Diagram, funnel chart

Description automatically generated**Allgemeines Prozessmodell der Netzwerkforensik**

|  |  |
| --- | --- |
| Preparation | Vorbereitung |
| Detection | Erkennung |
| Collection | Datensammlung |
| Preservation | Beweissicherung |
| Examination | Prüfung |
| Analysis | Analyse |
| Investigation | Untersuchung |
| Incident response | Incident Response |
| Presentation | Ergebnispräsentation |

**Vom Ereignis zum Vorfall**

Diagram

Description automatically generated

|  |  |
| --- | --- |
| IDS | IDS |
| Event | Ereignis |
| False positive | Fehlalarm |
| Confirmed | Bestätigtes |
| Assessment | Bewertung |
| Incident | Vorfall |
| No incident | Kein Vorfall |

Diagram

Description automatically generated**Illustration eines Protokollstacks**

|  |  |
| --- | --- |
| Virtual communication | Virtuelle Kommunikation |
| Scribe | Schreiber |
| Couriers | Kuriere |

Diagram

Description automatically generated**TCP/IP- und ISO/OSI-Schichtenmodelle im Vergleich**

|  |  |
| --- | --- |
| Linke Spalte aus dem Diagramm (TCP/IP) | |
| Application | Anwendungsschicht |
| Transport | Transportschicht |
| Network (Internet) | Netzwerkschicht (Internet) |
| Link | Verbindungsschicht |
| Physical | Bitübertragungsschicht |
| TCP/IP-Protokollsuite | TCP/IP |
| Rechte Spalte aus dem Diagramm (ISO/OSI) | |
| Application | Anwendungsschicht |
| Presentation | Darstellungsschicht |
| Session | Sitzungsschicht |
| Transport | Transportschicht |
| Network | Vermittlungsschicht |
| Link | Sicherungsschicht |
| Physical | Bitübertragungsschicht |
| ISO/OSI reference model | ISO/OSI-Referenzmodell |

Diagram

Description automatically generated**TCP/IP-Schichten und ihre Relevanz**

|  |  |
| --- | --- |
| Which data | Welche Daten |
| Which process | Welcher Prozess |
| Which machine | Welche Geräte |
| Integrity | Integrität |
| Bits | Bits |
| Application | Anwendung |
| Transport | Transport |
| Network | Netzwerk |
| Link | Verbindung |
| Physical | Bitübertragung |

Diagram

Description automatically generated**Schachtelung von Segmenten, Paketen und Frames**

|  |  |
| --- | --- |
| Frame | Frame |
| Packet = frame payload | Paket = Nutzdaten d. Frames |
| Segment = packet payload | Segment = Nutzdaten d. Pakets |
| Segment payload | Nutzdaten d. Segments |
| Frame header | Frameheader |
| Packet header | Paketheader |
| Segment header | Segmentheader |
| Frame trailer | Frametrailer |

Diagram

Description automatically generated**Organisationsstruktur der Internet Engineering Task Force**

|  |  |
| --- | --- |
| Internet society | Internet Society |
| IASA | IASA |
| IAB | IAB |
| IRTF | IRTF |
| IANA | IANA |
| RFC | RFC |
| IESG | IESG |
| Area | Bereich |

**RFCs mit Bezug zu HTTP/1.1**

Diagram

Description automatically generated

**TCP-Sende- und -Empfangspuffer**

Diagram

Description automatically generated

|  |  |
| --- | --- |
| Process | Prozess |
| Socket | Socket |
| TCP send buffer | TCP-Sendepuffer |
| TCP receive buffer | TCP-Empfangspuffer |
| Segments | Segmente |

Table

Description automatically generated**Der TCP-Header**

|  |  |
| --- | --- |
| Source port | Quellport |
| Destination port | Zielport |
| Sequence number | Sequenznummer |
| Acknowledgement number | Bestätigungsnummer |
| Data offset | Datenoffset |
| Reserved | Reserviert |
| Window size | Fenstergröße |
| Checksum | Prüfsumme |
| Urgent pointer | Urgent Pointer |
| Options | Optionen |
| Data | Daten |
| bytes | Byte |

