(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 117 210 A1** 2021.01.07

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 117 210.9**
(22) Anmeldetag: **30.06.2020**
(43) Offenlegungstag: **07.01.2021**

(51) Int Cl.: ***H04L 12/26*** (2006.01)
G06F 21/56 (2013.01)

(30) Unionspriorität:
16/460,255 **02.07.2019** **US**

(71) Anmelder:
CA, Inc., San Jose, CA, US

(74) Vertreter:
Dilg, Haeusler, Schindelmann Patentanwaltsgesellschaft mbH, 80636 München, DE

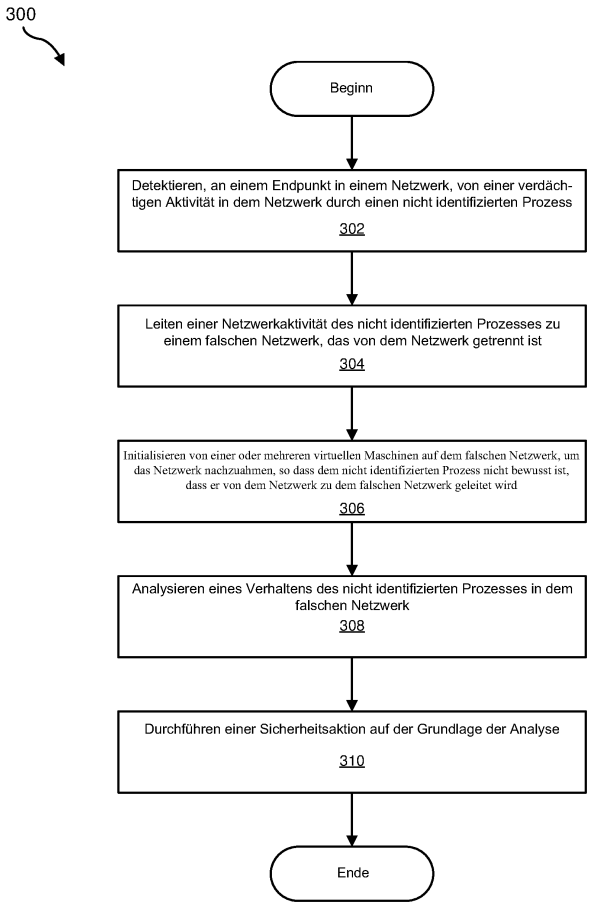
(72) Erfinder:
Shaker, Robert, Berkley, CA, US

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Systeme und Verfahren zur Analyse des Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung**

(57) Zusammenfassung: Das offenbarte computerimplementierte Verfahren zur Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung kann aufweisen: ein Detekieren von einer verdächtigen Aktivität in dem Netzwerk durch einen nicht identifizierten Prozess an einem Endpunkt in einem Netzwerk und Leiten der Netzwerkaktivität des nicht identifizierten Prozesses an ein falsches Netzwerk, das von dem Netzwerk getrennt ist. Das Verfahren kann auch ein Initialisieren von einer oder mehreren virtuellen Maschinen in dem falschen Netzwerk aufweisen, um das Netzwerk nachzuahmen, dass dem nicht identifizierten Prozess nicht bewußt ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wurde. Das Verfahren kann auch ein Analysieren eines Verhaltens des nicht identifizierten Prozesses in dem falschen Netzwerk und ein Durchführen einer Sicherheitsmaßnahme auf der Grundlage der Analyse aufweisen. Verschiedene andere Verfahren, Systeme und computerlesbare Medien werden ebenfalls offenbart.



Beschreibung

HINTERGRUND

[0001] Ein Computernetzwerk kann durch Schadprogramme (oder Malware) angegriffen werden, die auf einen bestimmten Endpunkt in dem Netzwerk abzielen. Sobald der Endpunkt infiltriert ist, können die Schadprogramme versuchen, das Netzwerk zu durchqueren. Die Schadprogramme können sich lateral zu anderen Endpunkten in dem Netzwerk bewegen, um Daten zu extrahierinen und/oder den Angriff zu verbreiten.

[0002] Herkömmlich werden verdächtige Netzwerkaktivitäten, die von einem Endpunkt aus erkannt werden, als Schadprogramm behandelt. Die verdächtigen Schadprogramme können an dem Endpunkt unter Quarantäne gestellt werden, um die Schadprogramme daran zu hindern, sich zu bewegen. Eine Quarantäne der Schadprogramme ist jedoch nicht immer ausreichend oder durchführbar. Beispielsweise kann eine neue Art von Schadprogramm in der Lage sein, ein Unter-Quarantäne-Gestellt-Werden zu umgehen. Der für das Schadprogramm verantwortliche Angreifer kann auch über den Quarantäne-Versuch benachrichtigt werden, wenn das Verhalten des Schadprogramms behindert wird. Alternativ kann ein Fehlalarm dazu führen, dass eine legitime Anwendung versehentlich unter Quarantäne gestellt wird.

[0003] Mit der vorliegenden Offenbarung wird daher ein Bedarf an Systemen und Verfahren zur Analyse des Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung identifiziert und angesprochen.

ZUSAMMENFASSUNG

[0004] Eine Aufgabe der Erfindung ist es, Systeme und Verfahren zur Analyse des Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung bereitzustellen. Diese Aufgabe wird durch die Gegenstände der unabhängigen Ansprüche gelöst.

[0005] In einem Beispiel kann ein Verfahren zur Analyse eines Netzwerkverhaltens über eine nachgeahmte (oder imitierte) Netzwerkumgebung Folgendes aufweisen: (a) Detektieren (oder Erkennen), an einem Endpunkt in einem Netzwerk, von einer verdächtigen Aktivität in dem Netzwerk durch einen nicht identifizierten Prozess, (b) Leiten (oder Durchleiten) der Netzwerkaktivität des nicht identifizierten Prozesses zu einem falschen Netzwerk, das von dem Netzwerk getrennt ist, (c) Initialisieren von einer oder mehreren virtuellen Maschinen in dem falschen Netzwerk, um das Netzwerk so nachzuahmen (oder zu imitieren), dass dem nicht identifizierten Prozess nicht bewusst ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird, (d) Analysieren des Verhaltens des nicht identifizierten Prozesses in dem falschen Netzwerk und (e) Durchführen einer Sicherheitsmaßnahme (oder Sicherheitsaktion) auf der Grundlage der Analyse.

[0006] In einigen Beispielen kann die Sicherheitsmaßnahme mindestens eine der Folgenden aufweisen: Netzwerkisolierung des Endpunkts, unter Quarantäne Stellen des nicht identifizierten Prozesses, Senden einer Benachrichtigung, Bereitstellen der Analyse an einen Administrator oder Veröffentlichen der Analyse.

[0007] In einigen Beispielen kann das Analysieren des Verhaltens ein Sammeln von forensischen Artefakte aufweisen, die indikativ sind für ein Verhalten im Zusammenhang mit dem nicht identifizierten Prozess. Die forensischen Artefakte können von zumindest einem von dem Endpunkt oder einem anderen Endpunkt des Netzwerks gesammelt werden. Die forensischen Artefakte können Speicherartefakte aufweisen.

[0008] In einigen Beispielen kann das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Einrichten einer geteilten Tunnelroute (split tunnel route) zwischen dem nicht identifizierten Prozess und dem falschen Netzwerk aufweisen. In einigen Beispielen kann das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Erstellen einer falschen Leittabelle für den nicht identifizierten Prozess, um den Verkehr zu dem falschen Netzwerk zu leiten, aufweisen.

[0009] In einigen Beispielen kann das Analysieren des Verhaltens auch ein Überwachen des Verhaltens aufweisen, ohne den nicht identifizierten Prozess zu behindern. In einigen Beispielen kann das Netzwerk eine Mehrzahl von Endpunkten aufweisen, und das falsche Netzwerk kann für jeden der Mehrzahl von Endpunkten eine virtuelle Maschine aufweisen.

[0010] In einer Ausführungsform kann ein System zur Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung aufweisen: mindestens einen physikalischen Prozessor und physikalischen Speicher, der computerausführbare Befehle enthält, die, wenn sie von dem physikalischen Prozessor ausgeführt werden, den physikalischen Prozessor dazu veranlassen, (a) an einem Endpunkt in einem Netzwerk eine verdächtige Aktivität im Netzwerk durch einen nicht identifizierten Prozess zu detektieren (oder erkennen), (b) die Netzwerkaktivität des nicht identifizierten Prozesses zu einem falschen Netzwerk, das von dem Netzwerk getrennt ist, zu leiten, (c) eine oder mehrere virtuelle Maschinen in dem falschen Netzwerk zu initialisieren, um das Netzwerk so nachzuahmen, dass dem nicht identifizierten Prozess nicht bewusst ist, dass er von dem Netzwerk in das falsche Netzwerk geleitet wird, (d) ein Verhaltens

des nicht identifizierten Prozesses in dem falschen Netzwerk zu analysieren, und (e) auf der Grundlage der Analyse eine Sicherheitsmaßnahme auszuführen.

[0011] In einigen Beispielen kann die Sicherheitsmaßnahme mindestens eine der Folgenden aufweisen: Netzwerkisolierung des Endpunkts, unter Quarantäne Stellen des nicht identifizierten Prozesses, Senden einer Benachrichtigung, Bereitstellen der Analyse an einen Administrator oder Veröffentlichen der Analyse.

[0012] In einigen Beispielen kann das Analysieren des Verhaltens ein Sammeln von forensischen Artefakten aufweisen, die indikativ sind für ein Verhalten im Zusammenhang mit dem nicht identifizierten Prozess. Die forensischen Artefakte können von mindestens einem der Endpunkte oder von einem anderen Endpunkt des Netzwerks gesammelt werden. Die forensischen Artefakte können Speicherartefakte aufweisen.

[0013] In einigen Beispielen kann die das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Einrichten einer geteilten Tunnelroute zwischen dem nicht identifizierten Prozess und dem falschen Netzwerk aufweisen. In einigen Beispielen kann das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Erstellen einer falschen Leittabelle für den nicht identifizierten Prozess, um den Verkehr zu dem falschen Netzwerk zu leiten, aufweisen.

[0014] In einigen Beispielen kann das Analysieren des Verhaltens auch ein Überwachen des Verhaltens aufweisen, ohne den nicht identifizierten Prozess zu behindern. In einigen Beispielen kann das Netzwerk eine Mehrzahl von Endpunkten aufweisen, und das falsche Netzwerk kann für jeden der Mehrzahl von Endpunkten eine virtuelle Maschine aufweisen.

[0015] In einigen Beispielen kann das oben beschriebene Verfahren als computerlesbare Befehle (oder Anweisungen) auf einem nicht-flüchtigen computerlesbaren Medium kodiert sein. Beispielsweise kann ein computerlesbares Medium einen oder mehrere computerausführbare Befehle aufweisen, die, wenn sie von mindestens einem Prozessor einer Recheneinrichtung (oder Computergerät) ausgeführt werden, die Recheneinrichtung dazu veranlassen können, (a) an einem Endpunkt in einem Netzwerk verdächtige Aktivitäten in dem Netzwerk durch einen nicht identifizierten Prozess zu erkennen, (b) die Netzwerkaktivität des nicht identifizierten Prozesses zu einem falschen Netzwerk, das von dem Netzwerk getrennt ist, zu leiten, (c) eine oder mehrere virtuelle Maschinen in dem falschen Netzwerk zu initialisieren, um das Netzwerk so nachzuahmen, dass dem nicht identifizierten Prozess nicht bewusst ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird, (d) ein Verhalten des nicht identifizierten Prozesses in dem falschen Netzwerk zu analysieren, und (e) auf der Grundlage der Analyse eine Sicherheitsmaßnahme durchzuführen.

[0016] In einigen Beispielen kann die Sicherheitsmaßnahme mindestens eine der Folgenden aufweisen: Netzwerkisolierung des Endpunkts, unter Quarantäne Stellen des nicht identifizierten Prozesses, Senden einer Benachrichtigung, Bereitstellen der Analyse an einen Administrator oder Veröffentlichen der Analyse.

[0017] Merkmale von jeder der hierin beschriebenen Ausführungsformen können in Übereinstimmung mit den hierin beschriebenen allgemeinen Prinzipien in Kombnation miteinander verwendet werden. Diese und andere Ausführungsformen, Merkmale und Vorteile werden bei der Lektüre der folgenden ausführlichen Beschreibung in Verbindung mit den beiliegenden Zeichnungen und Ansprüchen besser verstanden werden.

Figurenliste

[0018] Die beigefügten Zeichnungen illustrieren eine Anzahl von beispielhaften Ausführungsformen und sind Teil der Patentschrift. Zusammen mit der nachfolgenden Beschreibung zeigen und erklären diese Zeichnungen verschiedene Prinzipien der vorliegenden Offenbarung.

Fig. 1 ist ein Blockschaubild eines beispielhaften Systems für die Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung.

Fig. 2 ist ein Blockschaubild eines zusätzlichen beispielhaften Systems für die Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung.

Fig. 3 ist ein Ablaufdiagramm eines beispielhaften Verfahrens für die Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung.

Fig. 4A-4E sind Schaubilder, die einen beispielhaften Datenfluss entsprechend dem beispielhaften Verfahren von **Fig. 3** veranschaulichen.

Fig. 5A ist ein Schaubild einer beispielhaften Netzwerkumgebung.

Fig. 5B ist ein Schaubild einer falschen Netzwerkumgebung, die das Netzwerk der **Fig. 5A** nachahmt.

Fig. 6 ist ein Blockschaubild eines beispielhaften Rechensystems, das in der Lage ist, eine oder mehrere der hierin beschriebenen und/oder veranschaulichten Ausführungsformen zu implementieren.

Fig. 7 ist ein Blockschaubild eines beispielhaften Computernetzwerks, das in der Lage ist, eine oder mehrere der hierin beschriebenen und/oder veranschaulichten Ausführungsformen zu implementieren.

[0019] Durchgängig in allen Zeichnungen verweisen identische Bezugszeichen und Beschreibungen auf ähnliche, aber nicht notwendigerweise identische Elemente. Während die hierin beschriebenen beispielhaften Ausführungsformen verschiedenen Modifikationen und alternativen Formen unterliegen können, sind bestimmte Ausführungsformen in den Zeichnungen beispielhaft dargestellt und werden hierin ausführlich beschrieben. Es ist jedoch nicht beabsichtigt, dass die hierin beschriebenen beispielhaften Ausführungsformen auf die offenbarten besonderen Formen beschränkt sind. Vielmehr deckt die vorliegende Offenbarung alle Modifikationen, Äquivalente und Alternativen ab, die in den Schutzbereich der beigefügten Ansprüche fallen.

AUSFÜHRLICHE BESCHREIBUNG VON BEISPIELHAFTEN AUSFÜHRUNGSFORMEN

[0020] Die vorliegende Offenbarung bezieht sich allgemein auf Systeme und Verfahren zur Analyse von Netzwerkverhalten über eine nachgeahmte Netzwerkumgebung. So wie das weiter unten ausführlicher erläutert wird, können die hierin offenbarten Systeme und Verfahren durch Nachahmen einer Netzwerkumgebung mit einem falschen Netzwerk verdächtige Netzwerkaktivitäten von einem Endpunkt eines Netzwerks aus sicher überwachen und analysieren. Durch Weiterleiten der verdächtigen Netzwerkaktivität an das falsche Netzwerk können die hierin besprochenen Systeme und Verfahren in der Lage sein, verdächtige Schadprogramme (oder Malware) so zu täuschen, dass sie sich normal verhalten. Die Systeme und Verfahren dieser Offenbarung können das gesamte Verhalten von verdächtigen Schadprogrammen analysieren, um im Vergleich zu herkömmlichen Systemen Schadprogramme genauer zu identifizieren und Abhilfemaßnahmen gegen Schadprogramme zu ergreifen.

[0021] Darüber hinaus können die hierin beschriebenen Systeme und Verfahren die Funktionsweise einer Recheneinrichtung verbessern, indem sie potenzielle Malware erkennen und Abhilfemaßnahmen mit erhöhter Genauigkeit auswählen und somit die Wahrscheinlichkeit einer Infektion der Recheneinrichtung verringern. Diese Systeme und Verfahren können auch den Bereich der Netzwerksicherheit verbessern, indem sie ein falsches Netzwerk als Lockmittel (oder Köder) für eine Netzwerkumgebung verwenden.

