Aufgabenstellung Labor “Sichere Systeme”  
Risikoregister Nils Bachmann, Alex Dixon, Joshua Kristof

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-01 | Mithören von Messdaten | Sehr hoch | Niedrig | Niedrig | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindungen: EC-01 - TA-SM-01 <--> TA-PP-02  Betroffene intangible Assets: IA-SM-02 – Messdaten  Mithören von Messdaten zwischen Smart Meter und Provider Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Die Vertraulichkeit der Daten IA-SM-02 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt | TR-01-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-02 | Mithören von Anmeldedaten | Sehr hoch | Hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindungen: EC-01 - TA-SM-01 <--> TA-PP-02  Betroffene intangible Assets: IA-SM-03 – Anmeldedaten  Mithören von Anmeldedaten zwischen Smart Meter und Provider Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Die Vertraulichkeit der Daten IA-SM-03 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt | TR-02-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-03 | Beeinflussung der Verfügbarkeit | Hoch | Sehr hoch | Hoch | Reduzieren, Transferieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-01: TA-SM-01 <--> TA-PP-02  Betroffene tangible Asset: TA-PP-02 - Provider Portal  Betroffene Verbindung: EC-04: TA-PP-02 <--> TA-CP-05  Betroffene tangible Asset: TA-PP-02 - Provider Portal  Beeinflussung der Verfügbarkeit des Provider Portals TA-PP-02 durch Überlastung der API Schnittstelle oder einen DDOS Angriff. | | | | | |
| Anforderungen | | | | | |
| Verfügbarkeit des Provider Portals TA-PP-02 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verwendung von DDOS Protection Providern (z.B. Cloudflare), um das Risiko eines erfolgreichen DDOS Angriffs zu transferieren.  Verwendung von Rate Limiting, um das Risiko einer Überlastung der API Schnittstelle zu reduzieren. | | | | [Manueller Test] Rate Limiting  [Pentest] DDOS Angriff | TR-03-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-04 | Veränderung von Messdaten | Sehr hoch | Mittel | Mittel | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindungen: EC-01 - TA-SM-01 <--> TA-PP-02  Betroffene intangible Assets: IA-SM-02 – Messdaten  Veränderung von Messdaten zwischen Smart Meter und Provider Portal. Hierzu gehört auch die unberechtigte Nutzung der API Schnittstelle. | | | | | |
| Anforderungen | | | | | |
| Die Integrität, Authentizität, Identität und Vertraulichkeit der Daten IA-SM-02 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). Prüfung der Integrität und Identität (seitens des Clients) mit Hash-based message authentication code – HMAC innerhalb der Übertragung von HTTPS (TLS). Authentifikation des Clients über API Key. | | | | [Pentest] Wireshark Mitschnitt, [Manueller Test], [Design Review] | TR-04-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-05 | Veränderung von Messdaten | Niedrig | Mittel | Niedrig | Transferieren |
| Beschreibung | | | | | |
| Betroffene tangible Assets: TA-SM-01  Betroffene intangible Assets: IA-SM-02 – Messdaten  Veränderung von Messdaten im Smart Meter.  Dieses Risiko ist „out of scope“, wird der Vollständigkeit halber aber aufgenommen. | | | | | |
| Anforderungen | | | | | |
| Die Integrität, Authentizität und Vertraulichkeit der Daten IA-SM-02 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Vertragliche Verpflichtung zum fälschungssicheren Design der Hardware des Smart Meters. | | | | Pentest | TR-05-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-06 | Veränderung von Anmeldedaten | Niedrig | Niedrig | Niedrig | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindungen: EC-01 - TA-SM-01 <--> TA-PP-02  Betroffene intangible Assets: IA-SM-03 – Anmeldedaten  Veränderung von Anmeldedaten zwischen Smart Meter und Provider Portal. | | | | | |
| Anforderungen | | | | | |
| Die Integrität, Identität und Vertraulichkeit der Daten IA-SM-03 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Integritätsprüfungen (Hash-based message authentication code) innerhalb der Übertragung von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt | TR-06-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-07 | Veränderung von Konfigurationsdaten | Niedrig | Niedrig | Niedrig | Transferieren |
| Beschreibung | | | | | |
| Betroffene tangible Assets: TA-SM-01  Betroffene intangible Assets: IA-SM-01 – Konfigurationsdaten  Veränderung von Konfigurationsdaten im Smart Meter.  Dieses Risiko ist „out of scope“, wird der Vollständigkeit halber aber aufgenommen. | | | | | |
| Anforderungen | | | | | |
