WHITE PAPER

LEITFADEN FÜR FÜHRUNGSKRÄFTE ZUR BUDGETPLANUNG FÜR SICHERHEITSINFORMATIONS- UND EREIGNISMANAGEMENT (SIEM)

KOSTENANALYSE ZWEIER BEREITSTELLUNGSMODELLE: SELBSTVERWALTETE SIEMS I. VGL. ZU VERWALTETEN SIEM-DIENSTEN

Trustwave®

Smart security on demand

LEITFADEN FÜR FÜHRUNGSKRÄFTE ZUR BUDGETPLANUNG FÜR SICHERHEITSINFORMATIONS- UND EREIGNISMANAGEMENT (SIEM)

KOSTENANALYSE ZWEIER BEREITSTELLUNGSMODELLE: SELBSTVERWALTETE SIEMS I. VGL. ZU VERWALTETEN SIEM-DIENSTEN

INHALTSVERZEICHNIS

EINFÜHRUNG

Lösungen für Sicherheitsinformations- und Ereignismanagement (Security Information and Event Management, SIEM) gibt es seit mehr als zehn Jahren. Dennoch herrschen in der Branche längst nicht die Zufriedenheit und allgemeine Begeisterung für SIEM wie für andere Sicherheitstechnologien im gleichen Stadium. Aber SIEM muss einen wichtigen Platz in der Sicherheitsstrategie und im Sicherheitsinstrumentarium einer Organisation einnehmen. Warum? Die ursächlichen Probleme bestehen weiter und nehmen zu – wie kann man eine Panne in der IT-Infrastruktur entdecken, analysieren und reparieren? SIEM geht diese Probleme immer noch besser an als andere Lösungen. Der Frust entsteht häufig dadurch, dass die Kosten und Komplexität von Einrichtung und Betrieb eines SIEM unterschätzt werden. Um diese Herausforderungen zu meistern, wurden verwaltete SIEM-Dienste eingeführt, die die besonderen Bedürfnisse und Strategien von Organisationen jeder Größenordnung aufgreifen. Aber wie soll eine Organisation zwischen selbstverwaltetem und verwaltetem SIEM entscheiden?

Dieses White Paper will letzten Endes den Einkäufern von IT-Sicherheit ein aufschlussreiches Instrument an die Hand geben, damit sie die Kosten, Optionen und Kompromisse zwischen den beiden wichtigsten Einsatzmodellen von SIEM verstehen: selbstverwaltete (Do-it-yourself) und verwaltete Sicherheitsdienste (Managed Security Services). Es vergleicht die Kosten von SIEM unter zwei Bereitstellungsmodellen – selbstverwaltetes und verwaltetes SIEM – in drei Szenarien für unterschiedlich große Betriebe. Die Kostenvergleiche erfassen sowohl Investitionskosten (Anschaffungskosten) und Betriebsaufwendungen (laufende Betriebskosten).

Die drei vorgestellten Kundenszenarien gliedern sich in:

- Großunternehmen
- Mittelständischer Betrieb
- Kleinbetrieb

Der Wert dieser Szenarien ergibt sich aus der Anwendung und Anpassung des entsprechenden Szenarios an eine Organisation auf der Grundlage der Beschreibungen und Profile, die in dieser Analyse angegeben werden.

Wir sind uns bewusst, dass es neben den finanziellen auch strategische Überlegungen gibt. Das White Paper erörtert kurz drei strategische Problemstellungen sowie ihren direkten Einfluss auf die Kosten, die in diesen Gesprächen häufig erwähnt werden.

KOSTENMETHODIK

Die dargestellten Kostenmodelle wenden die Gesamtkostenmethodik an und integrieren die meisten indirekten Kosten beim Kauf eines SIEM über die gewöhnliche Laufzeit von drei Jahren. Wir berücksichtigen zum Beispiel Lohnkosten im Zusammenhang mit dem Betrieb des SIEM, wie:

- Schulungen
- Support für Einrichtung und Implementierung
- Fluktuation und Anwerbung von Mitarbeitern
- Komplette Lohnkosten (d. h. Gehalt und Gemeinkostenaufschlag)

Wir lassen absichtlich bestimmte indirekte Kosten unberücksichtigt, wie Raumbedarf im Rechenzentrum, Strom und Kühlung, die in den Anschaffungs- und Betriebskostenmodellen vieler Dienstanbieter enthalten sind. Für die verwaltete SIEM-Architektur von Trustwave muss ein SIEM-Gerät auf dem Firmengelände des Kunden stehen. Deshalb sind diese indirekten Kosten für beide Bereitstellungsmethoden gleich.

