ConSecur
[security and consulting]

Künstliche Intelligenz

- White Paper -

Autor: Inigo Urra

EMail: info@ consecur.de
Fon: +49 5931 9224-0

Tel: +49 5931 9224-69

ConSecur
[security and consulting]

Einleitung

In den letzten Jahren ist die Internetaktivität exponentiell gestiegen. Es sind mehr Daten generiert worden als je zuvor. Einer der Hauptgründe für diese Revolution ist das "Internet der Dinge", das dazu beigetragen hat, Tausende von verschiedenen Geräten zu verbinden.
Weiterhin machen die technologischen Fortschritte das „Internet der Dinge" immer schneller und zuverlässiger und somit erscheinen neue Dienste wie zum Beispiel Streaming-Video-Webseiten, neue Multiplayer-Spiele, Datenaustausch Dienste....

Die meisten Firmen nutzen neue Technologien in ihrer täglichen Arbeit. Selbst kleine Firmen kommen nicht mehr ohne eigene Webseite oder Computer in ihren Büros aus. In großen Firmen wird diese Entwicklung noch offensichtlicher, wo die „Business Intelligence" hilft bessere Entscheidungen zu treffen und Leute aus verschiedenen Ländern zusammenarbeiten und streng vertrauliche Informationen teilen.

Diese Vorteile verursachen jedoch ein unerwünschtes Problem. All diese Informationen müssen gesichert werden. Da die erzeugte und gespeicherte Datenmenge immer größer wird, wächst auch das Interesse diese Datenmenge zu entwenden oder zu modifizieren. Die große Menge an Daten erschwert die Erkennung verdächtiger Aktivitäten.

Einer der gegenwärtigen Einschränkungen im Angriffserkennungsprozess ist der Fakt, dass viele menschliche und wirtschaftliche Ressourcen benötigt werden (viel mehr Ressourcen als den Angriff auszuführen). Die Unternehmen investieren viel Geld damit die Angriffe zu entdecken. Gute Analysten sind schwer zu bekommen und deren Arbeitskapazität ist begrenzt. Selbst der beste Analyst braucht viel Zeit um jeden Angriff zu analysieren. Nach vielen Stunden Arbeit ist er müde und mürrisch und macht schnell Fehler.

ConSecur
[security and consulting]

Eine neue Lösung ist erforderlich, um dieses Problem zu lösen. Eine Lösung, bei der mehr Daten schneller und effizienter analysiert werden können.

Eine mögliche Lösung ist Aufgaben zu automatisieren und nur die wichtige Arbeit dem Analysten zu überlassen. Um dies zu erreichen, ist eine intelligente Technik notwendig, da die meisten Aufgaben nicht trivial sind. Eine andere Möglichkeit ist die Menge der Arbeit zu reduzieren. Dies kann erfolgen durch die Reduzierung der Anzahl der falschen Positiven, die durch die Angriffserkennungssysteme erzeugt worden sind.

Unser Vorschlag ist beide Ziele mit maschinellen Lerntechniken zu erreichen. Zum einen werden wir die Erstellung und Abstimmung der Angriffserkennungsregeln automatisieren. So wird die Zeit gespart, die benötigt wird, um die Angriffserkennungsregeln zu erstellen und abzustimmen. Weiterhin wird die Schaffung von besseren Qualitätsregeln die Anzahl der falschen Positive reduzieren, um unnötige Arbeit für den Sicherheitsbeauftragten zu vermeiden.

Ein Prototyp ist implementiert worden, um die Wirksamkeit dieses Ansatzes zu testen. In dieser Arbeit wird die Arbeitsweise dieses Prototyps erläutert. Im ersten Abschnitt wird der aktuelle Stand beschrieben. Nachfolgend werden die verschiedenen Maschinenlerntechniken und die verwendete Protokollquelle erläutert. Weiterhin wird die Funktionsweise des Prototyps erläutert. Schließlich werden die Schlussfolgerungen und die nächsten Schritte zur Erstellung eines autonomen Angriffserkennungssystems vorgeschlagen.

