**ISO/OSI Model versus TCP/IP Model.**

**ISO/OSI-Modell und TCP/IP-Modell im Vergleich**

A picture containing text, screenshot, font

Description automatically generated

|  |  |
| --- | --- |
| OSI Model | OSI-Modell |
| Application layer | Anwendungsschicht |
| Presentation | Darstellungsschicht |
| Session | Sitzungsschicht |
| Transport | Transportschicht |
| Network | Vermittlungsschicht |
| DataLink | Sicherungsschicht |
| Physical | Bitübertragungsschicht |
| TCP/IP Model | TCP/IP-Modell |
| Application layer | Anwendungsschicht |
| Transport | Transportschicht |
| Internet | Internetschicht |
| Network access | Netzzugangsschicht |

**Data flow between layers**

A picture containing text, screenshot, font, printing

Description automatically generated**Datenfluss durch die Schichten**

|  |  |
| --- | --- |
| Data fed into application layer of sender | Dateneinspeisung in die Anwendungsschicht des Senders |
| Encapsulation | Datenkapselung |
| Application header attaches to data | Anfügen des Anwendungsheaders an die Daten |
| Presentation header attaches to data | Anfügen des Darstellungsheaders an die Daten |
| Session header attaches to data | Anfügen des Sitzungsheaders an die Daten |
| Transport header attaches to data | Anfügen des Transportheaders an die Daten |
| Network header attaches to data | Anfügen des Netzwerkheaders an die Daten |
| Data link header and trailer attaches to data | Anfügen von Sicherungsheader und Trailer an die Daten |
| Application layer | Anwendungsschicht |
| Presentation layer | Darstellungsschicht |
| Session layer | Sitzungsschicht |
| Transport layer | Transportschicht |
| Network layer | Vermittlungsschicht |
| Data link layer | Sicherungsschicht |
| Physical layer | Bitübertragungsschicht |
| Sender A | Sender A |
| Receiver B | Empfänger B |
| Data Representation | Repräsentationsform der Daten |
| As data itself | Daten |
| Segments | Segmente |
| Packets | Pakete |
| Frames | Frames |
| Bits | Bits |
| Data received into application layer of receiver | Daten kommen auf der Anwendungsschicht des Empfängers an |
| Decapsulation | Entkapselung |
| Detaches application header | Entfernen des Anwendungsheaders |
| Detaches presentation header | Entfernen des Darstellungsheaders |
| Detaches session header | Entfernen des Sitzungsheaders |
| Detaches transport header | Entfernen des Transportheaders |
| Detaches network header | Entfernen des Netzwerkheaders |
| Detaches data link header and trailer | Entfernen von Sicherungsheader und Trailer |
| Data flows downwards | Abwärtsgerichteter Datenfluss |
| Data In the form of 0 and 1 | Daten in Form von Einsen und Nullen |
| Data flows upwards | Aufwärtsgerichteter Datenfluss |

**TCP three-way handshake**

**TCP-Drei-Wege-Handshake**A picture containing text, screenshot, font, number

Description automatically generated

|  |  |
| --- | --- |
| Client | Client |
| SYN | SYN |
| Synchronize Sequence Number | Synchronisierung der Sequenznummer |
| SYN and ACK | SYN und ACK |
| Acknowledgement of received message and sequence number to start next segment | Empfangsbestätigung einer Nachricht und Übermittlung der Sequenznummer für das nächste Segment |
| ACK | ACK |
| Acknowledgement of message from server | Bestätigung (engl. acknowledgement) einer zuvor vom Server gesendeten Nachricht |
| Server | Server |

**Zenmap GUI which scans the IP**

**IP-Scan auf der Zenmap-Oberfläche**

A screenshot of a computer

Description automatically generated with medium confidence

**FSteps of Nessus vulnerability scanning**

**Schritte eines Schwachstellenscans mit Nessus**A picture containing text, screenshot, font, purple

Description automatically generated

|  |  |
| --- | --- |
| Define the scan parameters, e.g., ports to be scanned, plugins to be enabled | Festlegung der Scan-Parameter (zu scannende Ports, zu aktivierende Plug-ins etc.) |
| Perform host discovery using protocols like TCP,UDP,ICMP to identify hosts | Identifizierung von Hosts über Protokolle wie TCP, UDP, ICMP |
| Perform port scan based on the available hosts | Port-Scan der verfügbaren Hosts |
| Conduct service detection to identify the service behind each port | Identifizierung der Dienste hinter den Ports |
| Detect the operating system | Erkennung des Betriebssystems |
| Run each host against a database of known vulnerabilities | Abgleich jedes Hosts mit einer Datenbank bekannter Schwachstellen |

**Commands of Metasploit**

A diagram of metasplolit commands

Description automatically generated with low confidence**Metasploit-Befehle**

|  |  |
| --- | --- |
| Show targets | show targets |
| Advanced | show advanced |
| Nops | show nops |
| Evasion | show evasion |
| Options | show options |
| Payload | show payload |
| Examples of Metasploit commands | Ausgewählte Metasploit-Befehle |

**Risk assessment within the risk management process**

**Risikoanalyse im Rahmen des Risikomanagementprozesses**

A diagram of a risk management process

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Access the risk | Risikoanalyse |
| Identifies the threats and assesses the risk in the organization | Identifizierung der relevanten Bedrohungen und Risiken |
| Information and communication flow | Informations- und Kommunikationsfluss |
| Framing the risk | Risikostrategie |
| Deals with creation of a risk management plan | Erstellung eines Risikomanagementplans |
| Monitor the risk | Risikoüberwachung |
| Considers the effectiveness of the response plans and how well they are maintained | Bewertung der Effektivität und Pflege der Reaktionspläne |
| Respond to the risk | Reaktion auf Risiken |
| Involves the organization’s response to the risk | Erstellung, Auswahl und Umsetzung von Reaktionsplänen |

