Whitepaper

telent
service • commitment • value

Systeme zur Angriffserkennung Anomaly Detection

Das IT-Sicherheitsgesetz 2.0 schreibt den Einsatz von Systemen zur Angriffserkennung für KRITIS-Bereiche fest. Aber nicht nur dort sind Werkzeuge zur Anomaly Detection, also solche, die die Netzwerkkommunikation permanent auf ungewöhnliche Kommunikationsmuster hin überwachen, sinnvoll. Wie arbeiten solche Systeme und wann ist ihr Einsatz angeraten? Darauf geben wir in diesem Whitepaper Antworten.

Angriffserkennung - Baustein moderner Securitykonzepte

Netzwerke sind mittlerweile hochkomplexe Gebilde, in die eine Vielzahl an Geräten eingebunden sind. Die Anzahl der Endpunkte wächst stetig. Viele technische Komponenten nutzen standardisierte Kommunikationsprotokolle und können mit Druckern, Smartphones und weiteren Geräten kommunizieren. Mit der Vernetzung vieler Teilnehmer, die durch das Phänomen Industrie 4.0 immer schneller voranschreitet, und dem Wunsch auf alles online zugreifen zu können, ergeben sich neue Angriffspunkte und Schwachstellen.

Malware wird immer komplexer

Zugleich werden Cyberangriffe und die dabei eingesetzte Schadsoftware immer komplexer und stellen Securityverantwortliche vor immer größer werdende Herausforderungen. Ein Beispiel wäre hier die Malware Stuxnet oder Industroyer, die, aufgrund der Komplexität, nicht erkannt worden sind. Die schier unglaubliche Flexibilität dieser (damals) einmaligen Schadsoftware zeigte auf, dass die zu dieser Zeit gängigen Sicherheitsmechanismen nicht mehr ausreichen.

Die Schadsoftware gelangt über einen von mehreren Microsoft Windows Zero Day Exploits (MS08-067 Schwachstelle, Windows Shell vulnerabilty (CVE-2010-2568) und einen Zero Day Bug im Printspooler) in die IT- und letztendlich auch die OT-Infrastruktur und verbreitet sich dann durch das Netzwerk weiter. Hierbei besteht die Möglichkeit verschiedene, abhängig von der der jeweiligen Infrastruktur und den ergriffenen Sicherheitsmaßnahmen, Schadcode-Module nachzuladen.

Im zweiten Schritt springt Stuxnet auf andere Systeme, darunter auch leittechnische Systeme, über. Zudem verfügt die Schadsoftware über verschiedene Mechanismen um sich selbst upzudaten oder die erlangten Informationen auf einen Webserver zu übertragen. Sie kann also genutzt werden, um sensible Daten abzuschöpfen – ein klassischer Fall von (Industrie-)Spionage. Im leittechnischen System angekommen, beobachtet die Software die Abläufe und klinkt sich in die Kommunikation ein. Als Man-in-the-Middle ist es für die Software nun ein leichtes, Produktionsdaten und Abläufe zu manipulieren.

Angriffserkennung - Neue Lösungen für neue Bedrohungen

Kurzum – die neuen Gegebenheiten, die mit der voranschreitenden Verwirklichung der Industrie 4.0 einhergehen, bedingen auch eine Anpassung und Erweiterung der zu treffenden Security-Maßnahmen.

Ein Baustein in einem sich veränderten Security-Konzept für die Produktion stellen Systeme zur Angriffserkennung - auch als Anomaly Detection Systeme bekannt - dar.

Ein System zur Angriffserkennung ist in der Lage, das Verhalten, dass die oben beschriebene Schadsoftware an den Tag legt als abnormales Angriffsmuster zu erkennen und dementsprechend zu reagieren.

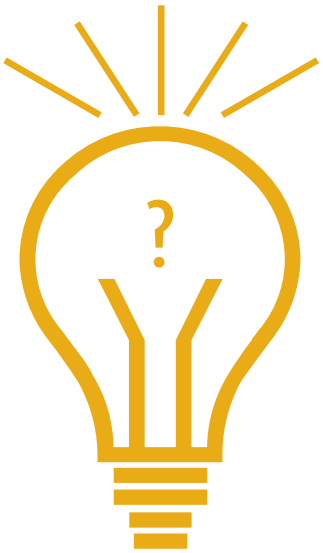
Zudem fallen dem System weitere Abweichungen von bekannten Mustern auf, wie etwa das Nachladen von Komponenten, das Installieren oder Manipulieren von Treibern oder der Versuch eine Verbindung ins Internet herzustellen, darstellen.

