Fremdgerät in einem Firmennetzwerk

Hausarbeit

vorgelegt von

Stavros Giannis, Lenny Scheiding, Ozan Ayik, Max Büschgens, Lars Heitmann

Prof. Dr. Marcus Niemietz
Cyber Security Management
Clavis - Institut für Informationssicherheit

Entstanden an der

Hochschule Niederrhein
University of Applied Sciences
Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Inhaltsverzeichnis

Abkürzungsverzeichnis

ARP Address Resolution Protocol

CPU Central Processing Unit

FTP File Transfer Protocol

GPU Graphics Processing Unit

HTTP Hypertext Transfer Protocol

IDS Intrusion Detection System

IoT Internet of Things

IP Internet Protocol address

IPS Intrusion Prevention System

IT Information Technology

MAC Media Access Control address

OSINT Open-Source-Intelligence

PC Personal Computer

PCAP Packet Capture

RAM Random Access Memory

ROM Read-Only Memory

SMTP Simple Mail Transfer Protocol

SSH Secure Shell

TCP Transmission Control Protocol

VM Virtual Machine

VPN Virtuale Private Network

Abbildungsverzeichnis

Listings

Tabellenverzeichnis

Zusammenfassung

Im Rahmen dieser wissenschaftlichen Arbeit wird die Vorgehensweise bei einer IT-Forensik Untersuchung, wie sie zur Ermittlung von Beweisen und Informationen über ein Gerät bei einem möglichen Vorfall genutzt wird. Die Untersuchung wird in sechs Schritte unterteilt: strategische Vorbereitung, operative Vorbereitung, Datensammlung, Untersuchung, Datenanalyse und Dokumentation. Dabei werden geeignete Tools ausgewählt und die Daten der betroffenen Komponenten gesammelt, um sie anschließend zu analysieren und zu dokumentieren. Der Text betont die Bedeutung von Dokumentation und Verfälschungsvermeidung während der Untersuchung. Die IT-Forensik ist ein wichtiger Bereich in der digitalen Welt, da sie bei der Untersuchung von möglichen Sicherheitsvorfällen oder Straftaten hilft, Beweise zu sammeln und Informationen über das betroffene Gerät zu erlangen. Dabei gibt es bestimmte Vorgehensweisen und Schritte, die befolgt werden müssen, um eine erfolgreiche Untersuchung durchführen zu können.

Zusammenfassend ist die IT-Forensik ein wichtiger Bereich bei der Untersuchung von möglichen Sicherheitsvorfällen und Straftaten. Es gibt bestimmte Vorgehensweisen und Schritte, die befolgt werden müssen, um eine erfolgreiche Untersuchung durchführen zu können. Auch die Identifikation des Schadenausmaßes nach einem Angriff auf ein Unternehmen ist von großer Bedeutung und erfordert die Analyse vorhandener Unternehmensprozesse. Die Nutzung von OSINT kann dabei helfen, weitere Informationen über den Angreifer und mögliche Schwachstellen im Unternehmen zu sammeln. Es ist wichtig, alle gesammelten Informationen sorgfältig zu analysieren und zu dokumentieren, um sie im Nachhinein nachvollziehbar zu machen und bei Bedarf als Beweismittel nutzen zu können.

1 Einführung

In der heutigen Zeit häufen sich Cyber-Angriffe. Angreifer werden dadurch in ihren Strategien und Herangehensweisen immer kreativer.
Diese Arbeit behandelt den Vorfall, dass ein „Eigenbau-PC“ in einem Unternehmen gefunden wird. Hierbei ist davon auszugehen, dass dieser eingesetzt wurde, um dem Unternehmen Schaden zuzufügen. Sowohl die Fähigkeiten und das eigentliche Schadensausmaß können nicht direkt nach dem Fund ermittelt und müssen weiter untersucht werden.
Nun befindet sich das Gerät auf der Dienststelle und im weiteren Verfahren soll ermittelt werden, welche Spuren sich auf diesem befinden, die auf einen Tatverdächtigen zurückzuführen sind.
Mithilfe einer forensischen Untersuchung werden diese Fragen aufgegriffen und beantwortet. Zunächst wird erklärt, wie eine forensische Analyse durchgeführt wird und wie eine genaue Kopie des gefundenen Datenträgers angefertigt werden muss.
Daraufhin wird ermittelt, mit welchen Methoden der Computer an sich identifiziert werden kann. Dabei wird sowohl auf die verarbeitete Hardware geachtet, als auch, welches Betriebssystem verwendet wurde und wie dieses ermittelt werden kann.
Im weiteren Verlauf werden Herangehensweisen definiert, wie die Fähigkeiten des „Eigenbau-PCs“ analysiert und herausgestellt werden können. Weitergehend wird erläutert, wie das gesamte Schadensausmaß, welches das fremde Gerät verursacht hat, definiert werden muss. Abschließend wird das OSINT Modell erklärt, welches für die Rückverfolgung des Täters genutzt werden kann.

2 Grundsätze der IT-Forensik

Die Praktik der IT-Forensik wird in unserem Fallbeispiel benötigt, um nicht nur logische Beweise für den Täter zu finden, sondern auch um die möglichen Fähigkeiten und gesammelten Daten des Gerätes zu ermitteln.

2.1 Vorgehensweise einer forensischen Untersuchung

Bevor eine Untersuchung durchgeführt werden kann, braucht es, wie in der medizinischen Forensik auch, ein Symptom, welches Auffälligkeiten in einem System aufweist. Im Falle der IT-Forensik kann dieses Symptom sich beispielsweise durch abnormales Verhalten von Teilsystemen oder ganzen Netzwerken ausdrücken. Sofern ein Nutzer diese Unregelmäßigkeiten nicht selbst bemerkt, muss mithilfe von integrierten Warnmechanismen über eine solche Anomalie informiert werden. Dieser Alarm muss aber auch dementsprechend dokumentiert werden, ansonsten kann die Basis der Untersuchung nicht nachvollzogen werden.
Für die weitere Vorgehensweise der forensischen Untersuchung bezieht sich das BSI auf ein Modell, welches in mehreren Prozessen gegliedert ist, die logisch aneinanderhängen und eine erfolgreiche Auswertung erleichtern. Jedoch gibt es für jede Art von Untersuchung oder Alarm auch eigene Modelle und darunter wieder eigene Prozesse, wobei der Großteil auf Strafverfolgungsbehörden abgestimmt ist. Zusammengefasst stellt das BSI das gesamte forensische Verfahren in sechs Abschnitten dar[1]:

- strategische Vorbereitung
- operationale Vorbereitung
- Datensammlung
- Untersuchung
- Datenanalyse
- Dokumentation