[0022] Im Folgenden werden mit Verweis auf die **Fig. 1-2** ausführliche Beschreibungen von beispielhaften Systemen für die Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung bereitgestellt. Ausführliche Beschreibungen entsprechender computerimplementierter Verfahren werden ebenfalls bereitgestellt im Zusammenhang mit **Fig. 3**. Ausführliche Beschreibungen eines beispielhaften Arbeitsablaufs werden im Zusammenhang mit **Fig. 4A-E** bereitgestellt. Ausführliche Beschreibungen einer nachgeahmten oder falschen Netzwerkumgebung werden ebenfalls bereitgestellt im Zusammenhang mit den **Fig. 5A-B**. Darüber hinaus werden im Zusammenhang mit den **Fig. 6** und **Fig. 7** ausführliche Beschreibungen eines beispielhaften Rechensystems und einer beispielhaften Netzwerkarchitektur bereitgestellt, die in der Lage sind, eine oder mehrere der hierin beschriebenen Ausführungsformen zu implementieren.

[0023] **Fig. 1** ist ein Blockschaubild eines beispielhaften Systems **100** für die Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung. So wie das in dieser Abbildung dargestellt ist, kann das beispielhafte System **100** ein oder mehrere Module **102** zum Durchführen von einer oder mehreren Aufgaben aufweisen. So wie das weiter unten ausführlicher erläutert wird, können die Module **102** ein Detektionsmodul **104**, ein Leitmodul **106**, ein Nachahmungsmodul **108**, ein Analysemodul **110** und ein Sicherheitsmodul **112** aufweisen. Obwohl sie als getrennte Elemente dargestellt sind, können eines oder mehrere der Module **102** in **Fig. 1** Teile von einem einzelnen Modul oder von einer einzelnen Anwendung darstellen.

[0024] In bestimmten Ausführungsformen können eines oder mehrere der Module **102** in **Fig. 1** eine oder mehrere Softwareanwendungen oder Programme darstellen, die, wenn sie von einer Recheneinrichtung ausgeführt werden, die Recheneinrichtung dazu veranlassen können, eine oder mehrere Aufgaben auszuführen. Zum Beispiel, und so wie das weiter unten ausführlicher beschrieben wird, können eines oder mehrere der Module **102** Module darstellen, die so gespeichert und konfiguriert sind, dass sie auf einer oder mehreren Recheneinrichtungen laufen, so wie die in **Fig. 2** dargestellten Einrichtungen (z.B. Recheneinrichtung **202** und/oder Server **206**). Eines oder mehrere der Module **102** in **Fig. 1** können auch alle oder Teile von einem oder mehreren Spezialcomputern repräsentieren, die konfiguriert sind, um eine oder mehrere Aufgaben auszuführen.

[0025] So wie das in **Fig. 1** dargestellt ist, kann das beispielhafte System **100** auch ein oder mehrere Speichergeräte, wie z.B. einen Speicher **140**, aufweisen. Der Speicher **140** repräsentiert allgemein jede Art oder Form einer flüchtigen oder nichtflüchtigen Speichereinrichtung oder -mediums, die/das in

der Lage ist, Daten und/oder computerlesbare Befehle zu speichern. In einem Beispiel kann der Speicher **140** eines oder mehrere der Module **102** speichern, laden und/oder aufrechterhalten. Beispiele für den Speicher **140** umfassen, ohne Beschränkung, Direktzugriffsspeicher (RAM, random access memory), Nurlesespeicher (ROM, read-only memory), Flash-Speicher, Festplattenlaufwerke (HDDs, hard disc drives), Festkörper-Laufwerke (SSDs, solid state drives), optische Plattenlaufwerke, Caches, Variationen oder Kombinationen von einem oder mehreren derselben und/oder jeder andere geeignete Speicher.

[0026] So wie das in **Fig. 1** dargestellt ist, kann das beispielhafte System **100** auch einen oder mehrere physikalische Prozessoren aufweisen, wie z.B. den physikalischen Prozessor **130**. Der physikalische Prozessor **130** repräsentiert allgemein jede Art oder Form einer hardware-implementierten Verarbeitungseinheit, die in der Lage ist, computerlesbare Befehle zu interpretieren und/oder auszuführen. In einem Beispiel kann der physikalische Prozessor **130** auf einen oder mehrere der in dem Speicher **140** gespeicherten Module **102** zugreifen und/oder diese modifizieren. Zusätzlich oder alternativ kann der physikalische Prozessor **130** eines oder mehrere der Module **102** ausführen, um die Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung zu ermöglichen. Beispiele für den physikalischen Prozessor **130** umfassen, ohne Beschränkung, Mikroprozessoren, Mikrocontroller, Zentraleinheiten (CPUs, central processing units), feldprogrammierbare Gitteranordnungen (FPGAs, field-programmable gate arrays), die Softcore-Prozessoren implementieren, anwendungsspezifische integrierte Schaltungen (ASICs, application-specific integrated circuits), Teile von einem oder mehreren derselben, Variationen oder Kombinationen eines oder mehrerer derselben und/oder jeder andere geeignete physikalische Prozessor.

[0027] So wie das in **Fig. 1** dargestellt ist, kann das beispielhafte System **100** auch ein oder mehrere zusätzliche Elemente aufweisen, wie z.B. eine virtuelle Maschine **120**. So wie er hierin verwendet wird, bezieht sich der Begriff „virtuelle Maschine“ allgemein auf jede Betriebssystemumgebung, die durch einen Manager von virtuellen Maschinen (virtual machine manager) (z. B. einen Hypervisor) von der Computerhardware abstrahierint wird. Die virtuelle Maschine **120** repräsentiert allgemein jede Art oder Form von virtueller Maschine, die mit Software und/oder Hardware implementiert ist (z.B. der Server **206**). Die virtuelle Maschine **120** kann einer anderen Recheneinrichtung entsprechen, wie etwa einem Endpunkt in einem Netzwerk.

[0028] Das beispielhafte System **100** in **Fig. 1** kann auf verschiedene Weise implementiert werden. Beispielsweise können das gesamte oder ein Teil des beispielhaften Systems **100** Teile des beispielhaften Systems **200** in **Fig. 2** darstellen. So wie das in **Fig. 2** dargestellt ist, kann das System **200** eine Recheneinrichtung **202** in Kommunikation mit einem Server **206** über ein Netzwerk **204** aufweisen. In einem Beispiel kann die gesamte oder ein Teil der Funktionalität der Module **102** von der Recheneinrichtung **202**, dem Server **206** und/oder jedem anderen geeigneten Rechensystem ausgeführt werden. So wie das weiter unten ausführlicher beschrieben wird, können eines oder mehrere der Module **102** aus **Fig. 1**, wenn sie von mindestens einem Prozessor der Recheneinrichtung **202** und/oder des Servers **206** ausgeführt werden, die Recheneinrichtung **202** und/oder den Server **206** in die Lage versetzen, eine Netzwerkumgebung nachzuahmen, um ein Netzwerkverhalten zu analysieren. Zum Beispiel, und so wie das weiter unten ausführlicher beschrieben wird, können eines oder mehrere der Module **102** die Recheneinrichtung **202** und/oder den Server **206** dazu veranlassen, an einem Endpunkt in einem Netzwerk eine verdächtige Aktivität im Netzwerk durch einen nicht identifizierten Prozess zu detektieren (oder erkennen) und die gesamte Netzwerkaktivität des nicht identifizierten Prozesses in ein falsches Netzwerk, das von dem Netzwerk getrennt ist, zu leiten, eine oder mehrere virtuelle Maschinen in dem falschen Netzwerk zu initialisieren, um das Netzwerk so nachzuahmen (oder zu imitieren), dass dem nicht identifizierten Prozess nicht bewusst ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird, ein Verhalten des nicht identifizierten Prozesses in dem falschen Netzwerk zu analysieren, und eine Sicherheitsmaßnahme auf der Grundlage der Analyse auszuführen.

[0029] Die Recheneinrichtung **202** repräsentiert allgemein jede Art oder Form einer Recheneinrichtung, die in der Lage ist, computerausführbare Befehle (oder Anweisungen) zu lesen. Beispielsweise kann die Recheneinrichtung **202** ein Endpunktgerät sein, auf dem Sicherheitssoftware auf der Client-Seite ausgeführt wird. Zusätzliche Beispiele für die Recheneinrichtung **202** umfassen, ohne Beschränkung, Laptops, Tablet-PCs, Desktops, Server, Mobiltelefone, Minicomputer (PDAs, personal digital assistants), Multimedia-Player, eingebettete Systeme, tragbare Geräte (z.B. intelligente Uhren, intelligente Brillen usw.), intelligente Fahrzeuge, intelligente Verpackungen (z.B. aktive oder intelligente Verpackungen), Spielekonsolen, so genannte „Internet-der-Dinge“-Geräte (z.B. intelligente Haushaltsgeräte usw.), Variationen oder Kombinationen von einem oder mehreren dieser Einrichtungen und/oder alle anderen geeigneten Recheneinrichtungen.

[0030] Der Server **206** repräsentiert allgemein jede Art oder Form einer Recheneinrichtung, die eine Netzwerkumgebung nachahmen kann. Beispielsweise kann der Server **206** ein Unternehmensserver sein, der mit mehreren Endpunkten verbunden ist.

Weitere Beispiele für den Server **206** umfassene, ohne Beschränkung, Sicherheitsserver, Anwendungsserver, Webserver, Speicherserver und/oder Datenbankserver, die so konfiguriert sind, dass sie bestimmte Softwareanwendungen ausführen und/oder verschiedene Sicherheits-, Web-, Speicher- und/oder Datenbankdienste bereitstellen. Obwohl er/sie als eine einzelne Einheit in **Fig. 2** dargestellt ist, kann der Server **206** eine Mehrzahl von Servern aufweisen und/oder repräsentieren, die in Verbindung miteinander arbeiten und/oder betrieben werden. In einigen Implementierungen kann der Server **206** mit der Recheneinrichtung **202** integriert sein.

[0031] Das Netzwerk **204** repräsentiert allgemein jedes Medium oder jede Architektur, das/die in der Lage ist, Kommunikation oder Datentransfer zu ermöglichen. In einem Beispiel kann das Netzwerk **204** Kommunikation zwischen der Recheneinrichtung **202** und dem Server **206** ermöglichen. In diesem Beispiel kann das Netzwerk **204** die Kommunikation oder den Datentransfer unter Verwendung von drahtlosen und/oder drahtgebundenen Verbindungen ermöglichen. Beispiele für das Netzwerk **204** umfassen, ohne Beschränkung, ein Intranet, ein Weitbereichsnetzwerk (WAN, wide area network), ein Lokalnetzwerk (LAN, local area network), ein Kleingerätenetzwerk (PAN, personal area network), das Internet, Stromleitungskommunikation (PLC, power line communications), ein zellulares Netzwerk (z.B. ein globales Mobilfunknetzwerk (GSM, Global System for Mobile Communication)-Netzwerk), Teile von einem oder mehreren derselben, Variationen oder Kombinationen von einem oder mehreren derselben und/oder jedes andere geeignete Netzwerk.

[0032] **Fig. 3** ist ein Ablaufdiagramm eines Beispiels für das computerimplementierte Verfahren **300** für die Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung. Die in **Fig. 3** gezeigten Schritte können mit jedem geeigneten computerausführbaren Code und/oder Rechensystem durchgeführt werden, einschließlich dem System **100** in **Fig. 1**, dem System **200** in **Fig. 2**, und/oder Variationen oder Kombinationen von einem oder mehreren derselben. In einem Beispiel kann jeder der in **Fig. 3** gezeigten Schritte einen Algorithmus darstellen, dessen Struktur mehrere Unterschritte enthält und/oder durch mehrere Unterschritte dargestellt wird, wofür nachstehend Beispiele ausführlicher bereitgestellt werden.

[0033] So wie das in **Fig. 3** dargestellt ist, können im Schritt **302** eines oder mehrere der hierin beschriebenen Systeme an einem Endpunkt in einem Netzwerk verdächtige Aktivitäten in dem Netzwerk durch einen nicht identifizierten Prozess detektieren (oder erkennen). Beispielsweise kann das Detektionsmodul **104**, als Teil der Recheneinrichtung **202** in **Fig. 2**, verdächtige Aktivitäten durch einen nicht identifizierten Prozess der Recheneinrichtung **202** erkennen.

[0034] Die hierin beschriebenen Systeme können den Schritt **302** auf verschiedene Weisen ausführen. In einem Beispiel kann das Detektionsmodul **104** die Netzwerkaktivität von einem nicht identifizierten Prozess der Recheneinrichtung **202** erkennen. Das Detektionsmodul **104** kann Netzwerkaktivität als ungewöhnlich kennzeichnen (oder markieren), wie etwa unerwarteten Netzwerkverkehr, unregelmäßigen Netzwerkverkehr, hohen Bandbreitenverbrauch usw. Der nicht identifizierte Prozess kann ein Prozess, ein Thread (oder Strang), eine Anwendung und/oder eine andere Software sein, die ausgeführt wird und die aufgrund unbekannter Bezeichner (oder Identifikatoren), versteckter Bezeichner usw. nicht identifiziert sein kann. Beispielsweise kann der nicht identifizierte Prozess ein Schadprogramm oder eine andere Sicherheitsbedrohung sein, oder kann eine gutartige Software sein, die möglicherweise nicht erkannt wird. Alternativ kann der nicht identifizierte Prozess ein bekannter Prozess sein, der sich abnormal verhält. Beispielsweise kann der nicht identifizierte Prozess eine bekannte Software sein, die durch bösartigen Code verändert worden sein kann oder mit neuen Funktionalitäten und/oder geänderten Einstellungen aktualisiert worden sein kann.

[0035] In einem anderen Beispiel kann das Detektionsmodul **104**, als Teil des Servers **206** in **Fig. 2**, ungewöhnliche Netzwerkaktivitäten detektieren (oder erkennen), die von der Recheneinrichtung **202** ausgehen. Zum Beispiel kann der Server **206** eine mögliche Sicherheitsbedrohung erkennen, die von der Recheneinrichtung **202** ausgeht.

[0036] **Fig. 4A** veranschaulicht einen Endpunkt **402**, der der Recheneinrichtung **202** entsprechen kann. Der Endpunkt **402** kann von einem Angreifer kompromittiert worden sein, so dass der nicht identifizierte Prozess ein Schadprogramm sein kann, das zunächst möglicherweise unentdeckt bleiben kann. Das Schadprogramm kann versuchen, andere Endpunkte zu infizieren, die mit Endpunkt **402** in einer Netzwerkumgebung verbunden sind, wie etwa eine Netzwerkumgebung **500A** in **Fig. 5A**.

[0037] **Fig. 5A** veranschaulicht eine Netzwerkumgebung **500A** mit einem Endpunkt **502** und Endpunkten **550A-C**, die über ein Netzwerk **504** verbunden sind. Der Endpunkt **502** kann eine Recheneinrichtung sein, wie etwa die Recheneinrichtung **202**, die dem Endpunkt **402** entspricht. Die Endpunkte **550A-C** können jeweils Recheneinrichtungen sein, wie etwa die Recheneinrichtung **202**. Das Netzwerk **504** kann ein Netzwerk, wie etwa das Netzwerk **204**, sein, das die Endpunkte **502** und **550A-C** verbindet. Eine verdächtige Aktivität kann von dem Endpunkt **502** aus erkannt werden. Beispielsweise kann der Endpunkt **502** ei-

ne Quelle für anormalen Netzwerkverkehr sein, der an den Endpunkt **550A** gesendet wird. Genauer gesagt kann ein nicht identifizierter Prozess, der auf dem Endpunkt **502** ausgeführt wird, die Quelle von anormalem Netzwerkverkehr zu dem Endpunkt **550A** sein.

[0038] Um zu **Fig. 3** zurückzukehren, im Schritt **304** können eines oder mehrere der hierin beschriebenen Systeme die Netzwerkaktivität des nicht identifizierten Prozesses zu einem falschen Netzwerk, das von dem Netzwerk getrennt ist, leiten. Beispielsweise kann das Leitmodul **106**, als Teil der Recheneinrichtung **202** in **Fig. 2**, die dem nicht identifizierten Prozess zugeordnete Netzwerkaktivität an den Server **206** weiterleiten, so dass die verdächtige Aktivität umgeleitet wird.

