(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
21. Januar 2016 (21.01.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/008778 A1

(51) Internationale Patentklassifikation:
H04L 12/24 (2006.01) *H04L 29/06* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2015/065547

(22) Internationales Anmeldedatum:
8. Juli 2015 (08.07.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
14177647.6 18. Juli 2014 (18.07.2014) EP

(71) Anmelder: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Erfinder: **KLOTH, Mathias**; Milchborntalweg 38, 51429 Bergisch Gladbach (DE). **WESTPHALEN, Michael**; Kornradenweg 65, 50999 Köln (DE).

(74) Anwalt: **KLINSKI, Robert**; Elsenheimerstraße 65, 80687 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR DETECTING AN ATTACK IN A COMMUNICATION NETWORK

(54) Bezeichnung : VERFAHREN ZUM ERKENNEN EINES ANGRIFFS IN EINEM COMPUTERNETZWERK

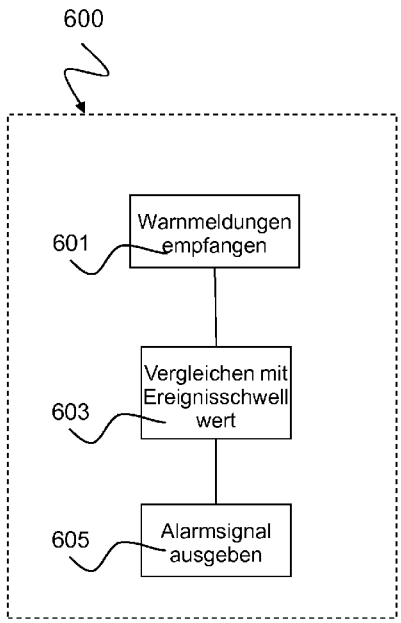

Fig. 6

601 Receive warning messages
603 Compare with event threshold value
605 Output alarm signal

(57) Abstract: The invention relates to a method (600) for detecting an attack in a computer network (410, 510) having a plurality of computers, comprising the following steps: receiving (601) a plurality of warning messages (102) from the computers, wherein the warning messages are based on different types (111, 112, 113, 114) of anomalies of the computer network; comparing (603) a quantity of the warning messages from the plurality of received warning messages (102) with a specified event threshold value, wherein the quantity of the warning messages is based on a same type (114) of an anomaly of the computer network; and outputting (605) an alarm signal (108) if the quantity of the warning messages that are based on the same type (114) of an anomaly of the computer network falls below the event threshold value.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren (600) zum Erkennen eines Angriffs in einem Computernetzwerk (410, 510) mit einer Mehrzahl von Computern, mit folgenden Schritten: Empfangen (601) einer Mehrzahl von Warnmeldungen (102) von den Computern, wobei die Warnmeldungen auf verschiedenen Typen (111, 112, 113, 114) von Anomalien des Computernetzwerks basieren; Vergleichen (603) einer Anzahlder Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen (102) mit einem vorgegebenen Ereignisschwellwert, wobei die Anzahlder Warnmeldungen auf einem selben Typ (114) einer Anomalie des Computernetzwerks basieren; und Ausgeben (605) eines Alarmsignals (108), falls die Anzahl der Warnmeldungen, die auf demselben Typ (114) einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

WO 2016/008778 A1

CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

Verfahren zum Erkennen eines Angriffs in einem Computernetzwerk

Die vorliegende Erfindung betrifft ein Verfahren und ein Analysesystem zum Erkennen eines Angriffs in einem Computernetzwerk.

Der Diebstahl von Unternehmensgeheimnissen geschieht oft unbemerkt durch Einschleusung von Schadprogrammen in das unternehmenseigene Computernetzwerk. Dabei kommen bei derartigen Angriffen teilweise selbstentwickelte und individuell für den konkreten Einsatz angepasste Schadprogramme zum Einsatz, die von den am Markt erhältlichen Äntivirenprodukten nicht oder erst sehr spät erkannt werden. Als potentielles Opfer eines digitalen Spionageangriffs können Unternehmen sich zwar vorbereiten, jedoch sind die genauen Umstände wie z.B. Ort, Zeitpunkt und Ausgestaltung meist unbekannt. Zur Erkennung und Abwehr derartiger Angriffe kann ein angegriffenes Unternehmen unter Umständen vor der Herausforderung stehen, eine große Menge heterogener Protokolldaten von unterschiedlichen Sicherheits- und Betriebssystemen zu einem sinnvollen und erkenntnisbringenden Zusammenhang zu verknüpfen.

Es ist die Aufgabe der vorliegenden Erfindung, einen Angriff in einem Computernetzwerk zu erkennen.

Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Vorteilhafte Weiterbildungsformen sind Gegenstand der abhängigen Ansprüche.

Die im Folgenden vorgestellten Verfahren und Systeme können auf der Aufzeichnung von Daten eines SIEM (Security Information and Event Management bzw. Sicherheitsinformations- und Ereignisverwaltung) Systems basieren. Ein SIEM System ist ein Begriff für Dienste von Software und Produkten, die Sicherheitsinformationsverwaltung („security information management“, SIM) mit Sicherheitsereignisverwaltung („security event management“, SEM) kombinieren. Die SIEM Technologie stellt eine Echtzeitanalyse von Sicherheitsalarmen zur Verfügung, die von Netzwerk-Hardware und Netzwerkanwendungen generiert werden können. SIEM kann in Form von Software, Anwendungen oder verwalteten Diensten vertrieben werden und auch dazu verwendet

werden, um sicherheitsrelevante Daten aufzuzeichnen und Reporte für Compliance Anwendungen zu erzeugen.

Die im Folgenden vorgestellten Verfahren und Systeme können einen Indikator oder ein Alarmsignal für einen Angriff auf ein Computersystem mit einem C2 (Command&Control)-Server liefern. Command&Control Server sind zentralisierte Maschinen bzw. Computerserver, die in der Lage sind Befehle zu senden und Antworten von Maschinen bzw. Computern zu erhalten, die Teil eines Botnetzes sind. Angreifer, die einen DDoS (distributed denial of service) Angriff starten wollen, können jederzeit spezielle Befehle mit Instruktionen, einen bestimmten Zielrechner anzugreifen, an den C2 Server ihres Botnetzes senden, und jede infizierte Maschine, die mit dem kontaktierten C2 Server kommuniziert, wird dementsprechend einen koordinierten Angriff gegen den Zielrechner starten.

Die im Folgenden vorgestellten Verfahren und Systeme können eingesetzt werden, um ein Computernetzwerk vor Angriffen aus Botnetzen zu schützen, insbesondere vor DDoS-Angriffen, Spamming-Angriffen, Sniffing-Angriffen, Phishing-Angriffen, Verbreiten von Malware, Key-Logging, Installieren unerwünschter Software, Identitätsdiebstahl, Manipulation des Computernetzwerks.

Die im Folgenden vorgestellten Verfahren und Systeme können im Bereich der Informationstechnologie (IT) eingesetzt werden. Informationstechnologie ist ein Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software. Die Informationstechnologie eines Unternehmens umfasst sämtliche technischen Einrichtungen zur Erzeugung, Verarbeitung und Weiterleitung von Informationen.

Um die Erfindung im Detail zu beschreiben, werden die folgenden Abkürzungen und Bezeichnungen verwendet:

IT:	Informationstechnologie.
SIEM:	Security Information and Event Management bzw. Sicherheitsinformations- und Ereignisverwaltung
SIM:	Security Information Management, Sicherheitsinformationsverwaltung

SEM: Security Event Management, Sicherheitsereignisverwaltung
C2 Server: Command&Control Server bzw. Befehls- und Kontroll-Server

Gemäß einem Aspekt betrifft die Erfindung ein Verfahren zum Erkennen eines Angriffs in einem Computernetzwerk mit einer Mehrzahl von Computern, mit folgenden Schritten: Empfangen einer Mehrzahl von Warnmeldungen von den Computern, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks basieren; Vergleichen einer Anzahl der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert, wobei die Anzahl der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren; und Ausgeben eines Alarmsignals, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

Der Vorteil eines solchen Verfahrens liegt darin, dass das Verfahren schnell und zuverlässig ein Alarmsignal bei einem bevorstehenden Angriff auf das Computernetzwerk auslösen kann. Die Computer des Computernetzwerks erzeugen stets eine Vielzahl von Warnmeldungen, beispielsweise bei nicht funktionierendem Software-Update, wenn der Prozessor überlastet ist, wenn ein Update der Software bisher nicht durchgeführt wurde, wenn ein Passwort falsch eingegeben wurde, wenn der Zugriff auf das Internet vorübergehend nicht möglich ist, wenn der Zugriff auf bestimmte Daten nicht möglich ist, etc. Diese Warnmeldungen sind bedingt durch bestimmte Anomalien des Computernetzwerks, die während des Betriebs häufiger oder weniger häufig vorkommen und zumeist eine Interaktion des Benutzers erfordern, um sie zu beheben. Dabei treten unkritische bzw. leichte Anomalien des Computersystems, wie beispielsweise nicht durchgeführter Software-Update oder Überlastung des Prozessors sehr häufig auf und sind leicht zu beheben. Kritische Anomalien, wie beispielsweise unerwarteter Ausfall bestimmter Komponenten des Systems oder Unzugänglichkeit selten genutzter Systemressourcen, treten dagegen nur sehr selten auf und so auch diesbezügliche Warnmeldungen.

Die Grundidee, auf der das Verfahren basiert, ist nun die Erkennung eines möglichen oder bevorstehenden Angriffs auf das Computernetzwerk bzw. Computersystem basierend auf solch kritischen Anomalien des Netzwerks. Hierzu können lediglich die

Anzahl auftretender Warnmeldungen den möglichen Anomalien des Computernetzwerks zugeordnet und gezählt werden. Falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, einen Ereignisschwellwert unterschreitet, so kann durch die Auslösung eines Alarms der Nutzer des Computernetzwerks gewarnt werden, dass ein möglicher Angriff bevorsteht oder bereits stattgefunden hat.