**TCP-Drei-Wege-Handshake**

Diagram

Description automatically generated

|  |  |
| --- | --- |
| Client | Client |
| Server | Server |

Diagram

Description automatically generated**Trennung von TCP-Verbindungen**

Diagram

Description automatically generated**SYN-Flood-Angriff**

|  |  |
| --- | --- |
| Attacker | Angreifer:in |
| Server | Server |
| Counterfeit addresses | Gefälschte Adressen |
| Buffers | Puffer |

Diagram

Description automatically generated**RST-Angriff**

|  |  |
| --- | --- |
| Client | Client |
| Seg | Seg |
| RST | RST |
| Server | Server |
| Attacker | Angreifer:in |

Diagram

Description automatically generated**Session Hijacking**

|  |  |
| --- | --- |
| Client | Client |
| Seg | Seg |
| Server | Server |
| Attacker | Angreifer:in |
| Server’s TCP read buffer | TCP-Lesepuffer des Servers |

**Leitungsvermittlung und Paketvermittlung**

Diagram

Description automatically generated

|  |  |
| --- | --- |
| Circuit switching | Leitungsvermittlung |
| Physical connection | Physische Verbindung |
| Packet switching | Paketvermittlung |
| Packets are distributed | Verteilte Pakete |

**Bestandteile einer IP-Adresse**

Table

Description automatically generated

|  |  |
| --- | --- |
| Network | Netzwerkkennung |
| Host | Hostkennung |

**Dezimal-, Binär- und Hexadezimalschreibweise einer IP-Adresse**Diagram

Description automatically generated

|  |  |
| --- | --- |
| Decimal | dezimal |
| Binary | binär |
| Hexadecimal | hexadezimal |
| Padding | Auffüllung mit Nullen |
| Valid padding | gültige Auffüllung |
| Shortening | Kurzschreibweise |

**Verknüpfung dreier Netzwerke mithilfe von drei Routern**

Diagram

Description automatically generated

**MAC-Teilschicht im TCP/IP-Schichtenmodell**Diagram

Description automatically generated

|  |  |
| --- | --- |
| Application | Anwendung |
| Transport | Transport |
| Network (Internet) | Netzwerk (Internet) |
| (Data) link | Verbindung |
| (Data) link layer | Verbindungsschicht |
| MAC sublayer | MAC-Teilschicht |
| Physical | Bitübertragung |
| TCP/IP layer model | TCP/IP-Schichtenmodell |