Eine indirekte Ausgabe, die die meisten Firmen bei der Budgetplanung für ihr SIEM nicht erfassen, sind die Personalkosten im Zusammenhang mit Anwerbung, Fluktuation und fortlaufenden Schulungen und Zertifizierungen der Mitarbeiter. Diese Kosten können erheblich sein. Dieses White Paper nutzt allgemein veröffentlichte Standards zur Erfassung dieser Kosten.

DEFINITIONEN UND BESCHREIBUNGEN

In der IT-Branche verwenden verschiedene Anwender oft unterschiedliche Begriffe, was zu Missverständnissen und falschen Schlussfolgerungen führen kann. Um der Klarheit willen zeigen wir die Definitionen der Begriffe, die wir in diesem Text verwenden.

Selbstverwaltet

Ein Bereitstellungsmodell für den Einsatz einer Sicherheitslösung, bei dem der Kunde die SIEM-Lösung auf seinem Gelände kauft, einsetzt und betreibt – sowohl Software als auch Hardware. Wartung und Support sind inbegriffen und folgen üblichen Kaufpraktiken für selbstverwaltete Lösungen. Die Mitarbeiter des Kunden sind für Einrichtung und Betrieb des Systems verantwortlich. Der Erfolg hängt davon ab, dass der Kunde Größe und Budget für die Lösung adäquat veranschlagt und Mitarbeiter mit der notwendigen Erfahrung und Ausbildung bereitstellt.

Verwaltetes SIEM, geliefert durch verwaltete Sicherheitsdienste

Als Anbieter von verwalteten Sicherheitsdiensten (Managed Security Services Provider, MSSP) hält Trustwave ein breites Portfolio an Sicherheitsdiensten, darunter verschiedene SIEM-Dienste bereit. Unter dem Modell der verwalteten Sicherheitsdienste zahlt der Kunde eine Servicegebühr (Abonnement) an Trustwave für die Bereitstellung bestimmter SIEM-Dienste.

Trustwave bietet drei Arten verwalteter SIEM-Dienste, die den wichtigsten Betriebskomponenten eines SIEM entsprechen. Dazu gehören:

1. Eigenständige Protokollüberwachung in der Cloud: Trustwave implementiert und pflegt die Plattform für die SIEM-Technologie und deckt den grundlegenden Systembetrieb ab, darunter:
   - Geräteverwaltung
   - Erfassung der Protokolle in den globalen Security Operations Centers (SOCs) von Trustwave
   - Darstellung der Daten und Geräteinformationen über das Trustwave TrustKeeper® Portal auf der Grundlage von Einstellungen, die je nach Servicemodell vom Kunden oder von Trustwave vorgegeben wurden
   - Gesundheitscheck für das System (gegen Entrichtung einer zusätzlichen Servicegebühr)
2. Compliance-Überwachungsdienst: Auf der Grundlage der erfassten und verarbeiteten Protokolldaten des Kunden durch die SOCs von Trustwave mailt der tägliche Compliance-Berichtdienst den Kunden einen Analysebericht zum Protokoll, damit Compliance-Auflagen erfüllt werden können. Der Compliance-Dienst kann auf Berichte zu bestimmten Geräten zugeschnitten werden. Trustwave implementiert und pflegt die Plattform für die SIEM-Technologie.
3. Überwachungsdienst zur Bedrohungsanalyse: Auf der Grundlage der erfassten und verarbeiteten Logdaten des Kunden durch die SOCs von Trustwave arbeitet der Überwachungsdienst zur Bedrohungsanalyse mit maschinellen und menschlichen Analysen an der Aufdeckung und Vermeidung von Sicherheitsvorfällen und Datenpannen. Der Dienst kann auf Berichte zu bestimmten Geräten eingestellt werden. Der SIEM Überwachungsdienst zur Bedrohungsanalyse umfasst:
   - Automatisierte Analyse der Kundendaten auf der Grundlage von Korrelationen, die von Trustwave speziell für die Umgebung und das Risikoprofil des Kunden erarbeitet wurden
   - Menschliche Überwachung der SIEM-Tätigkeit, Analyse von Warnhinweisen, Untersuchung von Warnhinweisen mit Priorität
   - Verständigung des Kunden über bedenkliche Vorfälle, die zusätzliche Aufmerksamkeit und Untersuchungen vor Ort sowie Behebung durch die Sicherheitstechniker des Kunden erfordern

Der Kunde und Trustwave vereinbaren die Arten von Dienstleistungen, damit der Kunde seine Geschäfts- und Sicherheitsziele erreichen kann. Dieses Servicemodell verknüpft Trustwave enger mit dem Kundenerfolg als herkömmliche Modelle, die eine Technologie in Lizenz vergeben, und lösen das **Problem der ungenutzten Software**.