Moderne Anomaly Detection Systeme erkennen zudem Angriffe auf bekannte Schwachstellen und ermöglichen darüber hinaus, alle Teilnehmer der Netzwerk-Kommunikation zu identifizieren sowie diese über ein entsprechendes Monitoring zu visualisieren.

Ein positiver Nebeneffekt bei der Nutzung ist, dass diese Lösungen die zuständigen Mitarbeiter unterstützen und zur Entlastung der entsprechenden Stellen führen. Damit sind die Zeiten vorbei, in denen sich ein Administrator täglich durch tausende von Logfiles wühlt. Das System bereitet diese automatisch auf und alarmiert bei Bedarf die entsprechenden Stellen umgehend – etwa wenn Auffälligkeiten auftreten.

Was ist eine Anomalie eigentlich?

Denkansätze - Anomaly Detection in der Cybersecurity



Anomaly Detection Systeme bieten, in Ergänzung zu „klassischen“ Sicherheitsmaßnahmen, wie etwa Virenscanner oder VPN, einen Mehrwert für die Security-Landschaft. Doch was ist eigentlich eine Anomalie und wie funktioniert diese Art der Angriffserkennung überhaupt?

Dazu ein paar Denkansätze:

- Was ist normal?
- Was ist abnormal?
- Wann soll alarmiert werden?
- Wie geht das System mit bestimmten Ereignissen um?
- Welche Anomalien führen zu kritischen Zuständen und gefährden meine IT – oder Produktionslandschaft?

Anomalie - Die Abweichung

Als Anomalie bezeichnet man das Abweichen von der Norm oder anders gesagt, ein unerwartetes Verhalten. Von einem Netzwerkgerät, das plötzlich ein anderes Kommunikationsprotokoll nutzt, bis hin zu Netzwerkverkehr, der eine neue Route nimmt, sind viele unterschiedlich geartete Anomalien möglich. Anomalien können vielseitig gestrickt sein und sind immer abhängig vom Blickwinkel.

Um diesen Sachverhalt zu verdeutlichen, verlassen wir kurz die Welt der Informationstechnologie. Nehmen wir eine Bank und deren Mitarbeiter. Während hier ein Mitarbeiter in Freizeitkleidung eher auffällt, ist dieses äußerliche Auftreten in einem Kindergarten normal. Somit ergeben sich, je nach Sichtweise, unzählige unterschiedlich gelagerte Anomalien. Die Kunst hierbei besteht im Erfassen des „Normalzustandes“.

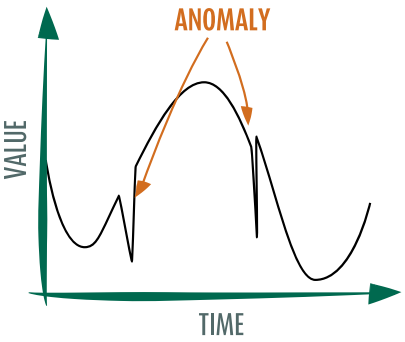
Die Kunst des Lernens

Um überhaupt feststellen zu können was eine Anomalie ist, muss die eingesetzte Lösung erst feststellen, wie der „Normalzustand“ aussieht. Und das bei unterschiedlichen Netzwerk-Strukturen, die sich, je nach Einsatzzweck und Branche, maßgeblich unterscheiden.
Auch hierzu eine Analogie, um dieses Problem zu verdeutlichen: Eine Bäckerei nutzt andere Werkzeuge, Abläufe und Zutaten als ein Sushi Restaurant. Bei der Bäckerei wird das Nutzen von Algenblättern als Anomalie wahrgenommen, während es für das Sushi Restaurant essentieller Bestandteil des Geschäftes ist. Hier schließt sich der Kreis zur Technik. Während es im Unternehmen X beispielsweise völlig normal ist, dass Virtual Network Computing (VNC) genutzt wird, ist es im Unternehmen Y nicht gewünscht.
Zur Ermittlung des Normalzustandes beobachtet ein Anomaly Detection System die gesamte IT- und OT-Architektur und das idealerweise ohne sich bemerkbar zu machen. Meist geschieht dies durch passive Sensoren, die den mitgeschnittenen Datenverkehr an eine zentrale Aufnahmestelle übermitteln. Die Aufnahmestelle speichert sämtliche Informationen und lernt somit den Netzwerkalltag kennen.