**Address Resolution-Protokoll in einem LAN**Diagram

Description automatically generated with medium confidence

|  |  |
| --- | --- |
| MAC | MAC |
| ARP Table | ARP-Tabelle |

**Schritte zur Ermittlung der MAC-Adresse**

Text

Description automatically generated

|  |  |
| --- | --- |
| An IP packet is to be sent to a specific IP address. In order to do this via the link layer (Ethernet), the corresponding MAC must be found. | Ein IP-Paket soll an eine bestimmte IP-Adresse gesendet werden. Um diesen Vorgang über die Verbindungsschicht (Ethernet) abzuwickeln, muss die entsprechende MAC-Adresse bekannt sein. |
| The sender or forwarder looks in its internal ARP table for an entry for the destination. If an entry exists, a corresponding Ethernet frame can be constructed and sent over the line. | Der Absender bzw. die Weiterleitung sucht in der eigenen, internen ARP-Tabelle nach einem Eintrag zum Zielsystem. Ist ein solcher Eintrag vorhanden, kann ein entsprechender Ethernet-Frame erstellt und verschickt werden. |
| If no entry exists in the local ARP table (also called the ARP cache), the MAC address has to be found out. To do this, a local broadcast message (an ARP request) is sent out on the link layer. This broadcast message contains: | Falls die lokale ARP-Tabelle (die auch als ARP-Cache bezeichnet wird) keinen solchen Eintrag enthält, muss die MAC-Adresse ermittelt werden. Zu diesem Zweck wird über die Verbindungsschicht eine lokale Broadcastmeldung versendet. Diese hat folgenden Inhalt: |
| The MAC and IP addresses of the system asking for the MAC address | die MAC- und IP-Adresse des Systems, das nach der MAC-Adresse fragt |
| An all-zero value representing the desired MAC address of the destination system | ein nur aus Nullen bestehender Platzhalter für die gewünschte MAC-Adresse des Zielsystems |
| The IP address of the system whose MAC address is requested | die IP-Adresse des Systems, dessen MAC-Adresse angefordert wird |
| The ARP request reaches all systems connected locally to the network segment, i.e., without going through a router. If a system with the corresponding IP address receives the request, it can send an ARP reply. This reply can also be broadcast to all link-local systems or directed specifically to the original sender. The ARP reply follows the same format as the request and contains: | Die ARP-Anfrage erreicht alle Systeme, die mit dem lokalen Netzwerksegment verbunden sind und passiert demnach keinen Router. Wenn ein System mit der fraglichen IP-Adresse die Anfrage empfängt, kann es eine ARP-Antwort senden – entweder an alle verbindungslokalen Systeme oder ausschließlich an den ursprünglichen Absender. Dabei folgt die Antwort demselben Format wie die Anfrage und enthält: |
| the MAC and IP addresses of the desired system as a new sender | die MAC- und IP-Adresse des gesuchten Systems als Absender |
| the MAC and IP addresses of the original system as the recipient | die MAC- und IP-Adresse des ursprünglichen Systems als Empfänger |
| With this reply, the original sender can store an entry for the recipient in ist ARP cache. This information is then used to translate IP packets with the same destination to Ethernet frames. | Auf dieser Grundlage kann der ursprüngliche Absender im eigenen ARP-Cache einen Eintrag für den Empfänger anlegen. Die darin enthaltenen Informationen lassen sich nutzen, um an das fragliche System adressierte IP-Pakete in Ethernet-Frames zu übersetzen. |

Diagram

Description automatically generated**Funktionsweise des Routing Information Protocol**

|  |  |
| --- | --- |
| Routing table for R4 | Routingtabelle für den Server R4 |
| Destination | Ziel |
| Gateway | Gateway |
| Interface | Schnittstelle |
| Cost | Kosten |
| Timer | Timer |

Diagram

Description automatically generated**BGP-Peering von drei autonomen Systemen**

Table

Description automatically generated with medium confidence**Hierarchische Reihenfolge der Domainnamen**

|  |  |
| --- | --- |
| login | login |
| Hostname | Hostname |
| Subdomain | Unterdomäne |
| Domain | Domäne |
| Top-level domain | Top-Level-Domain |

**Hostnamen-Hierarchie mit Zoneneinteilung**

Diagram, engineering drawing

Description automatically generated

Diagram, engineering drawing

Description automatically generated**Verschiedene Arten von DNS-Lookups**

|  |  |
| --- | --- |
| Authoritative/recursive lookup | Autoritative/rekursive Namensauflösung |
| ISP DNS server | DNS-Server des ISP |
| Local DNS server | Lokaler DNS-Server |
| Client system | Clientsystem |
| Possibly cached | Cache-Abfrage |

**DNSSEC-Überprüfung**

Diagram

Description automatically generated

|  |  |
| --- | --- |
| Key pair A (Root trust anchor) | Schlüsselpaar A (Root/Vertrauensanker) |
| Key pair B | Schlüsselpaar B |
| Key pair C | Schlüsselpaar C |
| Com zone | com-Zone |
| Example.com | example.com |
| Generated using | erzeugt mit |
| Verified by | validiert durch |
| Zone specific private key | Zonenspezifischer privater Schlüssel |
| Public key | Öffentlicher Schlüssel |
| Hash of subordinate public key | Hashwert des untergeordneten öffentlichen Schlüssels |
| Record signature | Signatur des Ressourceneintrags |