[1] vgl. BSI (2011), S. 24

Anhand der Aufzählung erkennt man, dass eine jede forensische Untersuchung mit einer gezielten Vorbereitung beginnt. Dabei werden geeignete Tools identifiziert, die im Verlauf der Untersuchung benutzt werden, dabei ist wichtig, dass für jede Untersuchung wahrscheinlich andere Hilfsmittel benutzt werden müssen. Ebenso werden die Kriterien und Begründung der Auswahl dokumentiert und können im weiteren Verlauf angepasst werden. Ziel solcher Tools sollte sein, die Datengewinnung zu erhöhen.
Im nächsten Schritt beginnt die Sammlung von Daten der betroffenen Komponenten, welche ebenfalls, wie die benutzten Tools, dokumentiert werden muss. Besonders wichtig dabei ist, dass die betroffenen Daten bei der Speicherung nicht verfälscht werden dürfen. Falls dies doch der Fall ist oder Datensätze nicht vollständig sind, muss der Grad der Verfälschung bewertet und gerechtfertigt werden. Insgesamt soll am Ende ein dokumentiertes Verfahren entstehen, in dem ein Abbild aller betroffenen Datenträger, die für die Untersuchung benötigt werden, erstellt werden.
Erst in der Untersuchung werden die Daten an sich extrahiert und auch eingegrenzt. Beispielsweise empfiehlt das BSI, einige oder alle Daten mit Checksummen zu überprüfen. Damit stellt man sicher, ob die Daten verändert oder unbekannt sind. Andererseits kann sich während der Überprüfung herausstellen, dass die allgemeine Überprüfung auf weitere Komponenten oder Systeme ausgeweitet werden muss. Der gesamte Prozess der Untersuchung muss dokumentiert werden.
Die Datenanalyse beschreibt die Zusammenfassung und logische Abfolge von einzelnen Teilkomponenten und Untersuchungen. Ebenfalls kann sich die Untersuchung dabei auf andere Komponenten ausweiten, die zu diesem Zeitpunkt nicht betrachtet wurden. Diese müssen dann dokumentiert und einzeln abgearbeitet werden.
Der finale Schritt einer jeden forensischen Untersuchung ist die Zusammenfassung aller Dokumentationen der einzelnen Phasen, um damit einen oder mehrere Abschlussberichte zu generieren. Dabei muss darauf geachtet werden, welches Organ einer Organisation diesen Bericht enthält. Zum Beispiel enthält ein Bericht für einen Systemadministrator mehr technische Details als für das Management. Auch enthält der Bericht mögliche Verbesserungsvorschläge für die betroffene Anlage und auch weitere Vorgehensweisen. Diese können die allgemeine Struktur einer Anlage betreffen, oder auch wie mit möglichen Warnungen umgegangen wird [2].

[2] vgl. BSI (2011), S. 24

2.2 Die beweissichernde Anfertigung eines Datenträgerbilds

In einer forensischen Untersuchung ist es wichtig, keine Daten während der Untersuchung zu verändern. Dies würde nicht nur die Ergebnisse verfälschen, sondern auch die eigentliche Untersuchung an sich. Aus diesem Grund sollte man immer für eine Untersuchung eine Kopie des zu untersuchenden Datenträgers erstellen. Dadurch wird das eigentliche System nicht verändert und es eröffnet mehr Spielraum für die Untersuchung. Ein weiterer Vorteil ist, dass mehrere verschiedene Teams oder Personen gleichzeitig am gleichen Datenträgerabbild arbeiten können, da dieser beliebig oft kopiert werden kann. Dieser Vorgang, um ein Datenträgerabbild zu erstellen, im Englischen auch „Image“ genannt, wird allgemein als forensische Duplikation bezeichnet.
Das BSI stellt für eine forensische Duplikation folgende Anforderungen[3].:

- **Physische Kopie** – Von jedem Datenträger muss der gesamte Dateipfad und Systemumgebung auf einem physischen Gerät gespeichert werden
- **Fehlerbehandlung** - Falls Lesefehler auftreten oder Abschnitte korrumpiert sind und damit nicht mehr ausgelesen werden können, muss dies dokumentiert werden. Diese Lücken werden dann, durch in der Untersuchung vorher festgelegte Füllmuster, ersetzt.
- **Vollständigkeit des Abbildes** - Falls Partitionen auf dem Abbild bestehen, muss darauf geachtet werden, diese zunächst zu erkennen und falls ebenfalls Reservierungen des Speichers vorliegen, diese zu deaktivieren. Dadurch garantiert man ein vollständiges Image.
- **Unveränderbarkeit** – Um eine garantierte Unveränderbarkeit zu erzielen, müssen alle erstellten Abbilder mit einer kryptografischen Checksumme, auch genannt Hashwert, geprüft werden. Falls bei der Erstellung Daten verändert wurden, sind die Checksummen verschieden

Um einen absoluten Schreibschutz zu garantieren, dass während der Untersuchung keine Daten bearbeitet oder verändert werden, müssen sogenannte Writeblocker eingesetzt werden. Diese verhindern jeglichen Schreibzugriff auf den gesamten Datenträger, sodass die darauf vorhandenen Daten nur gelesen, aber nicht verändert werden können. Diese Writeblocker sind eine zuverlässige Versicherung gegen eine Veränderung der Daten und können an verschiedenen Schnittstellen des Systems angebracht werden. Ebenfalls sollte man auf forensische Betriebssysteme oder Software verzichten, da diese selbst beim Booten bereits Daten, auch wenn nur minimal, verändern können[4].

[3] vgl. BSI (2011), S. 26
[4] vgl. BSI (2011), S. 26

Der Arbeitsverlauf zur Erstellung lässt sich rudimentär auf drei Arbeitsschritte beschränken[5]:

1. Am Anfang müssen die Datenträger identifiziert und je nach System die zu benutzenden Werkzeuge angepasst werden.
2. Daraufhin wird die eigentliche forensische Duplikation unter Berücksichtigung der vorher genannten Schritte durchgeführt. Heißt, es wird ein vollständiges und physisches Abbild des Datenträgers erstellt.
3. Im letzten Schritt wird überprüft, ob das Verfahren erfolgreich war. Dafür benutzt man eine Checksumme, um das Abbild mit dem Original zu vergleichen. Falls diese übereinstimmen, ist das Image eine perfekte Kopie.

[5] vgl. BSI (2011), S. 27

3 Identifizierung des Betriebssystems

3.1 Identifizierung des Computers

Durch die Information, dass der Eigenbau-PC sich in einem Bodentank befindet, muss es sich um ein kleines und kompaktes Gerät handeln. Dies schränkt die möglichen Arten von Computern ein. In unserem Szenario wird ein Raspberry Pi verwendet, welcher der Kategorie eines SoCs zugeordnet werden kann.
Ein SoC kann als integrierte Schaltung verstanden werden, die alle Komponenten eines elektronischen Systems auf einem einzigen Chip vereint. Dies beinhaltet unter anderem die Central Processing Unit (CPU), Graphics Processing Unit (GPU), Random Access Memory (RAM), Read-Only Memory (ROM) und weitere Peripherie-Bauteile wie Sensoren, Kommunikationsmodule und mehr[1].

3.2 Die Boot-Sektor-Analyse

Ein Verfahren zur Identifikation von Betriebssystemen auf SoC-Geräten, das sich auf den Byte-Sektor bezieht, besteht darin, die ersten Sektoren einer Festplatte oder eines anderen Speichermediums zu analysieren, um Informationen über das Betriebssystem zu erhalten. Die ersten Sektoren einer Festplatte werden als Boot-Sektoren bezeichnet und enthalten in der Regel wichtige Informationen über das Betriebssystem, das auf dem SoC ausgeführt wird. Bei diesem Verfahren werden zunächst die ersten Sektoren