Nachhilfe

Das System zur Angriffserkennung kennt nun den Netzwerkalltag und muss, mit Unterstützung des Menschen, noch individuell angepasst werden. Gehört es zum Beispiel zum Inbetriebnahme-Prozess einen PC initial, also ohne das Eingreifen eines Menschen (Zeroconf) in Betrieb zu nehmen und während der Lernphase wurde kein Rechner in Betrieb genommen, würde ein Gerät mit Zerconf als Anomalie gemeldet werden. Aus diesem Grund ist es von essentieller Bedeutung, dass das System Nachhilfe erhält und ein solcher Vorgang ebenfalls als „normal“ deklariert wird. Hierbei sollte beachtet werden, dass das System nur so gut und granular arbeiten kann, wie der Mensch es ihm vorgibt. Ein Lehrer, der nur oberflächliches Wissen hat, wird nie in der Lage sein, seinem Schüler tiefergehendes Wissen zu vermitteln.
Ohne Kenntnis darüber welche kritischen Zustände möglich sind und was meinen Betrieb gefährden kann, ist es nicht möglich, dem System dies beizubringen.

Vom Schüler zum Lehrer



Nach Abschluss der Lernphase verfügt das Anomaly Detection System über das Wissen, das es für seine tägliche Arbeit benötigt. Ab diesem Zeitpunkt erkennt das System auftretende Fehler und Angriffsmuster automatisch. Von einfachen Angriffen bis hin zu Zero-Day-Exploits, die in der Regel abnorme Abläufe oder komplexe, dem System nicht bekannte, Muster beinhalten.
Außerdem können auch bewusste Manipulationen oder nicht erlaubte Datenzugriffe durch eigene Mitarbeiter erkannt und entsprechend nachverfolgt werden. Ein Nachinstallieren von neuen Komponenten oder das Herstellen einer Verbindung nach außen, von einem Client, der dies noch nie getan hat, wird ebenfalls festgestellt. Es entsteht eine große Bandbreite an Use–Cases, die mithilfe von Anomaly Detection Systemen abgedeckt werden können.

Zusammenfassung

Durch die Möglichkeit von Alarmierungen bei einem Verdacht auf eine Anomalie und bei der vereinfachten Darstellung der erkannten Anomalien unterstützt ein Anomaly Detection System, die für Cybersecurity zuständigen Mitarbeiter bei Ihrer Arbeit in einem Unternehmen. Hierdurch können nicht nur die Mitarbeiter effizienter eingesetzt, sondern auch ein Reporting sauber umgesetzt werden.
Das Assetmanagement kann ebenfalls optimiert werden, da die Lösung Informationen zu Hardwarekomponenten vorhält, die sich visualisieren und auswerten lassen. Wenn ein solches System ernsthaft genutzt wird, kann es eines der mächtigsten Security Werkzeuge in der IT–Landschaft werden und den Menschen lehren, wie wichtig es ist, Abweichungen und unerwartete Verhalten zu erkennen.
Insgesamt lässt sich also konstatieren, dass Anomaly Detection Systeme helfen, das Security-Niveau einer IT- und OT-Landschaft enorm zu erhöhen.

Sie haben Fragen zu Systemen zur Angriffserkennung, Anomaly Detection oder zur Netzwerkanalyse? Gerne beraten wir Sie individuell und finden gemeinsam die beste Lösung zum Schutz Ihrer Systeme.

telent
service • commitment • value

telent GmbH
Gerberstraße 34 | 71522 Backnang
Tel.: +49 7191 900-0
E-Mail: info.germany@telent.de

KORAMIS
Cybersecurity by telent

www.telent.de