

IDENTIFIKATION

- ❑ Monitoring aller relevanten Objekte im Netzwerk, wie Firewalls, Router, Switches, Betriebssysteme oder Anti-Virus Software.
- ❑ Ständige Analyse von Logdaten in Echtzeit, um Netzangriffe, verdächtiges Verhalten und Verletzungen von Sicherheitsrichtlinien aufzuspüren.
- ❑ Priorisierung der Informationen und Meldungen abhängig von kritischen Werten und vordefinierten Anwendungen, der Tageszeit und spezifischen Geschäftsprozessen oder Zielsetzungen.

ALARME und REPORTING

- ❑ Sofortige Alarmierung des zuständigen Personals oder Managements über mögliche Probleme per Email, Mobil-Telefon, Pager oder PDA.
- ❑ Definition und Generierung situationsspezifischer Mitteilungen für das zuständige Personal, basierend auf der Klassifizierung des Vorfalls.
- ❑ Erfüllung von regulatorischen Vorgaben mit Hilfe von mehr als 250 vordefinierten Reports für Management, Revision und IT-Audit.

REAKTION

- ❑ Aktive Reaktion auf Ereignisse mit automatisierten Tätigkeiten wie IP-Adresse blockieren, Routing auf Null setzen oder Netzwerkinterface sperren.
- ❑ Reaktion auf interne Vorfälle, Insider-Angriffe oder Verletzungen von Sicherheitsrichtlinien durch Sperren der Benutzerkonten, Ändern der Zugriffsrechte, Anhalten von Applikationen oder Herunterfahren von Diensten.
- ❑ Auswahl aus Hunderten von vordefinierten Regeln zusätzlich Erstellung kundenspezifischer Regeln für Ihre besondere IT-Umgebung.

WAS IST LOS IN IHREM NETZ?



DAS PROBLEM

Der Backbone Ihres Netzwerkes besteht aus einer Vielfalt an spezialisierten sicherheitsrelevanten Devices und Systemen, wie Firewalls, Router, Switches, Virens Scanner oder auch Intrusion Detection Systemen. Tagtäglich erzeugen diese Systeme eine wahre Flut an Logdaten und Events. Dieser unüberschaubare Ozean von Millionen an Daten enthält geschäftskritische Informationen, die für Ihr Unternehmen lebenswichtig sind, bzw. von regulierenden Behörden abverlangt werden. Die Aufgabe des Sammelns, der Überwachung und der Reaktion auf diese Informationen und Ereignisse kann ohne den Einsatz eines modernen Sicherheits-, Informations- und Event Management Systems (SIEM) nicht bewältigt werden.

Traditionelle Werkzeuge für die Analyse von Logdaten und auch das Netzwerkmanagement können beim Aufspüren krimineller Handlungen nur bedingt und sehr eingeschränkt, weil zeitversetzt helfen. Die verwendete Technologie ist von Natur aus passiv. Leider berichten die meisten Unternehmen, die solche „einfachen“ Lösungen einsetzen, dass diese Werkzeuge zu wenig leisten, um die Sicherheit der Netzwerke zu erhöhen. Einen Beitrag zur aktiven Verteidigung des Netzwerkes können diese Lösungen überhaupt nicht bieten.

DIE LÖSUNG

Systeme zur simplen Logdaten-Ablage und einfache forensische Werkzeuge (meist „hausgebacken“) können heutzutage nicht mehr die richtige Antwort sein. In einer Welt, in der der letzte Wurm das gesamte Internet in weniger als 10 Minuten überflutete, zählen Sekunden. Die Analyse in Echtzeit, direkt im Speicher, ist der Schlüssel zum Erfolg. Wenn das jetzt mit einer unternehmensweiten Netzwerkansicht kombiniert wird, können Sie sofort auf Netzangriffe und Insider-Attacken in Netzgeschwindigkeit reagieren. Es ist die Aufgabe Ereignisse zu erkennen, zu analysieren, zu korrelieren und sofort entsprechende Aktionen einzuleiten. TriGeo Network Security hat die reine passive Verwaltung von Logdaten mit völlig verzögerten Analyse in eine proaktive, echtzeitfähige Netzverteidigung verwandelt.

Nur die Lösung TriGeo SIM verbindet Logdaten-Echtzeitanalyse und Ereigniskorrelation mit Endpunktsicherheit zu einer einzigartigen „Active Response“ Technologie. Das Resultat ist eine noch nie dagewesene Netzwerktransparenz, -Sicherheit und -Kontrolle.