| Die Integrität, Authentizität und Vertraulichkeit der Daten IA-SM-01 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Vertragliche Verpflichtung zum fälschungssicheren Design der Hardware des Smart Meters. | | | | Pentest | TR-07-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-08 | Mithören von Meter-Daten | Sehr hoch | Mittel | Mittel | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04 - TA-PP-02 <--> TA-CP-05  Betroffene intangible Assets: IA-PP-05: Meter-Daten (Meters)  Mithören von Meter-Daten zwischen Provider Portal und Customer Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit der Meter-Daten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt, [Design Review] | TR-08-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-09 | Mithören von Customer-Daten | Sehr hoch | Hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04 - TA-PP-02 <--> TA-CP-05  Betroffene intangible Assets: IA-PP-06: Customer-Daten (Customers, Customers-Meters)  Mithören von Customer-Daten zwischen Provider Portal und Customer Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit der Customer-Daten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt, [Design Review] | TR-09-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-10 | Mithören von Messdaten | Sehr hoch | Niedrig | Niedrig | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04 - TA-PP-02 <--> TA-CP-05  Betroffene intangible Assets: IA-PP-07: Messdaten (InfluxDB)  Mithören von Messdaten zwischen Provider Portal und Customer Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit der Customer-Daten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt, [Design Review] | TR-10-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-11 | Veränderung von Meter-Daten | Sehr hoch | Mittel | Mittel | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04 - TA-PP-02 <--> TA-CP-05  Betroffene intangible Assets: IA-PP-05: Meter-Daten (Meters)  Veränderung von Meter-Daten zwischen Provider Portal und Customer Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit, Integrität, Identität und Authentizität der Meter-Daten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). Prüfung der Integrität und Identität (seitens des Clients) mit Hash-based message authentication code – HMAC innerhalb der Übertragung von HTTPS (TLS). Authentifikation des Clients über API Key. | | | | [Pentest] Wireshark Mitschnitt, [Manueller Test], [Design Review] | TR-11-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-12 | Veränderung von Customer-Daten | Sehr hoch | Hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04 - TA-PP-02 <--> TA-CP-05  Betroffene intangible Assets: IA-PP-06: Customer-Daten (Customers, Customers-Meters)  Veränderung von Customer-Daten zwischen Provider Portal und Customer Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit, Integrität, Identität und Authentizität der Meter-Daten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). Prüfung der Integrität und Identität (seitens des Clients) mit Hash-based message authentication code – HMAC innerhalb der Übertragung von HTTPS (TLS). Authentifikation des Clients über API Key. | | | | [Pentest] Wireshark Mitschnitt, [Manueller Test], [Design Review] | TR-12-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-13 | Veränderung von Messdaten | Sehr hoch | Mittel | Mittel | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04 - TA-PP-02 <--> TA-CP-05  Betroffene intangible Assets: IA-PP-05: Messdaten (InfluxDB)  Veränderung von Messdaten zwischen Provider Portal und Customer Portal, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit, Integrität, Identität und Authentizität der Meter-Daten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). Prüfung der Integrität und Identität (seitens des Clients) mit Hash-based message authentication code – HMAC innerhalb der Übertragung von HTTPS (TLS). Authentifikation des Clients über API Key. | | | | [Pentest] Wireshark Mitschnitt, [Manueller Test], [Design Review] | TR-12-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-14 | Beeinflussung der Verfügbarkeit des Smart Meters | Mittel | Niedrig | Niedrig | Transferieren, Akzeptieren |
| Beschreibung | | | | | |
| Betroffene tangible Asset: TA-SM-01 – Smart Meter  Beeinflussung der Verfügbarkeit des Smart Meters TA-SM-01 durch physische Beeinflussung.  Dieses Risiko ist „out of scope“, wird der Vollständigkeit halber aber aufgenommen. | | | | | |
| Anforderungen | | | | | |
| Verfügbarkeit des Smart Meters TA-SM-01 muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Vertragliche Verpflichtung zum tamperproofen Design der Hardware des Smart Meters. | | | | [Pentest] | TR-14-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-15 | Mithören von Anmeldedaten | Sehr hoch | Hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-02: TA-PP-02 <--> TA-AA-03  Betroffene intangible Asset: IA-PP-08: Administration-Anmeldedaten (Users)  Mithören von Anmeldedaten zwischen Provider Portal und CLI Administration, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit der Anmeldedaten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt | TR-15-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-16 | Mithören von Anmeldedaten | Sehr hoch | Sehr hoch | Sehr hoch | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-02: TA-PP-02 <--> TA-SA-05  Betroffene intangible Asset: IA-PP-09: Verbindungs-/Anmeldungsdaten an Server  Mithören von Anmeldedaten zwischen Provider Portal und System-Administration, bspw. durch einen Man-in-the-middle Angriff.  Dieses Risiko ist „out of scope“, wird der Vollständigkeit halber aber aufgenommen. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit der Anmeldedaten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verwendung von einem VPN und SSH für den Verbindungsaufbau. | | | | [Pentest], [Manueller Test] | TR-16-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-17 | Mithören von Customer-Daten | Sehr hoch | Hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-02: TA-PP-02 <--> TA-AA-03  Betroffene intangible Asset: IA-PP-06: Customer-Daten (Customers, Customers-Meters)  Mithören von Anmeldedaten zwischen Provider Portal und CLI Administration, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit von Customer-Daten muss jederzeit gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). | | | | [Pentest] Wireshark Mitschnitt | TR-17-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-18 | Veränderung von Konfigurations-/Log-Daten | Hoch | Mittel | Mittel | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-03: TA-PP-02 <--> TA-SA-04  Betroffene intangible Asset: IA-PP-04: Konfigurations-/Log-Daten  Veränderung von Konfigurations-/Log-Daten zwischen Provider Portal and System Administration, bspw. durch einen Man-in-the-middle Angriff. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit, Integrität, Identität und Authentizität der Konfigurations-/Log-Daten muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Übertragung mit Hilfe von HTTPS (TLS). Prüfung der Integrität und Identität (seitens des Clients) mit Hash-based message authentication code – HMAC innerhalb der Übertragung von HTTPS (TLS). Authentifikation des Clients über API Key. | | | | [Pentest] Wireshark Mitschnitt, [Manueller Test], [Design Review] | TR-18-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-19 | Kompromittierung der Provider Portal Datenbanken | Niedrig | Sehr hoch | Niedrig | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindungen: IC-02: TA-PP-02 <--> Relationale Datenbank / IC-03: TA-PP-02 <--> InfluxDB  Betroffene tangible Assets: TA-PP-02: Provider Portal  Kompromittierung der Datenbanken des Provider Portals. Brute-Force Angriff des SSH Logins. | | | | | |
| Anforderungen | | | | | |
| Vertraulichkeit, Integrität und Verfügbarkeit der Daten innerhalb der Datenbanken. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verschlüsselung der Daten in den Datenbanken. | | | | [Design Review] | TR-19-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-20 | Zugriff auf Meter-Daten durch nicht-autorisierte Customer Portale | Mittel | Hoch | Mittel | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04: TA-PP-02 <--> TA-CP-05  Zugriff auf Meter-Daten durch nicht-autorisierte Customer Portale, aufgrund fehlender Autorisierung der Customer Portale. | | | | | |
| Anforderungen | | | | | |
| Autorisierung der Customer Portale muss bei Zugriff gewährleistet sein. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Prüfung der Autorisierung der Customer Portale bei Zugriff auf Meter-Daten. | | | | [Design Review], [Pentest] | TR-20-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-21 | Customer API kompromittiert | Niedrig | Sehr hoch | Niedrig | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindung: EC-04 - TA-PP-02 <--> TA-CP-05  Betroffene tangible Assets: TA-PP-02: Provider Portal  Es besteht die Möglichkeit bei einer Kompromittierung des Customer Portals, dass der API-Key missbraucht wird, um so Angriffe gegen unsere API-Schnittstelle durchzuführen. | | | | | |
| Anforderungen | | | | | |
| Die Vertraulichkeit, Integrität und Verfügbarkeit des Provider Portals muss dauerhaft gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Zur Abwehr solcher Angriffe kann Input Validation bei Eingehenden Nachrichten der API-Schnittstelle angewendet werden. Das kann bspw. SQL-Injection Angriffe verhindern. | | | | [Code Review], [Automatisierter Test] | TR-21-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-22 | Smart Meter API kompromittiert | Niedrig | Hoch | Niedrig | Reduzieren |
| Beschreibung | | | | | |
| Betroffen Verbindung: EC-01 - TA-SM-01 <--> TA-PP-02  Betroffene tangible Assets: TA-PP-02: Provider Portal  Es besteht die Möglichkeit bei einer Kompromittierung des Smart Meters, dass der API-Key missbraucht wird, um so Angriffe gegen unsere API-Schnittstelle durchzuführen. | | | | | |
| Anforderungen | | | | | |
| Die Vertraulichkeit, Integrität und Verfügbarkeit des Provider Portals muss dauerhaft gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Zur Abwehr solcher Angriffe kann Input Validation bei Eingehenden Nachrichten der API-Schnittstelle angewendet werden. Das kann bspw. SQL-Injection Angriffe verhindern. | | | | [Code Review], [Automatisierter Test] | TR-22-01 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R-23 | Kompromittierung der Dateien | Niedrig | Sehr hoch | Niedrig | Reduzieren |
| Beschreibung | | | | | |
| Betroffene Verbindungen:  EC-03: TA-PP-02 <--> TA-SA-04  EC-04: TA-PP-02 <--> TA-CP-05  Durch unbefugten Zugriff könnten Daten verändert und gelöscht werden, ohne dass dies auffällt. | | | | | |
| Anforderungen | | | | | |
| Die Integrität der Dateien muss jederzeit gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Um das unbemerkte Verändern/Löschen von Daten zu verhindern werden Log-Dateien erstellt, durch welche ersichtlich ist, welche Aktionen vorgenommen wurden. | | | | [Code Review], [Pentest] | TR-23-01 |