Die Ausgabe eines Alarmsignals bei einem möglichen Angriff auf das Computernetzwerk kann damit flexibel, schnell und genau ausgeführt werden. Durch den modularen Aufbau des Verfahrens können die einzelnen Verfahrensschritte flexibel auf unterschiedlichen Software- oder Hardwarekomponenten realisiert werden, beispielsweise auf Komponenten innerhalb des Computernetzwerks oder auf externen Komponenten außerhalb des Computernetzwerks.

Gemäß einer Ausführungsform umfasst das Verfahren ein Empfangen der Mehrzahl von Warnmeldungen in einem vorgegebenen Zeitintervall.

Dies hat den Vorteil, dass Warnmeldungen, die auf verschiedenen Typen einer Anomalie des Computernetzwerks basieren, über den gleichen Zeitraum gemessen werden, so dass der Ereignisschwellwert sich für die verschiedenen Typen von Warnmeldungen stets auf den gleichen Zeitraum bezieht. Damit kann zuverlässig auf selten vorkommende Anomalien geschlossen werden, die einen möglichen oder bereits stattgefundenen Angriff auf das Computernetzwerk signalisieren. Das Verfahren arbeitet somit sehr präzise und zuverlässig.

Gemäß einer Ausführungsform umfasst das Verfahren ein Klassifizieren der Mehrzahl von Warnmeldungen bezüglich des Typs der von einer jeweiligen Warnmeldung angezeigten Anomalie.

Dies hat den Vorteil, dass aus der Vielzahl von eintreffenden Warnmeldungen schnell die relevanten Warnmeldungen ausgefiltert werden können, die eine kritische Anomalie des Computernetzwerks signalisieren.

Gemäß einer Ausführungsform umfasst das Verfahren ein Bestimmen des Typs der von einer Warnmeldung angezeigten Anomalie basierend auf einem Inhalt der Warnmeldung.

Dies hat den Vorteil, dass der Typ der Anomalie leicht bestimmt werden kann, beispielsweise durch Abfragen eines bestimmten Datenfelds oder Flags innerhalb der Warnmeldung, die beispielsweise als ein Datenpaket mit Header und Payload ausgeführt sein kann. Wenn die Anomalie basierend auf einem Inhalt der Warnmeldung bestimmt werden kann, so sind keine sonstigen Informationen zu dessen Bestimmung nötig, was das Verfahren einfach und zuverlässig macht.

Gemäß einer Ausführungsform umfasst das Verfahren ein Zählen der empfangenen Warnmeldungen, die bezüglich desselben Typs klassifiziert sind, in dem vorgegebenen Zeitintervall, um die Anzahl zu bestimmen; und ein Ausgeben des Alarmsignals falls die Anzahl der in dem vorgegebenen Zeitintervall gezählten Warnmeldungen, die bezüglich desselben Typs klassifiziert sind, den Ereignisschwellwert unterschreitet.

Dies hat den Vorteil, dass das Verfahren sehr einfach ausführbar ist, beispielsweise durch einen Schalter, eine Mehrzahl von Zählern und einen Timer bzw. eine Uhr. Der Schalter kann die Warnmeldungen basierend auf einem Typ der von ihnen signalisierten Anomalie einem jeweiligen der Zähler zuführen, der die Anzahl der ihm zugeführten Warnmeldungen zählt. Nach Ablauf einer bestimmten Zeit, angezeigt durch den Timer, können die Zählerwerte ausgelesen werden. Sobald einer der ausgelesenen Zählerwerte den Ereignisschwellwert unterschritten, kann Alarm ausgelöst werden. Damit ist das Verfahren mit einfachen Logik-Schaltungen realisierbar, beispielsweise auf einem IC oder einem Chip.

Gemäß einer Ausführungsform umfasst das Verfahren ein Bestimmen eines Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk basierend auf der Anzahl der Warnmeldungen, die den Ereignisschwellwert unterschreiten.

Dies hat den Vorteil, dass über den Wahrscheinlichkeitswert eine Wertung des Alarms möglich ist. Der Alarm kann bereits bei einer geringen Wahrscheinlichkeit eines Angriffs ausgelöst werden, der Wahrscheinlichkeitswert signalisiert dann eine Schwere des

Angriffs. Beispielsweise kann ein geringer Wahrscheinlichkeitswert als ein grünes Alarmlicht angezeigt werden, ein mittelgroßer Wahrscheinlichkeitswert durch ein gelbes Alarmlicht und ein hoher Wahrscheinlichkeitswert durch ein rotes Alarmlicht. Der Nutzer erhält durch den Wahrscheinlichkeitswert mehr Informationen über die Art bzw. Schwere des möglichen oder bevorstehenden Angriffs.

Gemäß einer Ausführungsform umfasst das Verfahren ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf zumindest einem der folgenden vorbestimmten Parameter: Schwarze Listen, Weiße Listen, Schwellenwerte, Ereigniszusammenhänge, und Definition von Gefährdungspotenzialen einzelner Nutzergruppen des Computernetzwerks.

Die hat den Vorteil, dass selten auftretende Ereignisse bzw. Anomalien des Computernetzwerks, die aber mit einem Normalzustand des Systems verbunden sein können, besser abgegrenzt werden können von selten auftretenden Ereignissen, die mit einer Gefährdung des Computernetzwerks verbunden sind. Anhand dieser Parameter kann die Wissensbasis des Nutzers des Computernetzwerks mit in die Erkennung eingebracht werden. So können Situationen aus der Vergangenheit (z.B. Schwellenwerte, Ereigniszusammenhänge) sowie aktuell vorliegende Gefahren (z.B. Blacklists, Whitelists, Gefährdungspotenziale einzelner Personengruppen) besonders berücksichtigt werden.

Gemäß einer Ausführungsform umfasst das Verfahren ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Anzahl von Besuchern des Computernetzwerks, insbesondere auf einer Anzahl von Besuchern einer Webseite des Computernetzwerks.

Dies hat den Vorteil, dass ein Angriff anhand der Anzahl von Besuchern zuverlässig erkannt werden kann. Wird eine Webseite von vielen unterschiedlichen Nutzern besucht, so kann dies den Normalzustand beschreiben. Bei Besuch der Webseite von nur wenigen Nutzern, kann ein Angriff auf die Webseite vorliegen. Hier können auch Daten der Nutzer mit in die Analyse einbezogen werden, beispielsweise deren IP-Adressen, Domain-Name Server, Zeit und Dauer des Zugriffs oder geographische Position, an der sie sich aufhalten. Beispielsweise kann es auffällig sein, wenn viele Nutzer aus verschiedenen geographischen Positionen auf eine Webseite zugreifen oder wenn während der Nacht

ein vermehrtes Aufkommen an Zugriffen beobachtet werden kann. Bei Nutzung solcher Informationen lässt sich die Zuverlässigkeit der Erkennung eines Angriffs noch weiter erhöhen.

Gemäß einer Ausführungsform umfasst das Verfahren ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Häufigkeit von selten ausgeführten Prozessen in dem Computernetzwerk.

Ein Computernetzwerk, das sich im Normalzustand befindet, arbeitet meist mit den gleichen Prozessen. Selten ausgeführte Prozesse können daher auf einfache Weise einen Hinweis für eine Anomalie und damit eine mögliche Gefährdung liefern.

Gemäß einer Ausführungsform umfasst das Verfahren ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Häufigkeit von Programmen, die auf einer vorgegebenen Gruppe aus der Mehrzahl von Computern in dem Computernetzwerk ausgeführt werden, insbesondere basierend auf einer Häufigkeit von Programmen, die erst ab einer vorgegebenen Zeit auf der vorgegebenen Gruppe von Computern ausgeführt werden.

Dies hat den Vorteil, dass das Verfahren anhand einer solchen Auswertung mögliche Virenprogramme oder Schadsoftware, die auf einzelnen oder einer kleinen Gruppe von Computern ausgeführt wird, leicht und zuverlässig erkennen kann.

Gemäß einer Ausführungsform umfasst das Verfahren ein Nutzen eines oder mehrerer der folgenden Systeme auf zumindest einem der Mehrzahl von Computern zum Erzeugen der Warnmeldungen: Virenscanner, Proxyserver, IDS, Angrifferkennungssystem, Firewall, Betriebssystem, Log Management System, SIEM System, Security Information and Event Management System.

Der Vorteil eines solchen Verfahrens liegt darin, dass die angeführten Systeme dahingehend genutzt werden können, verschiedene Kenngrößen des Systems zu ermitteln und über die Warnmeldungen weiterzuleiten. Mittels der Analyse einer Vielzahl

an Protokolldaten ist es dem Verfahren möglich eine Auffälligkeit bzw. Anomalie früher zu erkennen, als dies durch eine Betrachtung der aktuellen Netzwerkindikatoren möglich ist.

Zum Generieren der Warnmeldungen kann so auf bereits vorhandene Infrastruktur zurückgegriffen werden, beispielsweise bereits installierte Protokolldatensysteme, die eine Aufzeichnung relevanter Daten vornehmen. Die Analyse kann mit unterschiedlichen Analyseverfahren ausgeführt werden, beispielsweise mit Methoden der Künstlichen Intelligenz oder Neuronaler Netze und liefert zuverlässige Analyseergebnisse, die in Form von Ereignissen aufbereitet sein können. Die Analyse kann die Vielzahl an Daten, die in dem Computernetz vorliegen, auf die relevanten Aspekte begrenzen bzw. eine gewisse Anzahl relevanter Ereignisse liefern, die dann weiter eingegrenzt werden können.

Gemäß einer Ausführungsform umfasst das Verfahren ein Anpassen des Ereignisschwellwerts basierend auf der Anzahl der Warnmeldungen, die den Ereignisschwellwert unterschreiten.

Dies hat den Vorteil, dass in den Ereignisschwellwert Kenntnisse über das Computernetzwerk einfließen können, beispielsweise über die Struktur und die einzelnen Komponenten des Netzwerks. Der Indikator kann damit flexibel an sich ändernde Umgebungseinflüsse, beispielsweise zusätzliche Software- oder Hardwarekomponenten im Computernetzwerk, angepasst werden.

