

ArcSight Express

Erstklassiger Schutz für mittelständische Unternehmen

Research 013-040109-01

Überblick

Es ist leider eine Tatsache, dass Unternehmen aller Größen in unserer modernen, vernetzten Welt einer ganzen Reihe von Angriffen ausgesetzt sind. Malware, Datenverstöße und gesetzliche Vorschriften (sowie damit verbundene Strafen) nehmen immer mehr zu. Unglücklicherweise sind die meisten mittelständischen Firmen nicht in der Lage, für einen entsprechenden Zuwachs an Sicherheitspersonal zu sorgen; und in vielen Fällen wird dieses sogar abgebaut. Solche Unternehmen verfügen weder über spezialisierte Mitarbeiter noch über Sicherheitsadministratoren, und viele Firmen haben fast kein Sicherheitswissen oder überhaupt keine personellen Ressourcen in diesem Bereich.

Dennoch müssen diese Firmen wie ihre größeren „Geschwister“ auch ihre wichtigen Daten verwalten und schützen. Dazu gehören neben Finanzdaten auch vertrauliche Kundendaten und geistiges Eigentum. Diese Unternehmen unterliegen oft den gleichen gesetzlichen Vorschriften wie ihre größeren Wettbewerber, die ihrerseits aber viel größere Sicherheits- und Compliance-Budgets sowie mehr Ressourcen vor Ort zur Verfügung haben.

Ohne adäquates Sicherheitswissen und mit nur wenigen spezialisierten Sicherheitsadministratoren an Bord müssen mittelständische Unternehmen einen eigenen Weg finden, wie sie ihre Daten schützen können, ohne sich dabei zu überheben. Welche Sicherheitsüberwachungslösung auch eingesetzt wird: Sie muss die „Schwerarbeit“ übernehmen können und in der Lage sein, durch Automatisierung und integriertes Sicherheitswissen die Arbeit des IT-Administrators erheblich zu vereinfachen.

In diesem Papier werden die zentralen Sicherheits- und Compliance-Herausforderungen beschrieben, mit denen mittelständische Unternehmen in der heutigen Zeit zu kämpfen haben. Dabei wird die ArcSight Express-Familie, eine neue Appliance zur Compliance- und Sicherheitsüberwachung von ArcSight, vorgestellt. Organisationen, die einer zunehmenden Bedrohung ihrer Netzwerke und ihrer kritischen Daten ausgesetzt sind, deren Möglichkeiten und Wissen auf diesem Gebiet aber begrenzt sind, steht mit ArcSight Express eine einfache, automatisierte und kostengünstige Lösung zur Verfügung. ArcSight Express ist ein echter Sicherheitsexperte: In das Produkt ist eine umfangreiche Regel- und Berichtsammlung integriert, mit der die kritischsten Sicherheits- und Compliance-Probleme gelöst werden können, mit denen ArcSight-Kunden konfrontiert werden. Bei ArcSight Express wird insbesondere die Tatsache berücksichtigt, dass die meisten Unternehmen nicht die Mittel und Ressourcen haben, eine eigene spezialisierte Sicherheitsabteilung aufzubauen. Mit ArcSight Express wird die Erkennung von und die Benachrichtigung über Sicherheitsvorfälle automatisiert, und die IT-Mitarbeiter müssen sich nur noch darauf konzentrieren, wie sie am besten auf die Sicherheitsvorfälle reagieren.

Organisationen, die ArcSight Express einsetzen, erfreuen sich einer verbesserten Sicherheit und Compliance zu günstigeren Kosten mit einer automatisierten und kompetenten Sicherheitsanalyse und Überwachung, die bereits unmittelbar nach der Installation voll einsatzbereit ist.

Herausforderungen für mittelständische Unternehmen

Ein Unternehmen, das neben seinem Hauptsitz noch verschiedene externe Standorte und mehrere Hundert Mitarbeiter hat, setzt in der Regel eine Reihe ganz unterschiedlicher Sicherheitstechnologien ein, darunter Firewalls, Antivirenprogramme, Systeme zur Intrusion Prevention (IPS), Remote Access und VPNs. Jedes dieser Produkte wird über eine eigene Konsole gesteuert, und es kostet Ressourcen und Zeit, diese Systeme kontinuierlich funktionsbereit zu halten. Eine aktuelle Analyse durch das Small Business Technology Institute hat gezeigt, dass mehr als die Hälfte der befragten Unternehmen weder über die finanziellen Mittel, noch über das Fachwissen oder die nötigen personellen Ressourcen verfügen, um geeignete Sicherheitsverfahren umzusetzen.