[0039] Der Begriff „falsches Netzwerk“, so wie er hierin verwendet wird, bezieht sich allgemein auf ein Computernetzwerk, in dem eine oder mehrere Zieladressen für Endpunkte in dem Computernetzwerk Netzwerkverkehr an falsche Endpunkte leiten. Beispielsweise kann ein falsches Netzwerk eine echte Netzwerkumgebung nachahmen, so dass eine Netzwerktopologie und/oder Endpunkte des falschen Netzwerks denen der echten Netzwerkumgebung ähneln können. Das falsche Netzwerk kann einen Server aufweisen, der virtuelle Maschinen für die falschen Endpunkte verwaltet. Ein echter Endpunkt der echten Netzwerkumgebung, der möglicherweise nicht mit einem falschen Endpunkt in dem falschen Netzwerk repliziert (oder wiederholt) wird, kann das falsche Netzwerk durchqueren und mit den falschen Endpunkten kommunizieren. In Bezug auf den echten Endpunkt kann das falsche Netzwerk allgemein nicht von der echten Netzwerkumgebung unterscheidbar erscheinen. Über die oberflächliche Netzwerkinteraktion hinaus kann das falsche Netzwerk jedoch Einschränkungen aufweisen, die möglicherweise aufdeckbar sein können. Beispielsweise können Änderungen der Netzwerktopologie für die echte Netzwerkumgebung nicht auf das falsche Netzwerk übertragen werden, oder die falschen Endpunkte können Diskrepanzen aufweisen, wenn sie die Endpunkte der echten Netzwerkumgebung nachahmen.

[0040] Die hierin beschriebenen Systeme können die Netzwerkaktivität des nicht identifizierten Prozesses auf verschiedene Weise leiten. In einem Beispiel kann eine geteilte Tunnelroute (split tunnel route) zwischen dem nicht identifizierten Prozess und dem falschen Netzwerk eingerichtet werden. Zum Beispiel kann in **Fig. 4B** das falsche Netzwerk durch einen Server **406** implementiert werden, der dem Server **206** entsprechen kann. In anderen Implementierungen kann das falsche Netzwerk beispielsweise mit einer virtuellen Maschine auf dem Endpunkt **402** implementiert werden. In wieder anderen Implementierungen kann das falsche Netzwerk mit einem Gateway, der mit einem alternativen Netzwerk verbunden ist, implementiert werden. In **Fig. 4B** kann das Leitmodul **106**, als Teil von dem Endpunkt **402**, die geteilte Tunnelroute zwischen dem Endpunkt **402** und dem Server **406** einrichten. Die aufteilte Tunnelroute kann auf den nicht identifizierten Prozess beschränkt sein oder kann zusätzliche Anwendungen aufweisen. In einigen Implementierungen kann der gesamte Netzwerkverkehr von dem Endpunkt **402** an den Server **406** weitergeleitet werden.

[0041] Für den nicht identifizierten Prozess kann eine Falsch-Leittabelle (false routing table) erstellt werden, um Verkehr von dem nicht identifizierten Prozess zu dem falschen Netzwerk zu leiten. Beispielsweise kann die Falsch-Leittabelle eine neue Leittabelle auf den Endpunkt **402** sein oder eine Änderung einer vorhandenen Leittabelle sein, die von dem Endpunkt **402** verwendet wird. Das Leitmodul **106** kann die vorhandene Leittabelle umschreiben, um die aufgeteilte Tunnelroute einzurichten.

[0042] **Fig. 5B** zeigt ein falsches Netzwerk **500B**, das eine Netzwerkumgebung **500A** nachahmt, so wie das weiter unten beschrieben wird. Das falsche Netzwerk **500B** kann mit einem Server **506** implementiert werden, der möglicherweise dem Server **206** entspricht. In **Fig. 5A** kann der Endpunkt **502** mit dem Netzwerk **504** verbunden sein. In **Fig. 5B** kann diese Verbindung durch eine geteilte Tunnelroute zwischen dem Endpunkt **502** und dem Server **506** ersetzt werden. Diese aufgeteilte Tunnelroute kann bestimmten Netzwerkverkehr, der ursprünglich an das Netzwerk **504** gerichtet war, zu dem Server **506** umleiten.

[0043] In bestimmten Implementierungen kann den Server **506**, anstatt dem Endpunkt **502** neu zu konfigurieren, bestimmten Netzwerkverkehr, der an das Netzwerk **504** gerichtet ist, aktiv abfangen. In solchen Implementierungen kann der Server **506** ein Gateway oder ein anderes Netzwerkgerät zwischen dem Endpunkt **502** und dem Netzwerk **504** sein.

[0044] Um zu **Fig. 3** zurückzukehren, können im Schritt **306** eines oder mehrere der hierin beschriebenen Systeme eine oder mehrere virtuelle Maschinen in dem falschen Netzwerk initialisieren, um das Netzwerk so nachzuahmen, dass dem nicht identifizierten Prozess nicht bewusst ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird. Beispielsweise kann das Nachahmungsmodul **108**, als Teil der Recheneinrichtung **202** in **Fig. 2**, für das falsche Netzwerk eine virtuelle Maschine für jeden Endpunkt des Netzwerks initialisieren.

[0045] Die hierin beschriebenen Systeme können den Schritt **306** auf verschiedene Weisen ausführen. In einem Beispiel kann das Netzwerk eine Mehrzahl von Endpunkten aufweisen und das falsche Netz-

werk kann eine virtuelle Maschine für jeden von der Mehrzahl von Endpunkten aufweisen. Beispielsweise kann das Nachahmungsmodul **108**, als Teil des Servers **406** in **Fig. 4C**, virtuelle Maschinen **420** initialisieren. Virtuelle Maschinen **420** können speziell die Endpunkte des Netzwerks imitieren. Virtuelle Maschinen **420** können zum Beispiel ein Klon der jeweiligen Endpunkte sein. Auf virtuellen Maschinen **420** können ähnliche Software-Suites ausgeführt werden und sie können ähnliche Netzwerkverkehrsmuster aufweisen. In bestimmten Implementierungen können virtuelle Maschinen **420** Dateien, Datenbanken und andere Datenstrukturen nachahmen (oder imitieren), um falsche Ziele für potenzielle Schadprogramme zu liefern. Virtuelle Maschinen **420** können alternativ auch vereinfachte Versionen der jeweiligen Endpunkte sein, zum Beispiel ein abgesicherter Modus. In anderen Implementierungen können virtuelle Maschinen **420** generische Versionen der jeweiligen Endpunkte sein, wie etwa Dummy-Maschinen, die fähig sind für minimale Interaktion.

[0046] Fig. 5B veranschaulicht virtuelle Maschinen **520A-C**, die jeweils den Endpunkten **550A-C** entsprechen können. Der Server **506** kann virtuelle Maschinen **520A-C** auf der Grundlage der Kenntnis der Endpunkte **550A-C** initialisieren. Beispielsweise kann der Server **506** die Endpunkte **502** und **550A-C** im Netzwerk **504** so verwalten, dass der Server **506** eine Netzwerktopologie des Netzwerks **504** kennt. Um die Netzwerkumgebung **500A** nachzuahmen, kann der Server **506** virtuelle Maschinen **520A-C** zum Nachahmen von Endpunkten **550A-C** initialisieren. Weil virtuelle Maschinen **520A-C** möglicherweise auf dem Server **506** ablaufen können, kann der Netzwerkverkehr von dem Endpunkt **502** zu dem Netzwerk **504** (z. B. Endpunkte **550A-C)** stattdessen zu dem Server **506** geleitet werden.

[0047] Dem nicht identifizierten Prozess auf Endpunkt **502** ist möglicherweise nicht bewusst, dass der Netzwerkverkehr für den nicht identifizierten Prozess von der Netzwerkumgebung **500A** auf das falsche Netzwerk **500B** umgeleitet wurde. Beispielsweise kann der Server **506** eine Netzwerkverbindung zwischen dem Endpunkt **502** und dem Endpunkt **520A** mit einer Netzwerkverbindung zwischen dem Endpunkt **502** und dem Endpunkt **550A** umleiten. Ähnliche Netzwerkverbindungen mit den Endpunkten **520B-C** können jeweils mit Netzwerkverbindungen mit den Endpunkten **550B-C** umgeleitet werden. Genauer gesagt kann der Server **506** Daten von dem Endpunkt **502** mit einem Ziel von dem Endpunkt **550A** empfangen. Der Server **506** kann die empfangenen Daten stattdessen an die virtuelle Maschine **520A** weiterleiten. Der Server **506** kann anschließend eine Antwort von der virtuellen Maschine **520A** empfangen und die Antwort an den Endpunkt **502** weiterleiten.

[0048] In bestimmten Implementierungen können virtuelle Maschinen **520A-C** auf von dem Server **506** getrennten Recheneinrichtung implementiert werden. Beispielsweise kann die Netzwerkumgebung **500A** physikalisch so nachgeahmt werden, dass virtuelle Maschinen **520A-C** Recheneinrichtung, die jeweils Endpunkte **550A-C** nachahmen, sein können.

[0049] Das Nachahmen der Netzwerkumgebung **500A** kann es dem nicht identifizierten Prozess ermöglichen, sich ungehindert auf dem falschen Netzwerk **500B** zu verhalten, ohne die Netzwerkumgebung **500A** zu gefährden. Wenn es sich bei dem nicht identifizierten Prozess beispielsweise ein Schadprogramm ist, kann das Schadprogramm laterale (oder seitliche) Angriffe auf die Endpunkte **550A-C** versuchen. Das Schadprogramm kann stattdessen die virtuellen Maschinen **520A-C** angreifen, ohne die Endpunkte **550A-C** zu gefährden. Darüber hinaus kann das Nachahmen des Netzwerks eine Wahrscheinlichkeit verringern, dass ein potenzieller Angreifer, der das Schadprogramm kontrolliert (oder steuert), davor gewarnt wird, entdeckt zu werden. Beispielsweise kann der potenzielle Angreifer eine Änderung der Netzwerktopologie, blockierte Kommunikation und/oder andere Sicherheitsmaßnahmen bemerken. Der Angreifer kann mit Gegenmaßnahmen reagieren, die die Auswirkungen von Abhilfemaßnahmen mildern können.

[0050] So wie das in **Fig. 3** dargestellt ist, können im Schritt **308** eines oder mehrere der hierin beschriebenen Systeme ein Verhalten des nicht identifizierten Prozesses in dem falschen Netzwerk analysieren. Beispielsweise kann das Analysemodul **110**, als Teil der Recheneinrichtung **202** in **Fig. 2**, den Netzwerkverkehr von dem nicht identifizierten Prozess zu virtuellen Maschinen in dem falschen Netzwerk analysieren.

[0051] Die hierin beschriebenen Systeme können den Schritt **308** auf verschiedene Weisen ausführen. In einem Beispiel kann das Analysieren des Verhaltens ein Sammeln von forensischen Artefakte aufweisen, die indikativ sind für ein dem nicht identifizierten Prozess zugeordnetes Verhalten. Das Analysemodul **110** kann, als Teil des Endpunkts **402** in **Fig. 4D**, forensische Artefakte von dem Endpunkt **402** sammeln, um das Verhalten des nicht identifizierten Prozesses zu analysieren.

[0052] Zusätzlich oder alternativ können die forensischen Artefakte von einem anderen Endpunkt des Netzwerks gesammelt werden. Beispielsweise kann das Analysemodul **110**, als Teil des Servers **506** in **Fig. 5B**, die forensischen Artefakte von dem Endpunkt **502** und/oder von einer oder mehreren virtuellen Maschinen **520A-C** sammeln. In einigen Beispielen können die forensischen Artefakte Speicherartefakte aufweisen. Beispielsweise können Speicher-

artefakte ausführbaren Code, geänderte Speicherbereiche, gesendete/empfangene Daten usw. aufweisen. Andere Artefakte können von dem falschen Netzwerk **500B** ebenfalls gesammelt werden.

[0053] Die forensischen Artefakte können mit einer Datenbank von Artefakten verglichen werden, die böswilliges Verhalten anzeigen können. Bestimmte Artefakte können indikativ sein für potenzielle Sicherheitsbedrohungen, während bestimmte andere Artefakte gutartig sein können. In einigen Beispielen können die gesammelten Artefakte identifiziert und mit gewichteten Punktzahlen (scores) versehen werden, die einen Bedrohungsgrad angeben. Wenn eine kombinierte gewichtete Punktzahl einen Bedrohungsschwellenwert erfüllt, kann bestimmt werden, dass der nicht identifizierte Prozess bösartiger Code ist oder bösartigen Code enthält.

[0054] Das Analysieren des Verhaltens kann ein Überwachen des Verhaltens, ohne den nicht identifizierten Prozess zu behindern, aufweisen. Wenn der nicht identifizierte Prozess auf dem Endpunkt **502** beispielsweise ein Schadprogramm ist, kann das Schadprogramm Angriffe auf die Endpunkte **550A-C** versuchen. Das Schadprogramm kann sich möglicherweise nicht bewusst sein, dass die versuchten Angriffe, Endpunkte **550A-C** anzugreifen, in Wirklichkeit virtuelle Maschinen **520A-C** anstelle von Endpunkten **550A-C** angreifen können. Virtuelle Maschinen **520A-C** können Endpunkte **550A-C** effektiv fälschen. Auf diese Weise kann das Schadprogramm frei sein, zu versuchen, das Netzwerk **504** anzugreifen, ohne tatsächlich negative Auswirkungen auf das Netzwerk **504** zu verursachen. Das Netzwerk **504** kann vor der Ausnutzung durch das Schadprogramm, von dem Exfiltrieren von Daten durch das Schadprogramm und von anderen Sicherheitsbedrohungen durch das Schadprogramm geschützt werden. Darüber hinaus kann ein potenzieller Angreifer, der die Kontrolle (oder Steuerung) über das Schadprogramm hat, möglicherweise nicht darüber gewarnt sein, dass das Schadprogramm überwacht wird. Somit kann das Verhalten genau überwacht werden.

[0055] In bestimmten Fällen kann der nicht identifizierte Prozess jedoch ein legitimer Prozess sein. Beispielsweise kann der nicht identifizierte Prozess ein neuer Prozess sein, der möglicherweise noch nicht erkannt wird, oder kann eine bekannte Anwendung sein, die sich aufgrund neuer und/oder geänderter Funktionalitäten anders verhält. In solchen Beispielen kann es sein, dass eine Sicherheitsmaßnahme als Reaktion auf die verdächtige Aktivität nicht notwendig ist. Anstatt sofort mit einer Sicherheitsmaßnahme auf die verdächtige Aktivität zu reagieren, kann das Einrichten des falschen Netzwerks Zeit geben, um den nicht identifizierten Prozess auf böswillige Absichten hin zu analysieren.

[0056] Darüber hinaus kann es in bestimmten Fällen vorkommen, dass eine Sicherheitsmaßnahme nicht sofort verfügbar ist als Reaktion auf das Erkennen der verdächtigen Aktivität des nicht identifizierten Prozesses. Beispielsweise kann es sein, dass für ein neu entdecktes Schadprogrammm eine geeignete Sicherheitsmaßnahme noch nicht bekannt ist. Unbekannte Schwachstellen werden möglicherweise nicht ausreichend behandelt, wenn eine Sicherheitsmaßnahme durchgeführt wird, bevor das Verhalten des Schadprogramms vollständig identifiziert ist. Zusätzlich und alternativ kann ein erheblicher Aufwand an Ressourcen erforderlich sein, um Angriffe zu identifizieren und die Auswirkungen der Angriffe zu blockieren oder anderweitig zu verändern. Einige Sicherheitsmaßnahmen werden möglicherweise nicht schnell genug ausgeführt, um das Schadprogramm ausreichend daran zu hindern, sich zu einem anderen Endpunkt zu bewegen. Das Umleiten des Netzwerkverkehrs auf ein falsches Netzwerk, so wie das hierin beschrieben ist, kann schneller durchgeführt werden als einige Sicherheitsmaßnahmen, um die Ausbreitung der Schadprogramm-Infektion ausreichend einzudämmen.

[0057] So wie das in **Fig. 3** dargestellt ist, können im Schritt **310** eines oder mehrere der hierin beschriebenen Systeme auf der Grundlage der Analyse eine Sicherheitsmaßnahme (oder Sicherheitsaktion) durchführen. Beispielsweise kann das Sicherheitsmodul **112**, als Teil der Recheneinrichtung **202** in **Fig. 2**, eine Sicherheitsmaßnahme auf der Recheneinrichtung **202** durchführen.