Gemäß einer Ausführungsform umfasst das Verfahren ein adaptives Anpassen des Ereignisschwellwerts in Abhängigkeit von zumindest einem der folgenden Ereignisse: Anwender-Feedbacks, Veränderungen in der Netzwerk-Architektur des Computernetzwerks, Änderungen in der Anzahl der Computer des Computernetzwerks.

Ein solches Verfahren hat den Vorteil, dass es sich flexibel an eine geänderte Struktur anpassen kann und dass das Wissen des Anwenders in die Entscheidungsfindung mit einfließen kann.

Gemäß einem Aspekt betrifft die Erfindung ein Analysesystem zum Erkennen eines Angriffs in einem Computernetzwerk mit einer Mehrzahl von Computern, mit: einem

Empfangsmodul, das ausgelegt ist, eine Mehrzahl von Warnmeldungen von den Computern zu empfangen, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks basieren; einem Vergleichsmodul, das ausgelegt ist, eine Anzahl der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert zu vergleichen, wobei die Anzahl der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren; und einem Ausgabemodul, das ausgelegt ist, ein Alarmsignal auszugeben, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

Der Vorteil eines solchen Analysesystems liegt darin, dass das System schnell und zuverlässig ein Alarmsignal bei einem bevorstehenden Angriff auf das Computernetzwerk auslösen kann. Das Analysesystem kann einen möglichen oder bevorstehenden Angriff auf das Computernetzwerk bzw. Computersystem zuverlässig basierend auf über die Warnmeldungen indizierte kritische Anomalien des Netzwerks erkennen. So müssen lediglich die Anzahl auftretender Warnmeldungen den möglichen Anomalien des Computernetzwerks zugeordnet und gezählt werden. Ist die Anzahl einer bestimmten Anomalie groß, d.h. überschreitet sie einen bestimmten Ereignisschwellwert, so ist von einer häufig auftretenden und daher als unkritischen zu klassifizierenden Anomalie des Computernetzwerks auszugehen. Ist die Anzahl einer bestimmten Anomalie dagegen klein, d.h. unterschreitet sie den Ereignisschwellwert, so ist von einer selten auftretenden und daher als kritisch zu klassifizierenden Anomalie des Computernetzwerks auszugehen. Bei Unterschreiten des Ereignisschwellwerts kann das Ausgabemodul ein Alarmsignal ausgeben, um den Nutzer des Computernetzwerks zu warnen, dass ein möglicher Angriff bevorsteht oder bereits stattgefunden hat.

Die Ausgabe eines Alarmsignals bei einem möglichen Angriff auf das Computernetzwerk kann damit flexibel, schnell und genau ausgeführt werden. Durch den modularen Aufbau des Analysesystems können die einzelnen Module flexibel auf unterschiedlichen Software- oder Hardwarekomponenten realisiert werden, beispielsweise auf Komponenten innerhalb des Computernetzwerks oder auf externen Komponenten außerhalb des Computernetzwerks.

Gemäß einer Ausführungsform umfasst das Analysesystem ein Klassifizierungsmodul, das ausgelegt ist, die Mehrzahl von Warnmeldungen bezüglich des Typs der von einer jeweiligen Warnmeldung angezeigten Anomalie zu klassifizieren.

Der Vorteil des Klassifizierungsmoduls liegt darin, dass es aus der Vielzahl von eintreffenden Warnmeldungen schnell die relevanten Warnmeldungen ausfiltern kann, die eine kritische Anomalie des Computernetzwerks signalisieren.

Gemäß einer Ausführungsform umfasst das Analysesystem ein Anpassungsmodul, das ausgelegt ist, den Ereignisschwellwert basierend auf der Anzahl der Warnmeldungen, die den Ereignisschwellwert unterschreiten, anzupassen.

Dies hat den Vorteil, dass das Anpassungsmodul den Ereignisschwellwert basierend auf Kenntnissen über das Computernetzwerk anpassen kann, beispielsweise in adaptiver Weise. Die Anpassung kann beispielsweise abhängig von der Struktur und den einzelnen Komponenten des Netzwerks erfolgen. Die Auslösung des Alarmsignals kann damit flexibel an sich ändernde Umgebungseinflüsse, beispielsweise zusätzliche Software- oder Hardwarekomponenten im Computernetzwerk, angepasst werden.

Weitere Ausführungsbeispiele werden Bezug nehmend auf die beiliegenden Zeichnungen erläutert. Es zeigen:

Fig. 1 eine schematische Darstellung einer Klassifikation 100 von Warnmeldungen in verschiedene Typen von Anomalien gemäß einer Ausführungsform;

Fig. 2 eine schematische Darstellung eines Analysesystems 200 zum Erkennen eines Angriffs auf ein Computernetzwerk gemäß einer Ausführungsform;

Fig. 3 eine schematische Darstellung eines Analysesystems 300 zum Erkennen eines Angriffs auf ein Computernetzwerk gemäß einer weiteren Ausführungsform;

Fig. 4 eine schematische Darstellung eines Szenarios 400 eines Angriffs auf eine Internet-Webseite 411 eines Computernetzwerks 410, wobei ein Analysesystem 200, 300 gemäß einer Ausführungsform den Angriff erkennt;

Fig. 5 eine schematische Darstellung eines Szenarios 500 eines Virenangriffs auf eine Gruppe von vernetzten Computern eines unternehmensinternen Computernetzwerks 510, wobei ein Analysesystem 200, 300 gemäß einer Ausführungsform den Angriff erkennt; und

Fig. 6 eine schematische Darstellung eines Verfahrens 600 zum Erkennen eines Angriffs auf ein Computernetzwerk gemäß einer Ausführungsform.

Fig. 1 zeigt eine schematische Darstellung einer Klassifikation 100 von Warnmeldungen in verschiedene Typen von Anomalien gemäß einer Ausführungsform. Zur Klassifikation werden Warnmeldungen 102 von Computern empfangen, die unterschiedliche Typen oder Arten von Warnungen transportieren. Die gesamte Menge 110 bzw. der gesamte Teil oder die gesamte Anzahl der Warnmeldungen enthält verschieden geartete Warnungen, die auf verschiedenen Anomalien eines Computernetzwerks basieren. Eine Anomalie des Computernetzwerks bedeutet dabei eine Unregelmäßigkeit oder eine Auffälligkeit des Computernetzwerks bzw. ein von der Norm abweichendes Muster z.B. infolge einer Störung. Eine Anomalie kann somit als ein Zustand des Computernetzwerks angesehen werden, der vom Erwarteten abweicht.

In Fig. 1 ist die Klassifikation der Warnmeldungen in einen ersten Typ 111 einer Anomalie, einen zweiten Typ 112 einer Anomalie, einen dritten Typ 113 einer Anomalie und einen vierten Typ 114 einer Anomalie dargestellt. Allerdings kann jede andere Anzahl von Typen auftreten. In Fig. 1 treten Warnmeldungen des ersten Typs 111 einer Anomalie am häufigsten auf, danach Warnmeldungen des zweiten Typs 112 einer Anomalie, danach Warnmeldungen des dritten Typs 113 einer Anomalie und am seltensten treten Warnmeldungen des vierten Typs 114 einer Anomalie auf.

Anhand der Anzahl der Warnmeldungen des jeweiligen Typs kann darauf geschlossen werden, ob sich das Computersystem in einem kritischen Zustand befindet, d.h. ob ein Angriff auf das Computersystem bevorsteht oder bereits stattgefunden hat. Unterschreitet die Anzahl der Warnmeldungen eines Typs von Anomalie, hier des vierten Typs 114, bezogen auf einen bestimmten Zeitraum eine bestimmte Schwelle, auch

Ereignisschwellwert genannt, so liegt ein kritischer Zustand vor und ein Alarmsignal 108 wird ausgelöst.

Die im Folgenden beschriebenen Verfahren und Analysesysteme können auf einer in Fig. 1 beschriebenen Klassifikation basieren.

Fig. 2 zeigt eine schematische Darstellung eines Analysesystems 200 zum Erkennen eines Angriffs in einem Computernetzwerk mit einer Mehrzahl von Computern gemäß einer Ausführungsform. Das Analysesystem 100 umfasst ein Empfangsmodul 201, ein Vergleichsmodul 203 und ein Ausgabemodul 205.

Mit dem Empfangsmodul 201 werden eine Mehrzahl von Warnmeldungen 102 von den Computern empfangen, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks entsprechend der Darstellung in Fig. 1 basieren.

Mit dem Vergleichsmodul 203 wird eine Anzahl bzw. ein Teil der Warnmeldungen 204 aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert verglichen, wobei die Anzahl bzw. der Teil der Warnmeldungen 204 auf einem selben Typ einer Anomalie des Computernetzwerks basieren, beispielsweise des vierten Typs 114, wie in Fig. 1 dargestellt.

Mit dem Ausgabemodul 205 wird ein Alarmsignal 108 ausgegeben, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, d.h. ein Ergebnis 206 des Vergleichsmoduls 203, den Ereignisschwellwert unterschreitet.

Im Folgenden wird das modular aufgebaute Analysesystem 200 näher beschrieben. Das Analysesystem 200 kann eine große Menge empfangener Warnmeldungen automatisiert korrelieren und auf das Vorliegen einer Anomalie und damit eines möglichen Indikators für einen Angriff analysieren. Als Datenquelle können z.B. gezielt ausgewählte Logdaten oder alternativ ein bereits installiertes SIEM (Security Information and Event Management)-System, genutzt werden. Der Zweck der Analyse ist es, die Menge der vorhandenen Daten durch bestimmte Analyseverfahren soweit zu reduzieren und in Form von Ereignissen bzw. „Events“ aufzubereiten, dass eine Fachkraft in die Lage versetzt wird,

potentielle Angriffe auf Basis der analysierten Logdaten zu erkennen. Das zugrunde liegende automatisierte Analyseverfahren basiert auf der Suche nach unbekannten und selten vorkommenden Ereignissen. Dabei steht die Häufigkeit des Auftretens eines bestimmten (oder vergleichbaren) Ereignisses in einem bestimmten Zeitraum, in direktem Zusammenhang zum „Bekanntheitsgrad“. Häufig auftretende Ereignisse werden dabei in ihrer Tendenz eher als bekannt klassifiziert und sind damit eher irrelevant. Selten vorkommende Ereignisse hingegen sind in ihrer Tendenz eher unbekannt und damit potentiell relevanter.