Administratoren haben oft nicht die Zeit oder das erforderliche Fachwissen, um die Tausende, ja manchmal Millionen Ereignisse, die von diesen Systemen erzeugt werden, in angemessener Weise zu überwachen. Das führt dann dazu, dass Sicherheitsvorfälle wie Viren, Würmer und Datenverstöße zwar gemeldet werden, dass aber die damit verbundenen Alarme in einem Meer von Ereignissen verloren gehen und lange Zeit unbeachtet bleiben. Daher besteht für Unternehmen, die kein spezielles Sicherheitspersonal haben, das Ziel darin, Sicherheitsvorfälle hinreichend früh sichtbar zu machen, damit Ausfallzeiten, Datenverluste oder schwerwiegende Beeinträchtigungen des Unternehmens verhindert werden können.

Der erste Schritt hin zu einer effektiven Sicherheit

Eine ausgezeichnete Möglichkeit zur Erhöhung der Effektivität einer Investition in Sicherheitslösungen ist, die Netzwerkaktivitäten sichtbar zu machen. Oft genug ist dies recht schwierig, und Organisationen müssen hier Prioritäten setzen und sich auf die wahrscheinlichsten Gefahren konzentrieren. Als Marktführer auf dem Gebiet des Security Information and Event Management (SIEM) verfügt ArcSight über umfangreiche Erfahrungen in der Zusammenarbeit mit mehr als 1.000 Organisationen, und wir konnten feststellen, dass viele Firmen am häufigsten mit einem oder mehreren der folgenden Probleme zu kämpfen haben:

- Bot-, Wurm- und Virenangriffe
- Erkennung von Hackerangriffen
- Bandbreitenverschwendung und Richtlinienvletzungen
- Nicht autorisierter Zugriff auf Anwendungen oder Systeme
- VPN-Sneak-Angriffe
- Auswirkungen auf Systeme und Benutzer
- Nicht bestandene Audits, Bußgelder und andere Strafen

Bot-, Wurm- und Virenangriffe

Malware kann bei Unternehmen, ihren Kunden und Partnern potenziell enormen Schaden anrichten. Computer Economics beziffert die Kosten, die Unternehmen 2007 allein durch Malware entstanden sind, auf über 13 Mrd. US-Dollar. Einige

der schlimmsten Viren haben sich in Minutenschnelle verbreitet und weltweit zu immensen finanziellen und betrieblichen Schäden geführt. Kleinere Unternehmen sind anfälliger gegen Virenangriffe, da Virendefinitionen u. U. nicht mehr aktuell sind oder Aktualisierungen von Antivirenprogrammen fehlschlagen. In anderen Fällen kann es sein, dass kritische Server bereits infiziert sind, dass die Infektion aber nicht bemerkt wird, wenn der Server keine Anzeichen einer Infektion zeigt. Die Fehler und Infektionen sind in den AV-Logs versteckt, sodass sie von Serveradministratoren nicht bemerkt werden. Das hat zur Folge, dass geschäftskritische Systeme Angriffen weitestgehend schutzlos ausgesetzt sind. Bots und Keylogger können die Ursache für Datenverluste sein, insbesondere für den Verlust von Kennwörtern und Identitätsdiebstahl. Im PCI-DSS-Standard (Payment Card Industry Data Security Standard) werden Unternehmen insbesondere dazu aufgefordert sicherzustellen, dass Antivirensoftware eingesetzt und regelmäßig aktualisiert wird. Wenn fehlgeschlagene Aktualisierungen nicht bemerkt werden, steigt das Risiko für die Systeme, und die Anfälligkeit der Firmen gegen Malware wächst, obwohl die Firmen glauben, rundum geschützt zu sein.