**Inherent risk and Residual Risk.**

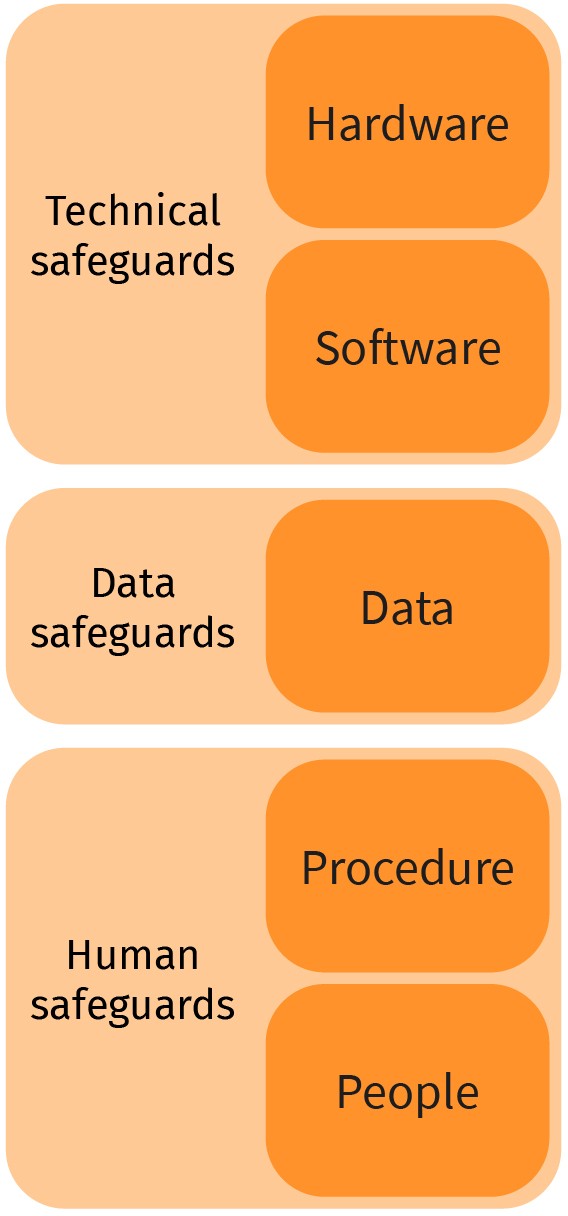
A picture containing diagram, design

Description automatically generated**Inhärentes Risiko und Restrisiko**

|  |  |
| --- | --- |
| Inherent risks | Inhärente Risiken |
| Applying controls | Kontollmechanismen |
| Residual | Restrisiko |

**Five components of Information system and related safeguards**

**Fünf Komponenten von Informationssystemen und dazu passende Sicherheitsmaßnahmen**



|  |  |
| --- | --- |
| Technical safeguards | Technische Sicherheitsmaßnahmen |
| Hardware | Hardware |
| Software | Software |
| Data | Datenbezogene Sicherheitsmaßnahmen |
| Human | Nutzerbezogene Sicherheitsmaßnahmen |
| Procedure | Prozesse |
| People | Personal |

**Security Evaluation Roles**

**Struktur des Sicherheitsbewertungsprozesses**

A picture containing text, screenshot, diagram, font

Description automatically generated

|  |  |
| --- | --- |
| TOE: Target of evaluation | EVG: Evaluierungsgegenstand (Target of Evaluation, TOE) |
| Instance | Prüfstelle |
| Certification | Zertifizierungsstelle |

**IDS Classification**

**IDS-Klassen**

A picture containing text, screenshot, font, design

Description automatically generated

|  |  |
| --- | --- |
| Considers patterns to detect intrusion | Bedrohungserkennung durch Musterabgleiche |
| Signature-based IDS/Rule-based IDS | Signaturbasiertes/regelbasiertes IDS |
| Classification based on approach | Klassifizierung nach Ansatz |
| Anomaly-based IDS/Behavior-based IDS | Anomalie-basiertes/verhaltensbasiertes IDS |
| Considers anomaly behavior as intrusion | Bedrohungserkennung anhand von Verhaltensanomalien |
| Intrusion Detection Systems | Intrusion-Detection-Systeme |
| Host-based IDS | Hostbasiertes IDS |
| Places IDS sensors in network | IDS-Sensoren im Netzwerk |
| Network-based IDS | Netzwerkbasiertes IDS |
| Classification based on data sources | Klassifizierung nach Datenquellen |
| Hybrid IDS | Hybrides IDS |
| Places IDS sensors in host and network | IDS-Sensoren auf Hosts und im Netzwerk |

**Working of Signature-based IDS**

**Funktionsweise eines signaturbasierten IDS**

A picture containing diagram, text, screenshot, line

Description automatically generated

|  |  |
| --- | --- |
| Incoming packets | Eingehende Pakete |
| Signature database | Signaturdatenbank |
| Matching | Signaturabgleich |
| Yes | Positiv |
| Alert | Warnung |
| System admin | Systemadministrator:in |
| no | Negativ |

**Working of Anomaly-based IDS**

**Funktionsweise eines verhaltensbasierten IDS**

A picture containing text, screenshot, font, diagram

Description automatically generated

|  |  |
| --- | --- |
| Incoming packets | Eingehende Pakete |
| Anomaly detection by comparing profiled behaviour | Erkennung von Anomalien durch Abgleiche mit Verhaltensprofilen |
| Real packets | Legitime Pakete |
| Profiling | Profilerstellung |
| Anomaly detected | Erkannte Anomalie |
| Alert | Warnung |
| System admin | Systemadministrator:in |

**NIDS and HIDS**

**NIDS und HIDS**

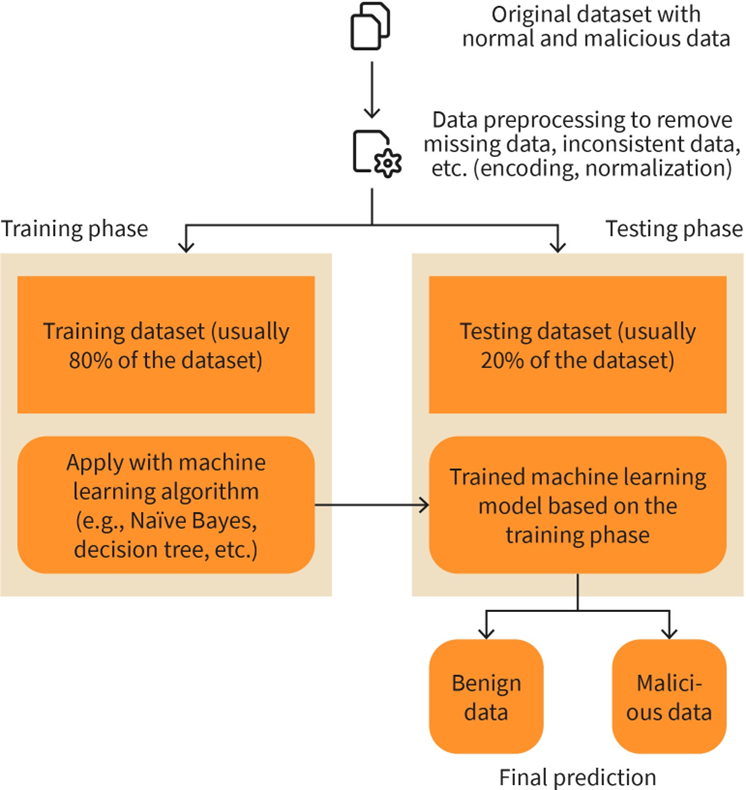
A picture containing text, screenshot, diagram, line

Description automatically generated

|  |  |
| --- | --- |
| Internet | Internet |
| Firewall | Firewall |
| Network-based IDS | Netzwerkbasiertes IDS |
| Printer Host-based IDS | Drucker-HIDS |
| PC Host-based IDS | PC-HIDS |
| Mobile Host-based IDS | Smartphone-HIDS |