Investitionskosten und Betriebskosten

Viele Anschaffungen (z. B. Server, Software usw.) haben eine Investitionskosten- und eine Betriebskostenkomponente. Die Umlage dieser Kosten auf die „richtigen“ Investitions- und Betriebskostentöpfe kann sich je nach Buchführungspraktiken schnell zu einer technischen Diskussion über die Rechnungslegung auswachsen. Dieses White Paper arbeitet mit einer einfachen und intuitiven Kostenumlage. Investitionskosten sind die Kosten, die zu Anfang für die Anschaffung der Produkte (Hardware und Software) durch den Kunden aufgewendet werden. Laufende Kosten, die mit der Verwendung der Produkte einhergehen (z. B. Support und Wartung), gelten als Betriebskosten. Diese Ausgaben gelten auch dann als Betriebskosten, wenn der Kunde zu Beginn des Nutzungszeitraums diese in voller Höhe bezahlt.

Kosten und Preise

Quellen für alle Kostendaten sind in Anhang 1 genannt.

ALLGEMEINE STRATEGISCHE KOMPROMISSE

Beim Vergleich der Bereitstellungsmodelle von selbstverwalteten und verwalteten Sicherheitsdiensten gibt es verschiedene strategische Überlegungen. Sie alle aufzugreifen würde den Rahmen dieses Textes sprengen. Die strategischen Kompromisse, die wir am häufigsten hören, sind jedoch folgende:

- Kostenumlage
- Strategische und taktische Kontrolle
- Bindung interner Fachleute und Erfahrungen
- Risikomanagement

Kostenumlage

Dieser Kompromiss betrifft die Umlage der Kosten auf Investitionskosten oder Betriebskosten. Die meisten Investitionskosten verlagern sich zu den Betriebskosten, wenn das Bereitstellungsmodell von selbstverwalteten auf verwaltete Sicherheitsdienste wie das verwaltete SIEM wechselt. Dieser Wechsel ermöglicht eine andere buchhalterische Behandlung der damit zusammenhängenden Kosten. Viele Firmen bevorzugen diese Verlagerung, sie hängt aber letzten Endes von Geschäfts-, Rechnungslegungs- und Budgetentscheidungen der einzelnen Organisationen ab. Die Vielfalt der Regeln zur buchhalterischen Behandlung übersteigt die Grenzen dieses White Papers.

Strategische und taktische Kontrolle

Einige Organisationen geben Informationssicherheit nur ungern an einen Dienstanbieter ab, denn sie fürchten, dass sie die Kontrolle über ihre Systeme und die Kapazität verlieren, auf Sicherheitsprobleme zu reagieren. Auf der Grundlage allgemeiner Annahmen zum MSSP-Modell mag dies eine vernünftige Schlussfolgerung sein. Ein MSSP hätte Zugang zu SIEM-Daten und könnte je nach Prozessgestaltung zum Weichensteller für Warnhinweise, Analysen und Reaktionen werden. Aber mit richtig definierten, verwalteten SIEM-Diensten und Prozessen können Organisationen das Maß an Kontrolle über ihre Systeme beibehalten, das ihren Sicherheits- und geschäftlichen Bedarf erfüllt. In vielen Situationen können verwaltete SIEM-Dienste dem Kunden mehr Kontrolle und bessere Endergebnisse bieten.