[0058] Die hierin beschriebenen Systeme können den Schritt **310** auf verschiedene Weisen durchführen. In einem Beispiel kann die Sicherheitsmaßnahme ein Isolieren des Endpunkts von dem Netzwerk aufweisen. Die Sicherheitsmaßnahme kann ein Unter-Quarantäne-Stellen des nicht identifizierten Prozesses an dem Endpunkt aufweisen. Die Sicherheitsmaßnahme kann ein Senden einer Benachrichtigung, beispielsweise an einen Administrator oder einen Sicherheitsanalytiker, aufweisen. Die Sicherheitsmaßnahme kann auch ein Bereitstellen der Analyse, beispielsweise an den Administrator oder den Sicherheitsanalytiker, aufweisen. Die Sicherheitsmaßnahme ferner ein Veröffentlichen der Analyse aufweisen, wie etwa ein Veröffentlichen auf einer Sicherheitswebsite zum Melden von Schadprogrammen.

[0059] Die Sicherheitsmaßnahme kann eine Bedrohung durch den nicht identifizierten Prozess auf der Grundlage der Analyse seines Verhaltens angemessen behandeln. Wenn in **Fig. 4** festgestellt wird, dass der nicht identifizierte Prozess ein Schadprogramm ist, kann das Sicherheitsmodul **112**, als Teil des Endpunkts **402**, den Endpunkt **402** von dem Netzwerk isolieren. Zusätzlich oder alternativ kann das Sicherheitsmodul **112** Binäritäten (oder Gegensatzpaare)

von dem Endpunkt **402**, die den nicht identifizierten Prozess aufweisen können, unter Quarantäne stellen (oder isolieren). In **Fig. 5B** kann das Sicherheitsmodul **112**, als Teil von dem Server **506**, den Endpunkt **502** von dem Netzwerk **504** isolieren. Andere Sicherheitsmaßnahmen zur Abhilfe können bei Bedarf automatisch eingeleitet werden.

[0060] Das Sicherheitsmodul **112** kann eine Benachrichtigung an einen Administrator senden. Beispielsweise kann das Sicherheitsmodul **112** eine Benachrichtigung an einen Netzwerkadministrator senden, die einen Bedrohungsgrad durch den nicht identifizierten Prozess angibt. Der Administrator kann dann eine geeignete Sicherheitsmaßnahme festlegen. In einigen Beispielen kann das Sicherheitsmodul **112** dem Administrator oder einem anderen Sicherheitsanalytiker die Analyse zur Verfügung stellen. Beispielsweise kann das Sicherheitsmodul **112** die Analyse an einen angewiesenen (oder benannten) Sicherheitsanalytiker weiterleiten. In anderen Fällen kann das Sicherheitsmodul **112** die Analyse an einen Verwahrort zur Identifizierung (repository for identification) veröffentlichen. Zum Beispiel kann das Sicherheitsmodul **112** neu identifizierte Artefakte auswerten (oder bewerten), teilweise auf der Grundlage einer kombinierten gewichteten Punktzahl, so wie das oben beschrieben ist. Das Sicherheitsmodul **112** kann die neu identifizierten Artefakte zu einer Datenbank von Artefakten hinzufügen. Das Sicherheitsmodul **112** kann den nicht identifizierten Prozess als Schadprogramm identifizieren und eine Zusammenfassung des identifizierten Verhaltens des Schadprogramms liefern. Alternativ dazu kann das Sicherheitsmodul **112** den nicht identifizierten Prozess als einen gutartigen Prozess identifizieren und den gutartigen Prozess auf eine entsprechende Positivliste (oder Whitelist) setzen. In einigen Beispielen kann das Sicherheitsmodul **112** gesammelte Artefakte bereitstellen, ohne den nicht identifizierten Prozess vollständig zu identifizieren. Beispielsweise hat das Sicherheitsmodul **112** möglicherweise nicht genügend Daten und/oder Zeit, um den nicht identifizierten Prozess zu analysieren und zu identifizieren. Der Sicherheitsanalytiker kann möglicherweise auf der Grundlage der von dem Sicherheitsmodul **112** bereitgestellten Teilanalyse feststellen, ob der nicht identifizierte Prozess ein Schadprogramm ist.

[0061] So wie das oben im Zusammenhang mit dem beispielhaften Verfahren **300** in **Fig. 3** erläutert ist, können die hierin beschriebenen Systeme und Verfahren das Netzwerkverhalten eines nicht identifizierten Prozesses überwachen, indem sie ein falsches Netzwerk verwenden, das ein echtes Netzwerk nachahmt. Nachdem eine verdächtige Netzwerkaktivität an einem Endpunkt erkannt worden ist, kann der Endpunkt eine geteilte Tunnelroute erstellen, die die verdächtige Netzwerkaktivität zu einem falschen Netzwerk lenkt. Das falsche Netzwerk kann automatisch Instanzen von virtuellen Maschinen starten, um für den Endpunkt ein echtes Netzwerk nachzuahmen. Mit Vorteil kann das falsche Netzwerk bei Bedarf in Echtzeit initialisiert werden kann und kann ein potenzielles Schadprogram effektiv isolieren, bis eine geeignete Abhilfemaßnahme bestimmt werden kann.

[0062] Die hierin beschriebenen Systeme und Verfahren können mit Vorteil verdächtige Netzwerkaktivitäten überwachen und analysieren, ohne einen potentiellen Angreifer über ein Überwachen zu alarmieren oder das echte Netzwerk der Ausbeutung und/oder Exfiltration auszusetzen. Obwohl der potentielle Angreifer möglicherweise irgendwann von dem falschen Netzwerk Kenntnis erlangt, kann den hierin beschriebenen Systemen und Verfahren genügend Zeit eingeräumt werden, um die verdächtige Netzwerkaktivität ausreichend zu analysieren. Darüber hinaus können die hierin beschriebenen Systeme und Verfahren die echten Endpunkte in der echten Netzwerkumgebung vor lateralen (oder seitlichen) Angriffen schützen, die von dem Endpunkt ausgehen. Jegliche derartigen lateralen Angriffe würden stattdessen die virtuellen Maschinen angreifen und sich in dem falschen Netzwerk verbreiten, wo ein Sicherheitssystem diese überwachen und beheben kann.

[0063] Sobald die Absicht hinter der verdächtigen Netzwerkaktivität ermittelt ist, können entsprechende Maßnahmen ergriffen werden. Wenn das Sicherheitsmodul **112** feststellt, dass die verdächtige Netzwerkaktivität bösartiges Verhalten ist, kann das Sicherheitsmodul **112** automatisch Abhilfemaßnahmen implementieren. Beispielsweise kann das Sicherheitsmodul **112** den Endpunkt von dem Rest des Netzwerks isolieren. Darüber hinaus kann das Sicherheitsmodul **112** die verdächtige Netzwerkaktivität identifizieren und die Identifizierung veröffentlichen, um bei zukünftigen Ermittlungen zu helfen. Das Sicherheitsmodul **112** kann auch vorgeschlagene Abhilfemaßnahmen zusammen mit der Identifizierung veröffentlichen.

[0064] **Fig. 6** ist ein Blockschaubild eines beispielhaften Rechensystems **610**, das in der Lage ist, eine oder mehrere der hierin beschriebenen und/oder veranschaulichten Ausführungsformen zu implementieren. Beispielsweise können das gesamte oder ein Teil des Rechensystems **610** allein oder in Kombination mit anderen Elementen einen oder mehrere der hierin beschriebenen Schritte ausführen und/oder ein Mittel zum Ausführen von einem oder mehreren der hierin beschriebenen Schritte sein (wie etwa einen oder mehrere der in **Fig. 3** dargestellten Schritte). Das gesamte oder ein Teil des Rechensystems **610** können auch andere hierin beschriebene und/oder veranschaulichte Schritte, Verfahren oder Prozesse ausführen und/oder ein Mittel zum Ausführen solcher Schritte, Verfahren oder Prozesse sein.

[0065] Das Rechensystem **610** repräsentiert im Großen und Ganzen jede/jedes Einzel- oder Multiprozessor-Recheneinrichtung oder -system, die/das in der Lage ist, computerlesbare Befehle auszuführen. Beispiele für das Rechensystem **610** sind, ohne Beschränkung, Arbeitsstationen (work stations), Laptops, Client-seitige Endgeräte, Server, verteilte Rechensysteme, handhaltbare Geräte oder jedes andere Rechensystem oder -gerät. In seiner grundlegendsten Konfiguration kann das Rechensystem **610** mindestens einen Prozessor **614** und einen Systemspeicher **616** enthalten.

[0066] Der Prozessor **614** repräsentiert allgemein jede Art oder Form einer physikalischen Verarbeitungseinheit (z.B. eine Hardware-implementierte Zentraleinheit), die in der Lage ist, Daten zu verarbeiten oder Befehle zu interpretieren und auszuführen. In bestimmten Ausführungsformen kann der Prozessor **614** Befehle von einer/m Software-Anwendung oder -Modul empfangen. Diese Befehle können den Prozessor **614** dazu veranlassen, die Funktionen von einer oder mehreren der hierin beschriebenen und/oder veranschaulichten beispielhaften Ausführungsformen auszuführen.

[0067] Der Systemspeicher **616** stellt allgemein jede Art oder Form eines flüchtigen oder nichtflüchtigen Speichergeräts oder -mediums dar, das in der Lage ist, Daten und/oder andere computerlesbare Befehle zu speichern. Beispiele für den Systemspeicher **616** sind, ohne Beschränkung, Direktzugriffsspeicher (RAM, random access memory), Nur-Lesespeicher (ROM, read only memory), Flash-Speicher oder jede andere geeignete Speichereinrichtung. Obwohl dies nicht erforderlich ist, kann das Rechensystem **610** in bestimmten Ausführungsformen sowohl eine flüchtige Speichereinrichtung (wie z.B. der Systemspeicher **616**) als auch eine nichtflüchtige Speichereinrichtung (wie z.B. das primäre Datenspeichergerät **632**, so wie das unten ausführlich beschrieben wird) enthalten. In einem Beispiel können eines oder mehrere der Module **102** aus **Fig. 1** in den Systemspeicher **616** geladen werden.

[0068] In einigen Beispielen kann der Systemspeicher **616** ein Betriebssystem **640** zur Ausführung durch den Prozessor **614** speichern und/oder laden. In einem Beispiel kann das Betriebssystem **640** Software enthalten und/oder darstellen, die Computer-Hardware- und Software-Ressourcen verwaltet und/oder die gemeinsame Dienste für Computerprogramme und/oder Anwendungen auf dem Rechensystem **610** bereitstellt. Beispiele für das Betriebssystem **640** umfassen, ohne Einschränkung, LINUX, JUNOS, MICROSOFT WINDOWS, WINDOWS MOBILE, MAC OS, APPLE'S IOS, UNIX, GOOGLE CHROME OS, GOOGLE'S ANDROID, SOLARIS, Variationen von einem oder mehreren derselben und/oder jedes andere geeignete Betriebssystem.

[0069] In bestimmten Ausführungsformen kann das beispielhafte Rechensystem **610** neben dem Prozessor **614** und dem Systemspeicher **616** auch eine oder mehrere Komponenten oder Elemente enthalten. Zum Beispiel kann, so wie das in **Fig. 6** dargestellt ist, das Rechensystem **610** eine Datenspeicher-Steuereinrichtung **618**, eine Eingabe-/Ausgabe- Steuereinrichtung **620** und eine Kommunikationsschnittstelle **622** enthalten, die über eine Kommunikationsinfrastruktur **612** miteinander verbunden sein können. Die Kommunikationsinfrastruktur **612** stellt allgemein jede Art oder Form von Infrastruktur dar, die in der Lage ist, die Kommunikation zwischen einer oder mehreren Komponenten einer Recheneinrichtung zu ermöglichen. Beispiele für die Kommunikationsinfrastruktur **612** sind, ohne Beschränkung, ein Kommunikationsbus (wie z.B. ein ISA (industry standard architecture), PCI (peripheral component interconnect), PCIe (PCI Express) -Bus oder ein ähnlicher Bus) und ein Netzwerk.

[0070] Die Datenspeicher-Steuereinrichtung **618** repräsentiert allgemein jede Art oder Form von Einrichtung, das in der Lage ist, Datenspeicher oder Daten zu verarbeiten oder die Kommunikation zwischen einer oder mehreren Komponenten des Rechensystems **610** zu steuern. Beispielsweise kann in bestimmten Ausführungsformen die Datenspeicher-Steuereinrichtung **618** die Kommunikation zwischen dem Prozessor **614**, dem Systemspeicher **616** und der Eingabe-/Ausgabe-Steuereinrichtung **620** über die Kommunikationsinfrastruktur **612** steuern.

[0071] Die Eingabe-/Ausgabe-Steuereinrichtung **620** repräsentiert allgemein jede Art oder Form eines Moduls, das in der Lage ist, die Eingabe- und Ausgabefunktionen einer Recheneinrichtung zu koordinieren und/oder zu steuern. In bestimmten Ausführungsformen kann die Eingabe-/Ausgabe-Steuereinrichtung **620** beispielsweise die Übertragung von Daten zwischen einem oder mehreren Elementen des Rechensystems **610** steuern oder ermöglichen, wie z.B. dem Prozessor **614**, dem Systemspeicher **616**, der Kommunikationsschnittstelle **622**, dem Anzeigeadapter (oder Bildschirmadapter) 626, der Eingabeschnittstelle **630** und der Datenspeicherschnittstelle **634**.

[0072] So wie das in **Fig. 6** dargestellt ist, kann das Rechensystem **610** auch mindestens eine Anzeigeeinrichtung (oder Bildschirmeinrichtung) 624 enthalten, die über einen Anzeigeadapter **626** an die Eingabe-/Ausgabe-Steuereinrichtung **620** gekoppelt ist. Die Anzeigeeinrichtung **624** stellt allgemein jede Art oder Form von Gerät dar, das in der Lage ist, die von dem Anzeigeadapter **626** weitergeleiteten Informationen visuell darzustellen. In ähnlicher Weise stellt der Anzeigeadapter **626** allgemein jede Art oder Form von Gerät dar, das in der Lage ist, Grafiken, Text und andere Daten von der Kommunikationsinfrastruktur

612 (oder von einem Rahmenpuffer (frame buffer), wie im Stand der Technik bekannt) zur Anzeige auf der Anzeigeeinrichtung **624** weiterzuleiten.

[0073] So wie das in **Fig. 6** dargestellt ist, kann das beispielhafte Rechensystem **610** auch mindestens eine Eingabeeinrichtung **628** enthalten, das über eine Eingabeschnittstelle **630** mit der Eingabe-/Ausgabe-Steuereinrichtung **620** gekoppelt ist. Die Eingabeeinrichtung **628** repräsentiert allgemein jede Art oder Form von Eingabegerät, das in der Lage ist, dem beispielhaften Rechensystem **610** Eingaben, entweder computer- oder menschenerzeugt, zu liefern. Beispiele für die Eingabeeinrichtung **628** sind, ohne Einschränkung, eine Tastatur, ein Zeigegerät, ein Spracherkennungsgerät, Variationen oder Kombinationen von einem oder mehreren derselben und/oder jedes andere Eingabegerät.

[0074] Zusätzlich oder alternativ kann das beispielhafte Rechensystem **610** zusätzliche Eingabe-/Ausgabe-Einrichtungen (oder -Geräte) enthalten. Das beispielhafte Rechensystem **610** kann zum Beispiel die Eingabe-/AusgabeEinrichtung **636** enthalten. In diesem Beispiel kann die Eingabe-/AusgabeEinrichtung **636** eine Nutzerschnittstelle enthalten und/oder darstellen, die die menschliche Interaktion mit dem Rechensystem **610** ermöglicht. Beispiele für die Eingabe-/Ausgabe-Einrichtung **636** sind, ohne Beschränkung, eine Computermaus, eine Tastatur, ein Monitor, ein Drucker, ein Modem, eine Kamera, ein Scanner, ein Mikrofon, ein Gerät mit Berührungsbildschirm, Variationen oder Kombinationen von einem oder mehreren derselben und/oder jede andere Eingabe-/Ausgabe- Einrichtung.