**Machine Learning for IDS**

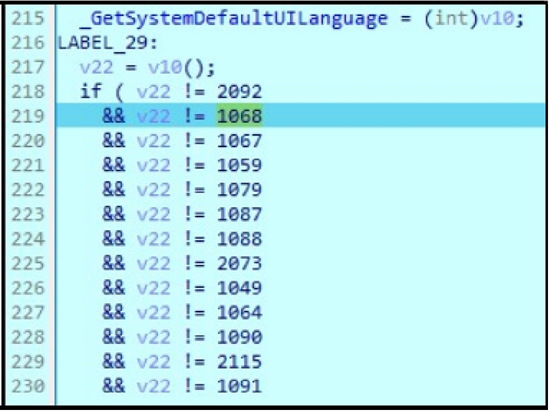
**IDS-Optimierung durch maschinelles Lernen**



|  |  |
| --- | --- |
| Original dataset with normal and malicious data | Ursprungsdatensatz mit legitimen und schädlichen Daten |
| Data preprocessing to remove missing data, inconsistent data, etc. (encoding, normalization) | Datenaufbereitung zur Entfernung fehlender oder inkonsistenter Daten (Kodierung, Normalisierung) |
| Training phase | Trainingsphase |
| Training dataset (usually 80% of the dataset) | Trainingsdatensatz (meist 80 % des Ausgangsdatensatzes) |
| Apply with machine learning algorithm (e-g, Naïve Bayes, decision tree, etc.) | Einspeisung in den ML-Algorithmus (bspw. naiver Bayes-Klassifikator oder Entscheidungsbaum) |
| Testing phase | Testphase |
| Testing dataset (usually 20% of the dataset) | Testdatensatz (meist 20 % des Ausgangsdatensatzes) |
| Trained machine learning model based on the training phase | Trainiertes ML-Modell |
| Benign data | Legitime Daten |
| Malicious data | Schädliche Daten |
| Final prediction | Einsatz im Realbetrieb |

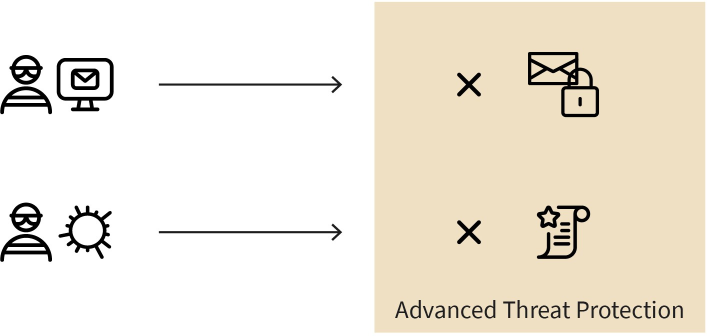
**Language Check IoC of LockBit 2.0 Ransomware**

**Sprachbasierter Bedrohungsindikator zur Erkennung der Ransomware LockBit 2.0**

****

**Advanced Threat Protection**

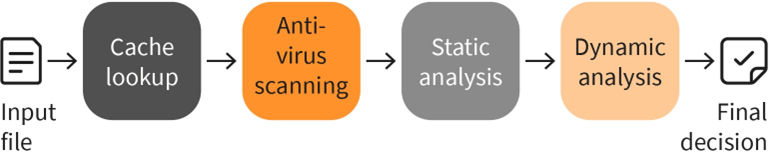
**Advanced Threat Protection**



|  |  |
| --- | --- |
| Advanced Threat Protection | ATP-Lösung |

**Example of Advanced Threat Protection**

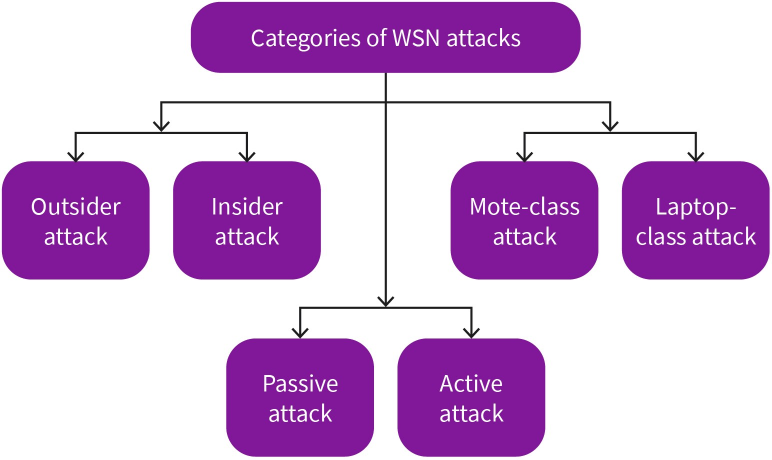
**Prüfprozess eines ATP-Systems**



|  |  |
| --- | --- |
| Input file | Inputdatei |
| Cache lookup | Cache-Abfrage |
| Anti-virus scanning | Antivirus-Scan |
| Static analysis | Statische Analyse |
| Dynamic analyses | Dynamische Analyse |
| Final decision | Endgültiges Urteil |

**Categories of WSN attacks**

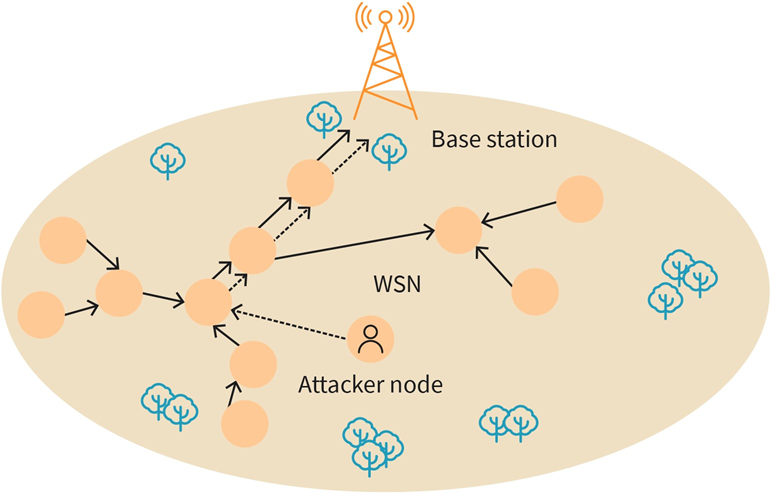
**Klassifizierungsschema für Angriffe auf Sensornetze**

****

|  |  |
| --- | --- |
| Categories of WSN attacks | Angriffe auf Sensornetze |
| Outsider attack | Outsider-Angriff |
| Insider attack | Insider-Angriff |
| Mote-class attack | Angriffe auf Knotenebene |
| Laptop-class attack | Angriffe auf Laptopebene |
| Passive attack | Passiver Angriff |
| Active attack | Aktiver Angriff |