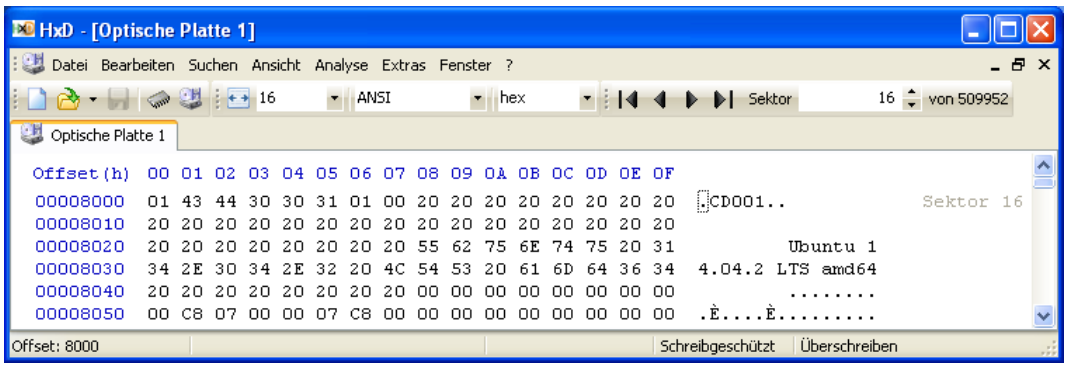

Abbildung 3.1: HxD als Disc-Editor

[1] vgl. Gupta et al. (2019)

der Festplatte ausgelesen und analysiert[2]. Dazu können spezielle Werkzeuge wie Disc-Editoren oder Hex-Editoren verwendet werden, die es ermöglichen, die Inhalte der Boot-Sektoren direkt zu betrachten und zu analysieren (s. Abb. 3.1). Die ausgelesenen Sektoren können dann mit Datenbanken von Betriebssystemen verglichen werden, um herauszufinden, welches Betriebssystem auf dem SoC ausgeführt wird.
Dieses Verfahren kann bei der Identifikation von Betriebssystemen auf SoCs hilfreich sein, da es direkt auf die Boot-Sektoren zugreift und somit möglicherweise Informationen liefern kann, die von anderen Methoden nicht erfasst werden. Allerdings ist es auch wichtig zu beachten, dass das Betriebssystem auf einem SoC möglicherweise verschlüsselt oder anderweitig geschützt sein kann, was die Analyse der Boot-Sektoren erschweren könnte[3].

3.3 Forensische Untersuchung von Linux

Das Linux Betriebssystem stellt standardgemäß einige Datensätze bereit, welche für die forensische Analyse verwendet werden kann. Dabei ist besonders wichtig zu erwähnen, dass die meisten der Dateien, welche in diesem Kapitel behandelt werden, nach Abschalten des Geräts nicht ohne weiteres wiederherstellbar sind. Daher ist es besonders wichtig, das Gerät nicht abzuschalten, da sonst Daten von besonderem Interesse verloren gehen. Darunter zählen unter anderem Informationen zu geladenen Kernelmodulen, IP-Verbindungsinformationen oder Hauptspeicherinhalte. Dennoch bietet der Linux-Kernel einen entscheidenden Vorteil. Diese Datensätze können in den Dateipfaden „/proc“ und „/sys“ gefunden werden. Angesichts dessen wird keine externe Software für die forensische Untersuchung benötigt[4].

3.3.1 Konfigurationsdaten

Konfigurationsdaten von Linux werden weitestgehend im Dateipfad „/proc“ abgelegt. Das Linux-Betriebssystem speichert verwendete Dateisysteme in der Datei „/proc/mounts“ ab. Hier werden alle Informationen zu Dateisystemen aufgelistet. Insbesondere die eingesetzten Datenträger in Verbindung mit dem Einhängepunkt (engl. mount), sowie welches Dateisystem benutzt wird, wo sich die Datenträger physisch befinden und welche Optionen an einem Dateisystem geknüpft sind. Darunter zählt bspw. der Lese- und Schreibzugriff[5].
Um die genutzten Swap-Dateisysteme unter Linux anzuzeigen, kann der Befehl

[2] vgl. Liu et al. (2019)
[3] vgl. Liu et al. (2019)
[4] vgl. Liu et al. (2019)
[5] vgl. BSI (2011), S. 127 f.

Iface	Destination	Gateway	Flags	RefCnt	Use	Metric	Mask	MUT	Window	IRTT
eth0	0000A8C0	00000000	0001	0	0	0	00FFFFFF	Cell 9	0	0
eth0	00000000	0100A8C0	0003	0	0	0	00000000	Cell 9	0	0

Tabelle 3.2: Aufbau einer Routen-Tabelle

„cat /proc/swaps“ verwendet werden. Swap-Dateisysteme erweitern den Arbeitsspeicher, indem auf freien Festplattenplatz zugegriffen wird. Unter Linux können Swap-Dateisysteme als Swap-Partitionen und Swap-Dateien verwendet werden. „/proc/swaps“ liefert eine Liste aller genutzten Swap-Dateisysteme mit der Position, Größe und deren aktuellen Auslastung [6].
In „/proc/modules“, „/sys/module“ und „/proc/config.gz“ werden Informationen zum Kernel hinterlegt. Eine Liste den geladenen Kernel-Modulen befindet sich in „/proc/modules“ und „/sys/module“ enthält für jedes dieser Module weitere Datensätze. Die „/proc/config.gz“-Datei enthält die Konfiguration zum Kernel. Diese Option ist jedoch nicht standardmäßig eingeschaltet und muss vorher im Kernel aktiviert werden. Daher benötigt dieser Schritt eine operative Vorbereitung. Die aktuelle Kernel-Version kann unter „/proc/version“ aufgerufen werden[7].
Eine Liste der vorhandenen Partitionen ist unter „/proc/partitions“ vorzufinden. Dabei werden die vorhandenen Partitionen auf dem System und deren Eigenschaften, wie die Größe, den Typ und das Dateisystem, aufgerufen [8].

3.3.2 Kommunikationsprotokolldaten

Netzwerkdaten sind für die forensische Untersuchung enorm wichtig. In diesem Kapitel werden nur die Kommunikationsdaten gesammelt, welche der Kernel zur Verfügung stellt. Darunter fallen beispielsweise MAC- und IP-Adressen.
Die Routen-Tabelle unter dem Befehl „route“ oder in „/proc/net/route“ liefert Informationen über Wege von TCP/IP-Pakete durch das Netzwerk. Der Weg von TCP/IP-Pakete hängt gewöhnlich von der Zieladresse ab. Diese Erkenntnis der Zieladresse kann der forensischen Untersuchung dabei helfen, Anhaltspunkte über weitere betroffene Systeme zu erhalten. Daher ist diese Datenquelle auch im Abschnitt der operationalen Vorbereitung relevant. Der Aufbau der Routen-Tabelle wird in Tabelle XY dargestellt. [9].

Um IP- und MAC-Adressen letzter Kommunikationspartner aufzulisten, kann der Befehl „cat /proc/net/arp“ verwendet werden. Die ARP-Tabelle ist der sogenannte ARP-Cache eines Computers. Diese speichert alle Informationen von kommunizierten Computern. Neben IP- und MAC-Adressen werden ebenfalls die verwendete Netz-

[6] vgl. BSI (2011), S. 128
[7] vgl. BSI (2011), S. 128 f.
[8] vgl. BSI (2011), S. 128
[9] vgl. BSI (2011), S. 129 f.

werkschnittstelle und der Hardwaretyp abgespeichert[10].

```
root@utopia:~# cat /proc/net/arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.85.26    0x1         0x2         00:1A:4F:85:0F:6D     *        eth1
192.168.85.31    0x1         0x2         00:12:43:30:C1:E7     *        eth1
192.168.85.1     0x1         0x2         00:0C:29:8A:B1:69     *        eth1
192.168.85.88    0x1         0x2         00:21:85:FB:66:3B     *        eth1
192.168.85.157   0x1         0x2         00:24:21:9C:71:34     *        eth1
192.168.85.24    0x1         0x2         00:16:38:AE:1D:F4     *        eth1
192.168.85.86    0x1         0x2         00:00:F0:20:C8:E6     *        eth1
192.168.85.30    0x1         0x2         00:0A:8A:A2:30:B5     *        eth1
192.168.85.128   0x1         0x2         00:30:1B:B8:1E:6C     *        eth1
```