[0075] Die Kommunikationsschnittstelle **622** stellt im allgemein jede Art oder Form von Kommunikationseinrichtung oder Adapter dar, die/der in der Lage ist, die Kommunikation zwischen dem beispielhaften Rechensystem **610** und einem oder mehreren zusätzlichen Geräten zu ermöglichen. Beispielsweise kann in bestimmten Ausführungsformen die Kommunikationsschnittstelle **622** die Kommunikation zwischen dem Rechensystem **610** und einem privaten oder öffentlichen Netzwerk einschließlich zusätzlicher Rechensysteme ermöglichen. Beispiele für die Kommunikationsschnittstelle **622** sind, ohne Beschränkung, eine drahtgebundene Netzwerkschnittstelle (wie etwa eine Netzwerkschnittstellenkarte), eine drahtlose Netzwerkschnittstelle (wie etwa eine drahtlose Netzwerkschnittstellenkarte), ein Modem und jede andere geeignete Schnittstelle. In mindestens einer Ausführungsform kann die Kommunikationsschnittstelle **622** eine direkte Verbindung zu einem entfernten Server (remote server) über eine direkte Verbindung zu einem Netzwerk, wie etwa dem Internet, herstellen. Die Kommunikationsschnittstelle **622** kann eine solche Verbindung auch indirekt bereitstellen, beispielsweise über ein lokales Netzwerk (wie etwa ein Ethernet-Netzwerk), ein Kleingerätenetzwerk (personal area network), ein Telefon- oder Kabelnetzwerk, eine Mobiltelefonverbindung, eine Satellitendatenverbindung oder jede andere geeignete Verbindung.

[0076] In bestimmten Ausführungsformen kann die Kommunikationsschnittstelle **622** auch einen Hostadapter darstellen, der so konfiguriert ist, dass er Kommunikation zwischen dem Rechensystem **610** und einem oder mehreren zusätzlichen Netzwerk- oder Datenspeichergeräten über einen externen Bus oder Kommunikationskanal ermöglicht. Beispiele für Hostadapter sind, ohne Beschränkung, SCSI (small computer system interface) - Hostadapter, USB (universal serial bus) -Hostadapter, IEEE-1394 (Institute of Electrical and Electronics Engineers) -Hostadapter, ATA (advanced technology attachment) -Hostadapter, PATA (parallel ATA), SATA (serial ATA) und eSATA (external SATA) -Hostadapter, Faserkanal (fibre channel) -Schnittstellenadapter, Ethernet-Adapter oder dergleichen. Die Kommunikationsschnittstelle **622** kann es dem Rechensystem **610** auch ermöglichen, sich im verteilten oder entfernten Rechnen (distributed or remote computing) zu beteiligen. Beispielsweise kann die Kommunikationsschnittstelle **622** Befehle von einem entfernten Gerät empfangen oder Befehle an ein entferntes Gerät zur Ausführung senden.

[0077] In einigen Beispielen kann der Systemspeicher **616** ein Netzwerkkommunikationsprogramm **638** zur Ausführung durch den Prozessor **614** speichern und/oder laden. In einem Beispiel kann das Netzwerkkommunikationsprogramm **638** Software enthalten und/oder darstellen, die es dem Rechensystem **610** ermöglicht, eine Netzwerkverbindung **642** mit einem anderen Rechensystem (nicht in **Fig. 6** dargestellt) herzustellen und/oder mit dem anderen Rechensystem über die Kommunikationsschnittstelle **622** zu kommunizieren. In diesem Beispiel kann das Netzwerkkommunikationsprogramm **638** den ausgehenden Verkehrsfluss leiten, der über die Netzwerkverbindung **642** an das andere Rechensystem gesendet wird. Zusätzlich oder alternativ kann das Netzwerkkommunikationsprogramm **638** die Verarbeitung des eingehenden Verkehrs, der von dem anderen Rechensystem über die Netzwerkverbindung **642** in Verbindung mit dem Prozessor **614** empfangen wird, leiten.

[0078] Obwohl dies in **Fig. 6** nicht in dieser Weise dargestellt ist, kann das Netzwerkkommunikationsprogramm **638** alternativ in der Kommunikationsschnittstelle **622** gespeichert und/oder geladen sein. Beispielsweise kann das Netzwerkkommunikationsprogramm **638** zumindest einen Teil der Software und/oder Firmware enthalten und/oder repräsentieren, die von einem Prozessor und/oder einer anwendungsspezifischen integrierten Schaltung

(ASIC), die in die Kommunikationsschnittstelle **622** integriert sind, ausgeführt wird.

[0079] So wie das in **Fig. 6** dargestellt ist, kann das Beispiel-Rechensystem **610** auch eine primäre Datenspeichereinrichtung **632** und eine Datensicherungs (backup) -Speichereinrichtung 633 enthalten, die über eine Speicherschnittstelle **634** an die Kommunikationsinfrastruktur **612** gekoppelt sind. Die Speichereinrichtungen **632** und **633** stellen allgemein jede Art oder Form von Speichereinrichtung oder Medium dar, das in der Lage ist, Daten und/oder andere computerlesbare Befehle zu speichern. Zum Beispiel können die Speichereinrichtungen **632** und **633** ein Magnetplattenlaufwerk (z.B. eine sogenannte Festplatte), ein Festkörperlaufwerk, ein Diskettenlaufwerk, ein Magnetbandlaufwerk, ein optisches Plattenlaufwerk, ein Flash-Laufwerk oder dergleichen sein. Die Speicherschnittstelle **634** stellt allgemein jede Art oder Form von Schnittstelle oder Einrichtung zum Übertragen von Daten zwischen den Speichereinrichtungen **632** und **633** und anderen Komponenten des Rechensystems **610** dar.

[0080] In bestimmten Ausführungsformen können die Datenspeichereinrichtungen **632** und **633** so konfiguriert sein, dass sie von einer Wechselspeichereinheit, die konfiguriert ist, um Computersoftware, Daten oder andere computerlesbare Information zu speichern, lesen und/oder darauf schreiben kann. Beispiele für geeignete Wechselspeichereinheiten sind, ohne Beschränkung, eine Diskette, ein Magnetband, eine optische Platte, ein Flash-Datenspeichergerät oder dergleichen. Die Speichereinrichtungen **632** und **633** können auch andere ähnliche Strukturen oder Einrichtungen enthalten, die das Laden von Computersoftware, Daten oder anderen computerlesbaren Befehlen in das Rechensystem **610** ermöglichen. Zum Beispiel können die Speichereinrichtungen **632** und **633** so konfiguriert sein, dass sie Software, Daten oder andere computerlesbare Informationen lesen und schreiben können. Die Speichereinrichtungen **632** und **633** können auch ein Teil des Rechensystems **610** sein oder können ein separates Gerät sein, auf das über andere Schnittstellensysteme zugegriffen wird.

[0081] Viele andere Geräte oder Subsysteme können an das Rechensystem **610** angeschlossen sein. Umgekehrt müssen nicht alle in **Fig. 6** abgebildeten Komponenten und Geräte vorhanden sein, um die hierin beschriebenen und/oder abgebildeten Ausführungsformen zu praktizieren. Die oben genannten Geräte und Untersysteme können auch auf andere Weise miteinander verbunden sein als das in **Fig. 6** dargestellt ist. Das Rechensystem **610** kann auch eine beliebige Anzahl von Software-, Firmware- und/oder Hardware-Konfigurationen verwenden. Zum Beispiel können eine oder mehrere der hierin offenbarten beispielhaften Ausführungsformen als Computerprogramm (auch als Computersoftware, Softwareanwendungen, computerlesbare Befehle oder Computersteuerlogik bezeichnet) auf einem computerlesbaren Medium kodiert sein. Der Begriff „computerlesbares Medium“, so wie er hierin verwendet wird, bezieht sich allgemein auf jede Form von Gerät, Träger oder Medium, das in der Lage ist, computerlesbare Befehle zu speichern oder zu tragen. Beispiele für computerlesbare Medien sind, ohne Beschränkung, übertragungsartige Medien, wie etwa Trägerwellen, und Medien der nichtflüchtigen Art, wie etwa Magnetspeichermedien (z.B. Festplatten, Bandlaufwerke und Disketten), optische Speichermedien (z.B. Compact Disks (CDs), Digital Video Disks (DVDs) und BLU-RAY-Disks), elektronische Speichermedien (z.B. Festkörperlaufwerke und Flash-Medien), und andere Verteilungssysteme.

[0082] Das computerlesbare Medium, welches das Computerprogramm enthält, kann in das Rechensystem **610** geladen werden. Das gesamte oder ein Teil des auf dem computerlesbaren Medium gespeicherten Computerprogramms kann dann im Systemspeicher **616** und/oder in verschiedenen Teilen der Speichereinrichtungen **632** und **633** gespeichert werden. Wenn ein in das Rechensystem **610** geladenes Computerprogramm durch den Prozessor **614** ausgeführt wird, kann es den Prozessor **614** dazu veranlassen, die Funktionen von einer oder mehreren der hierin beschriebenen und/oder veranschaulichten, beispielhaften Ausführungsformen auszuführen und/oder ein Mittel zur Ausführung dieser Funktionen zu sein. Zusätzlich oder alternativ können eine oder mehrere der hierin beschriebenen und/oder veranschaulichten beispielhaften Ausführungsformen in Firmware und/oder Hardware implementiert sein. Zum Beispiel kann das Rechensystem **610** als anwendungsspezifischer integrierter Schaltkreis (ASIC, application-specific integrated circuit) konfiguriert sein, der dazu eingerichtet ist, eine oder mehrere der hierin angegebenen beispielhaften Ausführungsformen zu implementieren.

[0083] Fig. 7 ist ein Blockschaubild einer beispielhaften Netzwerkarchitektur **700**, in der Client-Systeme **710**, **720** und **730** sowie Server **740** und **745** an ein Netzwerk **750** gekoppelt sein können. So wie das oben ausgeführt ist, können die gesamte oder ein Teil der Netzwerkarchitektur **700**, allein oder in Kombination mit anderen Elementen, einen oder mehrere der hierin offenbarten Schritte (wie z.B. einen oder mehrere der in **Fig. 3** dargestellten Schritte) durchführen und/oder ein Mittel zur deren Durchführung sein. Die gesamte oder ein Teil der Netzwerkarchitektur **700** kann auch zur Durchführung und/oder als Mittel zur Durchführung von anderen in dieser Offenbarung dargelegten Schritten und Merkmalen verwendet werden.

[0084] Die Client-Systeme **710**, **720** und **730** repräsentieren allgemein jede Art oder Form von Recheneinrichtung oder -system, wie etwa das beispielhafte Rechensystem **610** in **Fig. 6**. In ähnlicher Weise stellen die Server **740** und **745** allgemein Recheneinrichtungen oder -systeme dar, wie etwa Anwendungsserver oder Datenbankserver, die dazu eingerichtet sind, verschiedene Datenbankdienste bereitzustellen und/oder bestimmte Softwareanwendungen ablaufen zu lassen. Das Netzwerk **750** repräsentiert allgemein jedes Telekommunikations- oder Computernetzwerk, einschließlich zum Beispiel ein Intranet, ein WAN, ein LAN, ein PAN oder das Internet. In einem Beispiel können die Client-Systeme **710**, **720** und/oder **730** und/oder die Server **740** und/oder **745** das gesamte oder einen Teil des Systems **100** aus **Fig. 1** aufweisen.

[0085] So wie das in **Fig. 7** dargestellt ist, können eine oder mehrere Datenspeichergeräte **760(1)-(N)** direkt an den Server **740** angeschlossen sein. In ähnlicher Weise können das eine oder die mehreren Datenspeichergeräte **770(1)-(N)** direkt an den Server **745** angeschlossen sein. Die Datenspeichergeräte **760(1)-(N)** und die Datenspeichergeräte **770(1)-(N)** stellen allgemein jede Art oder Form von Datenspeichergerät oder Medium dar, das in der Lage ist, Daten und/oder andere computerlesbare Befehle zu speichern. In bestimmten Ausführungsformen können die Datenspeichergeräte **760(1)-(N)** und die Datenspeichergeräte **770(1)-(N)** NAS (network-attached storage) -Geräte darstellen, die so konfiguriert sind, dass sie mit den Servern **740** und **745** unter Verwendung verschiedener Protokolle, wie etwa Network File System (NFS), Server Message Block (SMB) oder Common Internet File System (CIFS), kommunizieren.

[0086] Die Server **740** und **745** können auch an eine Storage Area Network (SAN)-Struktur **780** angeschlossen werden. Die SAN-Struktur **780** repräsentiert allgemein jede Art oder Form von Computernetzwerk oder Architektur, die in der Lage ist, die Kommunikation zwischen einer Mehrzahl von Datenspeichergeräten zu ermöglichen. Die SAN-Struktur **780** kann die Kommunikation zwischen den Servern **740** und **745** und einer Mehrzahl von Datenspeichergeräten 790(1)-(N) und/oder einer intelligenten Datenspeicheranordnung **795** ermöglichen. Die SAN-Struktur **780** kann auch über das Netzwerk **750** und die Server **740** und **745** die Kommunikation zwischen den Client-Systemen **710**, **720** und **730** und den Datenspeichergeräten **790(1)-(N)** und/oder der intelligenten Datenspeicheranordnung **795** in der Weise ermöglichen, dass die Geräte **790(1)-(N)** und die Anordnung **795** den Client-Systemen **710**, **720** und **730** als lokal angeschlossene Geräte erscheinen. Wie bei den Datenspeichergeräten **760(1)-(N)** und den Datenspeichergeräten **770(1)-(N)** stellen die Datenspeichergeräte **790(1)-(N)** und die intelligente Datenspeicheranordnung **795** allgemein jede Art oder Form von Speichergerät oder Medium dar, das in der Lage ist, Daten und/oder andere computerlesbare Befehle zu speichern.

[0087] In bestimmten Ausführungsformen und unter Bezugnahme auf das beispielhafte Rechensystem **610** aus **Fig. 6** kann eine Kommunikationsschnittstelle, wie etwa die Kommunikationsschnittstelle **622** in **Fig. 6**, verwendet werden, um Konnektivität zwischen jedem Client-System **710**, **720** und **730** und dem Netzwerk **750** herzustellen. Die Client-Systeme **710**, **720** und **730** können beispielsweise mit einem Web-Browser oder einer anderen Client-Software auf Informationen auf dem Server **740** oder **745** zugreifen. Eine solche Software kann es den Client-Systemen **710**, **720** und **730** ermöglichen, auf Daten zuzugreifen, die auf dem Server **740**, dem Server **745**, den Datenspeichergeräten **760(1)-(N)**, den Datenspeichergeräten **770(1)-(N)**, den Datenspeichergeräten **790(1)-(N)** oder der intelligenten Datenspeicheranordnung **795** gehostet werden. Obwohl **Fig. 7** die Verwendung eines Netzwerks (wie z.B. das Internet) für den Datenaustausch darstellt, sind die hierin beschriebenen und/oder veranschaulichten Ausführungsformen nicht auf das Internet oder irgendeine bestimmte netzwerkbasierte Umgebung beschränkt.

[0088] In mindestens einer Ausführungsform können alle oder ein Teil von einer oder mehreren der hierin offenbarten beispielhaften Ausführungsformen als ein Computerprogramm kodiert sein und auf den Server **740**, den Server **745**, die Datenspeichergeräte **760(1)-(N)**, die Datenspeichergeräte **770(1)-(N)**, die Datenspeichergeräte **790(1)-(N)**, die intelligente Datenspeicheranordnung **795** oder eine beliebige Kombination davon geladen und darauf ausgeführt werden. Alle oder ein Teil von einer oder mehreren der hierin offenbarten beispielhaften Ausführungsformen können auch als Computerprogramm kodiert sein, auf dem Server **740** gespeichert sein, von dem Server **745** ausgeführt werden und über das Netzwerk **750** an die Clientsysteme **710**, **720** und **730** verteilt werden.

[0089] So wie das oben ausgeführt ist, können das Rechensystem **610** und/oder eine oder mehrere Komponenten der Netzwerkarchitektur **700** einen oder mehrere Schritte eines beispielhaften Verfahrens zur Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung, entweder allein oder in Kombination mit anderen Elementen, ausführen und/oder ein Mittel zur Ausführung derselben sein.