ConSecur
[security and consulting]

Inhalt

ConSecur
[security and consulting]

Ausgangssituation

Heute werden SIEM Systeme genutzt, um verdächtige Aktivitäten zu erkennen. Ein SIEM System (Security Information and Event Management System) ist ein Programm, dass in der Lage ist alle Informationen zu sammeln, die durch die verschiedenen Geräte im Netzwerk erzeugt worden sind. Jedes Gerät sendet Protokolle seiner Tätigkeit und somit die Möglichkeit jede Aktion in unserem System ausfindig zu machen.

Dennoch ist die eigentliche Aufgabe die verdächtigen Aktivitäten unter der riesigen Summe an normaler Aktivität zu erkennen. Eine Reihe von Regeln werden genutzt, um zu bestimmen welche Aktivitäten verdächtig sind und im Detail analysiert werden müssen. Diese Regeln sind im SIEM von einem Fachmann konzipiert und umgesetzt. Sobald die Regeln funktionieren, korrelieren die notwendigen Informationen und ein Alarm erfolgt wenn einer der Regeln Anwendung findet.

Problematisch wird es, wenn viele Variablen an der Implementierung der Regel beteiligt sind. Das menschliche Gehirn ist nicht dazu in der Lage große Menge an Informationen zur gleichen Zeit zu verwalten.

Ein Computer ist für diese Art von Aufgaben besser geeignet, da er eine große Anzahl von Variablen verwaltet und mehr Schwellenwerte überprüft als ein Mensch (zumindest in einer angemessenen Zeit).

Dies kann mit einem kleinen Beispiel leicht gezeigt werden. Nehmen wir an, wir wollen die nächste Regel umsetzen:

„Mehrere fehlgeschlagene Anmeldungen vom selben Nutzer“

Auch wenn es einfach aussieht, mehr als die erwarteten Informationen können korreliert werden, um die Genauigkeit zu verbessern. Der erste Schritt ist die Anzahl der fehlgeschlagenen Logins in einem vorgegebenen Zeitrahmen zu bestimmen (zum Beispiel 5 fehlgeschlagene Logins in einer Minute). Dies ist jedoch keine leichte Aufgabe, denn wir wollen unser System sicher halten ohne den Analysten mit falschen Positiven zu überladen.
Es sollten jedoch mehr Informationen berücksichtigt werden aufgrund der Tatsache, dass es riskanter ist, wenn ein Administrator eine brutale Attacke erleidet als ein normaler Nutzer. Auch die Zeit, in der die fehlgeschlagenen Logins auftreten, ist von großer Bedeutung. Ein fehlgeschlagener Login während der Nacht ist eigenartiger als während der Arbeitszeit.

ConSecur
[security and consulting]

Mehr Informationen können ebenso in Betracht gezogen werden. Doch wenn mehr Variablen vorgestellt werden, gibt es auch mehr Grenzwerte und es ist für den Menschen schwerer zu verwalten.

Unser Vorschlag ist das maschinelle Lernen zu nutzen, um genauere Regeln zu schaffen.
Der erste große Vorteil dieses Ansatzes ist die Zeitersparnis, um die Regeln zu implementieren und über die Zeit zu bestimmen. Der zweite Vorteil ist, dass genauere Regeln zu weniger falschen Positiven führen in dem die Arbeit der Analysten bei gefährlichen Angriffen fokussiert wird.

In den nächsten Abschnitten werden die verfügbaren Maschinenlerntechniken und die verwendete Logquelle erläutert.

ConSecur
[security and consulting]

1 Maschinelles Lernen

Maschinelles Lernen ist der Teil der künstlichen Intelligenz, der dem Computer die Fähigkeit gibt so zu lernen wie ein Mensch es tun würde. Wie ein Kind lernen kann Autos von Motorrädern zu unterscheiden, kann unser Programm ebenso die spezifischen Eigenschaften eines jeden Fahrzeugs lernen und klassifizieren.