Abbildung 3.3: Aufbau einer ARP-Tabelle

Da die MAC-Adresse eines Netzwerkadapter softwareseitig veränderbar ist, sollte die MAC-Adresse des vorliegenden Computers manuell erfasst werden. Die MAC-Adresse der ersten Netzwerkkarte kann unter „/sys/class/net/eth0/address“ aufgerufen werden. Um die MAC-Adresse weiterer Netzwerkkarten zu ermitteln, wird „eth0“ durch „eth1“ oder „eth2“ ersetzt. Besonders wichtig hierbei zu erwähnen ist, dass dieses Muster bei einem WLAN-Adapter abweicht[11].
Neben der MAC-Adresse eines Netzwerkadapters können ebenfalls gesendete und empfangene Pakete analysiert werden. Dabei besteht die Möglichkeit für jeden einzelnen Netzwerkadapter die Anzahl der übertragenen Datenmenge unter „/proc/net/dev“ herauszufiltern. Hierbei wird zusätzlich zwischen der Anzahl von verworfenen (drop) und fehlerhaften (errors) Netzwerkpakete unterschieden[12].
Um aktuelle Verbindung einzusehen, muss im Rahmen der strategischen Vorbereitung das Kernel-Modul „ip_conntrack“ geladen oder das „IP-Connectiontracking“ aktiviert werden. Danach ist es möglich unter „/proc/net/ip_conntrack“ und „/proc/-net/nf_conntrack“ aktive Verbindungen anzeigen zulassen[13].

3.3.3 Prozessdaten

Die Sammlung von Prozessdaten ermöglicht, Prozesse festzustellen, um weitere Programme als Beweismittel zu identifizieren. Daten über jeden einzelnen Prozess können unter „/proc/Prozessnummer“ gefunden werden. Dabei ist besonders interessant, welcher Prozess an welchem Programm gebunden ist. Des Weiteren lassen sich verwendete Dateien identifizieren, die im Unterverzeichnis „../fd“ gespeichert werden.[14].

[10] vgl. BSI (2011), S. 130
[11] vgl. BSI (2011), S. 130
[12] vgl. BSI (2011), S. 131
[13] vgl. BSI (2011), S. 131
[14] vgl. BSI (2011), S. 131

4 Identifikation von böswilligen Prozessen

Die Identifikation von böswilligen Prozessen ist ein wichtiger Aspekt der Cybersicherheit[1]. Böswillige Prozesse sind Programme oder Skripte, die ohne die Erlaubnis oder das Wissen des Benutzers auf einem Computer ausgeführt werden und Schaden anrichten können, zum Beispiel durch das Löschen von Dateien, das Stehlen von Daten oder das Verbreiten von Malware[2].
Es gibt verschiedene Möglichkeiten, diese Prozesse zu identifizieren. Eine Möglichkeit ist die Verwendung von Sicherheitssoftware, die böswillige Aktivitäten auf einem Computer überwacht und Alarm schlägt, wenn verdächtige Aktivitäten festgestellt werden[3]. Eine andere Möglichkeit ist die Überwachung von Netzwerkverkehr und die Suche nach Anomalien, die auf böswillige Aktivitäten hindeuten könnten[4]. In diesem Szenario gehen wir davon aus, dass der „Eigenbau-PC“ die ganze Netzwerkaktivität mitgeschnitten hatte.

4.0.1 Packet Sniffing

Das Packet Sniffing mit böswilliger Intention bezieht sich auf das Ausspähen von Datenpaketen im Netzwerkverkehr, mit dem Ziel, sensible Informationen zu stehlen oder Schaden anzurichten[5]. Diese Art von Packet Sniffing wird häufig von Hackern oder Kriminellen verwendet, um Zugriff auf geschützte Systeme zu erlangen oder Daten zu stehlen[6].
Um Packet Sniffing zu verhindern, gibt es verschiedene Sicherheitsmaßnahmen, die eingesetzt werden können. Eine Möglichkeit ist die Verwendung von Verschlüsselungstechnologien, um sicherzustellen, dass die Daten, die über das Netzwerk übertragen werden, nicht von Dritten abgefangen werden können[7]. Auch die Überwachung des Netzwerkverkehrs und die Erkennung von Anomalien kann dazu beitragen, böswillige Packet Sniffing-Aktivitäten zu identifizieren und zu verhindern. Diese Art von

[1] vgl. Khan et al. (2019)
[2] vgl. Wang, Zhao, Hu & Chen (2018)
[3] vgl. Khan et al. (2019)
[4] vgl. Wang, Zhao, Hu & Chen (2018)
[5] vgl. Zhao et al. (2016)
[6] vgl. Zhao et al. (2016)
[7] vgl. Wang, Zhao, Hu & Chen (2018)

Systemen nennt man Intrusion Prevention System (IDS) und Intrusion Detection System (IPS)[8].

4.0.1.1 Packet Sniffing: PCAP Dumps

PCAP (Packet Capture) Dumps sind Protokolle von Netzwerkverkehr, die von Packet Sniffing-Tools wie Wireshark erstellt werden. Sie enthalten Kopien von Datenpaketen, die im Netzwerkverkehr aufgezeichnet wurden, und können zur Analyse und Fehlerbehebung von Netzwerkproblemen verwendet werden. In manchen Fällen können aus PCAP Dumps Benutzernamen und Passwörter extrahiert werden, wenn sie im Klartext im Netzwerkverkehr übertragen werden. Dies kommt häufig bei Protokollen wie HTTP (Hypertext Transfer Protocol) oder FTP (File Transfer Protocol) vor, bei denen Benutzernamen und Passwörter im Klartext übertragen werden, anstatt verschlüsselt zu sein[9].
Um Benutzernamen und Passwörter aus PCAP Dumps zu extrahieren, können Sie Wireshark verwenden und den Netzwerkverkehr filtern, um nach diesen Informationen zu suchen. Sie können auch spezielle Tools verwenden, die für die Auswertung von PCAP Dumps entwickelt wurden und die Suche nach Benutzernamen und Passwörtern erleichtern. Es ist jedoch wichtig zu beachten, dass die meisten modernen Protokolle Benutzernamen und Passwörter verschlüsseln, um sie vor dem Abfangen zu schützen. In diesem Fall wäre es unmöglich, Benutzernamen und Passwörter direkt aus PCAP Dumps zu extrahieren. Stattdessen müssten Sie versuchen, die Verschlüsselung zu knacken, was eine sehr schwierige Aufgabe darstellen kann.

4.0.1.2 Packet Sniffing: in der Praxis

Der Befehl „tcpdump“ ist ein mächtiges Werkzeug zur Analyse von Netzwerkverkehr. Er ermöglicht es, Kopien von Datenpaketen im Netzwerk aufzuzeichnen und zu analysieren[10], um Probleme mit Netzwerkverbindungen zu identifizieren oder böswillige Aktivitäten zu überwachen.
In dieser wissenschaftlichen Arbeit werden wir uns mit dem Thema Packet Sniffing in SoC-Geräten auseinandersetzen und uns genauer damit beschäftigen, wie diese Geräte funktionieren und welche Risiken sie darstellen können[11]. Wir werden aufzeigen, wie Packet Sniffing in SoC-Geräten funktioniert und welche Daten ausspioniert werden können, um das Szenario nachzustellen. Wir werden dabei auf die verschiedenen Optionen und Filter, die „tcpdump“ bietet, eingehen und beleuchten, wie man damit

[8] vgl. Wang, Hu, Zhao & Chen (2018)
[9] vgl. Wang, Hu, Zhao & Chen (2018)
[10] vgl. Khan et al. (2019)
[11] vgl. Wang, Zhao, Hu & Chen (2018)

Datenpakete analysieren und visualisieren kann[12].