[0090] Während die vorstehende Offenbarung verschiedene Ausführungsformen unter Verwendung von spezifischen Blockschaubildern, Ablaufdiagrammen und Beispielen darlegt, können jede Blockschaubild-Komponente, jeder Ablaufdiagramm-Schritt, jede Operation und/oder jede Komponente,

die hierin beschrieben und/oder veranschaulicht sind, einzeln und/oder kollektiv unter Verwendung einer breiten Palette von Hardware-, Software- oder Firmware-Konfigurationen (oder einer beliebigen Kombination davon) implementiert werden. Darüber hinaus sollte jede Offenbarung von Komponenten, die in anderen Komponenten enthalten sind, in ihrer Natur als Beispiel betrachtet werden, weil viele andere Architekturen implementiert werden können, um die gleiche Funktionalität zu erzielen.

[0091] In einigen Beispielen können alle oder ein Teil des beispielhaften Systems **100** in **Fig. 1** Teile einer Cloud-Computing- oder netzwerkbasierten Umgebung darstellen. Cloud-Computing-Umgebungen können verschiedene Dienste und Anwendungen über das Internet bereitstellen. Diese Cloud-basierten Dienste (z.B. Software als ein Dienst (software as a service), Plattform als ein Dienst (platform as a service), Infrastruktur als ein Dienst (infrastructure as a service) usw.) können über einen Web-Browser oder eine andere Fernschnittstelle (remote interface) zugänglich sein. Verschiedene hierin beschriebene Funktionen können über eine Remote-Desktop-Umgebung oder jede andere Cloud-basierte Rechenumgebung bereitgestellt werden.

[0092] In verschiedenen Ausführungsformen können das gesamte oder ein Teil des beispielhaften Systems **100** in **Fig. 1** Mehrmandantenfähigkeit (multi-tenancy) innerhalb einer Cloud-basierten Rechenumgebung ermöglichen. Mit anderen Worten, die hierin beschriebenen Softwaremodule können ein Rechensystem (z.B. einen Server) so konfigurieren, dass die Mehrmandantenfähigkeit für eine oder mehrere der hierin beschriebenen Funktionen ermöglicht wird. Beispielsweise können eines oder mehrere der hierin beschriebenen Softwaremodule einen Server so programmieren, dass zwei oder mehr Clients (z.B. Kunden) eine Anwendung, die auf dem Server läuft, gemeinsam nutzen (oder teilen) können. Ein auf diese Weise programmierter Server kann eine Anwendung, ein Betriebssystem, ein Verarbeitungssystem und/oder ein Datenspeichersystem unter mehreren Kunden (z.B. Mietern) gemeinsam nutzen. Eines oder mehrere der hierin beschriebenen Module können auch Daten und/oder Konfigurationsinformationen einer mehrmandantenfähigen Anwendung für jeden Kunden so partitionieren, dass ein Kunde nicht auf Daten und/oder Konfigurationsinformationen eines anderen Kunden zugreifen kann.

[0093] Gemäß verschiedenen Ausführungsformen können das gesamte oder ein Teil des beispielhaften Systems **100** in **Fig. 1** in einer virtuellen Umgebung implementiert werden. Beispielsweise können die hierin beschriebenen Module und/oder Daten in einer virtuellen Maschine gespeichert und/oder ausgeführt werden. So wie er hierin verwendet wird, bezieht sich der Begriff „virtuelle Maschine“ allgemein auf jede Betriebssystemumgebung, die durch einen Manager für virtuelle Maschinen (virtual machine manager) (z.B. einen Hypervisor) von der Computerhardware abstrahiert wird. Zusätzlich oder alternativ dazu können sich die hierin beschriebenen Module und/oder Daten innerhalb einer Virtualisierungsschicht befinden und/oder ausgeführt werden. So wie er hierin verwendet wird, bezieht sich der Begriff „Virtualisierungsschicht“ allgemein auf jede Datenschicht (data layer) und/oder Anwendungsschicht (application layer), die eine Betriebssystemumgebung überlagert und/oder von dieser abstrahierint ist. Eine Virtualisierungsschicht kann von einer Software-Virtualisierungslösung (z.B. einem Dateisystemfilter) verwaltet werden, die die Virtualisierungsschicht so darstellt, als wäre sie Teil eines darunter liegenden Basisbetriebssystems. Beispielsweise kann eine Software-Virtualisierungslösung Aufrufe, die ursprünglich an Orte innerhalb eines Basis-Dateisystems und/oder Registratur (registry) gerichtet sind, an Orte innerhalb einer Virtualisierungsschicht umleiten.

[0094] In einigen Beispielen können das gesamte oder ein Teil des beispielhaften Systems **100** in **Fig. 1** Teile einer mobilen Rechenumgebung (oder Computerumgebung) darstellen. Die mobilen Rechenumgebungen können durch eine breite Palette von mobilen Recheneinrichtungen implementiert werden, einschließlich Mobiltelefone, Tablet-Computer, E-Book-Reader, persönliche digitale Assistenten, tragbare Recheneinrichtungen (z.B. Recheneinrichtungen mit einem am Kopf angebrachten Display, Smartwatches usw.) und dergleichen. In einigen Beispielen können die mobilen Rechenumgebungen eine oder mehrere eigene Merkmale aufweisen, einschließlich beispielsweise eine Abhängigkeit von Batterieleistung, Präsentation von jeweils nur einer Anwendung im Vordergrund zu einem bestimmten Zeitpunkt, Fernverwaltungsfunktionen, Touchscreen-Funktionen, Standort- und Bewegungsdaten (z.B. von globalen Positionierungssystemen, Gyroskopen, Beschleunigungsmessern usw.), eingeschränkte Plattformen, die Änderungen an Konfigurationen auf Systemebene einschränken und/oder die die Fähigkeit von Software von Drittanbietern dahingehend einschränken, das Verhalten von anderen Anwendungen zu inspizieren, Kontrollen, um die Installation von Anwendungen einzuschränken (z.B. nur von zugelassenen Anwendungsspeichern (application stores) stammend) usw. Verschiedene der hierin beschriebenen Funktionen können für eine mobile Rechenumgebung bereitgestellt werden und/oder können mit einer mobilen Rechenumgebung interagieren.

[0095] Darüber hinaus können das gesamte oder ein Teil des beispielhaften Systems **100** in **Fig. 1** Teile von Daten darstellen, mit ihnen interagieren, sie konsumieren, welche Daten von einem oder mehreren Systemen für das Informationsmanagement kon-

sumiert werden und/oder Daten erzeugen, die von einem oder mehreren Systemen für das Informationsmanagement konsumiert werden. So wie er hierin verwendet wird, kann sich der Begriff „Informationsmanagement“ auf den Schutz, die Organisation und/oder die Speicherung von Daten beziehen. Beispiele für Systeme für die Informationsverwaltung können, ohne Beschränkung, Datenspeichersysteme, Datensicherungssysteme, Archivierungssysteme, Replikationssysteme, Hochverfügbarkeitssysteme, Datensuchsysteme, Virtualisierungssysteme und dergleichen sein.

[0096] In einigen Ausführungsformen können alle oder ein Teil des beispielhaften Systems **100** in **Fig. 1** Teile darstellen von einem oder mehreren Systemen für Informationssicherheit, Daten erzeugen, die durch ein oder mehrere Systeme für Informationssicherheit geschützt werden, und/oder mit solchen Systemen kommunizieren. So wie er hierin verwendet wird, kann sich der Begriff „Informationssicherheit“ auf die Steuerung des Zugriffs auf geschützte Daten beziehen. Beispiele für Systeme für Informationssicherheit können, ohne Beschränkung, Systeme sein, die verwaltete Sicherheitsdienste bereitstellen, Systeme zur Verhinderung von Datenverlusten, Systeme zur Authentifizierung von Identitäten, Zugangskontrollsysteme, Verschlüsselungssysteme, Systeme zur Einhaltung von Richtlinien, Systeme zur Erkennung und Verhinderung von Eindringen (intrusions), elektronische Entdeckungssysteme und dergleichen.

[0097] Gemäß Beispielen können das gesamte oder ein Teil des beispielhaften Systems **100** in **Fig. 1** Teile darstellen von, kommunizieren mit und/oder Schutz erhalten von, einem oder mehreren Systemen für Endpunktsicherheit. So wie er hierin verwendet wird, kann sich der Begriff „Endpunktsicherheit“ auf den Schutz von Endpunktsystemen vor nichtautorisierter und/oder unrechtmäßiger Nutzung, Zugriff und/oder Steuerung beziehen. Beispiele für Systeme zum Schutz von Endpunkten können, ohne Beschränkung, Anti-Schadprogramm-Systeme, Nutzerauthentifizierungssysteme, Verschlüsselungssysteme, Datenschutzsysteme, Spam-Filterdienste und dergleichen sein.

[0098] Die hierin beschriebenen und/oder veranschaulichten Prozessparameter und Abfolgen von Schritten sind nur als Beispiel angegeben und können beliebig variiert werden. Während beispielsweise die hierin dargestellten und/oder beschriebenen Schritte in einer bestimmten Reihenfolge gezeigt oder besprochen sein können, müssen diese Schritte nicht unbedingt in der dargestellten oder besprochenen Reihenfolge durchgeführt werden. Die verschiedenen beispielhaften Verfahren, die hierin beschrieben und/oder veranschaulicht sind, können auch einen oder mehrere der hierin beschriebenen oder veranschaulichten Schritte weglassen oder zusätzliche Schritte zusätzlich zu den offenbarten enthalten.

[0099] Obwohl hierin verschiedene Ausführungsformen im Zusammenhang mit voll funktionsfähigen Rechensystemen beschrieben und/oder veranschaulicht wurden, können eine oder mehrere dieser beispielhafte Ausführungsformen als ein Programmprodukt in verschiedenen Formen verbreitet werden, unabhängig von der Art des computerlesbaren Mediums, das zur tatsächlichen Durchführung der Verbreitung verwendet wird. Die hierin offenbarten Ausführungsformen können auch unter Verwendung von Softwaremodulen implementiert werden, die bestimmte Aufgaben erfüllen. Diese Softwaremodule können Skript-, Stapel- oder andere ausführbare Dateien enthalten, die auf einem computerlesbaren Datenspeichermedium oder in einem Rechensystem gespeichert werden können. In einigen Ausführungsformen können diese Softwaremodule ein Rechensystem dazu konfigurieren, eine oder mehrere der hierin offenbarten beispielhaften Ausführungsformen auszuführen.

[0100] Darüber hinaus können eines oder mehrere der hierin beschriebenen Module Daten, physikalische Geräte und/oder Darstellungen von physikalischen Geräten von einer Form in eine andere umwandeln. Beispielsweise können eines oder mehrere der hierin beschriebenen Module Netzwerkverkehrsdaten, die umgewandelt werden sollen, empfangen, die Netzwerkverkehrsdaten umwandeln, ein Ergebnis der Umwandlung zum Identifizieren von potentiellen Schadprogrammen ausgeben, das Ergebnis der Umwandlung verwenden, um eine Sicherheitsmaßnahme durchzuführen, und das Ergebnis der Umwandlung speichern, um eine Datenbank von Schadprogrammen zu aktualisieren. Zusätzlich, oder alternativ, können eines oder mehrere der hierinin beschriebenen Module einen Prozessor, einen flüchtigen Datenspeicher, einen nichtflüchtigen Datenspeicher und/oder jeden anderen Teil einer physikalischen Recheneinrichtung von einer Form in eine andere umwandeln, indem sie auf der Recheneinrichtung ausgeführt werden, Daten auf der Recheneinrichtung speichern und/oder anderweitig mit der Recheneinrichtung interagieren.

[0101] Die vorstehende Beschreibung wurde bereitgestellt, um es anderen Fachleuten auf diesem Gebiet zu ermöglichen, verschiedene Aspekte der hierin offenbarten beispielhaften Ausführungsformen bestmöglich zu nutzen. Diese beispielhafte Beschreibung ist weder dazu gedacht, erschöpfend zu sein, noch auf irgendeine bestimmte, offenbarte Form beschränkt zu sein. Viele Modifikationen und Variationen sind möglich, ohne von dem Geist und dem Umfang der vorliegenden Offenbarung abzuweichen. Die hierin offenbarten Ausführungsformen sollten in jeder Hinsicht als veranschaulichend und nicht als be-

schränkend betrachtet werden. Bei der Bestimmung des Umfangs der vorliegenden Offenbarung sollte auf die beigefügten Ansprüche und ihre Äquivalente verwiesen werden.

[0102] Sofern nicht anders angegeben, sind die Begriffe „verbunden mit“ und „gekoppelt mit“ (und deren Ableitungen), so wie sie in der Beschreibung und den Ansprüchen verwendet werden, so auszulegen, dass sie sowohl eine direkte als auch eine indirekte (d.h. über andere Elemente oder Komponenten) Verbindung ermöglichen. Darüber hinaus sind die Begriffe „ein“ oder „eine“, so wie sie in der Beschreibung und in den Ansprüchen verwendet werden, so auszulegen, dass sie „mindestens eines von“ bedeuten. Schließlich sind aus Gründen der Nutzerfreundlichkeit die Begriffe „einschließlich“ und „umfassend“ (und ihre Ableitungen), wie sie in der Beschreibung und den Ansprüchen verwendet werden, austauschbar mit dem Wort „aufweisend“ und haben dieselbe Bedeutung wie dieses.

Patentansprüche

1. Ein computerimplementiertes Verfahren zur Analyse eines Netzwerk-Verhaltens über eine nachgeahmte Netzwerkumgebung, wobei zumindest ein Teil des Verfahrens von einer Recheneinrichtung, die mindestens einen Prozessor aufweist, durchgeführt wird, wobei das Verfahren aufweist:
Detektieren, an einem Endpunkt in einem Netzwerk, von einer verdächtigen Aktivität in dem Netzwerk durch einen nicht identifizierten Prozess;
Leiten einer Netzwerkaktivität des nicht identifizierten Prozesses zu einem falschen Netzwerk, das von dem Netzwerk getrennt ist;
Initialisieren von einer oder mehreren virtuellen Maschinen auf dem falschen Netzwerk, um das Netzwerk nachzuahmen, so dass dem nicht identifizierten Prozess nicht bewußt ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird;
Analysieren eines Verhaltens des nicht identifizierten Prozesses in dem falschen Netzwerk; und
Durchführen einer Sicherheitsmaßnahme auf der Grundlage der Analyse.

2. Das computerimplementierte Verfahren gemäß Anspruch 1, wobei die Sicherheitsmaßnahme mindestens eines der Folgenden aufweist:
Netzwerkisolierung des Endpunkts, unter Quarantäne Stellen des nicht identifizierten Prozesses, Senden einer Benachrichtigung, Bereitstellen der Analyse an einen Administrator oder Veröffentlichen der Analyse.

3. Das computerimplementierte Verfahren gemäß Anspruch 1 oder 2, wobei das Analysieren des Verhaltens ein Sammeln von forensischen Artefakten, die indikativ sind für ein dem nicht identifizierten Prozess zugeordnetes Verhalten, aufweist.

4. Das computer-implementierte Verfahren gemäß Anspruch 3, wobei die forensischen Artefakte von zumindest einem von dem Endpunkt oder einem anderen Endpunkt des Netzwerks gesammelt werden.

5. Das computerimplementierte Verfahren gemäß Anspruch 3 oder 4, wobei die forensischen Artefakte Speicherartefakte aufweisen.

6. Das computer-implementierte Verfahren gemäß einem der Ansprüche 1 bis 5, wobei das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Einrichten einer geteilten Tunnelroute zwischen dem nicht identifizierten Prozess und dem falschen Netzwerk aufweist.

7. Das computer-implementierte Verfahren gemäß einem der Ansprüche 1 bis 6, wobei das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Erstellen einer falschen Leittabelle für den nicht identifizierten Prozeß, um Verkehr zu dem falschen Netzwerk zu leiten, aufweist.

8. Das computer-implementierte Verfahren gemäß einem der Ansprüche 1 bis 7, wobei das Analysieren des Verhaltens ein Überwachen des Verhaltens, ohne den nicht identifizierten Prozess zu behindern, aufweist.

9. Das computer-implementierte Verfahren gemäß einem der Ansprüche 1 bis 8, wobei das Netzwerk eine Mehrzahl von Endpunkten aufweist und das falsche Netzwerk eine virtuelle Maschine für jeden von der Mehrzahl der Endpunkte aufweist.