**Path-based DoS in WSNs**

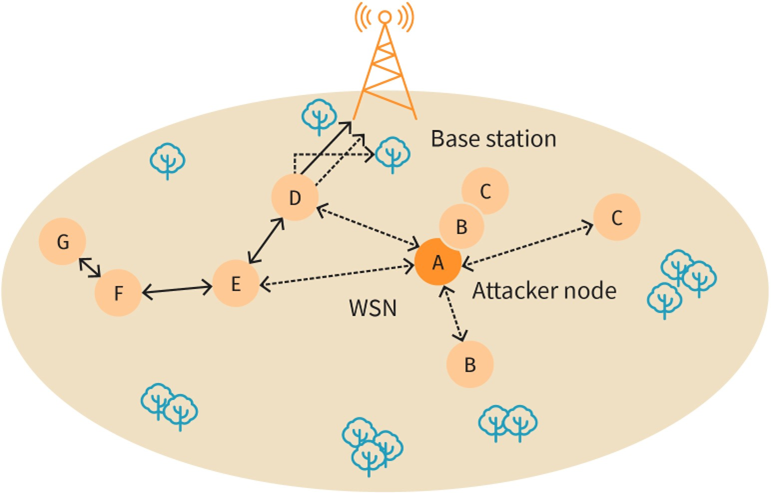
**Pfadbasierter DoS-Angriff auf ein Sensornetz**

****

|  |  |
| --- | --- |
| Base station | Basisstation |
| WSN | Sensornetz |
| Attacker node | Knoten der Angreifer:innen |

**Sybil attack in WSNs**

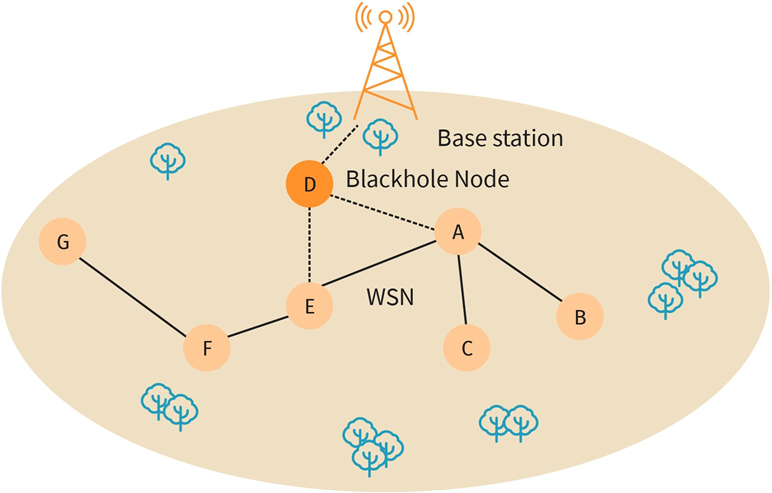
**Sybil-Angriff auf ein Sensornetz**

****

|  |  |
| --- | --- |
| Base station | Basisstation |
| WSN | Sensornetz |
| Attacker node | Knoten der Angreifer:innen |

**Blackhole attack in WSNs**

**Black-Hole-Angriff auf ein Sensornetz**

****

|  |  |
| --- | --- |
| Base station | Basisstation |
| Blackhole Node | Black-Hole-Knoten |
| WSN | Sensornetz |