Auf dieser Basis werden zusammen mit weiteren individuell festzulegenden Parametern wie z.B. Schwarzen Listen („Blacklists“), Weißen Listen („Whitelists“), Schwellenwerten, Ereigniszusammenhängen, sowie der Definition von Gefährdungspotentialen einzelner Personengruppen ein Wahrscheinlichkeitswert für das Vorliegen .eines Angriffs errechnet und bei Überschreiten eines bestimmten Schwellwertes zu einem Event korreliert und für weitere Analysen aufbereitet. Im Kern handelt es sich also um eine Häufigkeitsanalyse von Ereignissen bezogen auf einen bestimmten Zeitraum. Die Parameteranpassungen, die letztlich mitentscheidend für eine positive Anomalieerkennung sind, können durch das Analysesystem 200 teilautomatisiert ausgeführt werden. Dazu können Methoden aus dem Bereich der „Künstlichen Intelligenz" angewandt werden, wobei das Analysesystem 200 dem Anwender/Analysten konkrete Vorschläge, z.B. für die Anpassung eines bestimmten Schwellenwertes machen kann. Die Vorschläge können dabei unter anderem auf Basis von Anwender-Feedbacks und sich verändernden Rahmenbedingungen unterbreitet werden, wie z.B. festgestellten Veränderungen in der Netzwerk-Architektur oder vorhersehbaren Veränderungen in der Anzahl aktiver Netzwerkteilnehmer, beispielsweise zur Urlaubszeit. Dabei kann eine durch den Anwender oder Analysten getroffene Entscheidung über einen erteilten Vorschlag wiederum Einfluss auf zukünftige Vorschläge haben.

Fig. 3 zeigt eine schematische Darstellung eines Analysesystems 300 zum Erkennen eines Angriffs in einem Computernetzwerk mit einer Mehrzahl von Computern gemäß einer weiteren Ausführungsform. Das Analysesystem 300 umfasst ein Empfangsmodul 301, ein Klassifikationsmodul 309, ein Vergleichsmodul 305 und ein Ausgabemodul 307.

Mit dem Empfangsmodul 301 werden eine Mehrzahl von Warnmeldungen 102 von den Computern empfangen, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks entsprechend der Darstellung in Fig. 1 basieren.

Dabei können die Mehrzahl von Warnmeldungen in einem vorgegebenen Zeitintervall, beispielsweise von 1 Sekunde, 1 Minute, 5 Minuten, 30 Minuten oder 1 Stunde empfangen werden.

Zum Erzeugen der Warnmeldungen können beispielsweise eines oder mehrere der folgenden Systeme verwendet werden, die beispielsweise auf einem oder mehreren der Computer des Computernetzwerks installiert sein können: ein Virenscanner, ein Proxyserver, ein IDS (Angrifferkennungssystem), ein Firewall, ein Betriebssystem, ein Log Management System, ein SIEM System (Security Information and Event Management System).

Mit dem Klassifikationsmodul 309 wird die Mehrzahl von Warnmeldungen bezüglich des Typs 310 der von einer jeweiligen Warnmeldung angezeigten Anomalie klassifiziert. Die Warnmeldungen 304 werden in verschiedene Klassen eingeteilt, die mit einem Typ 310 von Anomalie des Computernetzwerks assoziiert sind, und an das Vergleichsmodul 305 weitergeleitet.

Die Mehrzahl von Warnmeldungen können somit bezüglich des Typs der von einer jeweiligen Warnmeldung angezeigten Anomalie klassifiziert werden. Der Typ der von einer Warnmeldung angezeigten Anomalie kann beispielsweise basierend auf einem Inhalt der Warnmeldung bestimmt werden, z.B. durch Auswertung eines Datenfeldes wie eines Headers oder einer Payload in der Warnmeldung.

Mit dem Vergleichsmodul 305 wird eine Anzahl bzw. ein Teil der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert verglichen, wobei die Anzahl bzw. der Teil der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren, beispielsweise des vierten Typs 114, wie in Fig. 1 dargestellt. Die jeweiligen Anzahlen bzw. Teile der Warnmeldungen entsprechen in Fig. 3 den Klassen, in welche die Warnmeldungen durch das Klassifikationsmodul 309 klassifiziert wurden. Das Vergleichsmodul kann den

Vergleich beispielsweise in einem vorgegebenen Zeitintervall durchführen, um eine Referenz zu haben.

Das Vergleichen kann beispielsweise durch Zählen der empfangenen Warnmeldungen, die bezüglich desselben Typs klassifiziert sind erfolgen, z.B. durch Zählen innerhalb eines vorgegebenen Zeitintervalls. Bei Unterschreiten des Ereignisschwellwerts der so gezählten Warnmeldungen innerhalb des vorgegebenen Zeitintervalls kann das Ausgabemodul 307 angewiesen werden, das Alarmsignal 108 auszugeben, z.B. über das Ergebnis 306 des Vergleichs.

Mit dem Ausgabemodul 307 wird das Alarmsignal 108 ausgegeben, falls die Anzahl der Warnmeldungen, die auf demselben Typ 310 einer Anomalie des Computernetzwerks basieren, d.h. die Anzahl der Warnmeldungen, die einer bestimmten Klasse zugeordnet wurden, den Ereignisschwellwert unterschreitet.

Das Ausgabemodul 307 kann zusätzlich zur Ausgabe des Alarmsignals einen Wahrscheinlichkeitswert für das Vorliegen eines Angriffs auf das Computernetzwerk bestimmen, beispielsweise basierend auf einer Analyse der Anzahl bzw. des Teils der Warnmeldungen, die den Ereignisschwellwert unterschreiten. Der Wahrscheinlichkeitswert kann ferner basierend auf einem oder mehreren der folgenden vorbestimmten Parameter bestimmt werden: Schwarze Listen, Weiße Listen, Schwellenwerte, Ereigniszusammenhänge, und Definition von Gefährdungspotenzialen einzelner Nutzergruppen des Computernetzwerks. Der Wahrscheinlichkeitswert für das Vorliegen eines Angriffs auf das Computernetzwerk kann ferner basierend auf einer Anzahl von Besuchern des Computernetzwerks bestimmt werden, insbesondere auf einer Anzahl von Besuchern einer Webseite des Computernetzwerks, wie im Folgenden zu Fig. 4 näher beschrieben. Der Wahrscheinlichkeitswert für das Vorliegen eines Angriffs auf das Computernetzwerk kann ferner basierend auf einer Häufigkeit von selten ausgeführten Prozessen in dem Computernetzwerk bestimmt werden, wie im Folgenden zu Fig. 5 näher beschrieben. Der Wahrscheinlichkeitswert für das Vorliegen eines Angriffs auf das Computernetzwerk kann ferner basierend auf einer Häufigkeit von Programmen, die auf einer vorgegebenen Gruppe aus der Mehrzahl von Computern in dem Computernetzwerk ausgeführt werden bestimmt werden, insbesondere basierend auf einer Häufigkeit von Programmen, die erst ab einer vorgegebenen Zeit auf der

vorgegebenen Gruppe von Computern ausgeführt werden, wie im Folgenden zu Fig. 5 näher beschrieben.

Das Analysesystem 300 kann ferner ein (in Fig. 3 nicht dargestelltes) Anpassungsmodul umfassen, mit dem der Ereignisschwellwert basierend auf dem Teil der Warnmeldungen, dessen Anzahl den Ereignisschwellwert unterschreitet, angepasst werden kann. Dazu kann beispielsweise ein Vorschlag zum Anpassen des Ereignisschwellwerts unterbreitet werden, der auf der Anzahl der Warnmeldungen basieren kann, die den Ereignisschwellwert unterschreiten. Der Vorschlag kann ferner auf Anwender-Feedbacks basieren und/oder Veränderungen in der Netzwerk-Architektur des Computernetzwerks, insbesondere Änderungen in der Anzahl der Computer des Computernetzwerks. Das Anpassen des Ereignisschwellwerts kann adaptiv erfolgen, beispielsweise in Abhängigkeit von zumindest einem der folgenden Ereignisse: Anwender-Feedbacks, Veränderungen in der Netzwerk-Architektur des Computernetzwerks, Änderungen in der Anzahl der Computer des Computernetzwerks.

Fig. 4 zeigt eine schematische Darstellung eines Szenarios 400 eines Angriffs auf eine Internet-Webseite 411 eines Computernetzwerks 410, wobei ein Analysesystem 200, 300 den Angriff erkennt. Der Angriff geht von einer kleinen Gruppe von Besuchern 420 der Internet-Webseite 411 aus. Das Analysesystem 200, 300 kann den in Fig. 2 oder Fig. 3 beschriebenen Systemen entsprechen.

Das Analysesystem 200 kann ein Empfangsmodul 201, ein Vergleichsmodul 203 und ein Ausgabemodul 205 umfassen. Mit dem Empfangsmodul 201 werden eine Mehrzahl von Warnmeldungen 102 von den Computern empfangen, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks entsprechend der Darstellung in Fig. 1 basieren. Mit dem Vergleichsmodul 203 wird eine Anzahl bzw. ein Teil der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert verglichen, wobei die Anzahl bzw. der Teil der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren. Mit dem Ausgabemodul 205 wird ein Alarmsignal 108 ausgegeben, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

Im Folgenden wird ein Betriebsmodus des Analysesystems 200, 300 beschrieben. Wenn viele verschiedene Benutzer ein bestimmtes System im Internet, z.B. eine Website 411 besuchen, dann ist dieser Vorgang mutmaßlich unkritisch, Wird das System jedoch nur von einer kleinen Benutzergruppe 420 angesprochen, dann könnte es sich hierbei ggf. um einen C2-Server handeln. Handelt es sich bei den betroffenen Nutzern zusätzlich um eine bestimmte Personengruppe mit erhöhtem Gefährdungspotential, generiert das Analysesystem 200, 300 ein Event bzw. ein Alarmsignal 108, welches dann von einer Fachkraft evaluiert werden kann.