Um unser Ziel zu erreichen, stellen wir Ihnen Informationen über unser Programm zur Verfügung. Nach dem Beispiel der Autos und Motorräder liefern wir einige Charakteristiken, damit der Computer die Unterschiede kennenlernt. Wir können zum Beispiel die Anzahl und das Gewicht der Räder von jedem Fahrzeug als Charakteristik auswählen. Nachfolgend eine Tabelle mit Informationen:

ID	Anzahl Räder	Gewicht	Klasse
1	2	300	Motorrad
2	4	1300	Auto
3	2	250	Motorrad

Tabelle: Fahrzeug Training Datensatz

Jede Spalte enthält Informationen über eine konkrete Eigenschaft von jedem Fahrzeug. In Tabelle 1 stellen zum Beispiel die ersten Spalten die Anzahl der Räder von jedem Fahrzeug dar. Jede Spalte beschreibt ein „Attribut“.

Es gibt jedoch eine Ausnahme, die letzte Spalte nennt sich “Klasse” und bestimmt zu welchem Typ jedes Fahrzeug gehört (in unserem Beispiel sind die möglichen Typen “Auto” und „Motorrad”).

In jeder Zeile der Tabelle werden die Informationen von jedem Fahrzeug eingetragen. Jede Zeile nennt sich „Instanz“.

Sobald wir alle Informationen gesammelt haben, können verschiedene maschinelle Lerntechniken je nach Ziel angewendet werden. Im Wesentlichen gibt es drei verschieden maschinelle Lerntechniken:

- überwachtes Lernen
- nicht überwachtes Lernen
- halb überwachtes Lernen

ConSecur
[security and consulting]

1.1 Überwachtes Lernen

Im überwachten Lernen enthält der Computer alle in der Tabelle 1 gezeigten Informationen. Zum einen bekommen wir die Klasse von jedem der Instanzen, die zur Unterscheidung verwendet werden. Zum anderen werden die normalen Attribute verwendet, um die Unterschiede zwischen den Instanzen der einzelnen Klassen zu lernen.

Das Programm extrahiert das Wissen aus den Instanzen. Hier wird ein „Modell" erzeugt, das genutzt wird um neue eingehende Instanzen zu klassifizieren. Es gibt viele unterschiedliche Modelle. In unserem Fall ist das Sinnvollste ein Modell, das aus einer Reihe von Regeln besteht:

WENN Anzahl der Räder = 4 DANN ist es ein Auto

Gewicht > 400 KG DANN ist es ein Auto

SONST ist es ein Motorrad

Dieses Regelwerk wird verwendet, um neue eingehende Instanzen zu klassifizieren. Zum Beispiel, wenn das Programm weitere Informationen über das Fahrzeug erhält:

ID	Anzahl Räder	Gewicht	Klasse
5	2	275	???

Tabelle 2: Eine neue eingehende Instanz

Nach den generierten Regeln wird unser Programm es als Motorrad klassifizieren, da es 2 Räder hat und das Gewicht weniger als 400 kg beträgt.

Diese Art vom maschinellen Lernen wird hauptsächlich verwendet, um Felder vorherzusagen. In diesem Beispiel ist es verwendet worden, um die Art des Fahrzeugs vorherzusagen. Der Nachteil dieser Lerntechniken ist, dass bereits klassifizierte Instanzen benötigt werden.

ConSecur
[security and consulting]

2 Nicht überwachtes Lernen

In diesem Fall hat unser Programm nur die Attribute jeder Instanz. Die Klasse steht für den Lernprozess nicht zur Verfügung:

ID	Anzahl Räder	Gewicht	Klasse
1	2	300	---
2	4	1300	---
3	2	250	---

Tabelle 3: Nicht überwachtes Training

Schlussfolgernd bedeutet dies, dass unterschiedliche Lernmethoden verwendet werden müssen. Nachstehend die wichtigsten Punkte, die wir nun machen können:

• **Clustering (Zusammenlagerung):** Wir können Gruppen mit ähnlichen Instanzen machen.
Sobald eine neue Instanz kommt, werden wir sie mit den verschiedenen Clustern vergleichen. In Tabelle 3 können wir zwischen zwei Clustern unterscheiden. Die beiden Instanzen, die mit den Motorrädern korrespondieren, haben ähnliche Werte und werden in einem Cluster zusammengefasst. Die letzte Instanz wird in einem separaten Cluster gesetzt.