Erkennung von Hackerangriffen

Organisation stehen unter permanentem Sperrfeuer durch Angriffe von außen, insbesondere Hacker- und Phishing-Angriffe. Hacker können in das Netzwerk eines Unternehmens eindringen, wenn die Sicherheitstechnologien nicht richtig funktionieren, und es kann sehr schwer sein, solche Angriffe zu erkennen. Ungewöhnliche Netzwerk- oder Kontoaktivitäten sind häufig ein Indiz für einen versuchten Hacker-Angriff. Beispielsweise können viele fehlgeschlagene Anmeldungen in kurzer Zeit an einem oder mehreren Systemen auf einen „Brute-Force-Login“ hindeuten, bei dem ein Hacker wiederholt versucht, unter Verwendung gängiger Kennwörter auf ein Konto zuzugreifen. Theoretisch sollten solche Angriffe leicht zu erkennen sein. Die Praxis zeigt jedoch, dass hierzu eine umfassende Überwachung und effektive Analyse erforderlich ist.

Bandbreitenverschwendung und Richtlinienverletzungen

Die nicht autorisierte Verwendung von Netzwerkressourcen eines Unternehmens hat in vielfacher Hinsicht Auswirkungen auf dessen Umsatz. Benutzer, die auf nicht autorisierte Websites zugreifen, Inhalte herunterladen, über Peer-to-Peer-Netzwerke miteinander kommunizieren und persönliche Dienste auf den Unternehmensnetzwerken ausführen, behindern die betrieblichen Abläufe und können sogar einen kompletten Ausfall der Online-Präsenz eines Unternehmens verursachen. Eine hohe Bandbreitenverschwendung kann ebenfalls auf die potenzielle Anwesenheit von Malware hindeuten.

Nicht autorisierter Zugriff auf Applikationen oder Systeme

Nicht autorisierte Kontoaktivitäten sind potenziell die größte Gefahr für jede Organisation. Wenn die Anmeldeinformationen für persönliche Systeme gefährdet sind oder von mehreren Benutzern gemeinsam verwendet werden, verliert das Unternehmen nahezu komplett die Fähigkeit, seine Infrastruktur und die kritischen

Vermögenswerte zu schützen oder Kontoaktivitäten überhaupt zu identifizieren. Kleinere Organisationen leiden häufig unter Hunderten von Ausspäh-Scans oder bösartigen Zugriffsversuchen, ohne sich dieser überhaupt bewusst zu werden, und typischerweise ist auch weder der Ursprung noch das Ziel solcher Angriffe bekannt.

VPN-Sneak-Angriffe

Bei einem Fernzugriff (Remote Access) werden gefährdete Punkte geöffnet, über die Bedrohungen in das System eindringen können. Insbesondere betrifft dies Würmer, Viren, Spyware, Hackerangriffe oder Identitätsdiebstahl. Bei kleineren Unternehmen kann es vorkommen, dass die Fernverbindung an einem oder an beiden Endpunkten ungeschützt oder unvollständig eingerichtet ist. Dies ist auch der Fall, wenn sich Benutzer von unsicheren Netzwerken (in Hotels, Cafés, Flughäfen, von Messen, von zuhause bzw. vom eigenen PC) aus mit einem System verbinden. Fernzugriff setzt das Netzwerk einer Bedrohung durch bösartige Benutzer und bösartige Software aus.

Auswirkungen auf Systeme und Benutzer

Wenn es zu einem Angriff gekommen ist, können Organisationen oft nicht ohne Weiteres feststellen, welche Systeme und Benutzer tatsächlich so betroffen sind, dass Abhilfemaßnahmen eingeleitet werden müssen. Das kann dazu führen, dass die Malware von einigen wenigen Benutzercomputern nicht entfernt wird und sich von dort aus wieder auf die bereits gesäuberten Systeme ausbreiten kann. Was man hier braucht, ist ein klarer Bericht, in dem aufgeführt wird, welche Systeme von einer speziellen Bedrohung betroffen sind, damit die Kosten und die Zeit für Abhilfemaßnahmen besser kontrolliert werden können.

Nicht bestandene Audits, Bußgelder und andere Strafen

Die hohen Kosten für die Einhaltung einer immer weiter steigenden Zahl an gesetzlichen Vorschriften und branchenspezifischen Regulatorien wirkt sich insbesondere bei kleineren Unternehmen stark auf den Umsatz aus. Ein typisches Unternehmen, das an einer US-Börse gelistet ist, seine Geschäfte über das Internet betreibt, für staatliche, lokale und Bundesbehörden arbeitet und mehrere Hundert Mitarbeiter hat, muss auf die Einhaltung von mehr als einem Dutzend gesetzlicher Vorschriften, branchenspezifischer und interner Regelungen achten, darunter SOX, PCI, Funktionstrennung, IT-Sicherheit, Vertraulichkeit von Mitarbeiterdaten und verschiedene andere Richtlinien.