Die Kontrolle durch den Kunden kann anhand von zwei Faktoren verbessert werden: bessere Sicht auf die Systeme und intelligentere Kontrolle. Diese Faktoren ergeben sich aus verschiedenen Eigenschaften des Service-Provider-Modells. Erstens basieren die verwalteten SIEM-Dienste auf nachweislich bewährten Praktiken und werden von Experten der Sicherheitsbranche bereitgestellt, die ihre Taktiken fortlaufend anhand des neuesten Sicherheitswissens verbessern. Viele Firmen können dieses Kaliber an Sicherheitswissen mit den verfügbaren Ressourcen und Geldern intern nicht aufbringen. Zweitens werden verwaltete Dienste das ganze Jahr rund um die Uhr bereitgestellt. Die Personalkosten für diesen Service verbieten sich für viele Firmen von selbst. Mit einem Anbieter von verwalteten Sicherheitsdiensten können Organisationen darauf vertrauen, dass immer jemand zur Stelle ist, um eine Sicherheitswarnung entgegenzunehmen, zu analysieren und darauf zu reagieren. Mit anderen Worten: Wenn Sie selbst niemanden haben, der Ihre Reaktion steuert, steht im Bedarfsfall jemand bereit. Drittens sind kundenzentrierte Dienste transparent und auf Kooperation ausgerichtet. Sie bieten dem Team in der Organisation in Echtzeit Zugriff auf alle SIEM-Daten – die SIEM-Informationen sind immer verfügbar. Schließlich können Kunden einen verwalteten SIEM-Dienst mit einem flexiblen Ansatz nutzen, der Kunden die Auswahl der gewünschten Dienstleistungen erlaubt. Dieses kooperative Modell erlaubt Kunden, spezielle Funktionen und Kenntnisse intern aufrechtzuerhalten.

Bindung interner Fachleute und Erfahrungen

Ein Teil der Kontrollfrage hat mit der Bindung interner Fachleute zu tun. Jede IT-Organisation möchte ihre Kapazität zur Definition und Ausführung der Dienste beibehalten, die sie bereitstellt. Mit der Weiterentwicklung von Sicherheitsbedrohungen helfen diese Fachleute mit ihrer Erfahrung der Organisation, sich wechselnden Umständen anzupassen. Aber muss denn eine IT-Organisation Mitarbeiter beschäftigen, die alle diese Dienste bereitstellen können? Kann sie sich das leisten? Je nach IT-Strategie, Umgebung und Risikoprofil müssen Organisationen entscheiden, ob die Kosten zur Beibehaltung bestimmter IT-Kompetenzen gerechtfertigt sind. Einige wichtige Überlegungen zu dieser Entscheidung sind:

- Gemeinkosten: Gibt es genügend Geld und Mitarbeiter, um interne SIEM-Mitarbeiter einzustellen und zu beschäftigen?
- Fluktuation und operative Kapazität: Jüngeren Umfragen[1] zufolge wechseln Mitarbeiter in der IT-Sicherheit ihre Stelle (intern oder extern) ungefähr alle zwei Jahre*. Es dauert durchschnittlich mehr als drei Monate, um diese Stellen wieder zu besetzen, und weitere vier bis sechs Wochen, um die neuen Kollegen einzuarbeiten. Organisationen müssen entscheiden, ob sie Zeiten akzeptieren können, in denen ihr SIEM unterbesetzt ist und wichtige Sicherheits- und Geschäftsziele nicht verwirklicht werden können.

Risikomanagement – Überwachung rund um die Uhr?

Der Kompromiss liegt hier zwischen Budget und Risiko. Organisationen müssen eine strategische Entscheidung zum Risikomanagement treffen und die annehmbare Dienstgüte für Überwachung und Pannen festlegen. Im selbstverwalteten Modell wird der Sicherheitsbetrieb rund um die Uhr aufgrund des Personalbedarfs teuer. (Einzelheiten hierzu siehe Szenario Großunternehmen.) Selbstverwaltete Organisationen können jedoch von ihrer Flexibilität profitieren und Personalausstattung und Dienstgüte entsprechend anpassen (d. h. Nacht-, Wochenend-, Feiertagsdienst usw.), um das richtige Verhältnis von Risikomanagement, Dienstgüte und Budget zu schaffen. Aber eine geringere Personalausstattung hat ihren Preis: das erhöhte Risiko infolge langsamerer Reaktionen auf Warnhinweise und Pannen. Eine geringere Dienstgüte muss den Richtlinien der Firma zum Risikomanagement entsprechen.

SZENARIO-ANALYSE

Im Folgenden sind drei Kundenszenarien dargestellt, die die Kosten für den Einsatz von selbstverwaltetem und verwaltetem SIEM vergleichen:

- Großunternehmen
- Mittelständischer Betrieb
- Kleinbetrieb

Diese Szenarien und die damit zusammenhängenden Verwendungen werden in den folgenden Abschnitten ausführlich beschrieben.

