Sehr geehrte Damen und Herren,

das ist eine technische Beschreibung, für nicht IT-ler nicht geeignet.

Das ist die Version 0.4, für Hinweise oder Fehlererkennungen bin ich sehr dankbar.

MfG Peter Kämper

PKA® Pre-Crime

Das System zur Vorhersage von Hackerangriffen

oder einfach Ausgerückt:

„Das ist die Glaskugel für Hackerangriffe“

Das PKA® Pre-Crime System ist in der Lage Netzwerkfehler, Produktionsstörungen und Angriffe sowohl von Innen als auch von Außen vorher zu sagen. Somit sind Sie in der Lage ein Schutzkonzept rechtzeitig auf zu bauen und zu testen.

Kurzfassung

Gegenstand der hier vorgestellten Arbeit ist ein patentiertes Vorhersagesystem, PKA® Pre-Crime System von PKA, für IT Angriffe von Außen und Innen. Das System berechnet die Eintrittswahrscheinlichkeit eines Hackerangriffs, die Angriffsarten, die „source“ eines Angriffes und schlägt entsprechende Schutzmöglichkeiten vor. Das System nutzt eine Vielzahl von Eingangsparametern.

Im wesentlichen muss das System den Hintergrund, das Warum eines Angriffes und seine Zusammenhänge erkennen. Erst wenn das Warum geklärt ist, kann eine eine Wahrscheinlichkeit berechnet werden. Das PKA® Pre-Crime arbeitet auf der Basis des Patentes von Peter Kämper.

Grundlagenbeispiel: Frau Merkel hat im Jahr 2015 Besuch vom damaligen Ministerpräsidenten der Ukraine bekommen. Diese Information ist in allen üblichen Tageszeitung und der allgemeinen Presse bekannt gegeben worden. Einige Tage nach dem Besuch wurde in der IT Sicherheitspresse veröffentlicht, dass an jenem Tag die Server der Bundesregierung mit DDOS Angriffe aus Russland überhäuft wurden und einige davon ausfielen.

Sollten sich die Voraussetzungen nicht ändern, ist bei einem zukünftigen Besuch erneut von Angriffen auszugehen bzw. kann berechnet werden. Das gleiche gilt für weitere Besuche bzw. Aktivitäten politischer, wirtschaftlicher oder sozialer Herkunft. Das bedeutet das alle Information der allgemeinen Presse ausgewertet werden müssen um den Hintergrund eines Angriffes zu erkennen, zu berechnen und eine Vorhersage zu berechnen.

Einleitung: „ Vorhersagbarkeiten“

Grundlage einer Prognose bilden die Fakten, bei uns, aus den aktuellen Nachrichten aus aller Welt und aus allen Medien im Zusammenhang mit den tatsächlichen Messwerten beim Kunden.

Die Messwerte beim Kunden bestehen dabei aus einer Zusammenfassung aller Netzwerk-Event aus dem Log-Server, der die Messung auf Unterschiede untersucht. Die Eingangsparameter liegen bei mehreren hundert Tausend Events.

Weitere Eingangsparameter kommen aus speziellen IT Security Foren unter anderem auch von den deutschen und europäischen Behörden.

Aus dem Datenmaterial werden Muster erkannt. Diese dienen der Vorlage für eine mögliche Simulation (spätere Version).

Das PKA® Pre-Crime erkennt historische Muster und berechnet eine erneute Eintrittswahrscheinlichkeit. Das Muster beschreibt die Voraussetzungen, die beim letzten Vorfall, Fehler, Produktionsstörung oder Angriff gegeben waren.

Das System vergleicht die aktuelle Situation mit den bekannten Angriffen. Die Eintrittswahrscheinlichkeit steigt mit je länger das Muster unverändert weiter läuft und keine Veränderungen eingetreten sind.

Die Wahrscheinlichkeit einer Prognose steigt linear zur Laufzeit der Mustererkennung. Kurz vor Eintritt liegt die Wahrscheinlichkeit bei nahezu 100%. Dabei wird eine hohe Zahl von bekannten Angriffsmustern gleichzeitig in Betracht gezogen.

Die Datenbasis ist extrem Umfangreich. Die Log-Daten beim Kunden können mehrere hundert GB betragen und werden automatisch und Iterativ nach Veränderung durchforstet. Hinzu kommen bis zu 10 GB pro Stunde aus den allgemein zur Verfügung stehenden Daten aus dem Internet.