**Node replication attack in WSNs**

**Replikationsangriff auf ein Sensornetz**

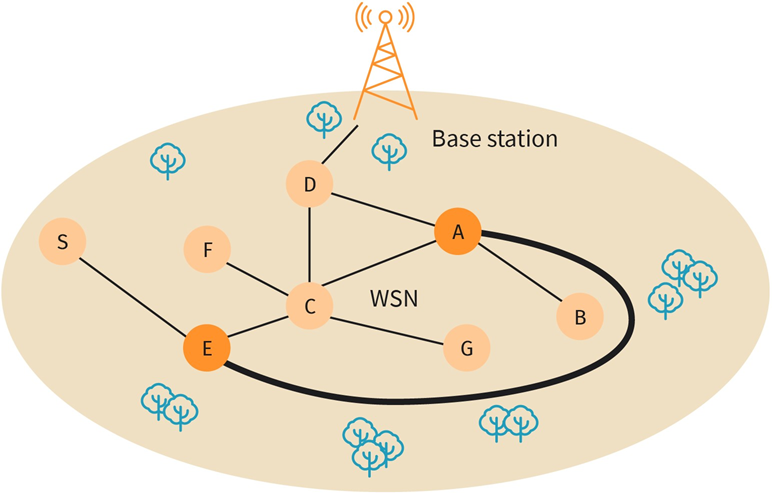
**A diagram of a base station

Description automatically generated with medium confidence**

|  |  |
| --- | --- |
| Base station | Basisstation |
| WSN | Sensornetz |

**Wormhole attack in WSNs**

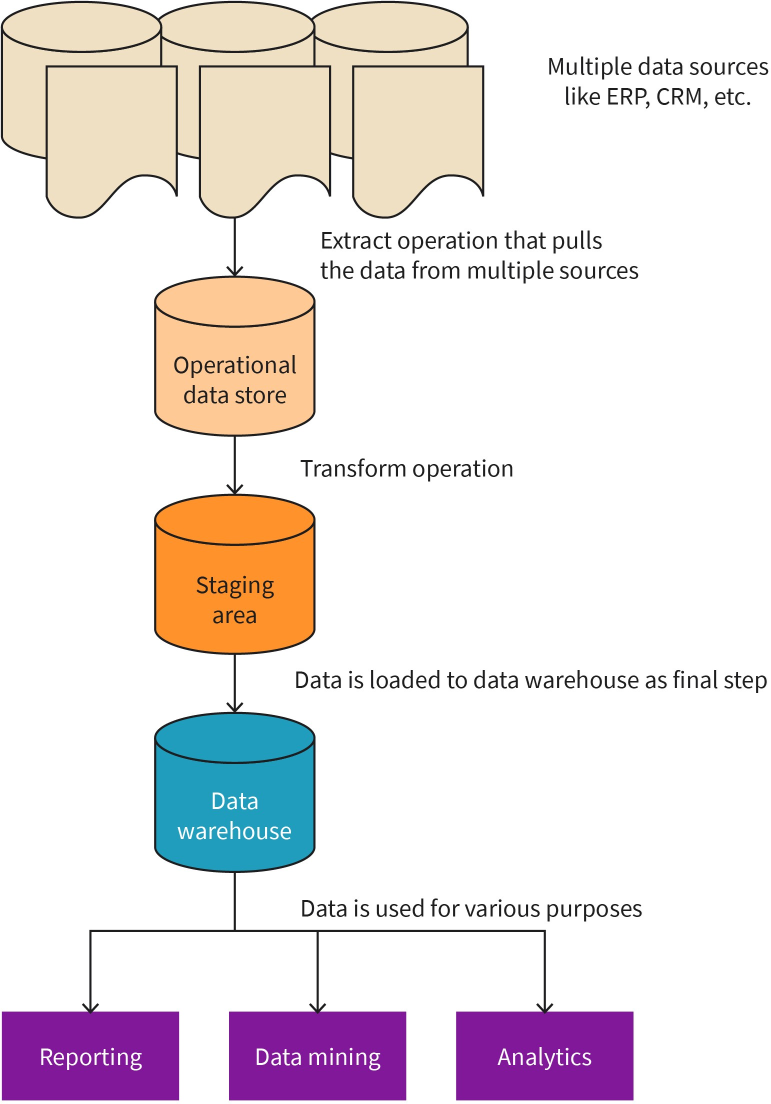
**Wurmloch-Angriff auf ein Sensornetz**

****

|  |  |
| --- | --- |
| Base station | Basisstation |
| WSN | Sensornetz |

**Working of ODS**

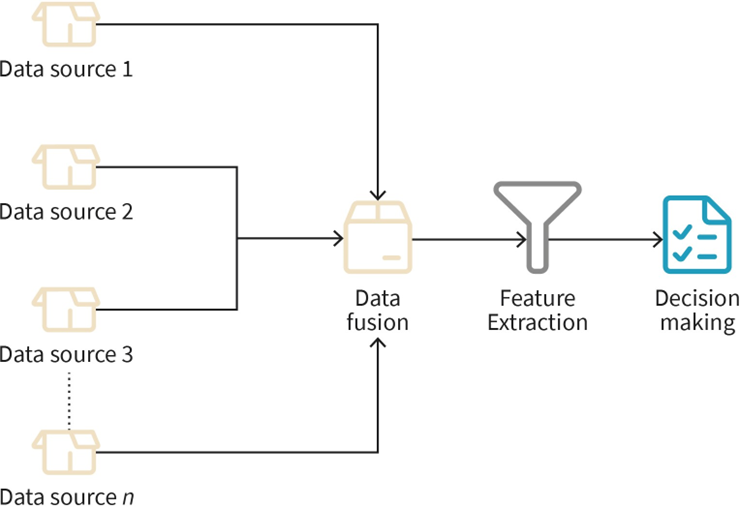
**Funktionsweise eines Operational Data Store**

****

|  |  |
| --- | --- |
| Operational data store | Operational Data Store |
| Staging area | Temporärer Zwischenspeicher |
| Data Warehouse | Data Warehouse |
| Reporting | Berichterstellung |
| Data Mining | Data-Mining |
| Analytics | Analysen |
| Multiple data sources like ERP, CRM, etc. | Verschiedene Datenquellen, darunter ERP- und CRM-Systeme |
| Extract operation that pulls the data from multiple sources | Datenextraktion |
| Transform operation | Umwandlungsprozess |
| Data is loaded to data warehouse as final step | Upload ins Data Warehouse |
| Data is used for various purposes | Einsatz der Daten für verschiedene Zwecke |

**Low-level Data fusion**

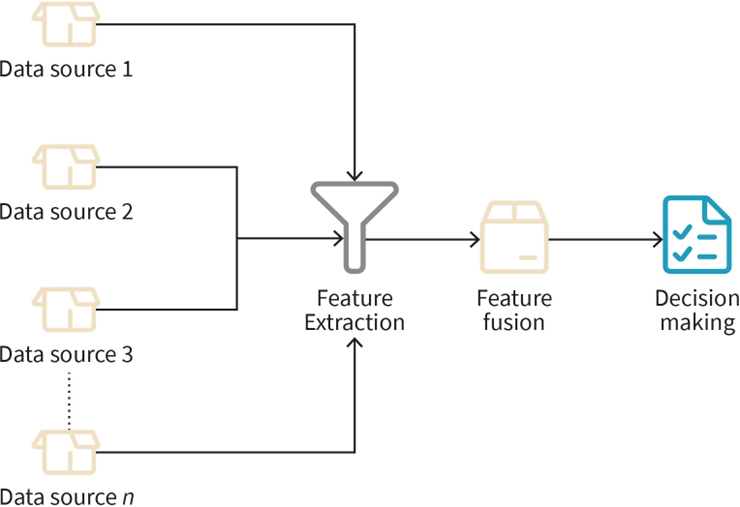
**Fusion auf Rohdatenebene**

****

|  |  |
| --- | --- |
| Data source | Datenquelle |
| Data Fusion | Datenfusion |
| Feature Extraction | Extraktion von Merkmalen |
| Decision making | Entscheidungsfindung |

**Medium-level Data fusion**

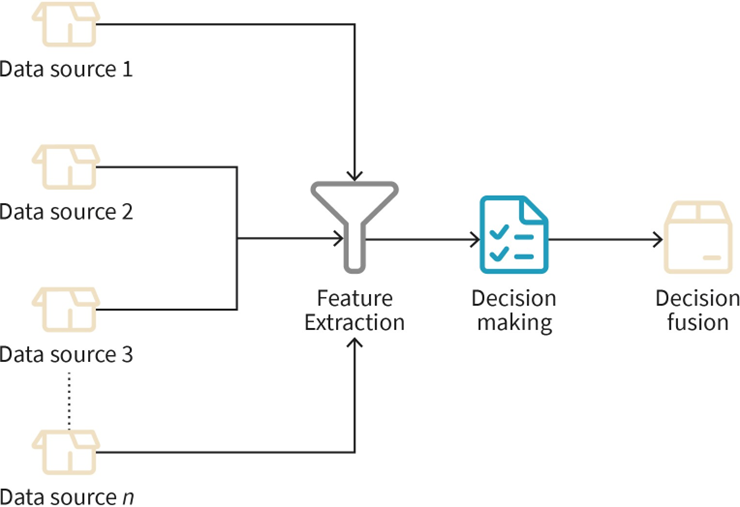
**Fusion auf Merkmalsebene**

****

|  |  |
| --- | --- |
| Data source | Datenquelle |
| Feature Extraction | Extraktion von Merkmalen |
| Feature Fusion | Fusion der Merkmale |
| Decision making | Entscheidungsfindung |