10. Ein System zur Analyse eines Netzwerkverhaltens über eine nachgeahmte Netzwerkumgebung, wobei das System Folgendes aufweist:
mindestens einen physikalischen Prozessor;
einen physikalischen Speicher, der computerausführbare Befehle aufweist, die, wenn sie von dem physikalischen Prozessor ausgeführt werden, den physikalischen Prozessor dazu veranlassen:
an einem Endpunkt in einem Netzwerk eine verdächtige Aktivität in dem Netzwerk durch einen nicht identifizierten Prozess zu detektieren;
eine Netzwerkaktivität des nicht identifizierten Prozesses an ein falsches Netzwerk, das von dem Netzwerk getrennt ist, zu leiten;
eine oder mehrere virtuelle Maschinen in dem falschen Netzwerk zu initialisieren, um das Netzwerk nachzuahmen, sodass dem nicht identifizierten Prozess nicht bewußt ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird;
ein Verhalten des nicht identifizierten Prozesses in dem falschen Netzwerk zu analysieren; und
auf der Grundlage der Analyse eine Sicherheitsmaßnahme durchzuführen.

11. Das System gemäß Anspruch 10, wobei die Sicherheitsmaßnahme mindestens eines der Folgenden aufweist: eine Netzwerkisolierung des Endpunkts, unter Quarantäne Stellen des nicht identifizierten Prozesses, Senden einer Benachrichtigung, Bereitstellen der Analyse an einen Administrator oder Veröffentlichen der Analyse.

12. Das System gemäß Anspruch 10 oder 11, wobei das Analysieren des Verhaltens ein Sammeln von forensischen Artefakte, die indikativ sind für ein dem nicht identifizierten Prozess zugeordnetes Verhalten hinweisen, aufweist.

13. Das System gemäß Anspruch 12, bei dem die forensischen Artefakte von mindestens einem der Endpunkte oder einem anderen Endpunkt des Netzwerks gesammelt werden.

14. Das System gemäß Anspruch 12 oder 13, wobei die forensischen Artefakte Speicherartefakte aufweisen.

15. Das System gemäß einem der Ansprüche 10 bis 14, wobei das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Einrichten einer geteilten Tunnelroute zwischen dem nicht identifizierten Prozess und dem falschen Netzwerk aufweist.

16. Das System gemäß einem der Ansprüche 10 bis 15, wobei das Leiten der Netzwerkaktivität des nicht identifizierten Prozesses ein Erstellen einer falschen Leittabelle für den nicht identifizierten Prozeß, um Verkehr zu dem falschen Netzwerk zu leiten, aufweist.

17. Das System gemäß einem der Ansprüche 10 bis 16, wobei das Analysieren des Verhaltens ein Überwachen des Verhaltens, ohne den nicht identifizierten Prozess zu behindern, aufweist.

18. Das System gemäß einem der Ansprüche 10 bis 17, wobei das Netzwerk eine Mehrzahl von Endpunkten aufweist und das falsche Netzwerk eine virtuelle Maschine für jeden von der Mehrzahl der Endpunkte aufweist.

19. Ein nicht-flüchtiges computerlesbares Medium, das einen oder mehrere computerausführbare Befehle aufweist, der oder die, wenn er oder sie von mindestens einem Prozessor einer Recheneinrichtung ausgeführt wird oder werden, die Recheneinrichtung dazu veranlassen:
an einem Endpunkt in einem Netzwerk eine verdächtige Aktivität in dem Netzwerk durch einen nicht identifizierten Prozess zu detektieren;
eine Netzwerkaktivität des nicht identifizierten Prozesses zu einem falschen Netzwerk, das von dem Netzwerk getrennt ist, zu leiten;
eine oder mehrere virtuelle Maschinen in dem falschen Netzwerk zu initialisieren, um das Netzwerk nachzuahmen, so dass dem nicht identifizierten Prozess nicht bewußt ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird;
ein Verhalten des nicht identifizierten Prozesses in dem falschen Netzwerk zu analysieren; und
auf der Grundlage der Analyse eine Sicherheitsmaßnahme durchzuführen.

20. Das nicht-flüchtige computerlesbare Medium gemäß Anspruch 19, wobei die Sicherheitsmaßnahme mindestens eines der Folgenden aufweist:
eine Netzwerkisolierung des Endpunkts, unter Quarantäne Stellen des nicht identifizierten Prozesses, Senden einer Benachrichtigung, Bereitstellen der Analyse an einen Administrator oder Veröffentlichen der Analyse.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

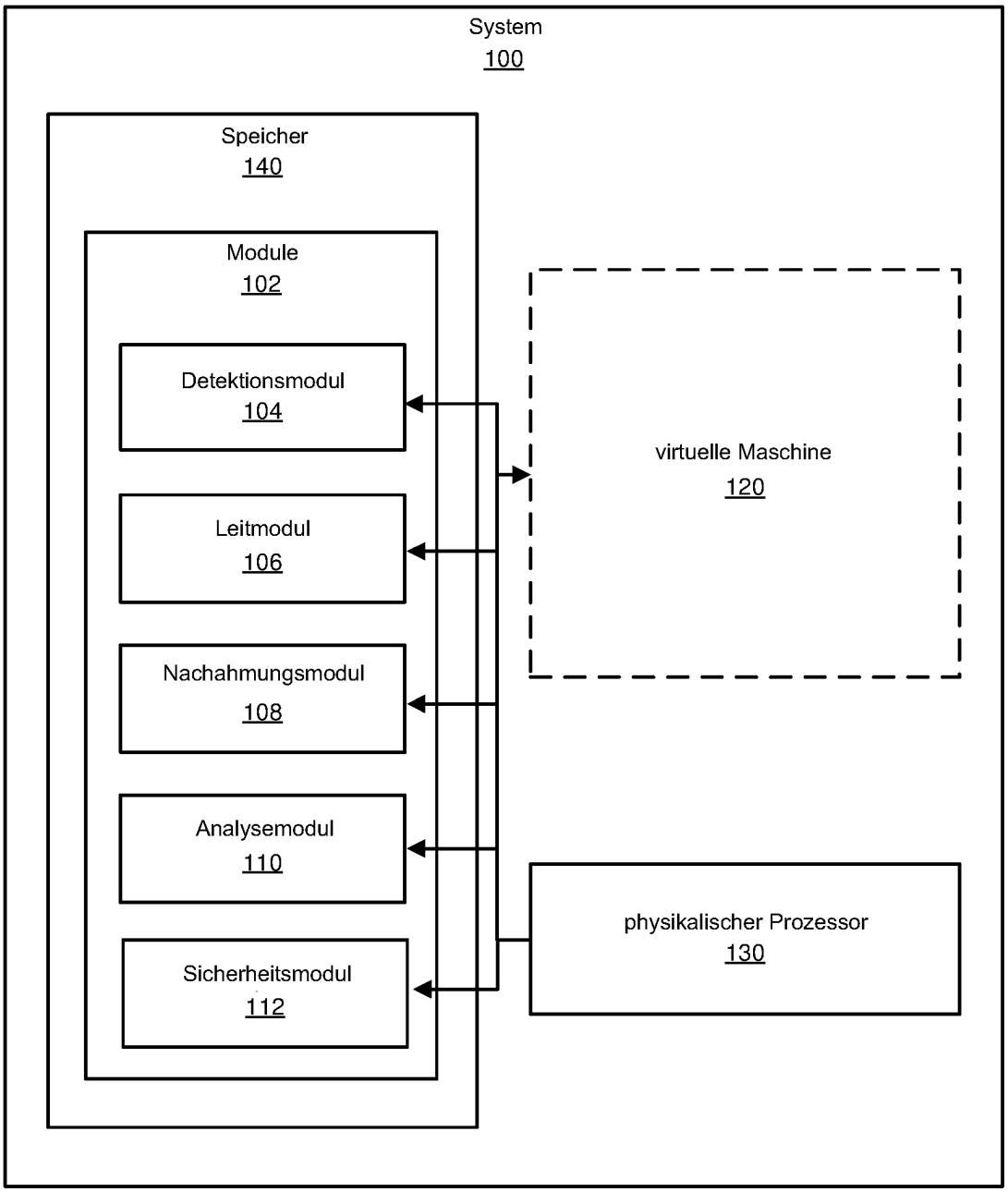


FIG. 1

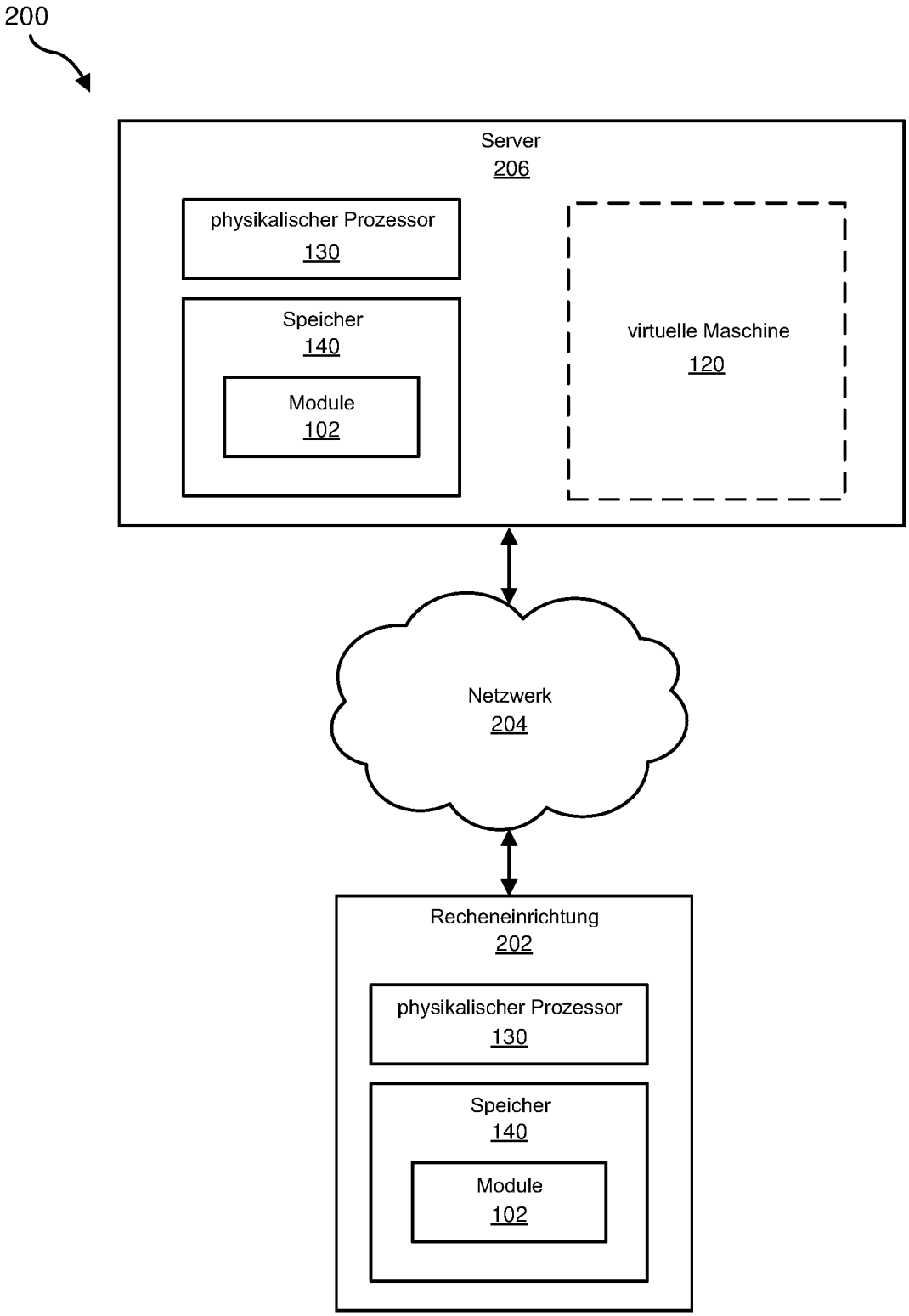

200
Server
206
physikalischer Prozessor
130
Speicher
140
Module
102
virtuelle Maschine
120
Netzwerk
204
Recheneinrichtung
202
physikalischer Prozessor
130
Speicher
140
Module
102

FIG. 2

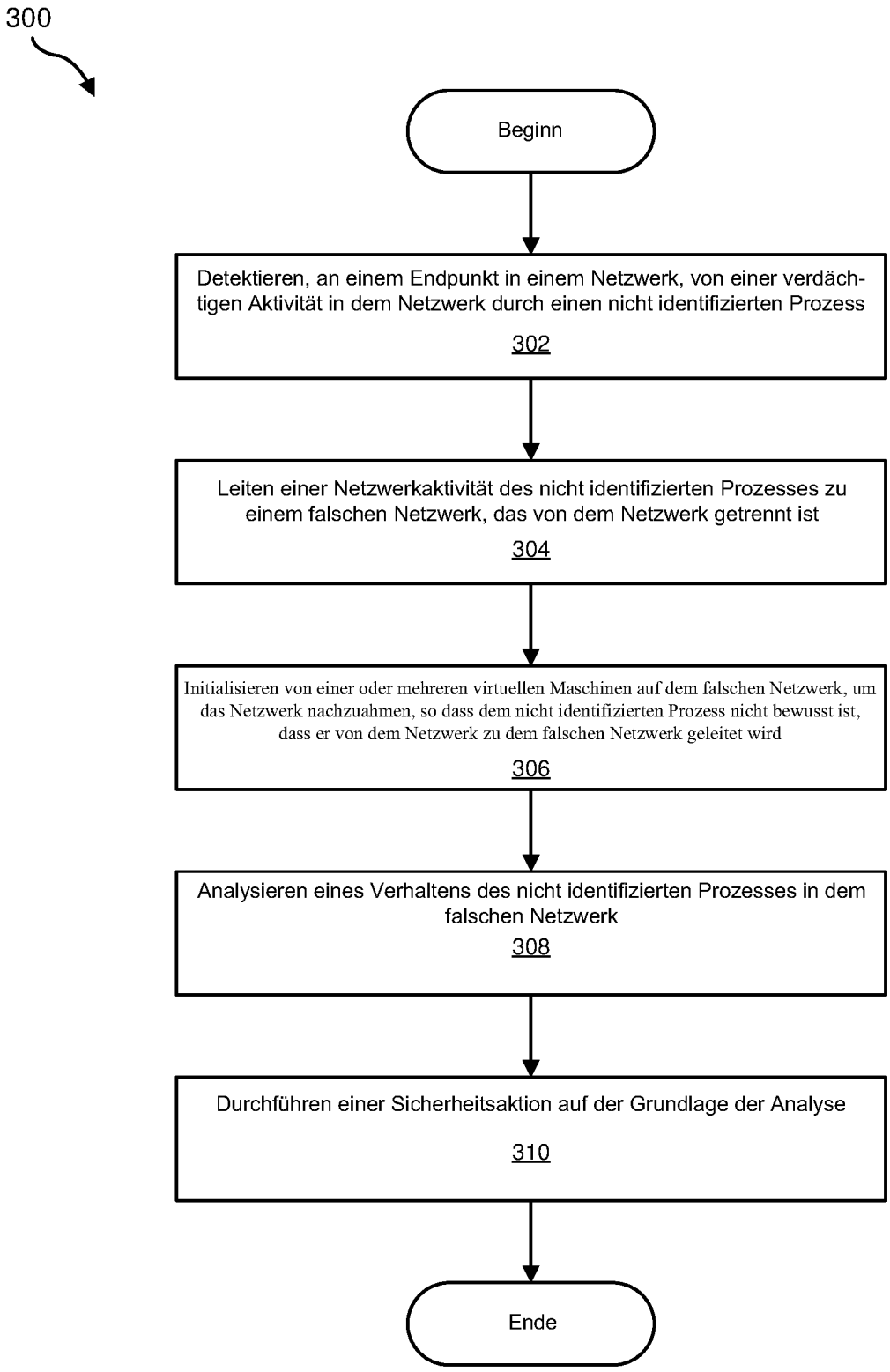

300
Beginn
Detektieren, an einem Endpunkt in einem Netzwerk, von einer verdächtigen Aktivität in dem Netzwerk durch einen nicht identifizierten Prozess
302
Leiten einer Netzwerkaktivität des nicht identifizierten Prozesses zu einem falschen Netzwerk, das von dem Netzwerk getrennt ist
304
Initialisieren von einer oder mehreren virtuellen Maschinen auf dem falschen Netzwerk, um das Netzwerk nachzuahmen, so dass dem nicht identifizierten Prozess nicht bewusst ist, dass er von dem Netzwerk zu dem falschen Netzwerk geleitet wird
306
Analysieren eines Verhaltens des nicht identifizierten Prozesses in dem falschen Netzwerk
308
Durchführen einer Sicherheitsaktion auf der Grundlage der Analyse
310
Ende