Anforderungen an das PKA® Pre-Crime:

- Berechnung der Eintrittswahrscheinlichkeit
- Vorhersagegenauigkeit
- Methodische Prognosen
- Entscheidungen müssen objektiv sein
- Kausalität
- Wahrscheinlichkeiten
- Abgrenzung zum Zufall und Falschinterpretation
- Objektivität
- Überprüfbarkeit
- Prognostiziertes Ergebnis
- Validität
- Prognose Techniken
- Kurz Mittel Langfristige Prognosen
- Qualitative und Quantifizierung
- Lineare Extrapolation – Vergangenheitswerte in die Zukunft prognostizieren

Generell gilt, das Vorhersagen zu Aktivitäten führen können und sollen.

Grundlagen zur Vorhersagbarkeit

Das PKA® Pre-Crime arbeitet auf der Grundlage zweier Vorhersage-Systeme.

Eines mit der formalisierten Methode, Datenvergleich aus historischen Daten beim Kunden.

Das andere System arbeite mit „Stimmung“ und „Meinung“ und versucht so einen Schwellwert zu berechnen, an dem die Soft-Skill Parameter in ihrer Häufigkeit und Deutlichkeit der Hürde eines Angriffes und deren Gefahren übersteigen.

Generell gilt:

Eine Vorhersage von Angriffen ist nur sinnvoll, wenn die Anzahl der Fehler kleiner ist als die Trefferquote.

Die formalisierte Methode: Historische Daten zur Auswertung

Die Messungen erfolgen über sehr sehr lange Zeiträume.
Eingangssysteme sind unter anderen:
- Firewall
- IDS
- Mail-Server, intern und extern
- Virenmeldung
- Virenschutz-System
- Update-Server
- Logfiles aller Server und Clients
- Alarmsysteme
- ACL (access control listen)
- Nagios
- SIEM

Das PKA® Pre-Crime System zeichnet in den lokalen Netzwerken Angriffe oder Störfälle als Muster auf.

Ein Muster kann dabei aus mehreren hundert Eingangssignalen über einen beliebigen Zeitraum bestehen.
Was der Inhalt oder die Bedeutung des Signales ist, ist zu diesem Zeitpunkt unerheblich. Es werden Muster gespeichert.

Der Endpunkt des Musters in das eingetroffene Ereignis. Dieser Punkt ist sowohl maschinell als manuell definierbar als Triggerpunkt (Störfall im Betrieb, Virenmeldung etc..).

Wenn die Eingangssituation, die zu einem Ereignis zugewiesen ist, wieder eintritt, ist kurz nach dem Eintritt die Vorhersage machbar aber noch nicht sinnvoll, da der parallele Verlauf vom bekannten Muster und der laufenden Mustererkennung zu klein ist.

Je länger ein Muster in der Wiederholung ist, desto größer ist die Eintrittswahrscheinlichkeit. Kurz vor dem Eintritt ist die Wahrscheinlichkeit bei nahe zu 100%.

Das andere Verfahren versucht mittels Internet-Recherche das WARUM zu klären.
Nach einem Angriff oder Störfall sucht das PKA® Pre-Crime im Internet nach allen Zusammenhängen die zum dem Ereignis oder zu dem Kunden gehören.

Die suche ist sehr umfangreich und iterativ. Bei jeder erneuten Suche werden die Such-Parameter angepasst ggf. neu definiert.

Die suche umfasst circa 10 GB pro Stunde, inklusive rekursiver Parametrisierung.

Das System soll automatisch den Hintergrund, das warum klären. Wenn das warum geklärt ist, kann ein Trigger gesetzt werden und ein Muster gespeichert werden.

Wenn, wie weiter oben beschrieben, das Eingangssignal der Besuch des Ministerpräsidenten ist, kann die rekursive Musteraufzeichnung das Eingangssignal zur Mustererkennung definieren und abspeichern.

Zusammenarbeit beider Pre-Crime Vorhersage-Systeme

Der Log-Server sendet seine Auswertungen an das zentrale Das PKA® Pre-Crime System. Das System aktualisiert die „search“ Parameter und arbeitet an der Auflösung des Hintergrundes für die Störung, den Ausfall oder den Angriff.

Erst wenn beide Systeme eine Erkennung zeigen, eine Wahrscheinlich berechnet ist und die Eintrittswahrscheinlichkeit höher als die Fehlerquote ist, meldet das System einen Eintrittspunkt in die Mustererkennung. Der Eintrittspunkt, der Triggerzeitpunkt wird rekursive in den historischen Daten gesucht und ggf. kann ein Rhythmus erkannt werden.

Nach ein Eintritt eines Vorfalles werden alle lokalen Daten und die zentralen Datenauswertungen zur Nachbereitung in das „*post-crime*“ System gesendet und mit anderen Vorfällen weiter verarbeitet.