Die Forderung nach der Einhaltung all dieser Vorschriften und Richtlinien schließt die Sammlung von Informationen aus den verschiedenen, in diesem Papier bis hierhin beschriebenen Quellen, deren Zusammenstellung in entsprechenden Berichten und die Auswertung potenziell mehrerer Hundert solcher Berichte im Hinblick auf bedeutungsvolle Informationen ein. Diese Aufgabenreihenfolge ist für die meisten Organisationen einfach nicht zu bewältigen, was dazu führt, dass entweder ihre Compliance-Bemühungen ins Leere laufen oder dass sie wirklich nur das absolute Minimum leisten können, um die Einhaltung der Compliance-Anforderungen zu demonstrieren.

Wir stellen vor: ArcSight Express

Mittelständische Unternehmen sind einem enormen wirtschaftlichen Druck ausgesetzt, ihre Kundenbasis erweitern, effizienter arbeiten, Kosten zu senken und Prozesse automatisieren zu müssen, um geschäftlich überlebensfähig zu sein. Dieser Druck wird oft durch eine immer komplexere IT-Infrastruktur aufgefangen, was dann aber meist bedeutet, dass die eingesetzten Sicherheitstools und -verfahren nicht mehr angemessen sind. Für Unternehmen, die trotz eines geringeren Budgets und Zeitdrucks ihre Sicherheit und Compliance verbessern möchten, bietet ArcSight Express eine erstklassige Sicherheitsüberwachung in einer einfachen, kostengünstigen Appliance-Lösung.

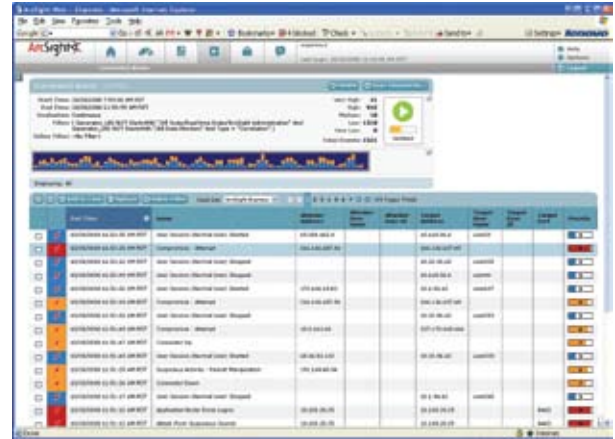
ArcSight Express ist eine SIEM-Appliance-Lösung, mit der Aktivitäten, die unternehmensweit an den Firewalls, Servern, Desktop-Computern, Antivirenprogrammen, IPS-Systemen, beim Fernzugriff, auf VPN-Geräten, Routern, Switches und anderen Verbindungsgeräten auftreten, erfasst und überwacht und entsprechende Berichte erstellt werden können. Das Produkt ist speziell auf die Bedürfnisse von Unternehmen zugeschnitten, denen nur begrenzte Ressourcen für die Installation und die fortlaufende Verwaltung zur Verfügung stehen. Mit ArcSight Express kann jedes Unternehmen auftretende Probleme einfach erkennen, da die sicherheitsrelevanten Informationen an einem zentralen Ort zusammengefasst werden.

In ArcSight Express sind die erforderlichen optimalen Verfahrensweisen (Best Practices) und ein umfassendes Sicherheitswissen integriert. Dieses Wissen liegt in Form von Regeln, Alarmen, Berichten und Dashboards vor, die auf die häufigsten, bereits beschriebenen Risikobereiche ausgerichtet sind. In dem Produkt wird dieses Wissen mit einer auf dem Markt führenden Korrelationsfunktion kombiniert. Auf diese Weise entsteht eine umfassende, leicht zu bedienende und wartungsarme Lösung, die sich auf die Aufgaben rund um die Überwachung der Geräte, des Netzwerks, der Infrastruktur und der Einhaltung der Compliance konzentriert, mit denen kleinere Unternehmen am häufigsten konfrontiert werden. Bei ArcSight Express wird insbesondere die Tatsache berücksichtigt, dass die meisten Unternehmen nicht die Mittel und Ressourcen haben, eine eigene spezialisierte Sicherheitsabteilung aufzubauen. Mit ArcSight Express wird die Erkennung von und die Benachrichtigung über Sicherheitszwischenfälle automatisiert, und die IT-Mitarbeiter müssen sich nur noch darauf konzentrieren, wie sie am besten auf die Sicherheitsvorfälle reagieren.

