Rekonstruktion, Überprüfung und Untersuchung
* Ereignisdatenquelle ist die Anwendung, diese hat Informationen über den Benutzer und den Kontext des Ereignisses -> diese Daten sind meist nur innerhalb der Anwendung verfügbar und nicht in verwandten Anwendungen
* Andere Datenquellen
  + Client-Software, zB Aktionen auf Desktop oder mobilen Geräten
  + Netzwerk-Firewalls
  + Application Firewalls
  + Datenbankanwendungen, zB automatische Audit-Trails
  + Reputationsüberwachungsdienste, zB Betriebszeit- oder Malware-Überwachung
  + Andere Anwendungen, zB Betrugsüberwachung, CRM
* Vertrauensgrad muss berücksichtigt werden, wenn Ereignisdaten in anderen Vertrauenszonen einbezogen werden