**High-level Data fusion**

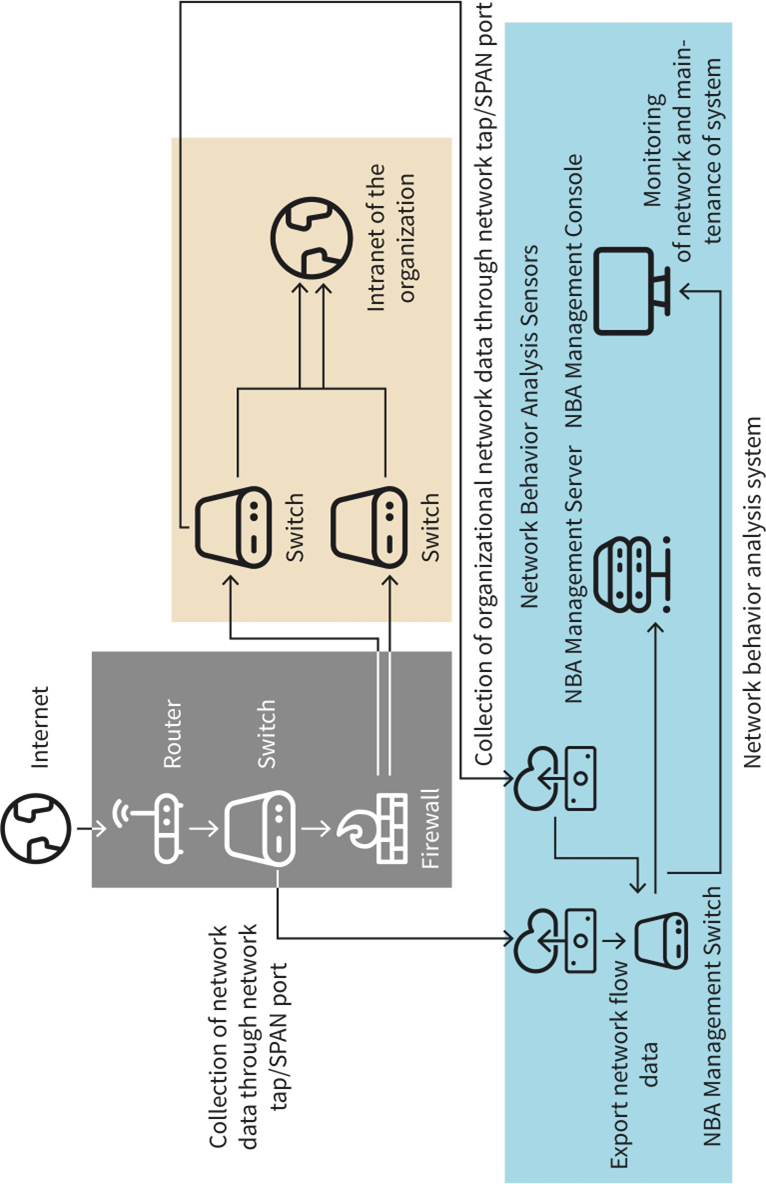
**Fusion auf Entscheidungsebene**

****

|  |  |
| --- | --- |
| Data source | Datenquelle |
| Feature Extraction | Extraktion von Merkmalen |
| Decision making | Entscheidungsfindung |
| Decision fusion | Entscheidungsfusion |

**Network Behaviour analysis model architecture**

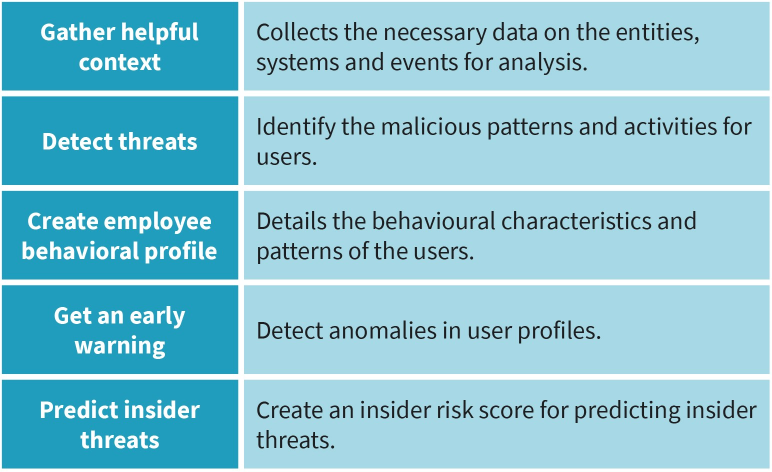
**Modellarchitektur zur Analyse des Netzwerkverhaltens**

****

|  |  |
| --- | --- |
| Collection of network data trough network tap/SPAN port | Sammlung von Netzwerkdaten über Netzwerk-TAPs und SPAN-Ports |
| Internet | Internet |
| Router | Router |
| Switch | Switch |
| Firewall | Firewall |
| Intranet of the organization | Intranet des Unternehmens/der Institution |
| Collection of organizational network data through network tap/SPAN port | Sammlung von Netzwerkdaten über Netzwerk-TAPs und SPAN-Ports |
| Export network flow data | Export der Netzwerkflussdaten |
| NBA Management Switch | NBA-Managementswitch |
| Network Behavior Analysis Sensors | Sensoren zur Analyse des Netzwerkverhaltens |
| NBA Management Server | NBA-Managementserver |
| NBA Management Console | NBA-Managementkonsole |
| Monitoring of network and maintenance of system | Netzwerküberwachung und Systempflege |
| Network behavior analysis system | System zur Analyse des Netzwerkverhaltens |

**Five levels of UEBA**

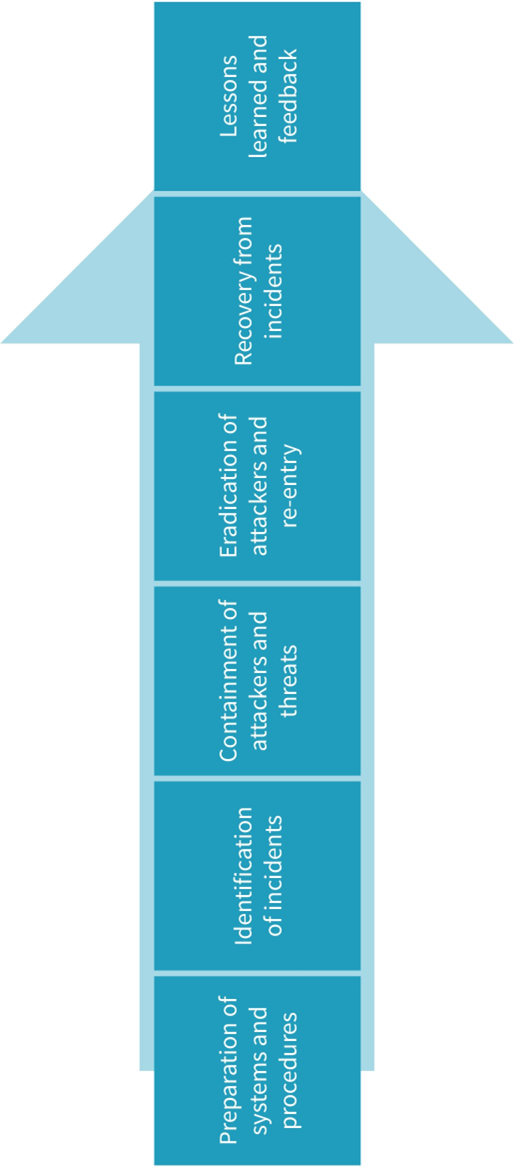
**UEBA-Ebenen**

****

|  |  |
| --- | --- |
| Gather helpful context | Sammlung hilfreicher Kontextinformationen |
| Detect threats | Bedrohungserkennung |
| Create employee behavioral profile | Erstellung von Verhaltensprofilen der Mitarbeiter:innen |
| Get an early warning | Frühzeitige Ausgabe von Warnungen |
| Predict insider threats | Prognose von Insider-Bedrohungen |
| Collects the necessary data on the entities, systems and events for analysis. | Zusammenführung der erforderlichen Nutzer-, Objekt-, System- und Ereignisdaten |
| Identify the malicious patterns and activities for users. | Identifizierung schädlicher Aktivitäten und Verhaltensmuster der Nutzer:innen |
| Details the behavioural characteristics and patterns of the users. | Detaillierte Beschreibung normaler Verhaltensmuster der Nutzer:innen |
| Detect anomalies in profiles. | Aufdeckung von Verhaltensanomalien durch Profilabgleiche |
| Create an insider risk score for predicting insider threats. | Quantitative Risikobewertung zur vorausschauenden Aufdeckung von Insider-Bedrohungen |