Zusammenfassung: Die Grundlagen einer Vorhersage sind Datenanalysen aus historischen Daten und Ereignissen.

PKA® Pre-Crime klärt folgende Fragen:

- Warum wurde angegriffen?
- Warum und wie wurde die Produktion gestört?
- Was führte zu dem technischen Fehler?
- Was sind die Ursachen?

Überblick über Angriffe

Laut Wikipedia werden Angriffe ausgeführt um den eigenen Machtbereich zu schützen oder zu erweitern. Ich denke, eine Wortklauberei, was die Definition eines IT Angriffes ist, muss hier nicht geführt werden.

IT Angriffe werden in zwei Gruppen unterteilt. Spionage und Sabotage.

Natürlich gibt es noch weitere untergeordnete Gruppen und Hintergründe, wie Spieltrieb, Mobbing oder pubertierende Jugendliche mit geistigen und sozialen Defiziten.

Vor dreißig Jahren wurden Angriffe in den unteren Layern durchgeführt. Das waren meist technische Angriffe auf der Basis von IP oder TCP. Heute werden die meisten Angriffe auf den Layern 7 (Applikation, meist http) und „8“ (Benutzer) durchgeführt.

Das Verhältnis von Sabotage zur Spionage wechselt häufiger. Zur Zeit ist die Spionage verbreiteter. Sabotage Aktivitäten sind zwar Hochaktuell, siehe Verschlüsselungs-Viren (*Ransom-Ware*), jedoch wird die Spionage durch Regierungen unterstützt und forciert. Die Spionage betrifft nicht nur das Militär sondern verstärkt die Industrie. Über das Thema „*Cyberwar*“ werden wir uns später unterhalten.

So ist seit Jahren bekannt, dass die US Geheimdienste einfach gerne alle Daten sammeln und bei Bedarf. später auswerten. Die Chinesen sind bekannt für Ihre sehr umfangreiche, aber nicht immer erfolgreiche Industriespionage.

Die Russen und die Israelis sind bekannt für ihr hohes technisches Fachwissen und das sie beim Hacken nicht auffallen (wollen). Aber genau so viel Geld geben die Franzosen, Holländer und Engländer für IT Spionage aus. Bei den deutschen Sicherheitsbehörden schaut das bei weiten nicht so aus.

Der Unterschied ist aber im wesentlichen, dass die Geschäftsführung eher bereit ist, in den Sabotageschutz zu investieren. Sicher verständlich, da die Produktionsstörungen sehr viel Geld kosten. Die Kosten der Störungen und eines Produktionausfalles sind einfach zu berechnen.

Die Kosten eines Spionageangriffes hingegen erscheinen unglaubwürdiger und sind schwer zu beziffern.

Aktuelle Angriffe:

Die aktuellsten Information finden Sie bei den Antiviren Herstellen, dem BSI und den üblichen Medien. Ich möchte hier keine weitere Plattform für aktuelle Angriffe eröffnen. Zur Zeit sind leider die *Ransom-Ware* Viren vermehrt unterwegs.

Hier ein paar Tipps zum Schutz bzw. Wiederherstellung

Nebst den üblichen Verfahren, wie Backup, keine Mailanhänge öffnen, Marcos deaktivieren, Mitarbeiter sensibilisieren könnten Sie noch den ACL („access control list“) Schutz verbessern. Mit dem Recht, „creator write only“, kann nur der Ersteller einer Datei, diese überschreiben. Nutzen Sie nicht die Gruppen Rechte „write“, dann darf der Benutzer in dessen Prozess der Virus arbeitet alle Gruppendateien ebenfalls überschreiben. Des Weiteren könnten Sie ein zweites Backup starten, das lediglich die Benutzerstrukturen sichert, nicht aber die ganzen Platten. So können Sie im Fehlerfalle schneller die Daten wieder herstellen.

Es muss entschieden werden, wie bei einer Erpressung gehandelt werden soll. Wenn Sie der Meinung sein sollten, dass Sie lieber bezahlen wollen, ohne das eine realistische Chance besteht, sollten Sie ggf. auch ein wenig mit dem Kauf von Bit-Coins vertraut machen.

Im Fehlerfall muss alles sehr schnell gehen.

Spionageaktivitäten festzustellen ist extrem schwierig und sehr aufwendig. Ich beschäftige mich damit seit 30 Jahren. Die einzige Möglichkeit besteht in der Korrelation der Logfiles und der Benutzeraktivitäten im Zusammenhang mit den Aktivitäten der Firewall und des IDS. Das macht der Log-Server für Sie automatisch. Deshalb können wir aber nicht alle Angriffe sehen.