• **Anomalie-Erkennung:** Das Ziel ist die Instanzen zu erkennen, die sich von den anderen unterscheiden. Sie werden Anomalien oder Ausreißer in unseren Daten sein. In Tabelle 3 ist der Ausreißer die zweite Instanz (diejenige, die mit dem Auto korrespondiert). Diese Werte unterscheiden sich von den anderen beiden Fällen (korrespondieren mit den Motorrädern).

ConSecur
[security and consulting]

3 Halb überwachtes Lernen

In dieser letzten Lerntechnik werden überwachtes und nicht überwachtes Lernen verbunden. Wir werden dem Computer die Klasse einiger Instanzen zur Verfügung stellen, aber nicht von allen:

ID	Anzahl Räder	Gewicht	Klasse
1	2	300	Motorrad
2	4	1300	Auto
3	2	250	---

Tabelle 4: Halb überwachtes Lernen

Diese Lerntechniken werden die bereits klassifizierten Instanzen sowie die Attribute der anderen nutzen, um das Modell zu erstellen.

ConSecur
[security and consulting]

4 Apache Webserver Logs

Ein SIEM System bekommt Protokolle von mehreren Quellen. Jede Protokollquelle liefert eine andere Art von Information und in einem anderen Format. In unserem Fall verwenden wir eine einzige Logquelle, um unseren Prototyp so einfach wie möglich zu machen. Wir verwenden einen Apache Webserver als Protokollquelle. Auch wenn es ein einfaches Beispiel ist, wird es ausreichen, um die Wirksamkeit dieses Ansatzes zu demonstrieren.

Der Apache-Webserver zeichnet viele Attribute für jede vom Nutzer gestellte Frage auf.

- IP (Internetprotokoll)
- Benutzername
- Datum
- HTTP Methode
- Angeforderte Ressource
- Größe der angeforderten Ressource
- Antwortcode

Diese Informationen werden jedoch in einer unverarbeiteten Form gesammelt. An dieser Stelle ist es für die meisten Maschinenlerntechniken immer noch nicht sinnvoll. Die Information müssen zusammengefasst werden und die interessanten Attribute für den Lernprozess extrahiert werden.

Jede Zeile der Protokollquelle stellt eine Anforderung eines Nutzers dar. Dabei kann jeder Nutzer mehrere Anfragen stellen. Um die Informationen zu kumulieren, können wir Folgendes berechnen: Anzahl der Verbindungen von jedem Nutzer gemacht, Anzahl der angeforderten Bytes...Dies sind die Attribute von jedem Nutzer, die genutzt werden, um sie zu klassifizieren.

Dieser Schritt wird einer der Wichtigsten sein. Die Auswahl der richtigen Attribute bestimmt den Erfolg unseres Programmes. Als Analogie mit dem Beispiel im letzten Abschnitt werden wir versuchen die verschiedenen Fahrzeuge zu klassifizieren. Wenn wir die Farbe als Attribut wählen, wird unser Programm nicht korrekt arbeiten, da wir gelbe Autos und gelbe Motorräder vorfinden. Wenn wir jedoch die Anzahl der Räder des Fahrzeugs, das Gewicht oder eine Kombination von beiden wählen, werden wir mit unserem Programm eine ziemlich hohe Genauigkeit erzielen.

Die gleiche Situation haben wir in der Angriffserkennung. Die gewählten Attribute müssen korrekt sein, um eine hohe Genauigkeit zu erzielen.