Fig. 5 zeigt eine schematische Darstellung eines Szenarios 500 eines Virenangriffs auf eine Gruppe von vernetzten Computern eines unternehmensinternen Computernetzwerks 510, wobei ein Analysesystem 200, 300 den Angriff erkennt. Das Analysesystem 200, 300 kann den in Fig. 2 oder Fig. 3 beschriebenen Systemen entsprechen.

Das Analysesystem 200 kann ein Empfangsmodul 201, ein Vergleichsmodul 203 und ein Ausgabemodul 205 umfassen. Mit dem Empfangsmodul 201 werden eine Mehrzahl von Warnmeldungen 102 von den Computern empfangen, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks entsprechend der Darstellung in Fig. 1 basieren. Mit dem Vergleichsmodul 203 wird eine Anzahl bzw. ein Teil der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert verglichen, wobei die Anzahl bzw. der Teil der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren. Mit dem Ausgabemodul 205 wird ein Alarmsignal 108 ausgegeben, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

Im Folgenden wird ein Betriebsmodus des Analysesystems 200, 300 beschrieben. Unter der Annahme, dass die meisten Office-PCs 511, 513, 515 in einem größeren Unternehmen vergleichbar konfiguriert sind und zum Großteil identische Softwareanwendungen P_1, P_2, P_3 genutzt werden, können durch den Vergleich einer hohen Anzahl von Prozesslisten 512, 514, 516 selten ausgeführte Programme P_{Virus} identifiziert werden. Ein Programm P_{Virus}, das beispielsweise nur auf einer kleinen Gruppe von Computern 515 ausgeführt wird und das auch erst seit einer kurzen Zeit, kann ein Hinweis auf eine kürzlich installierte Schadsoftware P_{Virus} sein. Das Analysesystem 200,

300 braucht also nicht nach bestimmten Prozessen zu suchen, sondern es kann durch Eliminierung der bekannten bzw. häufig vorkommenden Prozesse P_1, P_2, P_3 unbekannte Prozesse P_{Virus} identifizieren. Nach Auswertung der weiteren Parameter kann dieses Ereignis zu einem korrelierten Event bzw. einem Alarmsignal 108 zusammengefasst und einem Anwender oder Analysten zur weiteren Untersuchung vorgelegt werden.

Fig. 6 zeigt eine schematische Darstellung eines Verfahrens 600 zum Erkennen eines Angriffs auf ein Computernetzwerk gemäß einer Ausführungsform. Das Verfahren 600 umfasst ein Empfangen 601 einer Mehrzahl von Warnmeldungen von den Computern, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks basieren. Das Verfahren 600 umfasst ein Vergleichen 603 einer Anzahl bzw. eines Teils der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert, wobei die Anzahl bzw. der Teil der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren. Das Verfahren 600 umfasst ein Ausgeben 605 eines Alarmsignals, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

In einer Ausführungsform kann das Verfahren 600 ein Empfangen der Mehrzahl von Warnmeldungen in einem vorgegebenen Zeitintervall umfassen. In einer Ausführungsform kann das Verfahren 600 ein Klassifizieren der Mehrzahl von Warnmeldungen bezüglich des Typs der von einer jeweiligen Warnmeldung angezeigten Anomalie umfassen. In einer Ausführungsform kann das Verfahren 600 ein Bestimmen des Typs der von einer Warnmeldung angezeigten Anomalie basierend auf einem Inhalt der Warnmeldung umfassen. In einer Ausführungsform kann das Verfahren 600 ein Zählen der empfangenen Warnmeldungen, die bezüglich desselben Typs klassifiziert sind, in dem vorgegebenen Zeitintervall; und ein Ausgeben des Alarmsignals falls die Anzahl der in dem vorgegebenen Zeitintervall gezählten Warnmeldungen den Ereignisschwellwert unterschreitet umfassen. In einer Ausführungsform kann das Verfahren 600 ein Bestimmen eines Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk basierend auf der Anzahl der Warnmeldungen, die den Ereignisschwellwert unterschreiten umfassen.

In einer Ausführungsform kann das Verfahren 600 ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf zumindest einem der folgenden vorbestimmten Parameter: Schwarze Listen, Weiße Listen, Schwellenwerte, Ereigniszusammenhänge, und Definition von Gefährdungspotenzialen einzelner Nutzergruppen des Computernetzwerks umfassen. In einer Ausführungsform kann das Verfahren 600 ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Anzahl von Besuchern des Computernetzwerks, insbesondere auf einer Anzahl von Besuchern einer Webseite des Computernetzwerks umfassen. In einer Ausführungsform kann das Verfahren 600 ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Häufigkeit von selten ausgeführten Prozessen in dem Computernetzwerk umfassen.

In einer Ausführungsform kann das Verfahren 600 ein Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Häufigkeit von Programmen, die auf einer vorgegebenen Gruppe aus der Mehrzahl von Computern in dem Computernetzwerk ausgeführt werden umfassen, insbesondere basierend auf einer Häufigkeit von Programmen, die erst ab einer vorgegebenen Zeit auf der vorgegebenen Gruppe von Computern ausgeführt werden.

In einer Ausführungsform kann das Verfahren 600 ein Nutzen eines oder mehrerer der folgenden Systeme auf zumindest einem der Mehrzahl von Computern zum Erzeugen der Warnmeldungen umfassen: Virenscanner, Proxyserver, IDS, Angrifferkennungssystem, Firewall, Betriebssystem, Log Management System, SIEM System, Security Information and Event Management System. In einer Ausführungsform kann das Verfahren 600 ein Anpassen des Ereignisschwellwerts basierend auf der Anzahl der Warnmeldungen, die den Ereignisschwellwert unterschreiten umfassen. In einer Ausführungsform kann das Verfahren 600 ein Unterbreiten eines Vorschlags zum Anpassen des Ereignisschwellwerts basierend auf der Anzahl der Warnmeldungen, die den Ereignisschwellwert unterschreitet und ferner basierend auf Anwender-Feedbacks und/oder Veränderungen in der Netzwerk-Architektur des Computernetzwerks, insbesondere Änderungen in der Anzahl der Computer des Computernetzwerks

umfassen. In einer Ausführungsform kann das Verfahren 600 ein adaptives Anpassen des Ereignisschwellwerts umfassen, beispielsweise in Abhängigkeit von zumindest einem der folgenden Ereignisse: Anwender-Feedbacks, Veränderungen in der Netzwerk-Architektur des Computernetzwerks, Änderungen in der Anzahl der Computer des Computernetzwerks.

Ein Aspekt der Erfindung umfasst auch ein Computerprogrammprodukt, das direkt in den internen Speicher eines digitalen Computers geladen werden kann und Softwarecodeabschnitte umfasst, mit denen das zu Fig. 6 beschriebene Verfahren 600 ausgeführt werden kann, wenn das Produkt auf einem Computer läuft. Das Computerprogrammprodukt kann auf einem computergeeigneten Medium gespeichert sein und folgendes umfassen: computerlesbare Programmittel, die einen Computer veranlassen, eine Mehrzahl von Warnmeldungen von den Computern zu empfangen 601, wobei die Warnmeldungen auf verschiedenen Typen von Anomalien des Computernetzwerks basieren; eine Anzahl der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert zu vergleichen 603, wobei die Anzahl der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren; und ein Alarmsignal auszugeben 605, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet. Der Computer kann ein PC sein, beispielsweise ein PC eines Computernetzwerks. Der Computer kann als ein Chip, ein ASIC, ein Mikroprozessor oder ein Signalprozessor realisiert sein und in einem Computernetzwerk, beispielsweise einem Computernetzwerk wie in Fig. 4 oder Fig. 5 beschrieben, angeordnet sein.

Es ist selbstverständlich, dass die Merkmale der verschiedenen beispielhaft hierin beschriebenen Ausführungsformen miteinander kombiniert werden können, außer wenn spezifisch anderweitig angegeben. Wie in der Beschreibung und den Zeichnungen dargestellt müssen einzelne Elemente, die in Verbindung stehend dargestellt wurden, nicht direkt miteinander in Verbindung stehen; Zwischenelemente können zwischen den verbundenen Elementen vorgesehen sein. Ferner ist es selbstverständlich, dass Ausführungsformen der Erfindung in einzelnen Schaltungen, teilweise integrierten Schaltungen oder vollständig integrierten Schaltungen oder Programmiermitteln implementiert sein können. Der Begriff „beispielsweise“ ist lediglich als ein Beispiel

gemeint und nicht als das Beste oder Optimale. Es wurden bestimmte Ausführungsformen hierin veranschaulicht und beschrieben, doch für den Fachmann ist es offensichtlich, dass eine Vielzahl von alternativen und/oder gleichartigen Implementierungen anstelle der gezeigten und beschriebenen Ausführungsformen verwirklicht werden können, ohne vom Konzept der vorliegenden Erfindung abzuweichen.

