Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Computer Science and
Information Technology

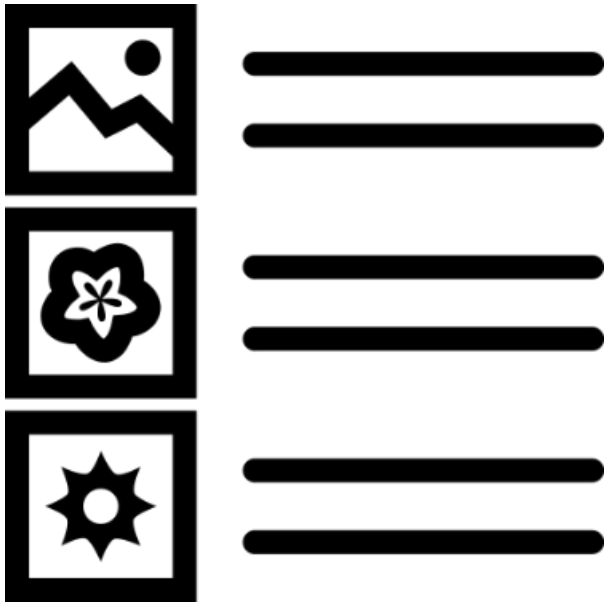
Logging & Monitoring

Anwendungsfälle

Logging & Monitoring in IT Umgebungen

Inhalt

- PCI DSS
- Telemetriedaten bei Windows
- Tesla Telematics Log Data
- Abwassermonitoring
- Finanzbuchaltung



PCI DSS (Umgang mit Kreditkarten)

- Die PCI regelt relativ detailliert Fragen rund ums Logging (https://www.pcisecuritystandards.org/)

- Firmen welche Dienstleistungen rund um den Gebrauch von CC anbieten müssen sich dran halten!

- Hintergrund ist natürlich:
  - "crime prevention" (Selbstschutz der Industrie)
  - Vertrauensbildung: "schaut was wir alles machen!"

- https://cybersecurity.att.com/blogs/security-essentials/pci-dss-logging-requirements-explained

Telemetriedaten bei Windows (1)

Windows sammelt laufend Telemetriedaten und sendet diese regelmässig an Microsoft.

Welche Telemetriedaten*? (je nach Windows- Version und Einstellung):
- Daten zu Abstürzen, zur Verwendungsdauer, zum CPU- und Speicherverbrauch einzelner Programme
- Daten zum Prozessor und Arbeitsspeicher
- Informationen zum Akku und anderer Hardware
- die Spezifikationen der Webcam
- Internet Explorer Versionsnummer
- Windows Variante - Infos zu Downloads, Updates, und Seitenabrufen im Windows App Store

* https://docs.microsoft.com/de-de/windows/privacy/required-windows-diagnostic-data-events-and-fields-2004

Telemetriedaten bei Windows (2)

- Dieses Verhalten lässt sich nur unter Win10 Enterprise abschalten

- Ein interessanter Bericht vom BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Analyse_Telemetriekomponente_1_0.pdf?__blob=publicationFile&v=1

Tesla Telematics Log Data (1)

- Tesla Fahrzeuge sammeln laufend Informationen zu fast alle denkbaren Parameter des Fahrzeuges sowie der Umgebung.

- Viele dieser Daten werden zentral bei Tesla selbst gespeichert. (welche das sind ist nur z.T. bekannt!)

- Man spricht davon, dass Tesla selbst eine Fz- Versicherung anbieten möchte und die Prämie zumindest teilweise von der Fahrweise des Fahrers abhängig machen möchte (https://teslamag.de/news/praemien-fahrstil-daten-tesla-eigene-versicherung-35791)

Tesla Telematics Log Data (2)

- Die Analytics der Daten passiert als auch bei Tesla selbst und nicht (nur) im Fz.

- Das muss nicht immer zugunsten des Besitzers ausgehen (https://www.greencarreports.com/news/1104505_tesla-can-look-at-owners-driving-behavior-any-time-is-that-legal)

- Der Fahrzeugbenutzer hat seit 2020 nur Zugang zum Event Data Recorder (EDR, https://edr.tesla.com/) voraus man sich einen Report generieren lassen kann (https://cdn.shopify.com/s/files/1/0522/0751/7864/files/Tesla-sample-EDR-Report-Y.pdf)

Abwassermonitoring

- Abwassermonitoring wird z.B. in der Epidemiologie angewendet, um Ausbrüche schneller und genauer erkennen und lokalisieren zu können.
- Durch Analysen des Abwassers zeigte sich z.B. COVID-19 früher als in offiziellen Statistiken oder man kann Hotspots besser erkennen.
  → Früherkennung
- Abwassermessungen machen auch den Verlauf der Infektionszahlen besser vorhersehbar
  → Verfolgung von Infektionsdynamiken
- Sie kann helfen, geografische Gebiete zu identifizieren, in denen die Viruslast besonders hoch ist
  → geografische Hotspots identifizieren

Finanzbuchhaltung

in der Finanzbuchhaltung können mittels Monitoring folgende Ziele adressiert werden:

- **Regulatorische Einhaltung**: Einhaltung aller relevanten gesetzlichen und regulatorischen Anforderungen.
- **Finanzielle Transparenz**: Bereitstellung klarer und transparenter Finanzinformationen für interne und externe Stakeholder.
- **Genauigkeit und Vollständigkeit**: Sicherstellung, dass alle finanziellen Transaktionen korrekt und vollständig erfasst sind.
- **Betrugserkennung und -verhinderung**: Identifizierung und Verhinderung von betrügerischen Aktivitäten.