Um die Datenpakete aufzuzeichnen, wird der angegebene Befehl (siehe Listing 3.2) ausgeführt.

```
:~$ sudo tcpdump -i eth0 -nn -s0 -v port 80 -w capture.pcap
```

Listing 4.1: Tcpdump Command Line

Er wird über die Kommandozeile oder ein Terminal aufgerufen und kann verwendet werden, um Datenpakete aufzuzeichnen, die über ein bestimmtes Netzwerkinterface (hier: „eth0“) gesendet werden. Die Optionen „-nn“ und „-s0“ geben an, dass „tcpdump“ keine Namensauflösung für IP-Adressen und Portnummern durchführen soll und dass die Größe der aufgezeichneten Datenpakete nicht beschränkt wird. Die Option „-v“ gibt an, dass „tcpdump“ detaillierte Informationen über die aufgezeichneten Datenpakete anzeigen soll.
Der Befehl beschränkt sich auf den Port 80, was bedeutet, dass nur Datenpakete, die an oder von diesem Port gesendet werden, aufgezeichnet werden. Port 80 ist der Standard-HTTP-Port und wird häufig für Webverkehr verwendet[13]. Wenn Sie diesen Befehl ausführen, wird „tcpdump“ alle Datenpakete aufzeichnen, die über das Netzwerkinterface „eth0“ und den Port 80 gesendet werden, und diese Informationen in detaillierter Form anzeigen. Die aufgezeichneten Datenpakete können

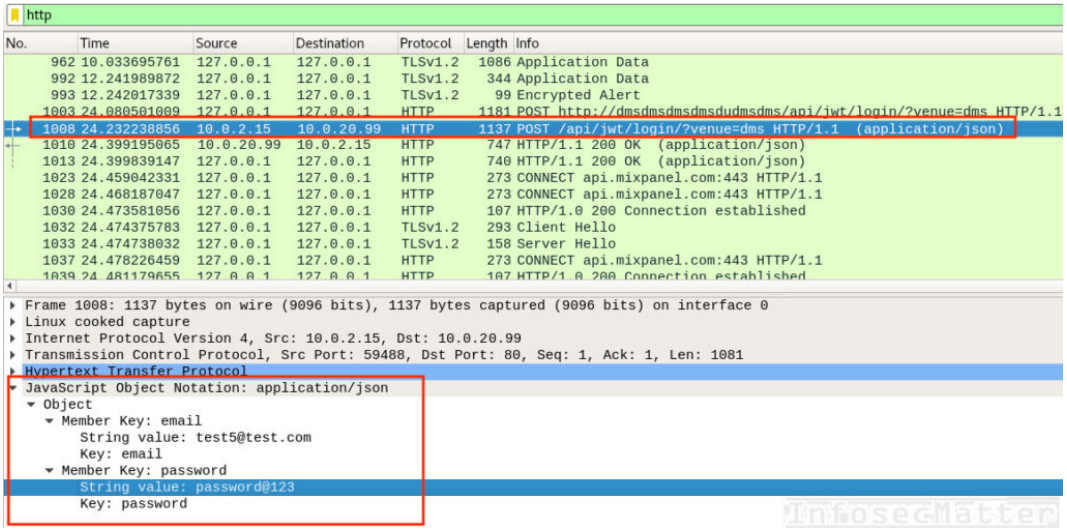

Abbildung 4.2: Wireshark als Packet-Editor

später mit Wireshark[14] oder einem anderen Packet Sniffing-Tool analysiert werden

[12] vgl. Wang, Hu, Zhao & Chen (2018)
[13] vgl. Project (2020)
[14] vgl. Dalal (2016)

(siehe Abbildung 3.3). Um Benutzernamen und Passwörter aus PCAP-Dateien zu extrahieren, können Sie ein Packet Sniffing-Tool wie Wireshark verwenden[15]. Wenn in der PCAP-Datei ein TCP-Stream vorhanden ist (das heißt, eine Reihe von aufeinanderfolgenden TCP-Datenpaketen, die Teil einer Netzwerkverbindung sind), können Sie den Stream öffnen und nach Benutzernamen und Passwörtern suchen. Wireshark zeigt nun den Inhalt des TCP-Streams[16] als Text an (siehe Abbildung 3.3). Sie können nun nach Benutzernamen und Passwörtern suchen, indem Sie den Text durchsuchen oder bestimmte Zeichenketten suchen.

Es ist jedoch wichtig zu beachten, dass viele moderne Protokolle Benutzernamen und Passwörter verschlüsseln, um sie vor dem Abfangen zu schützen[17].
Ebenso ist es wichtig zu erwähnen, dass mit dem Befehl alle Arten von Netzwerkverkehr aufzeichnen können[18], der über das angegebene Netzwerkinterface gesendet wird. Das bedeutet, dass sie alle möglichen Protokolle aufzeichnen können, die im Netzwerk verwendet werden.
Einige Beispiele für Protokolle[19], die mit „tcpdump“ aufgezeichnet werden können, sind:

- HTTP (Hypertext Transfer Protocol): Das HTTP-Protokoll wird verwendet, um Webseiten im Internet zu übertragen.
- FTP (File Transfer Protocol): Das FTP-Protokoll wird verwendet, um Dateien zwischen zwei Rechnern zu übertragen.
- SMTP (Simple Mail Transfer Protocol): Das SMTP-Protokoll wird verwendet, um E-Mails zu übertragen.
- SSH (Secure Shell): Das SSH-Protokoll wird verwendet, um sicheren Zugriff auf einen Remote-Rechner zu ermöglichen.

[15] vgl. Smith (2013)
[16] vgl. Williams (2014)
[17] vgl. Jones (2018)
[18] vgl. Chung (2017)
[19] vgl. Park (2019)

5 Methoden zur Identifikation des Schadenausmaßes

Nun haben wir durch unsere Forensik festgestellt, was der Angreifer nutzte, um den Unternehmen möglichen Schaden zuzufügen. Um das mögliche Schadensausmaß zu definieren, muss sich mit dem Unternehmen auseinandergesetzt werden, sowie der „Eigenbau-PC“ erneut betrachtet werden.

5.1 Die Rolle des geschädigten Unternehmens

Sollte das Unternehmen bereits eine Schwachstellenanalyse durchgeführt haben, werden zuvor gefährdete Protokolle, welche im Unternehmen verwendet werden, bekannt sein. Ebenfalls sollten bekannte interne offene Ports bereits in einer vorhergehenden Analyse definiert worden sein. Sollte das Unternehmen keine derartige Schwachstellenanalyse durchgeführt haben, sollte diese Analyse umgehend nachgeholt werden. Ebenfalls sollten alle sicherheitsrelevanten Passwörter geändert und im besten Fall noch gehärtet werden. Des Weiteren sollte analysiert werden, welcher Traffic durch das Unternehmensnetzwerk unverschlüsselt geleitet wurde und einfach auszulesen war, um eine ungefähre Abschätzung durchführen zu können, was der Angreifer erbeutet haben könnte. Durch diese Theorien, die durch die Annahme getroffen werden, was möglicherweise ein besonderes Interesse für den Angreifer gewesen sein könnte, kann auch die später tiefergehende IT-Forensik sich diesen annehmen und die Analyse auf Grundlage dieser Theorien ausweiten. Entsprechend muss die ermittelnde Behörde im engen Kontakt zum betroffenen Unternehmen stehen, um weiteren Schäden vorbeugen zu können. Hierbei ist zu beachten, dass durch die intensivere Zusammenarbeit Folgeschäden durch den Angreifer vorgebeugt werden können.
Dies sollte gleichzeitig mit der weiteren Analyse des schädlichen Gerätes erfolgen. Ebenfalls lassen sich Anleitungen finden, durch welche überprüft werden kann, ob bekannte Gefahren bereits im Unternehmen durch Verwendung von Standard Ports etc. vorhanden sind [1].