**Typische HTTP-Kommunikation**

Diagram

Description automatically generated

X

**Titel**

X

**Titel**

X

**Titel**

|  |  |
| --- | --- |
| Client | Client |
| Server | Server |
| Request | Anfrage |
| Response | Antwort |

**Typische HTTP/2-Kommunikation**

A picture containing diagram

Description automatically generated

|  |  |
| --- | --- |
| Client | Client |
| Server | Server |
| Request | Anfrage |
| Response | Antwort |
| Push | Push-Nachricht |

**Typische SMTP-Kommunikation**

Diagram

Description automatically generated with medium confidence

|  |  |
| --- | --- |
| Client | Client |
| Server | Server |
| Send email data | Übermittlung der E-Mail-Daten |
| Announce sender and recipient(s) | Nennung von Sender und Empfänger(n) |
| Connection and introduction | Verbindungsaufbau und Initiierung |
| Connect | Verbinden |
| Greeting | Bereitmeldung |
| EHLO <Client> | EHLO <Client> |
| Extensions | Erweiterungen |
| Mail from: <Sender> | MAIL FROM: <Absender> |
| RCPT TO: <Recipient> | RCPT TO: <Empfänger> |
| DATA | DATA |
| Msg ID | Nachr. ID |
| QUIT | QUIT |
| Acknowledgement or denial of commands | Bestätigung oder Ablehnung von Befehlen |

Table

Description automatically generated**Symmetrische XOR-Verschlüsselung**

|  |  |
| --- | --- |
| Original data stream | Ursprünglicher Datenstrom |
| Key | Schlüssel |
| Apply repeatedly | Wiederholung |
| Encrypted data stream | Verschlüsselter Datenstrom |
| Decrypted data stream | Entschlüsselter Datenstrom |

**Grundprinzipien der asymmetrischen Verschlüsselung**

Diagram

Description automatically generated

|  |  |
| --- | --- |
| Peer | Peer |
| Decrypt | Entschlüsselung |
| Encrypt | Verschlüsselung |
| Private key | Privater Schlüssel |
| Public key | Öffentlicher Schlüssel |

Diagram

Description automatically generated**SSH-Protokollstack**

|  |  |
| --- | --- |
| Linke Spalte (TCP/IP) | |
| Application | Anwendungsschicht |
| Transport | Transportschicht |
| Network (Internet) | Netzwerkschicht (Internet) |
| Link | Verbindungsschicht |
| Physical | Bitübertragungsschicht |
| TCP/IP | TCP/IP |
| Mittlere Spalte (SSH Protocol Stack) | |
| SSH connection protocol | SSH-Verbindungsprotokoll |
| interactive login | Interaktive Anmeldung |
| TCP/IP forwarding | TCP/IP-Weiterleitung |
| X11 forwarding | X11-Weiterleitung |
| Remote command execution | Ausführung von Remotebefehlen |
| User authentication protocol | Protokoll für die Benutzerauthentifizierung |
| SSH transport layer protocol | Transportschichtprotokoll |
| SSH protocol stack | SSH-Protokollstack |
| Rechte Spalte (ISO/OSI reference model) | |
| Application | Anwendungsschicht |
| Presentation | Darstellungsschicht |
| Session | Sitzungsschicht |
| Transport | Transportschicht |
| Network | Vermittlungsschicht |
| Link | Sicherungsschicht |
| Physical | Bitübertragungsschicht |
| ISP/OSI reference model | ISO/OSI-Referenzmodell |