Messen und Erkennen von Angriffen

Das Messen ist einfach. Die Analyse und der Beweis sind die Herausforderung.

Als Erfinder der PKA Firewall mit integriertem IDS weiß ich, wo auch die Grenzen sind. Ein IDS/IPS zeigt, auf Grundlage eines Mustervergleiches, mögliche Angriffe auf, mehr nicht.

Ob ein Angriff statt gefunden hat, oder nicht, kann das System nicht erkennen. Erst Auswirkungen an den Opfer-Rechner lassen eine Vermutung zu, bieten aber noch keinen Beweis.

Das PKA® Pre-Crime verarbeitet sowohl mögliche Erkennungen im IDS als auch Folgewirkungen am Server/Client, setzt die Relationen zueinander und vergleicht:

- Versuche, Auswirkungen, „drops“ und vieles mehr mit Erfahrungen anderer Angriffe und Störungen.

Log-Server Installation

Die Installation ist einfach: Sie installieren das Betriebssystem und den Log-Server nach Anweisung. Der Log-Server sollte virtualisiert werden und in seiner Größe anpassbar gestaltet werde.

Über Gruppenrichtlinien und Prozesse definieren Sie die Systeme, die ihre Log-files an den Log-Server senden sollen.

Lokal auf den Systemen können Sie die alten Log-Daten überschreiben.

Standardisiert werden Microsoft Logs in Sys-Logs umgewandelt. Der Server verarbeitet alle Typen und Arten von Sys-Logs, egal welches System. Individuell können weitere Systeme hinzugefügt werden: DEC Rechner, IBM Mainframes, Switches, Router, Nagios, SIEM, Management-Systeme, NAC usw..

Die Speicherung der Log-Files erfolgt nach dem aktuellen Bundesdatenschutzgesetz. Eine Zertifizierung ist angestrebt.
Die Löschung erfolgt Kundenseitig im Einvernehmen mit der GF/Vorstand und den Mitarbeitervertretungen.

Der Log-Server

erkennt Anomalien. Ihm ist es dabei egal, was die einzelnen Werte bedeuten. Der Server achtet lediglich auf die Unterschiede. Je länger der Log-Server protokolliert, desto feingliedriger werden die Messdaten und somit werden die Anomalien deutlicher.

Auch eine Anomalie kann über einen sehr langen Zeitraum als „normal“ eingestuft werden.

Beispiel: Wenn Sie nur einmal jährlich Ihre Steuerdaten versenden, dann ist das im ersten Jahr eine Ausnahme, nach einige Jahren wartet das System schon auf diese Aktivitäten, da das Ausbleiben eine Ausnahme wäre (und das ist der Trick bei dem Log-Server).

Somit brauchen Sie auch nicht den Log-Server kontrollieren. Das System lernt selbständig. Das System verfügt über ein „*Kommunikations-Modul*“. Dort wird festgelegt wann und wie Sie informiert werden sollen. Am Anfang braucht das System einige Monate um genügend Daten für die Analyse zu haben. Es macht also keinen Sinn in den ersten Tagen eine Analyse zu erwarten. Sie müssen lediglich die Server-Auslastung automatisiert kontrollieren.

Hintergründe von Angriffen

Ganz einfach: Geld und Macht

Auch hier hat sich in den letzten dreißig Jahren viel verändert. Früher waren viele „Spielkinder“ in den lokalen Netzwerken unterwegs.

So werden einfache „klick“ Versuche durchaus als Angriffsversuch definiert.

Gute Angreifer wollen nicht erkannt werden. Ein Angreifer will arbeiten, damit verdient er/sie sein Geld. Das technische Wissen ist in der Regel sehr hoch.

Eine einfache Sicherheitslücke ausnutzen ist nicht sinnvoll, da diese zeitnah geschlossen werden könnte. Besser ist es eine Funktion in einem Programm, das Internet Zugriff haben darf, zu nutzen. So kann ein veränderter Browser sehr lange die Daten an den Hacker versenden. Meist werden die sogar verschlüsselt versendet. So kann auch ein Kontentschutz-System keine Auffälligkeiten erkennen.

Auch die Aussage der Firewall-Hersteller: „Es gibt mehr interne Angriffe als externe Angriffe “ ist definitiv falsch. Meine Erfahrung zeigen deutlich, dass eine einfache Messung am Server, woher kommt der Angriff, zu ungenau ist.

Ein Angreifer übernimmt in der Regel ein internes System, einfachst durch den Browser, Mediaplayer, Office (Makro´s) oder weitere einfache Services die einen Zugang zum Internet haben.