[1] vgl. Software (n.d.)

5.2 Tiefergehende IT-Forensik des „Eigenbau-PCs“

Durch die bereits vorher durchgeführte Analyse können wir ungefähr einschätzen, welchen Schaden das Gerät im Unternehmen angerichtet haben könnte. Des Weiteren ist nun eine detaillierte Analyse des Gerätes notwendig für weitere Erkenntnisse. Als Erstes sollte von dem Gerät ein Abbild erstellt werden, damit keine Daten bei der Untersuchung verändert werden, was im Nachgang für die Behörden und rechtliche Schritte besonders zu erwähnen ist. Durch das Werkzeug Live View lässt sich dieses Abbild des Systems als VM aufsetzen und kann dort nur mit Lesezugriff weiter analysiert werden[2]. Jetzt kann durch Werkzeuge wie Sleuthkit weitere Analysen des Gerätes durchgeführt werden. Ebenfalls sollte versucht werden, mögliche Schwachstellen zu erkennen, die das System aufweist, um eine Rückverfolgung einleiten zu können. Eine tiefere Dateianalyse kann durch das Werkzeug MD5Deep angegangen werden[3].
Ebenfalls kann der Angreifer versucht haben, seine Spuren zu verwischen und Dateien gelöscht haben, aber auch dafür kann durch Software wie Recuva, Restoration und Undelete Plus versucht werden, gelöschte Dateien, Dokumente etc. wiederherzustellen. Für weitere forensische Herangehensweisen finden sie im Leitfaden IT Forensik Informationen für Windows, sowie Ubuntu Betriebssysteme [4].

5.3 Weiteres Vorgehen

Nun, da die tiefergehende IT-Forensik durchgeführt wurde, ist möglicherweise durch bestimmte Logs oder eine aktive erkennbare Weiterleitung der Daten an eine IP-Adresse hervorgegangen, welche weiter zurückverfolgt werden kann. Diese kann im folgenden durch die ermittelnde Behörde auf Antrag bei den Providern genutzt werden, um den möglichen Aermittelndees Angreifers zu bestimmen [5]. Natürlich ist zu erwähnen, dass eine IP-Verschleierung oder Umleitung über mehrere Länder durch den Angreifer genutzt werden kann und somit eine Weiterverfolgung des Angreifers komplizierter gestaltet, aber auch hierbei gibt es Schwachstellen, die ausgenutzt werden können, um eine Ermittlung erfolgreich zu gestalten.
Ebenfalls können VPN Anbietern von der Polizei kontaktiert werden und verfplichtet werden, die Anschrift des Nutzers herauszugeben. Heutzutage kann ebenfalls bei modernen VPN Anbietern durch VPN-Tracker oder durch Deep Packet Inspection auf den Angreifer schließen[6].

[2] vgl. BSI (2011) S.207
[3] vgl. BSI (2011) S. 192
[4] vgl. BSI (2011)
[5] vgl. Urheberrecht.de (n.d.)
[6] vgl. NordVPN (n.d.)

6 OSINT

Um Cyberkriminelle zurückverfolgen zu können, bedarf es der Sammlung von Informationen. Ein bewährtes Verfahren zur Informationssammlung ist Open Source Intelligence, kurz OSINT. Mit OSINT werden Informationen aus öffentlich zugänglichen Quellen gesammelt[1]. Eine Reihe unterschiedlicher Informationsquellen können hierzu herangezogen werden: akademische Veröffentlichungen wie Forschungsarbeiten, Medienquellen wie Zeitungen, Webinhalte wie Social-Media-Plattformen, sowie Informationen aus veröffentlichten Regierungsdokumenten etc.[2]. Sowohl analoge als auch digitale Daten stellen valide Informationsquellen dar, solange diese öffentlich zugänglich sind[3]. Nachfolgend wird OSINT mittels zwei ausgewählter Tools demonstriert. Die primäre Informationsquelle stellt bei dieser Demonstration das Internet dar. Für die OSINT Demonstration wurden die Tools Maltego und Shodan ausgewählt. Hauptgrund für diese Entscheidung sind bestehende Vorkenntnisse zu diesen Tools. Allerdings bringen Shodan und Maltego viele Qualitäten mit sich, was es attraktiv macht für eine Demonstration: Maltego bedient sich einer breiten Palette an Informationsquellen aus dem Internet; die gesammelten Daten werden auf eine unkomplizierte Weise dargestellt; und die gesammelten Daten sind verständlich und problemlos zu analysieren[4]. Überdies stellen die Entwickler des Tools eine Community Version zur Verfügung, welche kostenlos ist. Jede Person ist dadurch in der Lage, Maltego herunterzuladen und OSINT zu betreiben. Bei Shodan handelt es sich um eine Suchmaschine für im Internet exponierte Geräte[5]. Auf diese Weise können Informationen über Webserver, Mailserver, IoT-Devices etc. gesammelt werden, ohne Portscans durchzuführen[6]. Shodan bietet auf diese Weise eine unkomplizierte OSINT-Recherche, um detaillierte Informationen über ein System herauszufinden. Hierzu zählen die IP-Adresse, offene Ports, bekannte Schwachstellen, verwendete Technologien etc.[7]. Bei der Verwendung von Maltego ist das Verständnis zweier Begriffe notwendig: Entities and Transforms. Entitäten (Entity) sind mit Variablen vergleichbar: sie enthalten Daten, mit denen Maltego arbeitet, um weitere Informationen zu sammeln[8]. Es kann unter anderem sich bei einer Entität um einen Computer, ein Handy, eine IP-Adresse oder einen Domainnamen handeln (s. Abb. 1).

[1] vgl. Chauhan & Panda (2015), S. 16
[2] vgl. Chauhan & Panda (2015), S. 16
[3] vgl. Chauhan & Panda (2015), S. 16
[4] vgl. Chauhan & Panda (2015), S. 124
[5] vgl. Shodan (2022)
[6] vgl. Shodan (2022)
[7] vgl. Shodan (2022)
[8] vgl. Chauhan & Panda (2015), S. 124