**Diffie-Hellman-Schlüsselaustausch**

Diagram

Description automatically generated with medium confidence

|  |  |
| --- | --- |
| Peer | Peer |
| Calculate shared secret | Berechnung des gemeinsamen Geheimnisses |
| Secure communications channel | Sicherer Kommunikationskanal |
| Private key | Privater Schlüssel |
| Public key | Öffentlicher Schlüssel |
| Shared key | Gemeinsam verwendeter Schlüssel |

Diagram

Description automatically generated**Lokale Portweiterleitung**

|  |  |
| --- | --- |
| Client | Client |
| SSH | SSH |
| SSH traffic (Port 22) | SSH-Traffic (Port 22) |
| Firewall | Firewall |
| Intranet-server | Intranetserver |
| Server | Server |

Diagram

Description automatically generated**Remote-Portweiterleitung**

|  |  |
| --- | --- |
| Evil proxy | Feindlicher Proxy |
| Attacker | Angreifer:in |
| SSH traffic (port 22) | SSH-Traffic (Port 22) |
| Evil proxy | Feindlicher Proxy |
| Compromised victim | Opfer |

Diagram

Description automatically generated**IPSec-Protokollstack**

|  |  |
| --- | --- |
| Application | Anwendungsschicht |
| Transport | Transportschicht |
| Network (Internet) | Netzwerkschicht (Internet) |
| Link | Verbindungsschicht |
| Physical | Bitübertragungsschicht |
| TCP/IP | TCP/IP |
| The internet key exchange (IKE) | Internetschlüsselaustausch (IKE) |
| Encapsulating security payload (ESP) | Encapsulating Security Payload (ESP) |
| Authentication header (AH) | Authentifizierungsheader (AH) |
| IPSec protocol stack | IPSec-Protokollstack |

**Verarbeitung des ausgehenden Datenverkehrs**

Diagram

Description automatically generated

|  |  |
| --- | --- |
| IPSec boundary | IPSec-Perimeter |
| Protected interface | Geschützte Schnittstelle |
| SPD selection | SPD-Auswahl |
| Nested SAs | Verschachtelte SAs |
| Forwarding | Weiterleitung |
| Unprotected interface | Ungeschützte Schnittstelle |
| BYPASS | BYPASS |
| ICMP | ICMP |
| DISCARD | DISCARD |
| SPD cache | SPD-Cache |
| PROCESS (AH/ESP) | AH/ESP-Verarbeitung |

**Verarbeitung des eingehenden Datenverkehrs**Diagram

Description automatically generated

|  |  |
| --- | --- |
| Unprotected interface | Ungeschützte Schnittstelle |
| Demux | Demux |
| Not IPSec | Kein IPSec-Schutz |
| IPSec protected | IPSec-Schutz (PROTECT) |
| IPSec boundary | IPSec-Perimeter |
| IKE | IKE |
| Not | Kein |
| SPD-I | SPD-I |
| ByPASS | BYPASS |
| Forwarding | Weiterleitung |
| Protected | Geschützt |
| Discard | DISCARD |
| ICMP | ICMP |
| IPSec | IPSec |
| BYPASS | BYPASS |
| Process (AH/ESP) | AH/ESP-Verarbeitung |
| SAD Check | SAD-Prüfung |
| ICMP | ICMP |

Diagram

Description automatically generated**TLS-Protokollstack**

|  |  |
| --- | --- |
| Application | Anwendungsschicht |
| Transport | Transportschicht |
| Network (Internet) | Netzwerkschicht (Internet) |
| Link | Verbindungsschicht |
| Physical | Bitübertragungsschicht |
| TCP/IP | TCP/IP |
| Handshake protocol | Handshake Protocol |
| Cipher change protocol | Change Cipher Spec Protocol |
| Alert protocol | Alert Protocol |
| Record protocol | Record Protocol |
| TLS protocol stack | TLS-Protokollstack |