Bezugszeichenliste

100:	Klassifikation von Warnmeldungen
102:	Warnmeldungen
110:	gesamte Menge der Warnmeldungen
111	Anomalie eines ersten Typs
112	Anomalie eines zweiten Typs
113	Anomalie eines dritten Typs
114	Anomalie eines vierten Typs
108:	Alarmsignal
200:	Analysesystem
201:	Empfangsmodul
203:	Vergleichsmodul
205:	Ausgabemodul
204:	Warnmeldungen
206:	Ergebnis des Vergleichs
300:	Analysesystem
301:	Empfangsmodul
307:	Klassifizierungsmodul
303:	Vergleichsmodul
305:	Ausgabemodul
304:	Warnmeldungen
310:	Typen von Anomalien
306:	Ergebnis des Vergleichs
108:	Alarmsignal bzw. Indikator für Angriff auf das Computernetzwerk
400:	Szenario eines Angriffs auf eine Internet-Webseite eines Computernetzwerks
410:	Computernetzwerk
411:	Internet-Webseite
420:	kleine Gruppe von Besuchern
500:	Szenario eines Virenangriffs auf eine Gruppe von vernetzten Computern eines unternehmensinternen Computernetzwerks
510:	unternehmensinternes Computernetzwerk
511,	

513,
515: Rechner in Computernetzwerk
512,
514,
516: Prozesslisten auf den Rechnern
P_1,
P_2,
P_3: Prozesse, die auf den Rechnern ablaufen
P_{Virus}: Schadsoftware auf Rechner
600: Verfahren zum Bestimmen eines Indikators für einen Angriff auf ein Computernetzwerk
601: 1. Verfahrensschritt: Empfangen
603: 2. Verfahrensschritt: Vergleichen
605: 3. Verfahrensschritt: Ausgeben

PATENTANSPRÜCHE

1. Verfahren (600) zum Erkennen eines Angriffs in einem Computernetzwerk (410, 510) mit einer Mehrzahl von Computern, mit folgenden Schritten:

Empfangen (601) einer Mehrzahl von Warnmeldungen (102) von den Computern, wobei die Warnmeldungen auf verschiedenen Typen (111, 112, 113, 114) von Anomalien des Computernetzwerks basieren;

Vergleichen (603) einer Anzahl der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen (102) mit einem vorgegebenen Ereignisschwellwert, wobei die Anzahl der Warnmeldungen auf einem selben Typ (114) einer Anomalie des Computernetzwerks basieren; und

Ausgeben (605) eines Alarmsignals (108), falls die Anzahl der Warnmeldungen, die auf demselben Typ (114) einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

2. Verfahren (600) nach Anspruch 1, mit:

Empfangen der Mehrzahl von Warnmeldungen (102) in einem vorgegebenen Zeitintervall.

3. Verfahren (600) nach Anspruch 2, mit:

Klassifizieren der Mehrzahl von Warnmeldungen (102) bezüglich des Typs (111, 112, 113, 114) der von einer jeweiligen Warnmeldung angezeigten Anomalie.

4. Verfahren (600) nach Anspruch 2 oder 3, mit:

Bestimmen des Typs (111, 112, 113, 114) der von einer Warnmeldung (102) angezeigten Anomalie basierend auf einem Inhalt der Warnmeldung (102).

5. Verfahren (600) nach Anspruch 3 oder 4, mit:

Zählen der empfangenen Warnmeldungen (102), die bezüglich desselben Typs (114) klassifiziert sind, in dem vorgegebenen Zeitintervall, um die Anzahl zu bestimmen; und

Ausgeben des Alarmsignals (108) falls die Anzahl der in dem vorgegebenen Zeitintervall gezählten Warnmeldungen (102), die bezüglich desselben Typs (114) klassifiziert sind, den Ereignisschwellwert unterschreitet.

6. Verfahren (600) nach einem der vorstehenden Ansprüche, mit:

Bestimmen eines Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk basierend auf der Anzahl der Warnmeldungen (102), die den Ereignisschwellwert unterschreiten.

7. Verfahren (600) nach Anspruch 6, umfassend:

Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf zumindest einem der folgenden vorbestimmten Parameter:

Schwarze Listen,

Weiße Listen,

Schwellenwerte,

Ereigniszusammenhänge, und

Definition von Gefährdungspotenzialen einzelner Nutzergruppen des Computernetzwerks.

8. Verfahren (600) nach Anspruch 6 oder 7, umfassend:

Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Anzahl von Besuchern (420) des Computernetzwerks (410), insbesondere auf einer Anzahl von Besuchern (420) einer Webseite (411) des Computernetzwerks (410).

9. Verfahren (600) nach einem der Ansprüche 6 bis 8, umfassend:

Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Häufigkeit von selten ausgeführten Prozessen (P_{Virus}) in dem Computernetzwerk (510).

10. Verfahren (600) nach einem der Ansprüche 6 bis 9, umfassend:

Bestimmen des Wahrscheinlichkeitswerts für das Vorliegen eines Angriffs auf das Computernetzwerk ferner basierend auf einer Häufigkeit von Programmen (516), die auf einer vorgegebenen Gruppe aus der Mehrzahl von Computern (515) in dem Computernetzwerk (510) ausgeführt werden, insbesondere basierend auf einer Häufigkeit von Programmen (P_{Virus}), die erst ab einer vorgegebenen Zeit auf der vorgegebenen Gruppe von Computern (515) ausgeführt werden.

11. Verfahren (600) nach einem der vorstehenden Ansprüche, umfassend:

Nutzen eines oder mehrerer der folgenden Systeme auf zumindest einem der Mehrzahl von Computern zum Erzeugen der Warnmeldungen:

Virenscanner,

Proxyserver,

IDS, Angrifferkennungssystem,

Firewall,

Betriebssystem,

Log Management System,

SIEM System, Security Information and Event Management System.

12. Verfahren (600) nach einem der vorstehenden Ansprüche, umfassend:

Anpassen des Ereignisschwellwerts basierend auf der Anzahl der Warnmeldungen, die den Ereignisschwellwert unterschreiten.

13. Verfahren (600) nach einem der vorstehenden Ansprüche, mit adaptivem Anpassen des Ereignisschwellwerts in Abhängigkeit von zumindest einem der folgenden Ereignisse:

Anwender-Feedbacks,

Veränderungen in der Netzwerk-Architektur des Computernetzwerks,

Änderungen in der Anzahl der Computer des Computernetzwerks.

14. Analysesystem (200, 300) zum Erkennen eines Angriffs in einem Computernetzwerk (410, 510) mit einer Mehrzahl von Computern, mit:

einem Empfangsmodul (201, 301), das ausgelegt ist, eine Mehrzahl von Warnmeldungen (102) von den Computern zu empfangen, wobei die Warnmeldungen (102) auf verschiedenen Typen von Anomalien des Computernetzwerks basieren;

einem Vergleichsmodul (203, 305), das ausgelegt ist, eine Anzahl der Warnmeldungen aus der Mehrzahl der empfangenen Warnmeldungen mit einem vorgegebenen Ereignisschwellwert zu vergleichen wobei die Anzahl der Warnmeldungen auf einem selben Typ einer Anomalie des Computernetzwerks basieren; und

einem Ausgabemodul (205, 307), das ausgelegt ist, ein Alarmsignal (108) auszugeben, falls die Anzahl der Warnmeldungen, die auf demselben Typ einer Anomalie des Computernetzwerks basieren, den Ereignisschwellwert unterschreitet.

15. Analysesystem (300) nach Anspruch 14, mit

einem Klassifizierungsmodul (309), das ausgelegt ist, die Mehrzahl von Warnmeldungen bezüglich des Typs der von einer jeweiligen Warnmeldung angezeigten Anomalie zu klassifizieren.

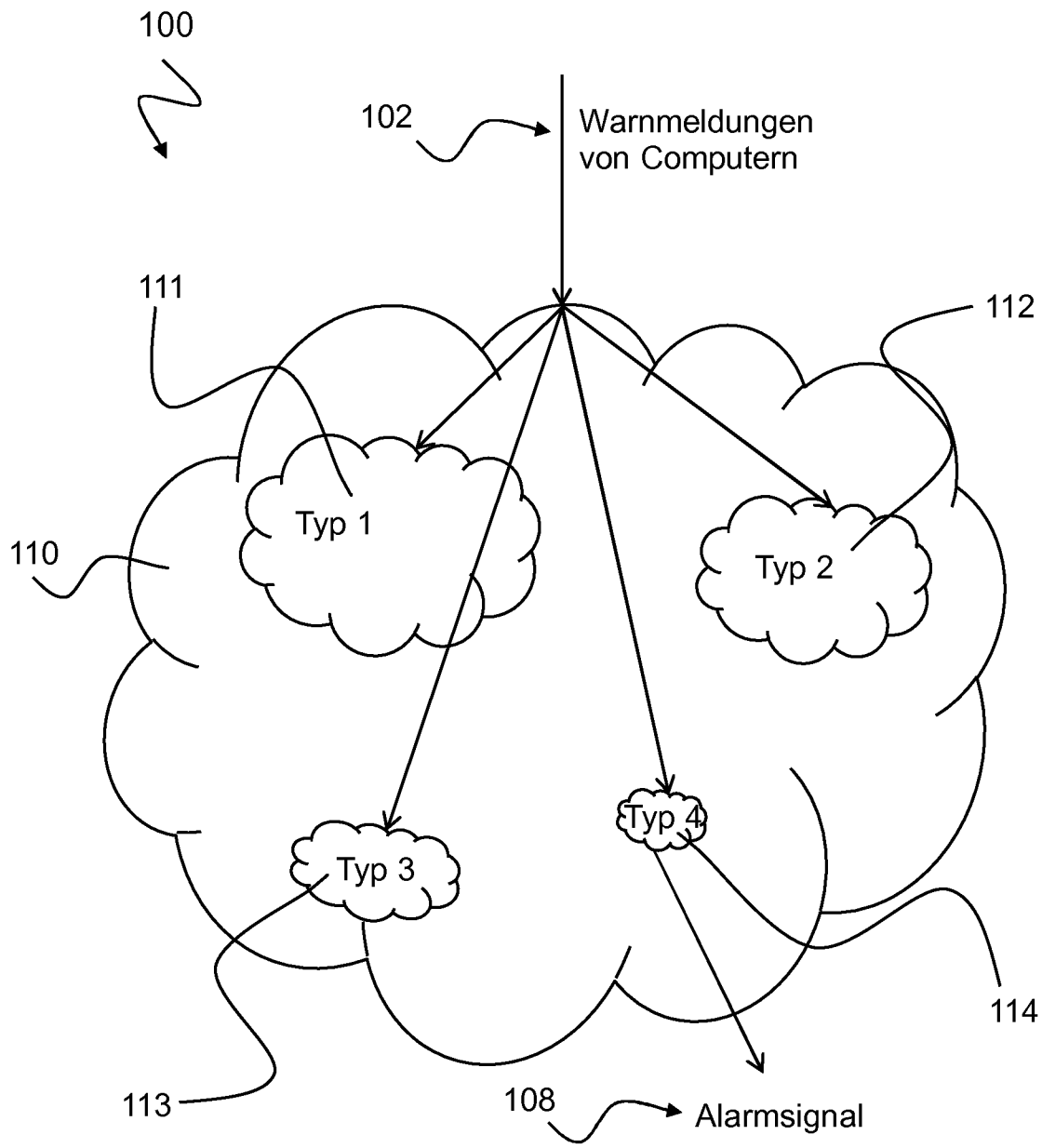
100
102
Warnmeldungen
von Computern
111
112
Typ 1
110
Typ 2
Typ 4
Typ 3
114
113
108
Alarmsignal