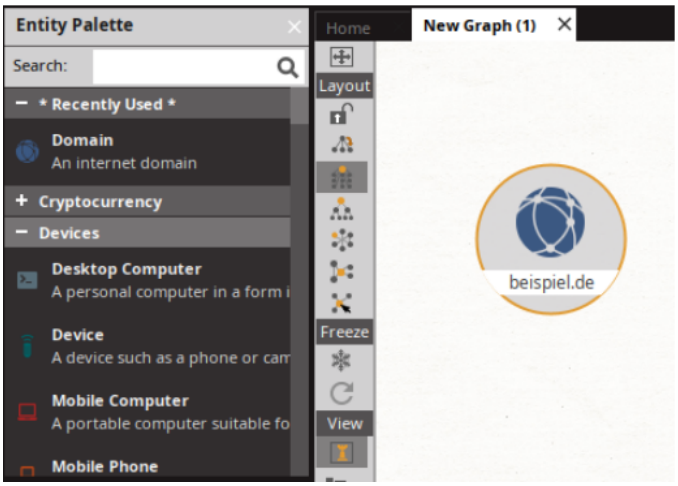

Abbildung 6.1: Entitäten in Maltego

Jede Entität wird durch ein Symbol repräsentiert (s. Abb. 1). So wird eine Domain in Maltego als blauer Globus dargestellt (s. Abb. 1). Transformationsfunktionen können nun Entitäten als Input verwenden, um weitere Informationen (weitere Entitäten) zu ermitteln (s. Abb. 2). So könnte es von Interesse sein, den Webserver der Domäne inklusive dessen offener Ports und Services zu identifizieren, um Informationen über das Ziel zu sammeln. Um diese Informationen mittels OSINT zu erfassen, werden Transformationsfunktionen verwendet (s. Abb. 2). Transformationsfunktionen (Transforms) sind Codeblöcke, die auf Entitäten angewandt werden[9]. Wenn eine Transformationsfunktion eine Entität als Input verwendet und daraus weitere Entitäten findet, wird ein Relationspfeil zwischen den beiden Entitäten generiert (s. Abb. 2). Maltego visualisiert auf diese Weise die Ergebnisse der OSINT-Recherche und vereinfacht die spätere Analyse. Graphen können auch manuell erstellt und mit Informationen gefüllt werden, um eine Recherche zu visualisieren und Beziehungen darzustellen. Nachfolgend wird ein Szenario beispielhaft durchgegangen, um den OSINT-Prozess von Maltego zu veranschaulichen.

Gegeben sei eine Domäne „beispiel.de“. Ziel ist es, die IP-Adresse des Webservers zu identifizieren, inklusive aller offenen Ports. Die Domäne als einzige zur Verfügung stehende Informationsquelle wird als Entität durch den Nutzer erstellt (s. Abb. 2). Mit einem Rechtsklick auf eine Entität werden eine Reihe von Transformationsfunktionen aufgelistet, die auf die Entität angewandt werden können (s. Abb. 2). Um nun die DNS-Namen der Domäne, die IP-Adresse, sowie die Ports zu ermitteln, können folgende Transformationsfunktionen verwendet werden: „To Subdomains“, um die Subdomains der Domain aufzulisten, „To IP-Adress“ um die IP-Adresse zu identifizieren und „To Services“, um die offenen Ports zu erfassen (s. Abb. 2). Geübte Nutzer können auf

[9] vgl. Chauhan & Panda (2015), S. 124

diese Weise innerhalb weniger Sekunden eine Reihe von wertvollen Informationen über eine Domain sammeln, ohne Portscans durchzuführen.

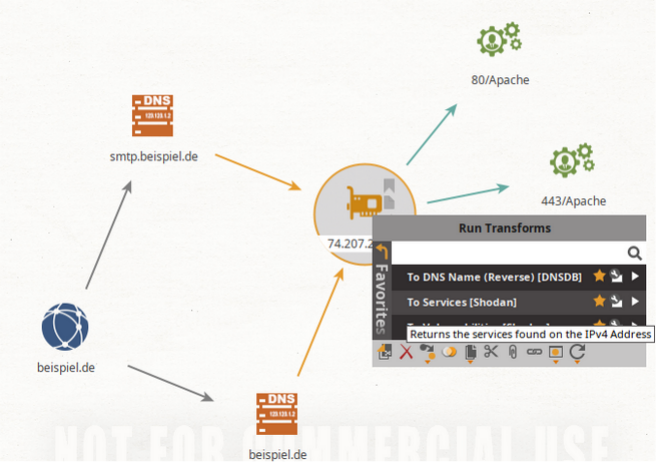

Abbildung 6.2: Beispiel Graph

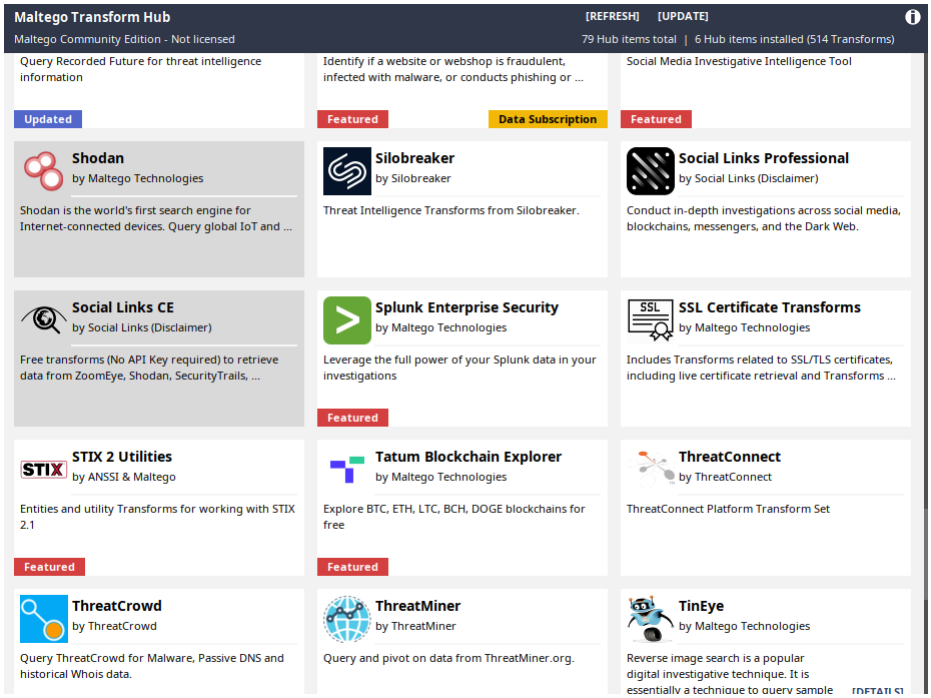

Abbildung 6.3: Pakete für Transformationsfunktionen

Welche Transformationsfunktionen verwendet werden können, hängt von den installierten Paketen in Maltego ab. Maltego bietet eine Reihe von Paketen an, welche

Transformationsfunktionen beinhalten (s. Abb. 3). Die OSINT-Suchmaschine Shodan ist ein mögliches Paket, welches installiert werden kann, um die Funktionalitäten der Suchmaschine in Maltego zu integrieren (s. Abb. 3).

Die visuelle Darstellung der Entitäten ermöglicht eine detaillierte Analyse von Beziehungen zwischen Entitäten, wie Personen, Organisationen und Geräten (s. Abb. 4). Hierdurch lassen sich Muster und Trends selbst in großen Datenmengen erkennen. Maltego ermöglicht sowohl das Durchführen von Ermittlungen, als auch das Festhalten der Ergebnisse einer Ermittlung in einem einzigen Graphen (s. Abb. 4). Jede Entität kann zusätzlich mit Informationen gefüllt werden, um die Ergebnisse einer Recherche festzuhalten. Mit diesen Qualitäten stellt Maltego insgesamt ein leistungsfähiges Werkzeug für Strafverfolgungsbehörden dar, mit dem sich Informationen aus verschiedenen Quellen für nachrichtendienstliche Zwecke sammeln und analysieren lassen[10].