**Man-in-the-Middle-Angriff bei Diffie-Hellman-Schlüsselaustausch**Diagram

Description automatically generated

|  |  |
| --- | --- |
| Peer | Peer |
| Attacker | Angreifer:in |
| Store key | Speicherung des Schlüssels |
| Initiate outgoing connection | Initiierung der ausgehenden Verbindung |
| Calculate shared secret | Berechnung des gemeinsamen Geheimnisses |
| Private key | Privater Schlüssel |
| Publickey | Öffentlicher Schlüssel |
| Shared key | Gemeinsam verwendeter Schlüssel |
| Compromised communication | Belauschte Kommunikation |
| Secure communications channel | Sicherer Kommunikationskanal |

**Reguläre Kommunikation über HTTPS (HTTP over TLS)**

Graphical user interface

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Client | Client |
| Trust anchors | Vertrauensanker |
| CERT | ZERT |
| Public key | Öffentlicher Schlüssel |
| Router(s) | Router |
| Web server | Webserver |

**Man-in-the-Middle-Angriff**Diagram

Description automatically generated

|  |  |
| --- | --- |
| Victim | Opfer |
| Trust anchors | Vertrauensanker |
| CERT | ZERT |
| Public key | Öffentlicher Schlüssel |
| Compromised trust anchored (Still trusted) | Kompromittierter Vertrauensanker (weiterhin als vertrauenswürdig eingestuft) |
| Attacker | Angreifer:in |
| Compromised router | Manipulierter Router |
| Web server | Webserver |
| Fake web server | Falscher Webserver |

**Signieren eines Zertifikats**Diagram

Description automatically generated

|  |  |
| --- | --- |
| Subject S | Antragsteller:in A |
| Certificate authority C | Zertifizierungsstelle Z |
| Generate key pair | Erstellung eines Schlüsselpaares |
| Generate CSR | Erstellung einer CSR |
| Validate identity | Identitätsprüfung |
| Generate and sign certificate | Erstellen und Signieren des Zertifikats |
| Use/deploy certificate | Installation/Nutzung des Zertifikats |
| Certificate/CSR | Zertifikat/CSR |
| Private key | Privater Schlüssel |
| Public key | Öffentlicher Schlüssel |
| Signature | Signatur |

Graphical user interface

Description automatically generated with medium confidence**Vertrauenskette**

|  |  |
| --- | --- |
| DigiCert global root certificate (Trust anchor) | Globales Root-Zertifikat von DigiCert (Vertrauensanker) |
| Subject | Inhaber |
| Issuer | Aussteller |
| DigiCert global root | DigiCert Global Root |
| Subject public key | Öffentlicher Schlüssel des Inhabers |
| Signature (By DigiCert global root) | Signatur von DigiCert Global Root |
| Digicert CA1 certificate (Intermediate) | DigiCert CA-1 (Zwischenzertifikat) |
| www.example.com certificate | Zertifikat für www.example.com |
| Verizon/CN= www.example.com | Verizon/CN= www.example.com |
| Mathematically dependent | mathematisch voneinander abhängig |
| Generated using | erzeugt mit |
| Verified by | validiert durch |
| Private key | Privater Schlüssel |
| public key | Öffentlicher Schlüssel |
| Certificate signature | Zertifikatsignatur |

Diagram

Description automatically generated**Prozessphasen des CRISP-DM-Modells**

|  |  |
| --- | --- |
| Business understanding | Business Understanding |
| Data understanding | Data Understanding |
| Data preparation | Data Preparation |
| Modeling | Modeling |
| Evaluation | Evaluation |
| Deployment | Deployment |
| Data | Daten |

