# Threat Source

## [Bedrohungsquelle]



|  |  |
| --- | --- |
| Threat | Bedrohung |
| Non-malicious | nicht böswillig |
| Non-human  | nicht menschlich |
| Malicious | böswillig |
| Human | menschlich |

## Risk Abstraction Diagram

## [Risikoabstraktionsdiagramm]



|  |  |
| --- | --- |
| Reputation loss | Reputationsverlust |
| Data exfiltration | Datenexfiltration |
| Employee misbehaviour | Fehlverhalten von Mitarbeitenden  |
| Malicious insider | Böswilliger Insider |
| Vulnerable web application | Angreifbare Webanwendung |
| Missing secure coding practice | Fehlen sicherer Programmierpraxis |

## Attack Path

## [Angriffspfad]



|  |  |
| --- | --- |
| Threat agents | Bedrohungsagenten |
| Attack vectors | Angriffsvektoren |
| Attack | Angriff |
| Security weakness | Sicherheitslücke |
| Weakness | Schwachstelle |
| Security controls | Sicherheitskontrollen |
| Control | Kontrolle |
| Technical impacts | Technische Auswirkungen |
| Asset | Vermögenswert |
| Function | Funktion |
| Business impact | Geschäftliche Auswirkungen |
| Impact  | Auswirkungen |

## Likelihood and Impact of a Threat

## [Wahrscheinlichkeit und Auswirkungen einer Bedrohung]



|  |  |
| --- | --- |
| Threat | Bedrohung |
| Threat agent | Bedrohungsagent |
| Attack vector | Angriffsvektor |
| Vulnerability | Sicherheitslücke |
| Security controls | Sicherheitskontrollen |
| Technical impact | Technische Auswirkungen |
| Business impact | Geschäftliche Auswirkungen |
| Likelihood | Wahrscheinlichkeit |
| Impact  | Auswirkungen |

## Likelihood and Impact Levels

## [Grad der Wahrscheinlichkeit und der Auswirkungen]

|  |
| --- |
| Likelihood and Impact Levels |
| **Value** | **Level** |
| 0 to <3 | LOW |
| 3 to <6 | MEDIUM |
| 6 to 9 | HIGH |

|  |
| --- |
| Grad der Wahrscheinlichkeit und der Auswirkungen |
| **Wert** | **Grad** |
| 0 to <3 | NIEDRIG |
| 3 to <6 | MITTEL |
| 6 to 9 | HOCH |

## Overall Risk Level (Risk Severity)

## [Grad des Gesamtrisikos (Schwere des Risikos)]

|  |  |
| --- | --- |
|  | Overall Risk Level (Risk Severity) |
| **Impact** | **HIGH** | MEDIUM | HIGH | CRITICAL |
| **MEDIUM** | LOW | MEDIUM | HIGH |
| **LOW** | INFORMATIONAL | LOW | MEDIUM |
|  | **LOW** | **MEDIUM** | **HIGH** |
| **Likelihood** |

|  |  |
| --- | --- |
|  | Grad des Gesamtrisikos (Schwere des Risikos) |
| **Auswirkungen** | **HOCH** | MITTEL | HOCH | KRITISCH |
| **MITTEL** | NIEDRIG | MITTEL | HOCH |
| **NIEDRIG** | INFOR­MATIONS-BEDINGT | NIEDRIG | MITTEL |
|  | **NIEDRIG** | **MITTEL** | **HOCH** |
| **Wahrscheinlichkeit** |

## Graphical Attack Tree: Opening a Safe

## [Grafische Darstellung eines Angriffsbaums: Öffnen eines Tresors]



|  |  |
| --- | --- |
| Open safe | Öffnen des Tresors |
| Open safe door | Tresortür öffnen |
| Open with force | Öffnen unter Anwendung von Gewalt  |
| Eavesdrop on password combination | Passwortkombination ausspionieren |
| Pick the safe lock | Das Tresorschloss aufbrechen |
| Open with force | Öffnen unter Anwendung von Gewalt  |
| Access to power tools | Zugang zu elektrischem Werkzeug |
| Break through safe wall  | Die Tresorwand aufbrechen |

## Process for Drawing a Node

## [Verfahren zum Zeichnen eines Knotens]



|  |  |
| --- | --- |
| Start | Start |
| Sub-nodes exhaustive? | Unterknoten vollständig? |
| Yes | Ja |
| Add sub-node | Unterknoten hinzufügen |
| No | Nein |
| Go to next node | Weiter zum nächsten Knoten |

## DFD Symbols

## [DFD-Symbole]



|  |  |
| --- | --- |
| External entity | Externe Entität |
| Data store | Datenspeicher |
| Data flow | Datenfluss |
| Process | Prozess |
| Trust boundary | Vertrauensgrenze |

## Example DFD

## [Beispiel für ein DFD]



|  |  |
| --- | --- |
| User | Nutzer:in |
| External system | Externes System |
| Corporate network | Firmennetzwerk |
| Gateway | Gateway |
| Cloud infrastructure  | Cloud-Infrastruktur |
| API broker | API-Broker |
| Data worker | Datenarbeiter |
| User management | Benutzerverwaltung |
| User database | Benutzerdatenbank |
| Log storage | Logspeicher |