ConSecur
[security and consulting]

Nach der Auswahl und Zusammenfassung der Informationen werden die gesammelten Attribute in einer Tabelle gesammelt und sehen wie folgt aus:

IP	Anzahl der Verbindungen	Anzahl angeforderte Daten
1.1.1.1	10	8
2.2.2.2	2000	2000
3.3.3.3	13	13

Tabelle 5: Extrahierte Attribute der Webserver Quellen

ConSecur
[security and consulting]

5 Unser Prototyp

Unser Prototyp besteht aus zwei verschiedenen Teilen. Der erste Teil ist ein neuer Angriffsdetektor. Hier werden nicht überwachte Maschinenlerntechniken genutzt, da wir versuchen etwas zu erkennen, was vorher noch nicht gesehen worden ist. Der Computer selbst muss das seltsame Verhalten erkennen. Der zweite Teil ist die Erkennung bereits bekannter Angriffe. Das System erlernt die bekannten Angriffsmuster und erkennt sie, sobald ein neuer Angreifer sie ausführt. In diesem letzten Teil werden überwachte Lerntechniken angewendet.

5.1 Unbekannte Angriffserkennungen

Der erste Teil unseres Prototyps ist zuständig für die Erkennung von unbekannten Angriffen.
Dies ist nützlich, um Zero-Day-Angriffe zu erkennen. Für diesen Teil werden nicht überwachte Lerntechniken genutzt, da wir noch keine klassifizierten Beispiele der Angriffe haben. Deshalb ist das Ziel Anomalien oder Ausreißer zu erkennen.

Die Idee dahinter ist, dass ein Angreifer ein anderes Nutzerverhalten hat als ein normaler Nutzer. Er wird Handlungen machen, die sonst niemand macht. Unser Prototyp sucht nach Ausreißern, Nutzer mit einem anderen Nutzerverhalten. Dann wird der Analyst überprüfen, ob das Verhalten unüblich aber normal ist oder ob es wirklich ein Angriff ist.

Nachdem wir dies auf unsere Testdaten angewendet haben, sind viele Ausreißer erkannt worden: Nutzer aus fremden Ländern, Nutzer mit vielen fehlgeschlagenen Verbindungen,....

Die hier generierten Regeln können in das SIEM System aufgenommen werden. Dort werden die seltsamen Verhaltensweisen vom System erkannt.

ConSecur
[security and consulting]

5.2 Bekannte Angriffserkennung

In diesem zweiten Teil werden bereits bekannte Angriffe aufgespürt. Da hier das überwachte Maschinenlernen genutzt wird, haben wir das Verhalten einiger Nutzer klassifiziert und eine Tabelle ähnlich wie die untenstehende erstellt:

IP	Anzahl Verbindungen	Anzahl angeforderte Dateien	Klasse
1.1.1.1	10	8	normal
2.2.2.2	2000	2000	verdächtig
3.3.3.3	13	13	normal

Tabelle 6: Klassifizierte Nutzer

Sobald unser Trainingsdatensatz fertig überwacht ist, können maschinelle Lerntechniken angewendet werden, um das Muster der einzelnen Aktivitäten kennenzulernen. Die erzielten Ergebnisse waren sehr erfolgreich und erreichten zwischen 85% und 95% Genauigkeit.

Diese Regeln können auch in das SIEM System mit aufgenommen werden, um die bekannten Angriffe zu erkennen. Die Idee ist den Trainingsdatensatz zu füttern und zu aktualisieren, um die generierten Regeln an den Änderungen im System anzupassen. Die Regeln werden periodisch angepasst, um die Grenzen in jedem Moment genau anpassen zu können. Auf diese Weise wird das Regelgenerierungsprogramm flexibler als die aktuellen, statischen Regeln.

ConSecur
[security and consulting]

6 Schlussfolgerung und nächste Schritte

Schlussfolgernd können wir nach dem Test des Prototyps sagen, dass das Nutzen von maschinellen Lerntechniken zur Cybersicherheit eine mögliche Lösung sein kann, um die eigentlichen Einschränkungen in diesem Bereich zu lösen.
Mit den richtigen Attributen und maschinellen Lerntechniken können genauere Regeln erstellt werden. Wir sind jedoch immer noch in den ersten Schritten der Einbeziehung dieser Techniken. Es sollten noch viele Verbesserungen vorgenommen werden bevor ein autonomes Angriffserkennungssystem in Betracht gezogen werden kann.