**Phases of incident response**

**IR-Phasen**

****

|  |  |
| --- | --- |
| Preparation of systems and procedures | Vorbereitende system- und prozessbezogene Maßnahmen |
| Identification of incidents | Identifizierung akuter Bedrohungen |
| Containment of attackers and threats | Eindämmung von Angriffen und Bedrohungen |
| Eradication of attackers and re-entry | Beseitigung der von den Angreifer:innen genutzten Zugangsmöglichkeiten |
| Recovery from incidents | Wiederherstellung |
| Lessons learned and feedback | Erkenntnisgewinnung und Feedback |

**Factors for selecting a security metric**

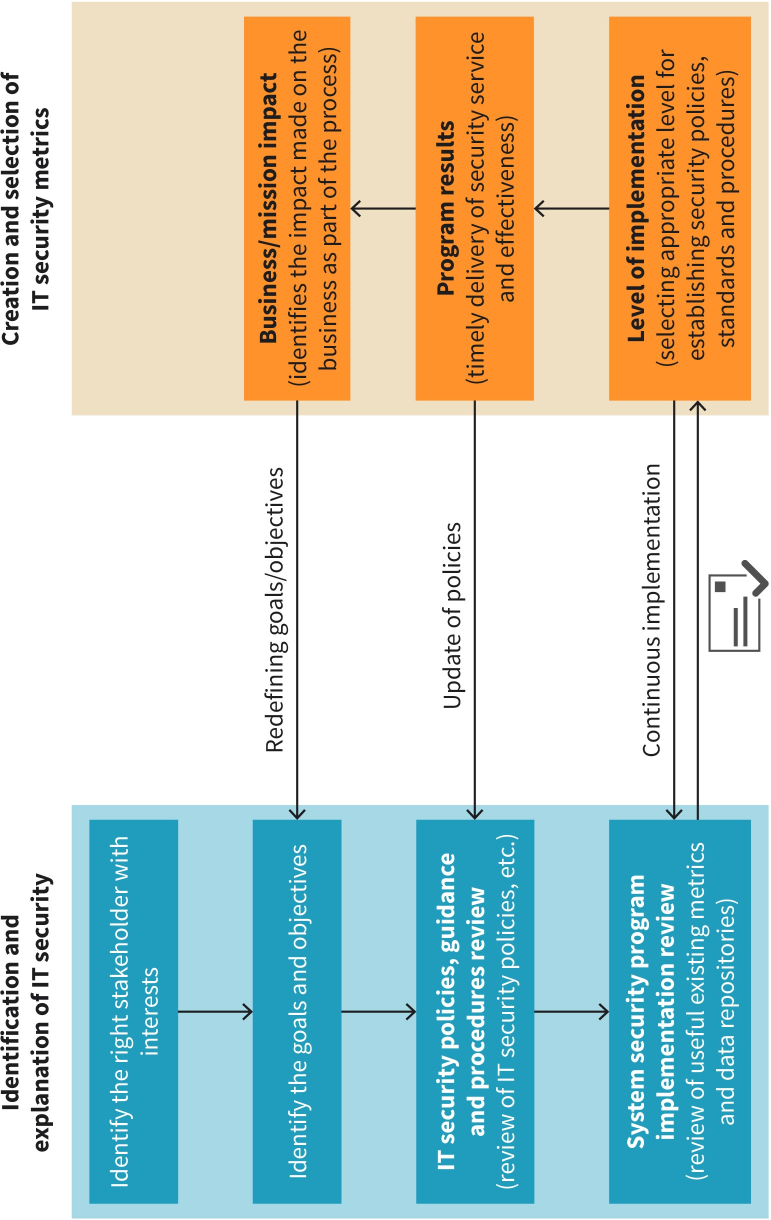
**Relevante Aspekte bei der Wahl einer Sicherheitsmetrik**

****

|  |  |
| --- | --- |
| Purpose | Zweck |
| Controllability | Prüfbarkeit |
| Context | Kontext |
| Best Practices | Best Practices |
| Quantitative | Quantifizierbarkeit |
| Data quality and ease of collection | Datenqualität und Erfassungsaufwand |
| Selection of security metrics | Auswahl sicherheitsrelevanter Kennzahlen |

**IT Security metric development process**

**Entwicklung von IT-Sicherheitsmetriken**

****

|  |  |
| --- | --- |
| Identification and explanation of IT security | Analyse der IT-Sicherheit |
| Identify the right stakeholder with interests | Identifizierung der relevanten Stakeholder mit Interessen |
| Identify the goals and objectives | Identifizierung der Zielsetzungen |
| IT security policies, guidance and procedures review (review of IT security policies etc.) | Evaluation der IT-Sicherheitsrichtlinien, -leitlinien und -prozesse |
| System security program implementation review (review of useful existing metrics and data repositories) | Evaluation der aktuellen Sicherheitsstrategie und ihrer Umsetzung (einschließlich bestehender Metriken und Datenbestände) |
| Redefining goals/objectives | Neudefinition der Zielsetzungen |
| Update of policies | Aktualisierung von Richtlinien |
| Continuous implementation | Kontinuierliche Implementierung |
| Creation and selection of IT security metrics | Erstellung und Auswahl von IT-Sicherheitsmetriken |
| Business/mission impact (identifies the impact made on the business as part of the process) | Auswirkungen auf Unternehmens-/Geschäftsbetrieb (im Rahmen des Prozesses) |
| Program results (timely delivery service and effectiveness) | Ergebnisse (zeitnahe Bereitstellung der gewünschten Sicherheitsdienste und Realisierung der angestrebten Effektivität) |
| Level of implementation (selecting appropriate level for establishing security policies, standards and procedures) | Wahl der Implementierungsebene (Auswahl der geeigneten Ebene zur Einführung von Sicherheitsrichtlinien, -standards und -prozessen) |

**Examples of primary and secondary stakeholder**

**Beispiele für primäre und sekundäre Stakeholder:innen**

****

|  |  |
| --- | --- |
| Primary stakeholder | Primäre Stakeholder:innen |
| Head of agency | Unternehmens-/Behördenleiter:in |
| Chief information officer (CIO) | Chief Information Officer (CIO) |
| Security program manager/Information system security officer (ISSO) | Leiter:in des Sicherheitsprogramms/IT-Sicherheitsbeauftragte:r |
| Program manager/system owner | Programmleiter:in/Systemeigentümer:in |
| System security officer | Systemsicherheitsbeauftragte:r |
| System administrator/network administrator | Systemadministrator:in/Netwerkadministrator:in |
| IT support personnel | IT-Support |
| Secondary stakeholder | Sekundäre Stakeholder:innen |
| Chief financial officer (CFO) | Chief Financial Officer (CFO) |
| Training organization | Schulungsabteilung |
| Human resources/personnel organization | Personalabteilung |
| Inspector general (IG) | Generalinspektor:innen |