ArcSight Express gibt es als Ein-Box- oder Zwei-Box-Lösung, und das Produkt besteht aus den folgenden Schlüsselkomponenten:

Die Korrelations-Appliance von ArcSight Express

Herzstück von ArcSight Express ist eine erstklassige, auf dem Markt führende Korrelations-Engine. Bei der Korrelations-Engine wird eine Vielzahl von Methoden eingesetzt, mit denen Ereignisse, die potenzielle Sicherheitsprobleme darstellen können, schnell erkannt werden.



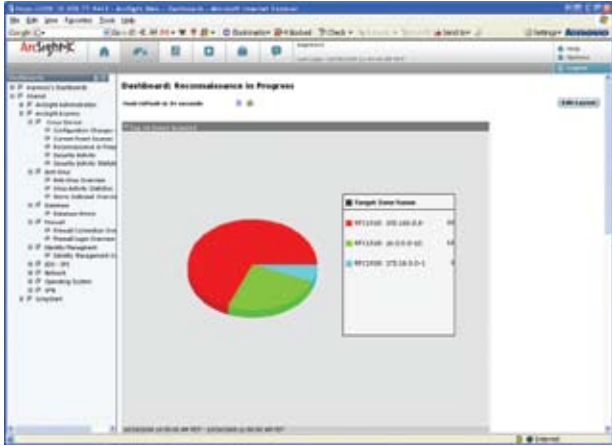
Die Korrelationsregeln berücksichtigen viele Attribute, anhand derer die Wichtigkeit der einzelnen Ereignisse bestimmt werden kann. Dazu gehören eine historische Trendanalyse, die Relevanz von Vermögenswerten, der Angriffsverlauf, eine statistische Analyse und andere Techniken. Dadurch wird sichergestellt, dass die Millionen irrelevanter Ereignisse herausgefiltert werden und dass Administratoren nur über die kritischen Vorfälle informiert werden. Daraufhin können sich diese auf die echten Probleme konzentrieren, ohne sich vorher durch Berge von Log-Daten wühlen oder jede einzelne der Konsolen für die vielen unterschiedlichen Sicherheitsprodukte überwachen zu müssen.

Integrierte aussagekräftige Korrelationsregeln, Dashboards und Berichte

ArcSight Express enthält einen Satz von Regeln, Berichten, Alarmen und Dashboards, mit denen kleinere Sicherheitsteams unmittelbar nach der Installation und ohne Berichtsvorlauf eine umfassende Sichtbarkeit der Systemumgebung erlangen können. Für die ohnehin stark belasteten IT-Teams entfällt so die Notwendigkeit, den entsprechenden Inhalt definieren und auf einer Entwicklungsplattform bereitstellen zu müssen.

ArcSight Express ist ein echter Sicherheitsexperte, der sich von Beginn an um alle beschriebenen Aufgaben kümmern kann:

- **Bots, Würmer und Virenberichte** – Neue Zero-Day-Exploits werden entdeckt, bevor sie Schaden anrichten können. Die Systemumgebung wird geprüft, und alle Viren, die sich darin ausbreiten, werden unschädlich gemacht. Es werden Berichte zu AV-Definitionen und fehlgeschlagenen AV-Aktualisierungen erstellt.
- **Erkennung von Hacker-Angriffen** – Das Produkt erkennt, woher Angriffe von außen kommen und welche Hosts/Server Ziel des Angriffs sind; es bietet Alarme für Netzwerkgeräte mit unterschiedlichen Alarmtypen und hält Firewall-Regeln und IDS/IPS-Signaturen aktuell.



Virus bzw. sein Wiedereindringen in die Systeme der Organisation zu verhindern.

- **Unterstützung für Compliance-Audits** – Das Produkt stellt in einfacher Weise die Informationen zusammen, die Auditoren und Führungskräfte benötigen, es demonstriert die Einhaltung von Richtlinien, erkennt Compliance-Verletzungen im Voraus, es identifiziert Lücken und behebt diese.