Fig. 1

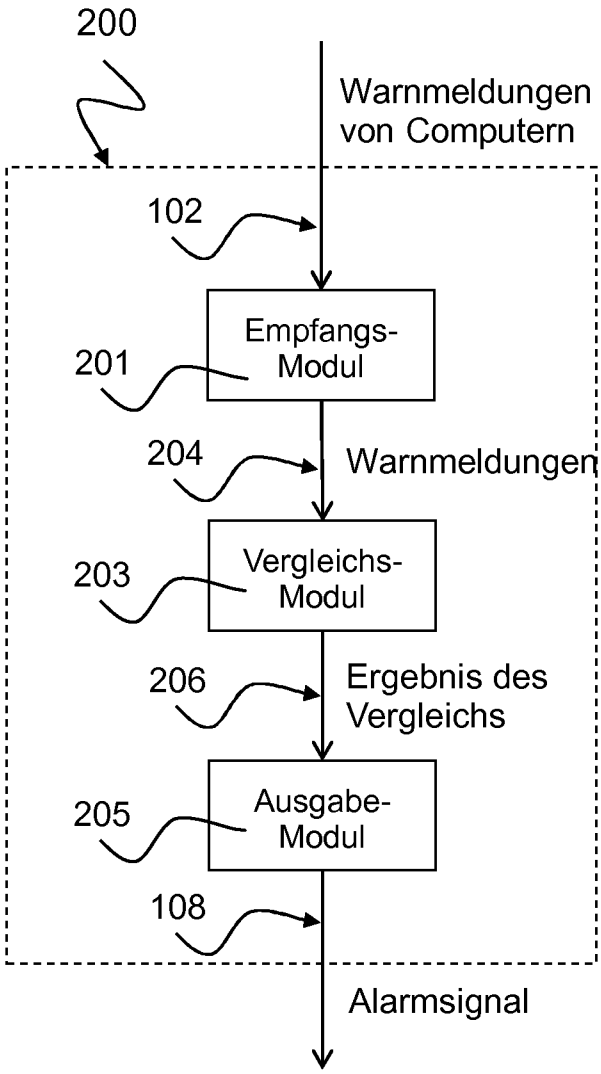
200
Warnmeldungen von Computern
102
Empfangs-Modul
201
204
Warnmeldungen
Vergleichs-Modul
203
206
Ergebnis des Vergleichs
Ausgabe-Modul
205
108
Alarmsignal

Fig. 2

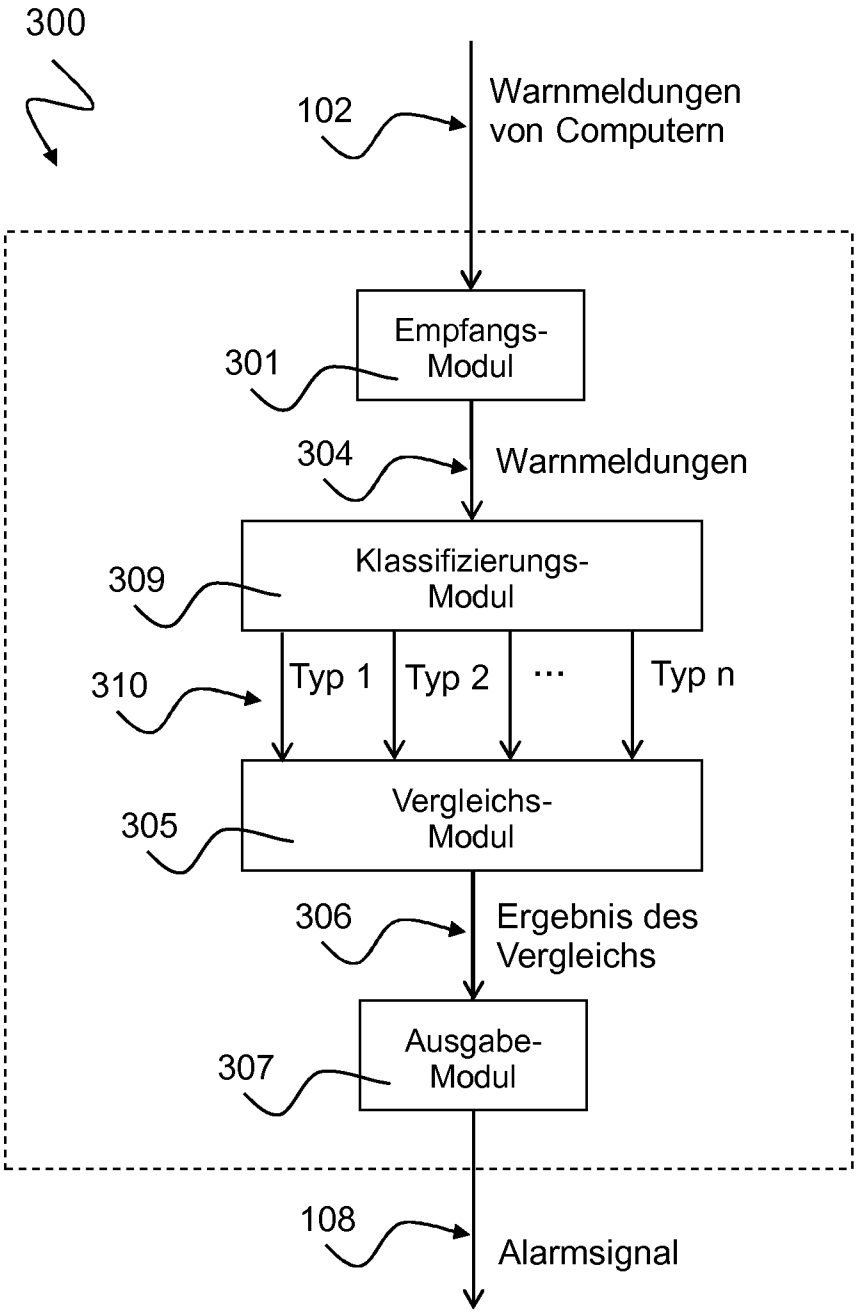
300
102
Warnmeldungen von Computern
Empfangs-Modul
301
304
Warnmeldungen
Klassifizierungs-Modul
309
310
Typ 1
Typ 2
...
Typ n
Vergleichs-Modul
305
306
Ergebnis des Vergleichs
Ausgabe-Modul
307
108
Alarmsignal