GESCHÄFTS-ANFORDERUNGEN

IT-Umgebung Vielfalt und Komplexität

Die heutige IT-Umgebung ist vielfältig und komplex: Netzwerkgeräte, Betriebssysteme, Anwendungen und und und... Immer mehr Hersteller produzieren eine überwältigende Anzahl von Alarmen und Berichten, die leider den Blick auf das Ganze verwischen. Unsicherheit macht sich breit. TriGeo SIM ist die strategische Lösung, die diese Daten sammelt, standardisiert, analysiert und Prioritäten für die Security erstellt; und zwar für Ihre gesamte IT-Umgebung.

Komplexe Vorschriften und Standards

Heutige Unternehmen kommen kaum noch hinterher, die rechtlichen Vorschriften, wie z.B. EuroSOX, Basel II, PCI, GLBA, NCUA, FDIC, HIPAA, SOX um nur einige zu nennen, einzuhalten. TriGeo SIM ist beides, eine einzigartige Netzwerkverteidigungs-Technologie UND eine abgenommene revisionssichere Lösung, die die Anforderungen an das Log-Management und das Event-Monitoring gewährleistet und Sie mit audit-sicheren Reports unterstützt und Ihre Unternehmens-Policies umsetzt und Sie bei der Einhaltung von SLA's unterstützt.



Personal und Ressourcen sind begrenzt

TriGeo wurde für das wirkliche Leben designed und gebaut. Nur sehr wenige Unternehmen können sich den Luxus eines 24/7-Sicherheits-Centers leisten, wenn sie überhaupt das Personal dazu haben. Die TriGeo SIM kommt als fertige Appliance. Für die Installation, Konfiguration oder auch Tuning stehen wir, Xnet Communications, Ihnen gerne zur Seite.

Mit dem Einsatz von TriGeo können Sie einen zusätzlichen Mitarbeiter mit echtzeit-netzwerk-analyse Fähigkeiten in Ihrem Team begrüßen.

Policy Implementierung und die Insider-Herausforderung

Die vergangenen Jahre zeigten ein Wachstum an Datendiebstahl, verursacht insbesondere durch eigene, interne Mitarbeiter. Ausgehend von dem finanziellen Anreiz sensitive, perso-

nenbezogene, oder auch Firmendaten illegal zu veräußern, müssen Sie erkennen, dass hier eine neue Herausforderung auf Sie zukommt. Mit der TriGeo SIM können Sie kontinuierlich Ihr Netz monitoren und aktiv dafür sorgen, dass Ihre IT-Richtlinien eingehalten werden. Verstöße können Sie nun zum Zeitpunkt des Entstehens feststellen, nachverfolgen und aktiv bekämpfen.

Frühwarnsystem und sofortige Reaktion

Neue Herausforderungen, wie undokumentierte Fehler, Zero-Day Attacks, Würmer und Viren entstehen täglich neu. Die Attacks werden zudem immer intelligenter, mutieren und überfluten alles. Wenn ein Produktsystem oder –Dienst versagt, leidet das komplette Unternehmen und verursacht häufig auch erhebliche finanzielle Schäden. TriGeo verwendet patentierte Technologien, die es Ihnen erlauben sicherheitsrelevante Vorfälle in Sekunden (nicht Tagen!) zu erkennen und reagieren.

Über TRIGEO

TriGeo Network Security bietet Systeme für Sicherheitsinformationen und Event Management (SIEM). Speziell designed für das Corporate-Umfeld. Das vielfach ausgezeichnete Produkt kombiniert Echtzeit-Log-Analysen, Event-Korrelation und Endpunkt-Sicherheit mit einer einzigartigen aktiven Reaktions-Technologie. Das Ergebnis ist: völlige Netzwerktransparenz, -Sicherheit und Reaktionsfähigkeit.

TriGeo hat ihren Einsatz über vertikale Märkte hinweg: Gesundheitswesen, Behörden, Produktion, Handel und Medien/Unterhaltung. TriGeo wurde 2007 von Gartner als führend im Bereich SIEM und dem „Magischen Quadrant“ positioniert.

Im deutschsprachigen Raum (D/A/CH) wird das Produkt TriGeo über den Platinum Partner Xnet Communications GmbH vertrieben. Xnet ist seit über 10 Jahren als Systemintegrator und Distributor im Bereich Netzwerke und Security für namenhafte Corporate-Kunden tätig. Das Produktportfolio wird mit eigenen Softwareprodukten abgerundet und ergänzt.

Nehmen Sie Kontakt auf

Für weitere Informationen, oder auch für eine Live-Demo der Produkte, wenden Sie sich bitte an Xnet Communications GmbH – Vertrieb unter Tel.: 040 – 89 702 – 0 oder besuchen Sie www.xdsnet.de.



TriGeo
Network Security

Holen Sie sich TriGeo und gewinnen Sie den Überblick!