**Structure of ISO/IEC 27001 standard**

**Struktur des Standards ISO/IEC 27001**

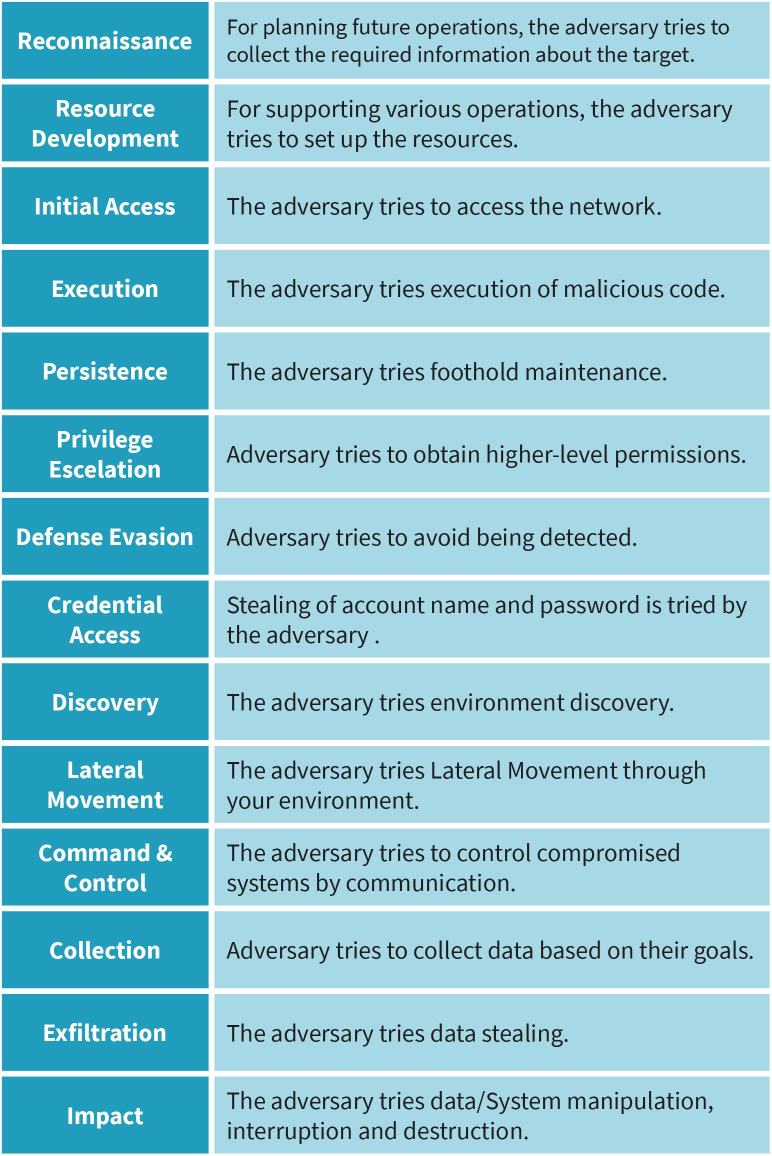
**#**A picture containing text, screenshot, font, number

Description automatically generated

|  |  |
| --- | --- |
| Chapters for formality | Formelle Kapitel |
| Foreword | Foreword: Vorwort |
| Introduction: overview of the standard | Introduction: Überblick über den Standard |
| Scope: mentions the generic ISMS requirements | Scope: allgemeine Anforderungen an ein ISMS |
| Normative references: mandatory read standards | Normative references: vorausgesetzte Standards |
| Terms and definitions: similar to the ISO/EC 27000 standard | Terms and definitions: Grundbegriffe (ähnlich wie im ISO/IEC-Standard 27000) |
| Bibliography | Bibliography: Literaturverzeichnis |
| Chapters mandatory for certification | Obligatorische Kapitel für die Zertifizierung |
| Context of the organization: Provides organizational context | Context of the organization: organisatorische Kontextinformationen |
| Leadership: Deals with leadership of management | Leadership: Rolle des Managements bei der Umsetzung |
| Planning: abstracts the information on managing the changes in ISMS | Planning: Informationen zur Verwaltung der Änderungen am ISMS |
| Support: Assigns adequate and competent resources | Support: Zuweisung kompetenter Ressourcen |
| Operation: Outlines various operations | Operation: Kursorische Beschreibung verschiedener Prozesse |
| Performance Evaluation: Deals with monitoring, estimating etc. | Performance Evaluation: Überwachung, Messung usw. |
| Improvement: Refines ISMS | Improvement: Verbesserung von ISMS |
| Discretionary chapters | Ergänzende Kapitel |
| Annex A: Deals with security controls detailed in IDO/IEC | Annex A: In ISO/IEC 27002:2022 beschriebene Sicherheitsmechanismen |
| Explained more fully in ISO/IEC 27002:2022 | Ausführlichere Erklärungen in ISO/IEC 27002:2022 |

**14 tactics in the enterprise matrix**

**14 Angriffstaktiken aus der Enterprise Matrix**

****

|  |  |
| --- | --- |
| Reconnaissance | Aufklärung |
| Resource Development | Ressourcenentwicklung |
| Initial Access | Erster Zugang |
| Execution | Ausführung |
| Persistence | Persistenz |
| Privilege Escelation | Ausweitung der Zugriffsrechte |
| Defense Evasion | Umgehung von Sicherheitsmaßnahmen |
| Credential Access | Zugriff auf Anmeldedaten |
| Discovery | Ausspähung der Umgebung |
| Lateral Movement | Ausbreitung im Netzwerk |
| Command & Control | Command & Control |
| Collection | Datensammlung |
| Exfiltration | Ausschleusung |
| Impact | Sabotage |
| For planning future operations, the adversary tries to collect the required information about the target. | Sammlung der für künftige Hackeroperationen nötigen Informationen über das Angriffsziel |
| For supporting various operations, the adversary tries to set up the resources. | Erlangung und Einrichtung der für den Angriff erforderlichen Ressourcen |
| The adversary tries to access the network. | Eindringen in das Netzwerk |
| The adversary tries execution of malicious code. | Aktivierung von Schadcode in der Zielumgebung |
| The adversary tries foothold maintenance. | Sicherung eines dauerhaften Zugangs zur Zielumgebung |
| Adversary tries to obtain higher-level permissions. | Erlangung erweiterter Zugangsberechtigungen |
| Adversary tries to avoid being detected. | Tarnung der schädlichen Aktivitäten |
| Stealing of account name and password is tried by adversary. | Diebstahl von Kontonamen und Passwörtern |
| The adversary tries environment discovery. | Nähere Erkundung der Zielumgebung |
| The adversary tries Lateral Movement through your environment. | Ausweitung der Zugriffsrechte auf weitere Netzwerksegmente und -systeme |
| The adversary tries to control compromised systems by communication. | Übermittlung von Anweisungen an kompromittierte Systeme |
| Adversary tries to collect data based on their goals. | Akkumulation der gewünschten Daten |
| Adversary tries data stealing. | Diebstahl der Daten |
| Adversary tries data/system manipulation, interruption and destruction. | Manipulation, Schädigung und Zerstörung von Datenbeständen und Systemen |