Fig. 3

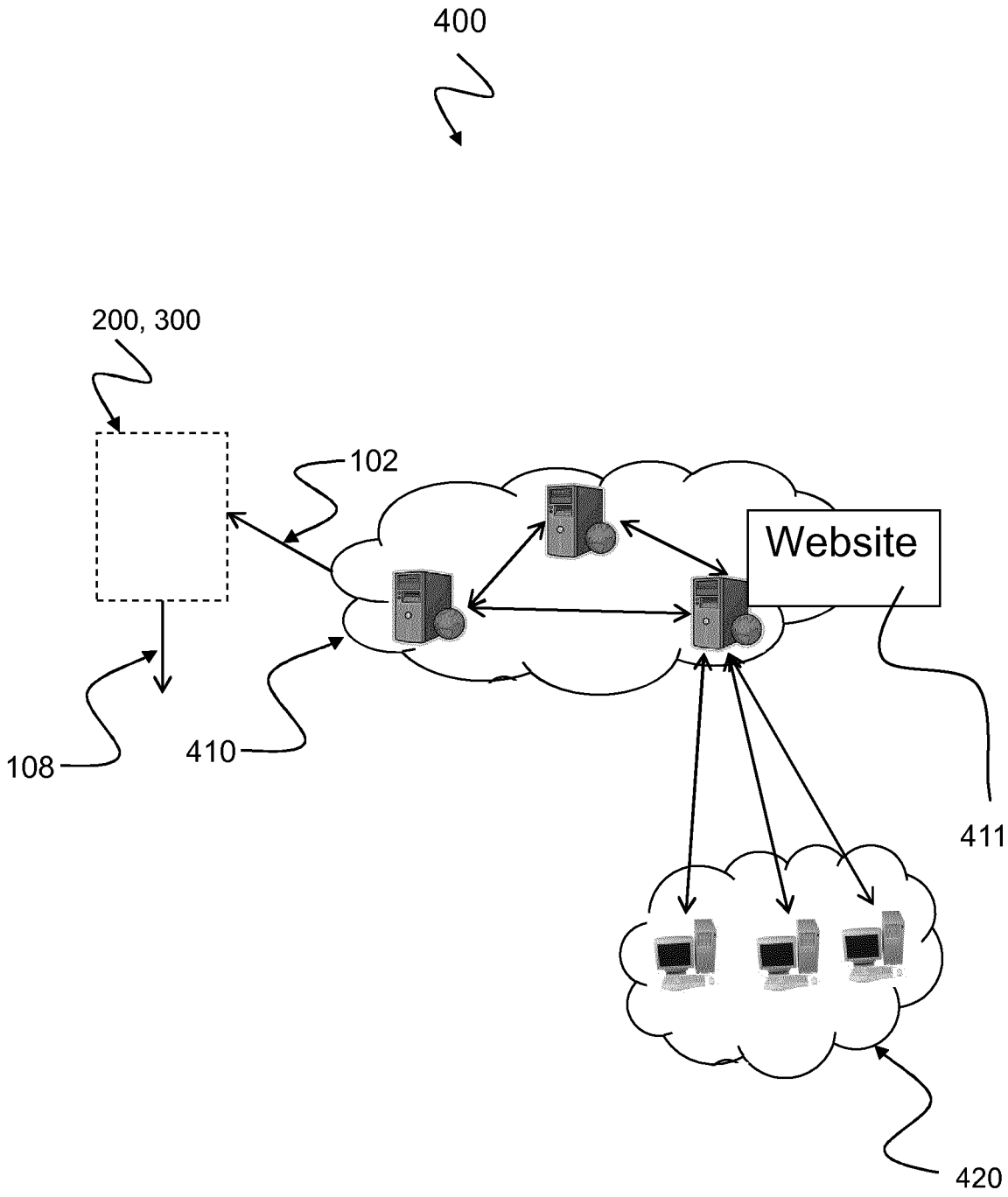

Fig. 4

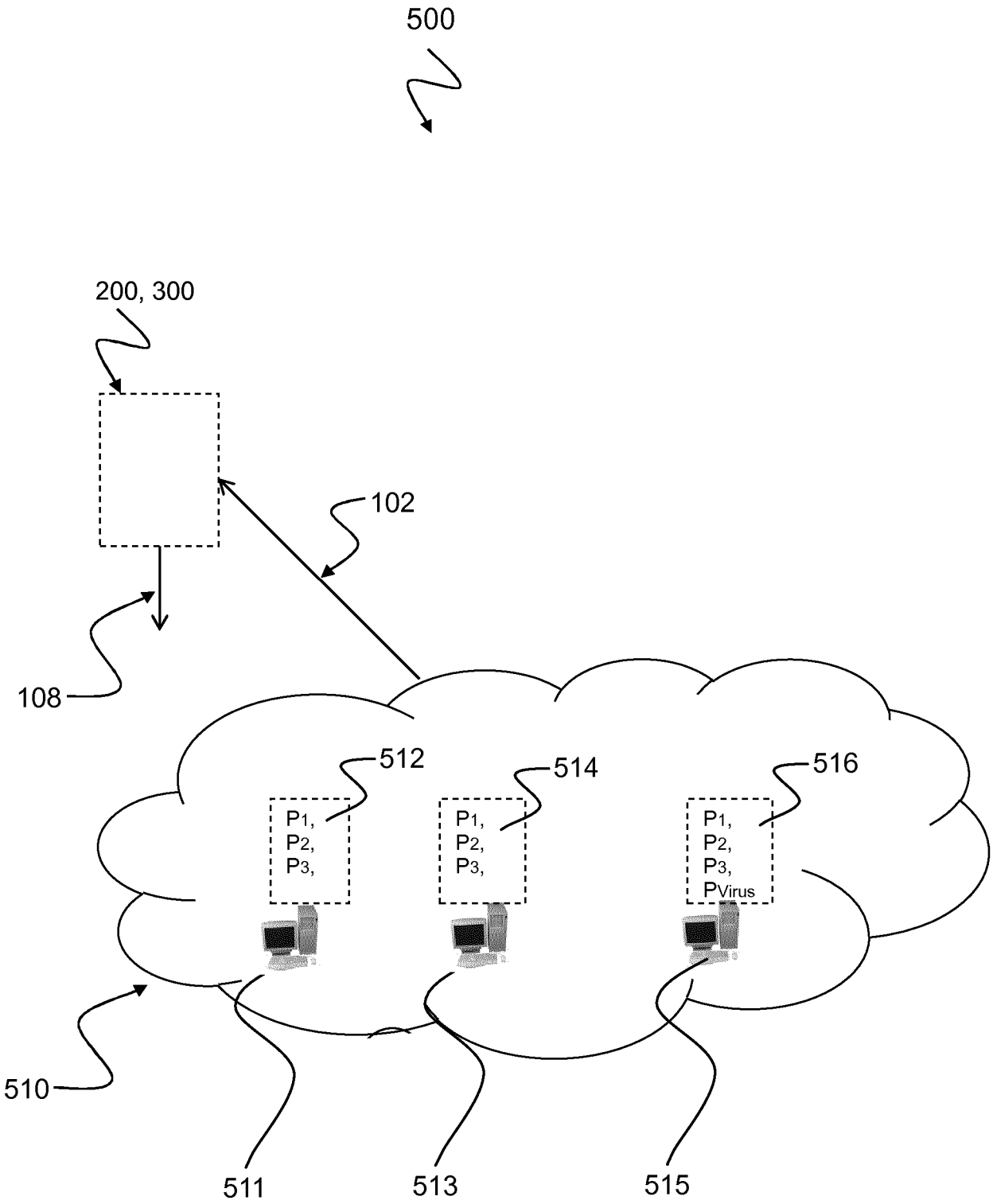
500
200, 300
102
108
512
514
516
P1,
P2,
P3,
P1,
P2,
P3,
P1,
P2,
P3,
PVirus
510
511
513
515

Fig. 5

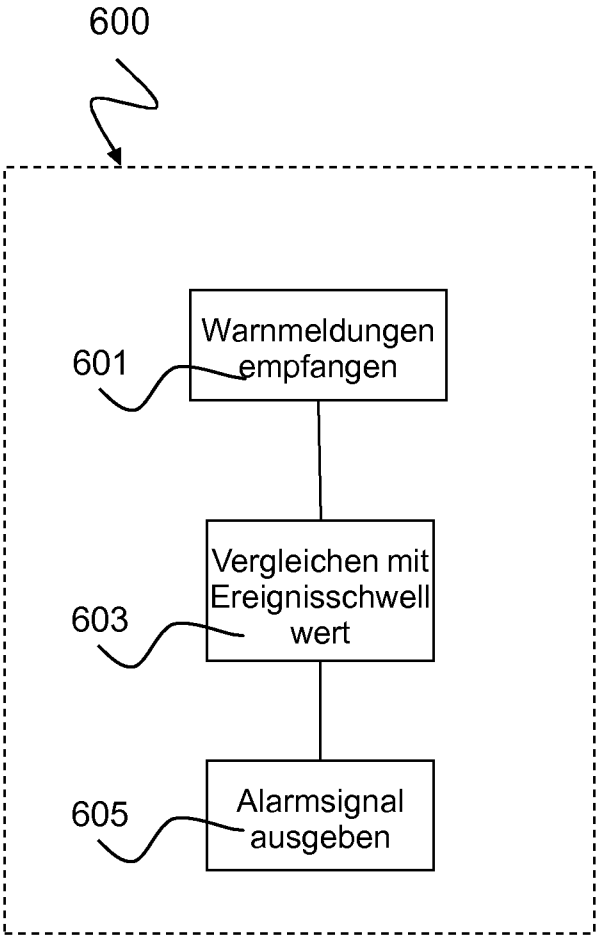
600
Warnmeldungen empfangen
601
Vergleichen mit Ereignisschwellwert
603
Alarmsignal ausgeben
605

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/065547

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/24 H04L29/06
ADD. H04L41/0604

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/082886 A1 (MANGANARIS STEFANOS [US] ET AL) 27 June 2002 (2002-06-27) abstract claim 10 paragraph [0022] paragraph [0031] - paragraph [0048] -----	1-15
A	US 2008/209517 A1 (NIGHTINGALE TODD W [US] ET AL) 28 August 2008 (2008-08-28) abstract paragraph [0029] -----	1-15
A	WO 2013/016245 A1 (TURGEON ANNE-MARIE [US]; EIDELMAN SERGEY [US]; FIGURA MARK [US]; IVANY) 31 January 2013 (2013-01-31) abstract paragraph [0073] -----	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 July 2015	04/08/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hornik, Valentin

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/065547

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002082886 A1	27-06-2002	NONE	
US 2008209517 A1	28-08-2008	NONE	
WO 2013016245 A1	31-01-2013	EP 2734926 A1	28-05-2014
		EP 2734927 A1	28-05-2014
		EP 2734928 A2	28-05-2014
		EP 2735122 A1	28-05-2014
		US 2013182577 A1	18-07-2013
		US 2013182578 A1	18-07-2013
		US 2013182579 A1	18-07-2013
		US 2013182700 A1	18-07-2013
		WO 2013016242 A2	31-01-2013
		WO 2013016244 A1	31-01-2013
		WO 2013016245 A1	31-01-2013
		WO 2013016246 A1	31-01-2013

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2015/065547

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L12/24 H04L29/06
ADD. H04L41/0604

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2002/082886 A1 (MANGANARIS STEFANOS [US] ET AL) 27. Juni 2002 (2002-06-27) Zusammenfassung Anspruch 10 Absatz [0022] Absatz [0031] - Absatz [0048] -----	1-15
A	US 2008/209517 A1 (NIGHTINGALE TODD W [US] ET AL) 28. August 2008 (2008-08-28) Zusammenfassung Absatz [0029] -----	1-15
A	WO 2013/016245 A1 (TURGEON ANNE-MARIE [US]; EIDELMAN SERGEY [US]; FIGURA MARK [US]; IVANY) 31. Januar 2013 (2013-01-31) Zusammenfassung Absatz [0073] -----	1-15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. Juli 2015	04/08/2015

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hornik, Valentin

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2015/065547

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2002082886 A1	27-06-2002	KEINE	
US 2008209517 A1	28-08-2008	KEINE	
WO 2013016245 A1	31-01-2013	EP 2734926 A1	28-05-2014
		EP 2734927 A1	28-05-2014
		EP 2734928 A2	28-05-2014
		EP 2735122 A1	28-05-2014
		US 2013182577 A1	18-07-2013
		US 2013182578 A1	18-07-2013
		US 2013182579 A1	18-07-2013
		US 2013182700 A1	18-07-2013
		WO 2013016242 A2	31-01-2013
		WO 2013016244 A1	31-01-2013
		WO 2013016245 A1	31-01-2013
		WO 2013016246 A1	31-01-2013