Die ArcSight Express Log-Management-Appliance – Ein effizienter, selbstverwaltender Speicher

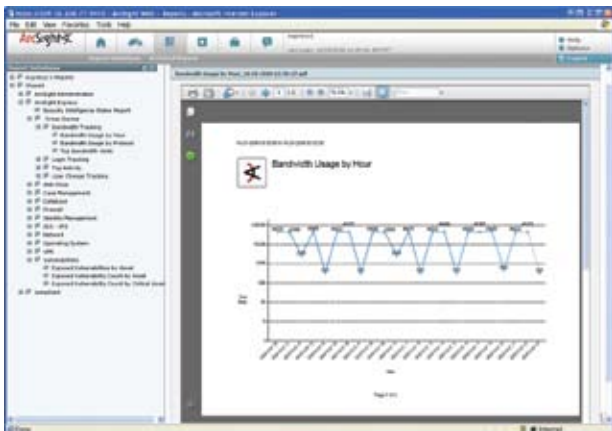
In den Compliance-Regelungen werden üblicherweise Aufbewahrungszeiträume für Ereignis-Log-Daten festgelegt. ArcSight Express beinhaltet eine komplette, auf dem Markt führende Log-Management-Appliance, die eine langfristige Datenaufbewahrung ermöglicht. Die Log-Daten werden in einem effizienten, komprimierten Format gespeichert, und sie können jederzeit schnell durchsucht und analysiert werden, ohne dass dazu die gespeicherten Daten wieder entpackt werden müssen. Außerdem ist für die meisten Compliance-Regelungen bei ArcSight Express keine separate, zusätzliche Speicherinfrastruktur zur Erfüllung der Datenaufbewahrungsanforderungen erforderlich. Bei der Log-Management-Appliance in ArcSight Express muss der Kunde nicht wie bei anderen, konkurrierenden Log-Management-Produkten Kompromisse eingehen und sich zwischen schneller Datenerfassung, schneller Suche und hoher Komprimierungsrate entscheiden. Die Log-Management-Appliance von ArcSight Express bietet eine einzigartige Datenspeicherungsarchitektur, durch die Logs extrem schnell erfasst werden können, die eine gleichzeitige Suche mit einer hohen Geschwindigkeit ermöglicht und bei der eine durchschnittliche Datenkomprimierungsrate von 10:1 aufrechterhalten wird.

ArcSight Connectors

Zum besseren Verständnis der gesamten Sicherheitsaufstellung der Organisation ist es notwendig, Logs von allen Geräten auf dem Netzwerk zu erfassen. ArcSight Express ermöglicht mit seiner integrierten Komponente ArcSight Connectors eine gebrauchsfertige Sammlung von Ereignis-Logs von über 275 Geräten. Die Connectors-Komponente erfasst Ereignis-Logs in ihrem ursprünglichen Format und normalisiert und kategorisiert sie anschließend in ein gängiges Format, damit sie einfacher korreliert und analysiert werden können. Beispielsweise sehen Konfigurationsänderungen auf einem Linux-Server, einem Cisco-Router und einer Oracle-Datenbank allesamt unterschiedlich aus. ArcSight Connectors wandeln all diese verschiedenen Ereignisse in ein gemeinsames Format, sodass es möglich wird, in einfacher Weise Berichte zu ALLEN Konfigurationsänderungen im gesamten Unternehmen zu erstellen. Das hat zur Folge, dass Sicherheitsadministratoren deutlich weniger Zeit dafür aufwenden müssen, erst die Relevanz jedes einzelnen Ereignisses ermitteln zu müssen.

Die Architektur von ArcSight Connectors ermöglicht zudem eine „zukunftsichere“ Überwachung in dem Sinn, dass das System auch dann weiter funktioniert, wenn die bestehende Netzwerktechnologie ausrangiert und durch die eines neuen Anbieters ersetzt wird.

- **Berichte zu Bandbreitenverschwendung und Richtlinienverletzung** – Das Produkt überwacht die Verwendung teurer Netzwerkkressourcen, erlaubt die kontrollierte Ausführung geschäftskritischer Komponenten und verhindert den nicht autorisierten Zugriff auf Dienste und Anwendungen auf dem Netzwerk. Es verwendet Variationen in der Bandbreite als Frühwarnsystem zur Erkennung von Malware.