Von diesem System aus geht der Angreifer mit der Benutzer-Identität des übernommen Systems weiter an die nächsten Rechner. Wenn ich am „nächsten

Rechner“ messe, werde ich einen internen Angriff zählen. Das ist aber nicht richtig.

Jetzt gibt es die besonderen Hintergründe, wie weiter oben gezeigt.
Die Motivation eines besonderen Angriffes, wie der Besuch des Ministerpräsidenten, kann über die Auswertung öffentlicher Medien erfasst werden. Und genau das ist das neue an diesem System.

Erst wenn dieser Hintergrund bekannt ist, kann die Wiederholbarkeit berechnet werden. Auch kann der Rhythmus einer Wiederholung einen eigenen Rhythmus haben.

Im Gegensatz dazu können die vielen Standardangriffen, wie Geldautomaten hacken, Kreditkarten und deren Systeme zu hacken, nur so weit vorher gesagt werden, das sie weiterhin stattfinden werden. Das Pre-Crime System nutzt die Information zu Standardangriffen zwar auch, setzt diese aber im normal Fall in der Priorität nach unten.

Neue Angriffe, wie die „*Fake-news*“ gegen Politiker, kurz vor den Wahlen, um diese zu beeinflussen sind mittlerweile auch nicht mehr.

Ziel:

Es gilt den besonderen Angriff zu erkennen und die Standardschutzmaßnahmen gegen die Standardangriffe aufzubauen.

Aufbau PKA® Pre-Crime

Das PKA® Pre-Crime besteht aus dem lokalen Log-Server und einer Instanz in der PKA Pre-Crime Cloud. Ihre Instanz läuft im gesicherten Modus. Ihre Instanz berechnet ihre Angriffswahrscheinlichkeiten.

Ihre Instanz arbeitet dabei mit der zentralen Instanz zusammen und erhält die Zusammenhänge der zentralen Intelligenz, welche auch durch Ihre Auswertung wiederum weiter steigt.

Bei größeren Netzwerken kann ein eigenes Pre-Crime System vor Ort Sinn machen. Das lokale Pre-Crime erkennt dabei besser die lokalen Gegebenheiten und gleicht eine Vorauswertung mit der zentralen Intelligenz ab.

Das gilt auch für die Log-Server, die bei größeren Netzwerken kaskadiert werden sollten. Erst der Segment Master des Log-Server Segmentes kommuniziert mit dem lokalen oder dem zentralen Pre-Crime Server.

Einsatzgebiete für Vorhersagbarkeiten

Hackerangriffe / Fehler / Störungen in der Produktion

Das Ziel ist eine frühzeitige Erkennung von Gefahren.
Durch die Vorhersage sind Sie in der Lage sich und das Netz vorzubereiten.

Es können sowohl technische Schutzmaßnahmen entwickelt und getestet werden als auch nicht technische Prozesse. Mitarbeiter können auf den Ernstfall trainiert werden, Verhaltensweisen überprüft und Prozesse erstellt werden.

Dabei ist Ihre Motivation sekundär. Es ist egal ob ein Hackerangriff die Produktion stört oder ein Fehler in Ihrem Netzwerk. Letztendlich ist ein Sabotageangriff eines Hacker in seiner Auswirkung gleich. Warum ein Switch, ein Server oder ein Motor ausfällt ist nicht wichtig, wichtiger wäre das Wissen wann geschieht das wieder.

Somit ist das Pre-Crime für den Angriffsschutz genau so wertvoll wie für die für die Produktionssicherung.

Jede Produktionsumgebung ist individuell. In jeder Umgebung können Fehler und Störungen automatisch oder manuell administriert werden. Die Größe Ihrer Umgebung ist dabei nicht entscheidend.

Beim Angriffsschutz: Die Häufigkeit eines möglichen Angriffes ist zwar interessant aber nicht wirklich wichtig. Es reicht ein Angriff mittleren Schadens um das Pre-Crime zu begründen.

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung
DE 10 2015 115 672.5
über die Einreichung einer Patentanmeldung

Aktenzeichen:	10 2015 115 672.5
Anmeldetag:	17. September 2015
Anmelder/Inhaber:	Kämper, Peter, 83233 Bernau, DE
Bezeichnung:	Pre-Crime-Verfahren und -System zur vorhersehbaren Abwehr von Hackerangriffen
IPC:	H04L 12/26

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der Teile der am 17. September 2015 eingereichten elektronischen Dokumente dieser Patentanmeldung unabhängig von gegebenenfalls durch das Druckverfahren bedingten Farbabweichungen.

München, den 6. Oktober 2016
Deutsches Patent- und Markenamt
Die Präsidentin
Im Auftrag

Köllner

A 9161(E)/1.12