FIG. 3

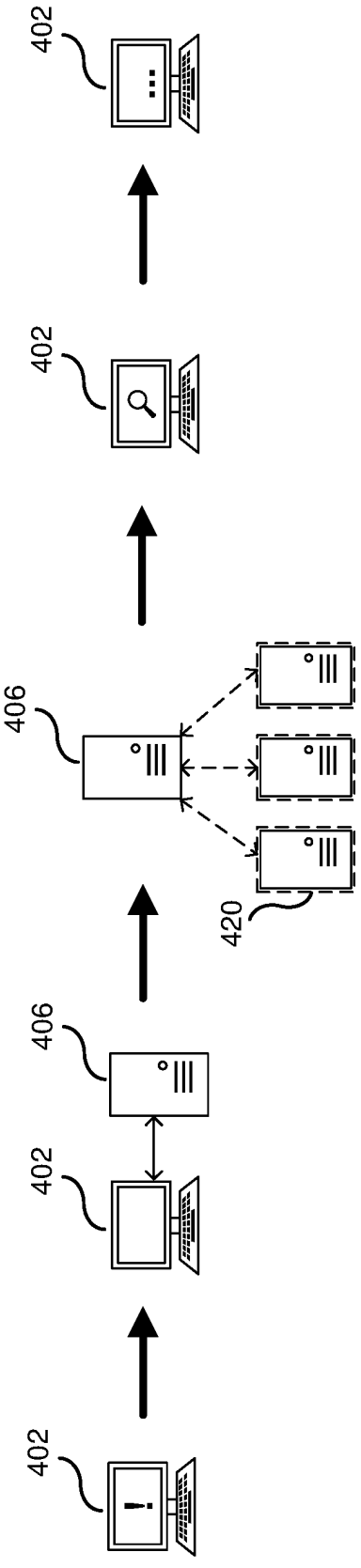


FIG. 4A FIG. 4B FIG. 4C FIG. 4D FIG. 4E

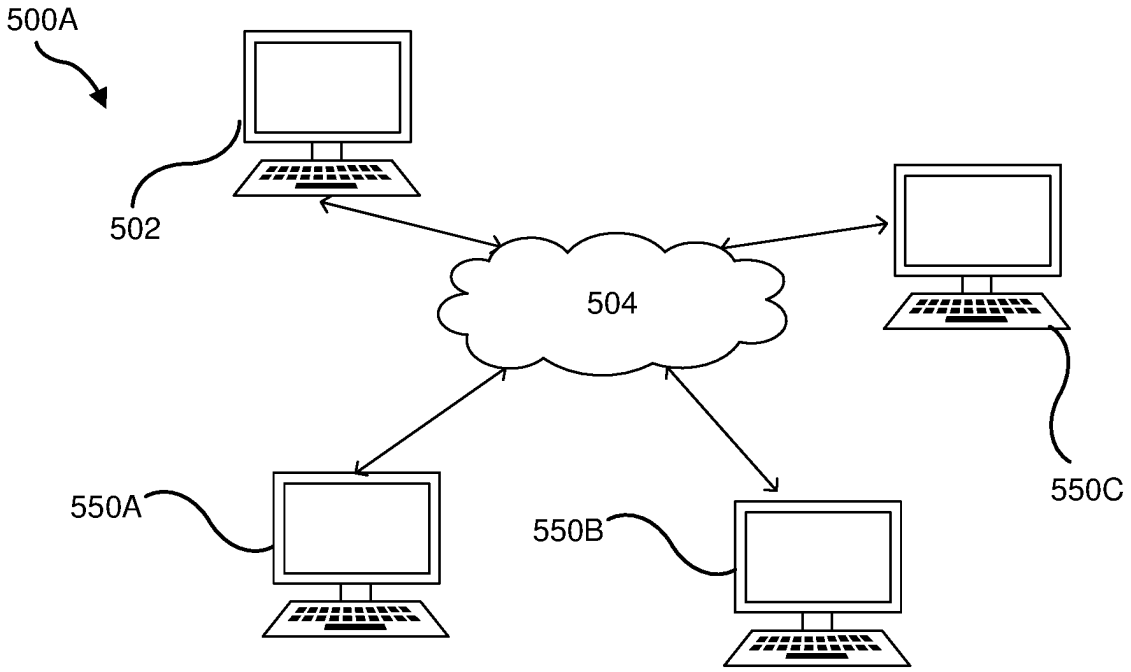


FIG. 5A

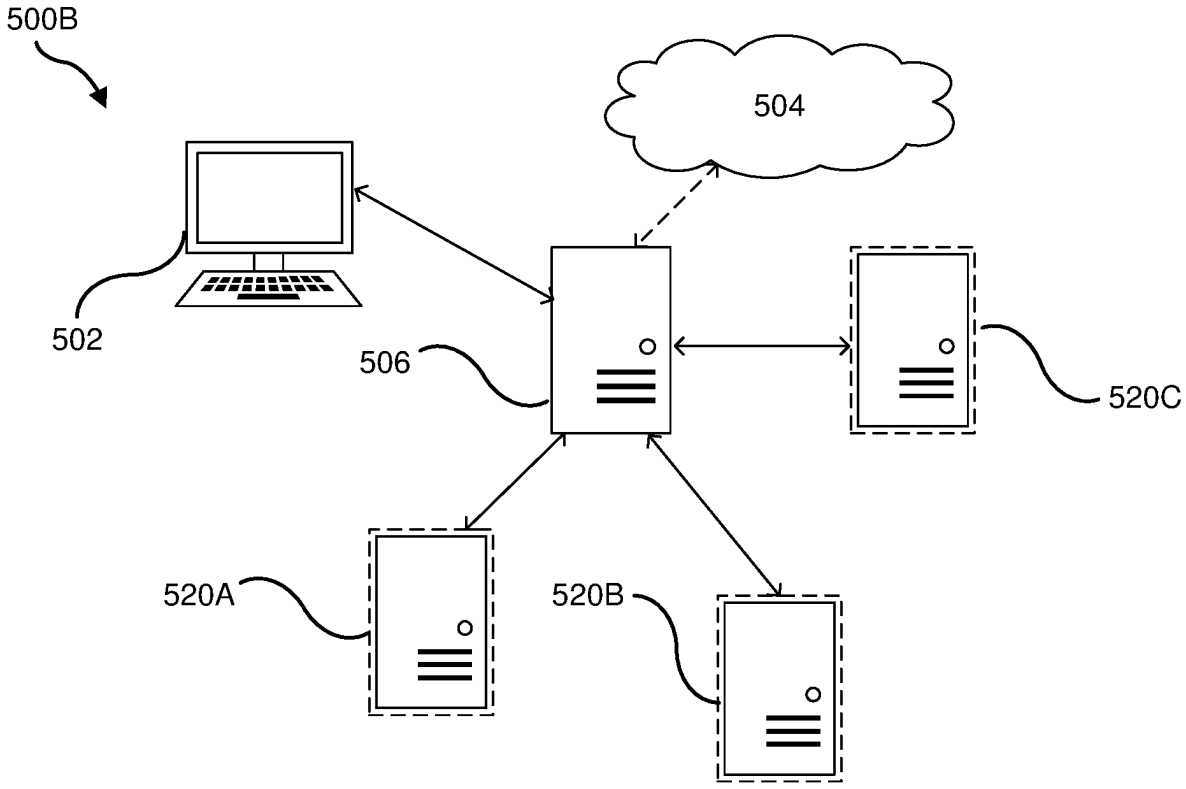


FIG. 5B

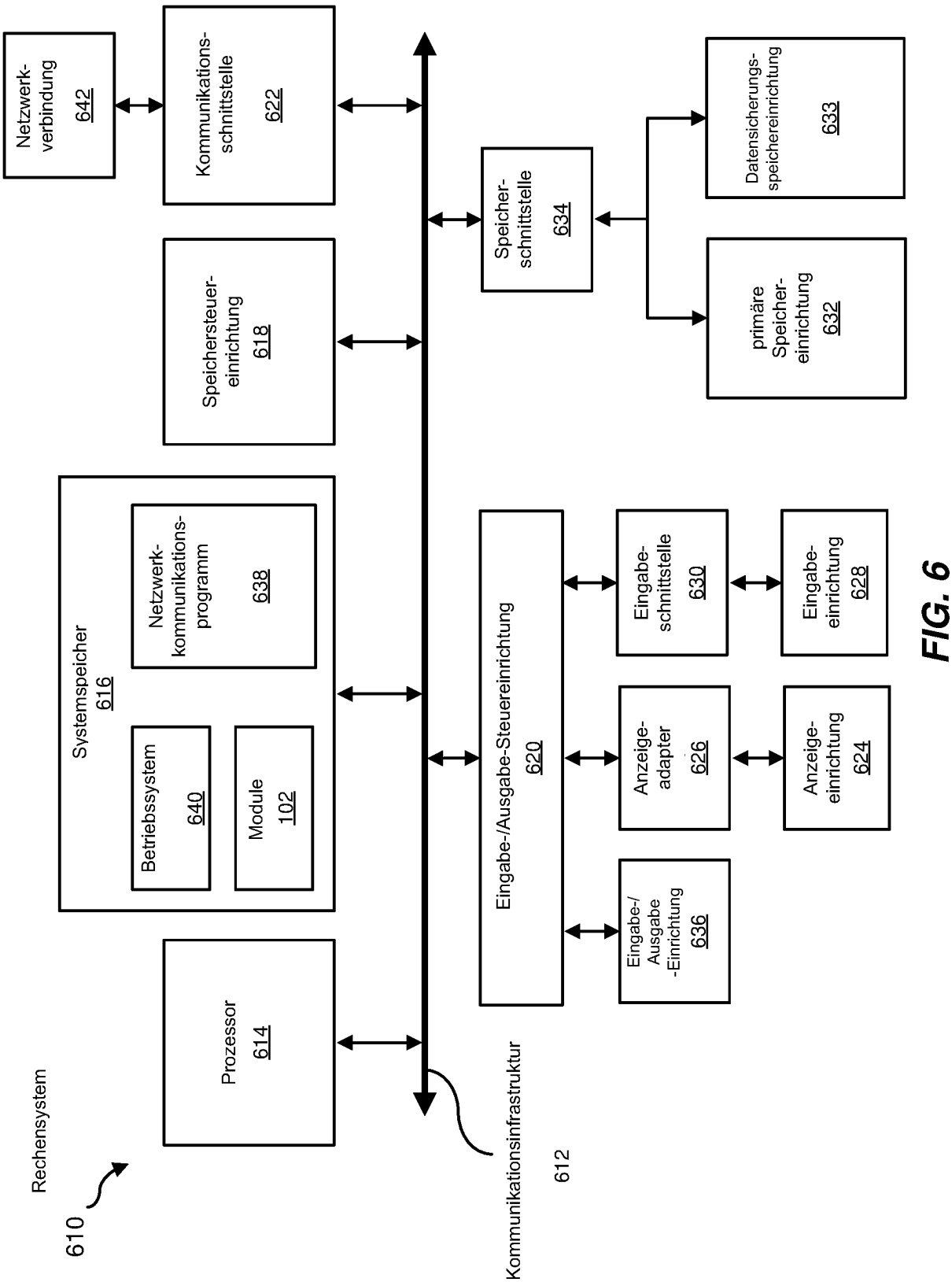

Rechensystem
610
Prozessor
614
Systemspeicher
616
Betriebssystem
640
Module
102
Netzwerk-
kommunikations-
programm
638
Speichersteuer-
einrichtung
618
Kommunikations-
schnittstelle
622
Netzwerk-
verbindung
642
Kommunikationsinfrastruktur
612
Eingabe-/Ausgabe-Steuereinrichtung
620
Eingabe-/
Ausgabe
-Einrichtung
636
Anzeige-
adapter
626
Eingabe-
schnittstelle
630
Anzeige-
einrichtung
624
Eingabe-
einrichtung
628
Speicher-
schnittstelle
634
primäre
Speicher-
einrichtung
632
Datensicherungs-
speichereinrichtung
633

FIG. 6

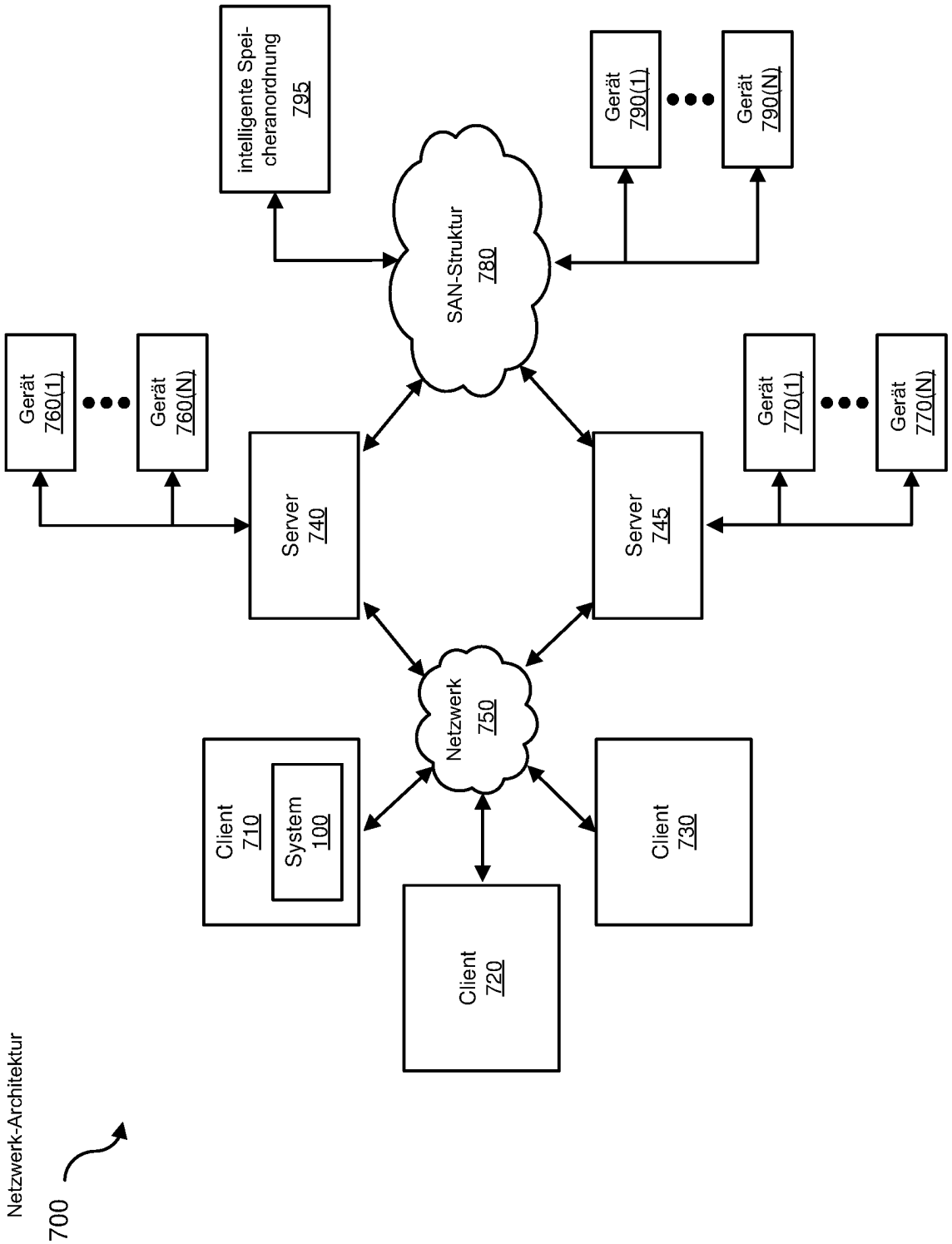


FIG. 7