## STRIDE-per-Interaction

## [STRIDE-per-Interaction]

|  |
| --- |
| STRIDE-per-Interaction |
| **#** | **Element** | **Interaction** | **S** | **T** | **R** | **I** | **D** | **E** |
| 1 | Process (Gateway) | The process has outgoing data flow to an external entity |  |  | x |  |  |  |
| 2 |  | The process receives data from an external entity | x |  |  |  | x | x |
| 3 |  | The process sends data to another process (data worker) | x |  | x | x | x | x |
| 4 |  | The process receives data from another process (data worker) | x |  | x |  | x | x |
| 5 | Process (Data worker) | The process sends data to another process (gateway) | x |  | x | x | x | x |
| 6 |  | The process receives data from another process (gateway) | x |  | x |  | x | x |
| 7 |  | The process sends data to another process (API broker) | x |  | x | x | x | x |
| 8 |  | The process receives data from another process (API broker) | x |  | x |  | x | x |
| 9 |  | The process sends data to a data store (Log storage) | x |  |  | x |  |  |
| 10 | Data Flow (Gateway / external) | Crosses environment boundary |  | x |  | x | x |  |
| 11 | Data Flow (Gateway / data worker) | Crosses environment boundary |  | x |  | x | x |  |
| 12 | Data Store (Log storage) | The data storage has inbound data flow |  | x | x | x | x |  |
| 13 | External Interactor (External system) | External interactor passes input to process | x |  | x | x |  |  |
| 14 |  | External interactor gets input from process | x |  |  |  |  |  |

|  |
| --- |
|  |
| **#** | **Element** | **Interaktion** | **S** | **T** | **R** | **I** | **D** | **E** |
| 1 | Prozess (Gateway) | Der Prozess sendet ausgehende Datenströme an eine externe Entität |  |  | x |  |  |  |
| 2 |  | Der Prozess empfängt Daten von einer externen Entität | x |  |  |  | x | x |
| 3 |  | Der Prozess sendet Daten an einen anderen Prozess (Datenarbeiter) | x |  | x | x | x | x |
| 4 |  | Der Prozess empfängt Daten von einem anderen Prozess (Datenarbeiter) | x |  | x |  | x | x |
| 5 | Prozess (Datenarbeiter) | Der Prozess sendet Daten an einen anderen Prozess (Gateway) | x |  | x | x | x | x |
| 6 |  | Der Prozess empfängt Daten von einem anderen Prozess (Gateway) | x |  | x |  | x | x |
| 7 |  | Der Prozess sendet Daten an einen anderen Prozess (API-Broker) | x |  | x | x | x | x |
| 8 |  | Der Prozess empfängt Daten von einem anderen Prozess (API-Broker) | x |  | x |  | x | x |
| 9 |  | Der Prozess sendet Daten an einen anderen Datenspeicher (Logspeicher) | x |  |  | x |  |  |
| 10 | Datenfluss (Gateway/extern) | Überschreitet die Umgebungsgrenze |  | x |  | x | x |  |
| 11 | Datenfluss (Gateway/Datenarbeiter) | Überschreitet die Umgebungsgrenze |  | x |  | x | x |  |
| 12 | Datenspeicher (Logspeicher) | Der Datenspeicher hat einen eingehenden Datenfluss |  | x | x | x | x |  |
| 13 | Externer Interaktor (externes System) | Der externe Interaktor wandelt Eingaben in Prozesse um | x |  | x | x |  |  |
| 14 |  | Der externe Interaktor empfängt Eingaben von Prozessen | x |  |  |  |  |  |

## Risk Management Pyramid

## [Risikomanagementpyramide]



|  |  |
| --- | --- |
| Communication and reporting | Kommunikation und Berichterstattung |
| Risk management across levels | Stufenübergreifendes Risikomanagement |
| Level 1 Organization | Stufe 1: Organisation |
| Level 2 Mission/Business Process | Stufe 2: Auftrags-/Geschäftsprozess |
| Level 3 Information System | Stufe 3: Informationssystem |

## Dataflow Diagram of a Web Application

## [Datenflussdiagramm einer Webanwendung]



|  |  |
| --- | --- |
| User | Nutzer:in |
| Cloud subscription | Cloud-Abonnement |
| Virtual machine | Virtuelle Maschine |
| Front end | Frontend |
| Backend | Backend |
| Database | Datenbank |
| Cloud infrastructure | Cloud-Infrastruktur |

## SEI Risk Management Paradigm

## [SEI-Risikomanagement-Modell]



|  |  |
| --- | --- |
| Control | Kontrollieren |
| Identify | Identifizieren |
| Analyze | Analysieren |
| Track | Nachverfolgen |
| Plan | Planen |
| Communicate | Kommunizieren |

## Risk assessment and evaluation list

## [Risikobewertungs- und -evaluierungsliste]



|  |  |
| --- | --- |
| Date | Datum |
| ID | ID |
| Risk Name | Risikobezeichnung |
| Plan | Plan |
| Deadline | Frist |
| Control | Kontrolle |
| Done | Erledigt |
| Information disclosure due to missing encryption in transit | Offenlegung von Informationen aufgrund fehlender Verschlüsselung bei der Übertragung |
| Implement encryption in transit | Verschlüsselung bei der Übertragung einführen |
| Test if the connection is encrypted | Überprüfen, ob die Verbindung verschlüsselt ist |
| Possible lateral movement in the corporate network | Mögliche laterale Bewegung im Firmennetzwerk |
| Implement network segregation | Netzwerktrennung umsetzen |
| Review the network architecture and check the possible connection between devices | Netzwerkarchitektur überprüfen und mögliche Verbindungen zwischen Geräten kontrollieren |
| SLA cannot be met in case of a cloud region failure | Servicevertrag kann bei Ausfall einer Cloud-Region nicht erfüllt werden  |
| Build a backup environment in another cloud region | Eine Backup-Umgebung in einer anderen Cloud-Umgebung aufbauen |
| Do failover tests and confirm the proper availability of the second region | Failover-Tests durchführen und ordnungsgemäße Verfügbarkeit der zweiten Region bestätigen |