**Definition der CRISP-DM-Phasen**

Graphical user interface, text, application

Description automatically generated

|  |  |
| --- | --- |
| Business understanding. In this phase, data analysts form and deepen an understanding of business-relevant processes and factors. This is a technology-independent phase. | Business Understanding: In dieser Phase machen sich die Datenanalyst:innen mit den geschäftlich relevanten Prozessen und Faktoren vertraut. Dabei ist das Vorgehen unabhängig von den im Unternehmen genutzten Technologien. |
| Data understanding. In this phase, the relationships are formed between the gathered data and the factors that influence them. This includes the integration and consolidation of gathered data in a data warehouse, and its enrichment with hierarchical dimensions, annotations, and external data sources. | Data Understanding: Hier werden die verfügbaren Daten zusammengeführt und vor dem Hintergrund der ermittelten Einfluss- und Erfolgsfaktoren auf ihre Nutzbarkeit geprüft. Das bedeutet unter anderem, dass alle Bestände in einem sogenannten Data Warehouse konsolidiert, in hierarchische Strukturen eingegliedert und mit Anmerkungen und Informationen aus externen Datenquellen angereichert werden. |
| Data preparation/data cleaning. In this phase, the structured data for specific or unspecific questions are selected from the data warehouse. The data is also transformed in order to facilitate its subsequent processing. A selected portion of a data warehouse is also called a "data mart." | Data Preparation/Data Cleaning: In dieser Phase werden die zur Beantwortung spezifischer oder unspezifischer Fragen nötigen Daten aus dem Data Warehouse ausgewählt und zu einem sogenannte „Data Mart“ zusammengefasst. Dessen Inhalt wird dann so aufbereitet, wie dies für die anschließende Datenverarbeitung erforderlich und optimal ist. |
| Modeling/data mining. In this step, data mining techniques and technologies are applied in order to find patterns in the data and build models that represent the discovered patterns. | Modeling/Data Mining: Dieser Schritt basiert auf Data-Mining-Methoden und -Technologien, mit denen Muster in den Daten identifiziert und in repräsentative Modelle übersetzt werden können. |
| Evaluation. The models that are derived using data mining techniques need to be put to the test to ensure that they represent real interrelations. If the models pass the test, they can be interpreted in order to gain previously undiscovered knowledge. | Evaluation: Die mithilfe von Data-Mining-Methoden erstellten Modelle müssen getestet werden, damit sichergestellt ist, dass sie die realen Zusammenhänge präzise abbilden. Nach bestandener Prüfung lassen sie sich zur Gewinnung neuer Erkenntnisse nutzen. |
| Deployment. This last phase provides feedback to the process. Depending on the interpretation of the identified interrelations, this can include future business decision and expose the need for further data sources. | Deployment: In der letzten Phase erfolgt die Rückmeldung der erzielten Ergebnisse an die Entscheidungsträger:innen. So können die identifizierten Zusammenhänge beispielsweise als Basis für künftige geschäftliche Entscheidungen oder für einen Business Case zur Implementierung weiterer Datenquellen dienen. |

Diagram

Description automatically generated**Knowledge Discovery in Databases und Netzwerkforensik im Vergleich**

|  |  |
| --- | --- |
| Business understanding and data understanding | Business Understanding und Data Understanding |
| Preparation | Vorbereitung |
| Data preparation | Data Preparation |
| Detection | Erkennung |
| Collection | Datensammlung |
| Preservation | Beweissicherung |
| Examination | Prüfung |
| Modeling | Modeling |
| Analysis | Analyse |
| Investigation | Untersuchung |
| Presentation | Ergebnispräsentation |
| Evaluation | Evaluation |
| Incident response | Incident Response |
| Deployment | Deployment |