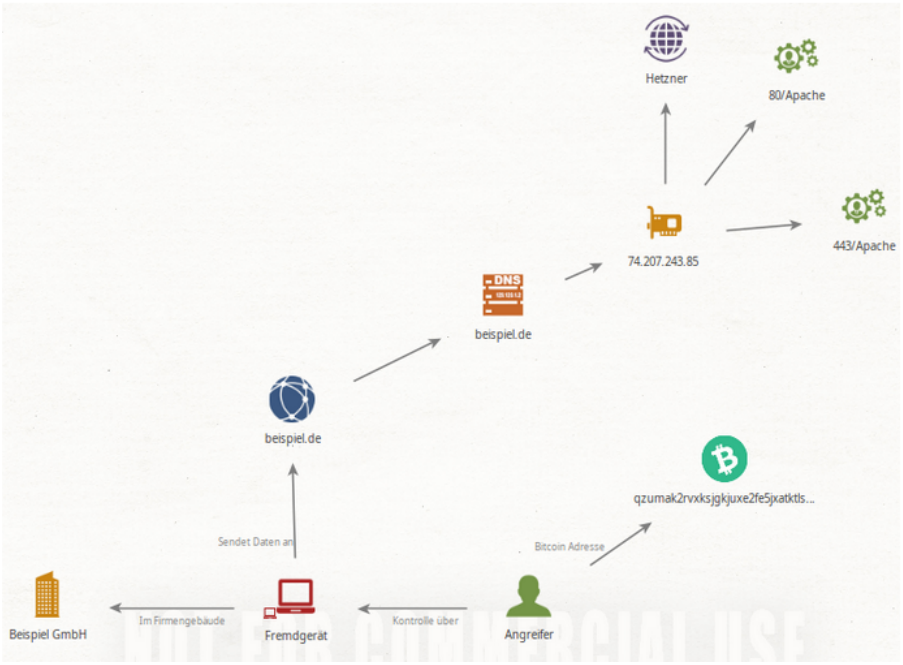

Abbildung 6.4: Maltego-Graph für das Fallbeispiel

[10] vgl.Maltego (2020)

7 Fazit

Die vorgestellte Fallstudie zeigt, dass der im Bodentank gefundene Personal Computer (PC) wahrscheinlich ein Eigenbau war, da es keine bekannten Hersteller von Computern dieser Größe gibt. Bei der Untersuchung mit geeigneten Tools wurde festgestellt, dass auf dem PC das Betriebssystem „Ubuntu“ lief und Programme zum Ausspähen und Analysieren des Netzwerkverkehrs installiert waren. Dies deutet darauf hin, dass der Täter versucht hat, den internen Netzwerkverkehr des Unternehmens abzufangen und möglicherweise Spuren in Form von Protokollen oder verwendeten Programmen zu hinterlassen. Außerdem wurde der abgefangene Datenverkehr an einen externen Server gesendet, was eine weitere Spur hinterließ.
Die Bedeutung der Kommunikation zwischen der Agentur und dem Unternehmen sowie der Reaktion des Unternehmens auf den Vorfall sollte nicht unterschätzt werden. Diese Interaktion kann dazu beitragen, weiteren Schaden zu verhindern. Die Verfolgung des Täters durch OSINT ist ebenso wichtig wie die forensische Untersuchung der betroffenen Ressourcen. Die Verfolgung von Cyberkriminellen liefert wichtige Informationen über den Modus Operandi der Täter und hilft Unternehmen, Angriffsvektoren zu verstehen. Überdies können die Untersuchung eines Vorfalls und die Verfolgung von Cyberkriminellen zu einem tieferen Verständnis des Vorfalls führen.
In dieser Fallstudie kam es in einem Unternehmen zu einem Vorfall, der zur Entdeckung eines unbekannten Geräts führte. Es wurde festgestellt, dass das Gerät den Netzwerkverkehr des Unternehmens ausspioniert hatte. Durch den Einsatz forensischer Methoden wurden die Software auf dem Gerät und seine Fähigkeiten ermittelt. Ein OSINT wurde eingeleitet, um den verantwortlichen Cyberkriminellen aufzuspüren. Obwohl der Täter letztlich nicht gefunden wurde, wurde der OSINT-Prozess dennoch als wichtig für die Strafverfolgung erachtet.
Insgesamt veranschaulicht dieser Fall den Nutzen der IT-Forensik bei der Unterstützung der Polizei bei der Untersuchung von Cyber-Vorfällen. Durch eine sorgfältige Untersuchung der Beweise und den Einsatz spezieller Techniken und Tools kann das Unternehmen wertvolle Informationen sammeln, die bei der Identifizierung und Reaktion von weiteren fremden Geräten helfen.

Literaturverzeichnis

BSI (2011), 'Leitfaden „it-forensik“'. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1, Zugriff am 2. Januar 2023.

Chauhan & Panda (2015), Hacking Web Intelligence - Open Source Intelligence and Web Reconnaissance Concepts and Techniques, IEEE.

Chung, M. (2017), 'Recording all network traffic with tcpdump', International Journal of Advanced Research in Computer Science **8**(3), 189–193.

Dalal, R. (2016), 'Wireshark: A network protocol analyzer', International Journal of Advanced Research in Computer Science **7**(3), 175–178.

Gupta, A., Gupta, A. & Singh, C. (2019), 'Systems on a chip: A survey', IEEE Access **7**, 112812–112822.

Jones, D. (2018), 'Preventing the sniffing of encrypted passwords', International Journal of Cyber Security **13**(1), 45–50.

Khan, U., Khan, M. S., Yousaf, M. & Lee, K.-J. (2019), 'Identification of malicious processes in cyber security: A review', International Journal of Information Security and Privacy **13**(1), 54–68.

Liu, Z., Zeng, Z., Zhang, M. & Qi, H. (2019), Preventing soc piracy through secure boot, in '2019 International Conference on Computer Science and Information Technology (CSIT)', IEEE, pp. 181–186.

Maltego (2020), 'State of the german police it infrastructure and the importance of osint capabilities'. https://www.maltego.com/blog/state-of-the-german-police-it-infrastructure-and-the-importance-of-osint-capabili
Zugriff am 2. Januar 2023.

NordVPN (n.d.), 'Vpn zurückverfolgen'.
URL: https://nordvpn.com/de/blog/vpn-zuruckverfolgen/

Park, J. (2019), Network Protocols: A Comprehensive Guide, John Wiley and Sons.

Project, L. D. (2020), Tcpdump Options and Filters.
URL: https://www.tcpdump.org/manpages/tcpdump.1.html

Shodan (2022), 'Search engine for the internet of everything'. https://www.shodan.io/, Zugriff am 2. Januar 2023.

Smith, J. (2013), Packet Sniffing: Techniques and Tools, O'Reilly Media.

Software, S. (n.d.), 'Offene ports und ihre schwachstellen'.
URL: https://specopssoft.com/de/blog/offene-ports-und-ihre-schwachstellen/

Urheberrecht.de (n.d.), 'Ip-adresse zurückverfolgen'.
URL: https://www.urheberrecht.de/ip-adresse-zurueckverfolgen/

Wang, X., Hu, W., Zhao, B. & Chen, Z. (2018), Packet sniffing detection and prevention in cyber security: A survey, in 'Proceedings of the 2018 International Conference on Cyber Security and Privacy', ACM, pp. 9–16.

Wang, X., Zhao, B., Hu, W. & Chen, Z. (2018), Detection of malicious processes in cyber security: A survey, in 'Proceedings of the 2018 International Conference on Cyber Security and Privacy', ACM, pp. 1–8.

Williams, B. (2014), 'Analyzing tcp streams with wireshark', International Journal of Network Security **15**(2), 109–115.

Zhao, B., Hu, W., Chen, Z. & Wang, X. (2016), 'Intrusion detection and prevention systems: A survey', International Journal of Network Security **18**(2), 129–144.