- **Erkennung von nicht autorisiertem Zugriff auf Anwendungen und Systeme** – Das Produkt bestimmt, auf welchen Systemen möglicherweise kompromittierte Benutzerkonten vorliegen, indem es Brute-Force-Login-Versuche oder ungewöhnliche Anmeldeaktivitäten auf kritischen Servern erkennt.
- **Erkennung von VPN-Sneak-Angriffen** – Das System erkennt die Fernzugriffsmuster in Ihrer Organisation. Es verhindert, dass nicht berechtigte Benutzer in das Unternehmensnetzwerk gelangen, erkennt infizierte Computer, die zum Zugriff auf interne Ressourcen verwendet wurden, und es erkennt Fernzugriffsmuster für lokale und entfernte Benutzer.
- **Auswirkungen auf System und Benutzer** – Das Produkt erkennt, welche Systeme und Benutzer von Infektionen oder Angriffen betroffen sind, um die Ausbreitung eines

Automatisierte Sicherheitsüberwachung: Fallmanagement und Ablaufsteuerung

In ArcSight Express ist eine vollfunktionale Engine für Fallmanagement und Ablaufsteuerung integriert. Diese Engine automatisiert die Erstellung von Fällen und die Benachrichtigung der Administratoren für den Fall, dass ein Sicherheitsvorfall erkannt wird. Auf diese Weise können Vorgänge, die sonst ein gut besetztes Security Operations Center (SOC) benötigen würden, über PDAs und Benachrichtigungen über E-Mail, SMS oder Pager verwaltet werden. ArcSight Express kann also auch in Umgebungen eingesetzt werden, in denen keine ausgewiesenen SOC-Mitarbeiter oder Sicherheitsadministratoren verfügbar sind.

Einfacher Einsatz und Verwaltung

Kleinere Organisationen suchen nach SIEM-Lösungen, die sich schnell bereitstellen lassen, und bei denen der zusätzliche Aufwand zur Einrichtung und Aktivierung minimal ist. ArcSight Express enthält bereits die notwendigen Regeln, Alarme, Berichte und Dashboards und ist damit sofort einsatzbereit.

ArcSight Express wird entweder als eine oder zwei Appliances geliefert. So entfallen die Probleme, die mit dem Erwerb, der Konfiguration und Sicherung separater Hardware verbunden sind. Für die laufende Verwaltung unterstützt ArcSight Express eine agentenfreie Sammlung. Dadurch entfällt für kleinere Unternehmen die Notwendigkeit, spezielle Softwareagenten zur Weiterleitung einzusetzen. Das betrifft insbesondere eine Reihe von Windows-Geräten, die ihre Logs nicht selbst an ArcSight Express weiterleiten können.

Schließlich verwendet ArcSight einen selbstverwaltenden Speicher, der keinerlei externe Speicher- oder Datenbankressourcen erfordert.

Zusammenfassung

Mittelständische Unternehmen haben mit genau denselben Herausforderungen rund um Sicherheit und Compliance zu kämpfen wie große Konzerne. Allerdings müssen mittelständische Firmen beim Schutz ihrer Netzwerke mit begrenzten Budgets, eingeschränkten personellen Ressourcen und oft auch geringerem Wissen auskommen. Eine starke SIEM- und Log-Management-Lösung kann helfen, die Analyse der Daten zu sicherheitsrelevanten Ereignissen zu automatisieren. Das macht sich in einer Verringerung der vom IT-Personal benötigten Zeit und Arbeitsleistung bemerkbar. Besonders wichtig ist dies für Organisationen, die nicht über ein spezialisiertes Sicherheitspersonal verfügen.

ArcSight Express ist das auf dem Markt führende Produkt zur Sammlung und Korrelation von Ereignissen und zum Log-Management für Organisationen, die eine kostengünstige und wartungsarme Lösung benötigen. Als Ihr Sicherheitsexperte kümmert sich ArcSight Express sofort nach der Bereitstellung um alle häufig auftretenden Sicherheitsprobleme. Organisationen, die Probleme mit der Kontrolle und Überwachung ihrer Netzwerke haben, werden von der Leistungsfähigkeit und Einfachheit von ArcSight Express begeistert sein.



Wenn Sie mehr erfahren möchten, wenden Sie sich an ArcSight.
Über E-Mail an: info@arcsight.com oder telefonisch unter +44 (0)870 351 6510

© 2009 ArcSight, Inc. Alle Rechte vorbehalten. ArcSight und das ArcSight-Logo sind Warenzeichen von ArcSight, Inc. Alle anderen hier erwähnten Produkt- und Firmennamen sind möglicherweise Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Eigentümer.