**Forensische Äquivalente der KDD-Phasen**

Text

Description automatically generated

|  |  |
| --- | --- |
| The business and data understanding stages in CROSP-DM are very similar to the preparation stage. In the network forensics process, the preparation stage includes training with regard to new threats and constant assessment of the IT landscape. | Die Phasen „Business Understanding“ und „Data Understanding“ aus dem CRISP-DM-Modell finden ihre Entsprechung in der Vorbereitungsstufe aus unserem generischen Ablaufmodell für die Netzwerkforensik. Im Vordergrund stehen hier präventive Maßnahmen wie beispielsweise die Sensibilisierung der Belegschaft für neue Bedrohungen und die kontinuierliche Evaluation der IT-Infrastruktur. |
| The data preparation phase in CRISP-DM can be matched with the detection, collection, and preservation stages in network forensics. In both processes, a reliable base for further analysis is formed. | Das Äquivalent zur CRISP-DM-Phase „Data Preparation“ sind Erkennung, Datensammlung und Beweissicherung aus dem allgemeinen Forensikmodell. Denn in beiden Prozessen geht es an dieser Stelle um die Schaffung einer verlässlichen Datengrundlage für anschließende Analysen. |
| The modeling stage in CRISP-DM is equivalent to the examination and analysis steps in network forensics. Advanced techniques are used to uncover patterns and interrelationships. | Die CRISP-DM-Stufe „Modeling“ korrespondiert in der Netzwerkforensik mit den Phasen „Prüfung“ und „Analyse“, da hier wie dort moderne Verfahren zur Identifizierung von Mustern und Zusammenhängen eingesetzt werden. |
| the evaluation phase in CRISP-DM is similar to the investigation and presentation stages in network forensics. The identified patters are evaluated and put into the context of a running investigation. In network forensics, however, ther is a stronger coupling with the previous stage. A running investigation very rapidly introduces new research questions that must be andwered in a timely manner through data analysis. If an investigation can be concluded, the gathered and evaluated evidence is presented to authorities and decision makers. | Die Phase „Evaluation“ aus dem CRISP-DM ähnelt den Stufen „Untersuchung“ und „Ergebnispräsentation“ aus der Netzwerkforensik. In beiden Fällen werden die identifizierten Muster im Kontext eines laufenden Projekts bzw. einer laufenden Ermittlung betrachtet. Allerdings weist die Netzwerkforensik an dieser Stelle eine deutlich stärkere Kopplung mit den vorherigen Stufen auf, weil im Rahmen einer forensischen Untersuchung immer neue Forschungsfragen hinzukommen, die dann so rasch wie möglich mithilfe von Datenanalysen beantwortet werden müssen. Abgesehen davon werden gesammelte forensische Erkenntnisse nach Abschluss der Untersuchung nicht nur an die involvierten Entscheidungsträger:innen, sondern auch an die zuständigen Behörden übermittelt. |
| The deployment phase in CRSIP-DM can be compared to the incident response step in network forensics. In KDD, the uncovered knowledge is put into effect in the business. In network forensics, the deiscovered knowledge leads to an improvement in IT security measures. | Die Abschlussphase des CRISP-DM („Deployment“) entspricht am ehesten der Stufe „Incident Response“ aus der Netzforensik. Am Ende des KDD-Prozesses werden die gewonnenen Erkenntnisse zur Optimierung des Geschäftsbetriebs genutzt. In der Netzwerkforensik ermöglichen die Ergebnisse gezielte Verbesserungen der IT-Sicherheitsmaßnahmen. |

Diagram

Description automatically generated

|  |  |
| --- | --- |
| Preparation | Vorbereitung |
| Detection | Erkennung |
| Incident response | Incident Response |

Diagram

Description automatically generated

|  |  |
| --- | --- |
| Client | Client |
| Server | Server |

Table

Description automatically generated

|  |  |
| --- | --- |
| System Accesses Across Network Segments | Systemzugriffe aus verschiedenen Netzwerksegmenten/Abteilungen |
| System | System |
| Department | Abteilung |
| Source code repository | Quellcode-Repository |
| Intranet | Intranet |
| Document management system | Dokumentverwaltungssystem |
| Financial accounting system | Finanz- und Buchhaltungssystem |
| Software development | Softwareentwicklung |
| Public relations | Public Relations |
| Accounting | Buchführung |
| Quality assurance | Qualitätssicherung |