Die erste Verbesserung ist verschiedene Logquellen wie eine Firewall, einen Proxy... zu integrieren. Die größte Herausforderung ist hier die Informationen auf ein verständliches Format für den Computer zu normalisieren. Jedes Gerät protokolliert die Informationen anders und das gleiche Feld kann in vielerlei Hinsicht dargestellt werden.
Ein interessanter Weg um dieses Problem zu lösen ist eine Funktionalität zu integrieren um die unterschiedlichen Logquellenformate und Attribute zu erlernen. Nach dem Erlernen sollte das Programm in der Lage sein neue Logquellen zu erhalten und die bereits bekannten Attribute wie die IP-Adresse, Termine, etc. automatisch zu erkennen.

Der nächste Schritt ist die Aktivität von jedem Nutzer auf eine nützliche und effiziente Weise zu verbinden. Wie wir gesehen haben, ist die Auswahl der Attribute wichtig und die riesige Menge an Daten, mit denen das Programm zu tun hat, erfordert eine intelligente Auswahl.
Nicht alle Nutzer sind gleichermaßen gefährlich. Somit sollten auch nicht alle Nutzer mit der gleichen Sorgfalt analysiert oder mit der gleichen Menge an Informationen bearbeitet werden. Eine mögliche Lösung ist die Nutzer abhängig von ihrem Risiko zu priorisieren und die Gefährlichsten detaillierter zu analysieren.

Nach diesem Prozess wird unser Programm alle notwendigen Informationen für die Erkennung neuer Angriffe haben. Wie wir bereits gesehen haben, sind nicht überwachte Lerntechniken für diese Aufgabe sehr effektiv und wir brauchen keine klassifizierten Daten, um diese maschinellen Lernalgorithmen anzuwenden. Allerdings müssen wir noch die bereits bekannten Angriffe erkennen und dafür brauchen wir markierte Daten. Die Idee hier ist es die Trainingsdaten mit den besten Instanzen zu diesem Zweck zu aktualisieren und zu erhalten. Der erste Schritt dafür ist den Prozess der Etikettierung neuer Daten zu automatisieren, wenn neue Angriffe entdeckt werden. Eine automatische Auswahl der besten Instanzen für das Training wäre auch hilfreich.

ConSecur
[security and consulting]

An dieser Stelle sind wir in der Lage bekannte Angriffe sowie neue Angriffe zu erkennen. Der nächste Schritt ist die Wahl der besten maschinellen Lerntechnik. Wahrscheinlich ist die beste Lösung eine spezielle Klassifikation für jede Lerntechnik zu entwickeln. Eine automatische Auswahl der besten Maschinenlerntechnik sowie deren Parameter muss durchgeführt werden.

Viele Verbesserungen könnten in die Erkennung mit aufgenommen werden. Unser Prototyp erkennt nur, ob es sich um normale oder verdächtige Aktivitäten handelt. Eine detaillierte Klassifikation könnte besser funktionieren und sollte in der Lage sein die verschiedenen Angriffstypen zu klassifizieren.

Sobald das Programm einen Nutzer eingestuft hat, sollte es in der Lage sein die besten Aktionen aufgrund der Ergebnisse wie das Blockieren einer IP, das Löschen eines Nutzers...vorzuschlagen. Außerdem muss aufgezeigt werden wie diese Entscheidung getroffen worden ist, da dies eine große Hilfe für den Analytiker ist.

Wie wir sehen können, sind dies die ersten Schritte der neuen Angriffserkennungstechniken. Mit etwas Zeit und Arbeit werden neue Erkennungswege entwickelt. Diese werden in der Lage sein mehr Angriffe zu erkennen und zwar in einer noch genaueren Weise über die riesige Aktivität der Netzwerke.