Großunternehmen

Das Szenario für Großunternehmen bildet eine große Organisation mit mindestens 10.000 Mitarbeitern ab. Das wesentliche Attribut für diese Analyse ist die Anzahl der IT-Geräte, die für die Größenbestimmung des Systems und die Preisgestaltung der Dienstleistung herangezogen wird. Die Anzahl der Arbeitsplatzrechner hängt mit der Anzahl an Mitarbeitern zusammen, ist aber nicht mit ihr identisch. Einige Organisationen haben aufgrund ihrer Branchenzugehörigkeit oder der dort verrichteten Arbeit mehr Mitarbeiter als Arbeitsplatzrechner.

Größenbestimmung der Plattform: Anzahl und Art der Geräte

- 10.000 Arbeitsplatzrechner
- 30 Schutzeinrichtungen (IDS, Firewall usw.)
- 60 Netzwerkgeräte
- 125 Server
- 15.000 Ereignisse pro Sekunde (~1 Mrd. Ereignisse pro Tag)

1. Quellen: Ponemon Institute, „Understaffed and at Risk:Today's IT Security Department", Februar 2014.

Vorrangige Verwendung der Sicherheitseinrichtungen

- Sicherung des Netzwerks
- Erfüllung der Auflagen zur Compliance
- Bedrohungs- und Risikoanalyse
- Eindämmung von Pannen und globale Reaktion auf Vorfälle

Beschreibung der selbstverwalteten Lösung

- SIEM-Plattform: Trustwave SIEM Enterprise (SIEM-E)
- Software- und Hardware-Support und Wartung: 3 Jahre

Beschreibung der von Trustwave verwalteten SIEM-Lösung

- Laufzeit des Abonnements: 3 Jahre
- Plattform-Managementdienste (Systemadministration)
  - Von Trustwave verwalteter Gerätedienst
  - Gesundheitscheck von Trustwave (vierteljährliche Analyse der Systemleistung und Aktualisierungen)
- Compliance-Dienste: Von Trustwave verwaltete Dienste zur Compliance-Überwachung für die Arbeitsplatzrechner
- Bedrohungsanalysedienste: Von Trustwave verwaltete Überwachungsdienste zur Bedrohungsanalyse für IDS, Firewalls und Server
  - Der verwaltete Überwachungsdienst zur Bedrohungsanalyse umfasst auch Compliance-Berichte für diese Geräte

Schulung und Implementierung: 10-tägige Schulung zu Anwendung und Implementierung

- Trustwave bietet eine Schulung zu Anwendung und Implementierung am Standort. Die Dauer der Schulung richtet sich nach Umfang und Komplexität der Einrichtung.

Bereitschaft und Reaktion auf Vorfälle

- Trustwave bietet weitreichende Bereitschafts- und Reaktionsdienste, die auf die Ziele, Branche und interne Umgebung des Kunden zugeschnitten und in einem individuellen Reaktionsprogramm zusammengestellt werden können. Dieser Sicherheitsservice ist nicht Bestandteil dieser Kostenanalyse.

Wir weisen darauf hin, dass die Personalstruktur für das Szenario in Großunternehmen sich von den anderen Szenarien unterscheidet. Zwei Annahmen liegen diesem Unterschied zugrunde:

1. Ein Großunternehmen braucht die Dienstgüte für Überwachung, Reaktionszeiten und Wiederherstellungsdienste eines rund um die Uhr einsatzbereiten Security Operations Centers (SOC), um die Richtlinien zum Risikomanagement zu erfüllen. Personelle Unterbesetzung wurde als ein Faktor bei weithin bekannt gewordenen Datenpannen in Großunternehmen genannt. Für die Besetzung rund um die Uhr sind mindestens 4,5 Sicherheitsanalysten notwendig.
2. Da die Beschäftigung eines halben Sicherheitsanalysten etwas ineffizient ist, geht dieses Szenario davon aus, dass ein fünfter Analyst eingestellt wird. Die übrige Zeit des Analysten wird auf andere SIEM-Aufgaben verteilt, insbesondere Systemadministration und Behebung von Vorfällen. Deshalb sind die Kosten in diesem Szenario Null.

Diese Annahmen fließen in die Kostentabelle auf der nächsten Seite ein.

2. Quelle: RedLambda.com, „Is IT Security Being Impacted by Attrition?“, November 2014.
http://www.redlambda.com/blog/is-it-security-being-impacted-by-attrition

GROSSUNTERNEHMEN

Hinweis: Es handelt sich um ein Fallbeispiel aus den USA.

Investitionskosten (einmalige Kosten)		
	Selbstverwaltetes SIEM	**Verwaltetes SIEM**
SIEM-Gerät	245.000 USD	
Schulung der Endnutzer • 10-tägige Schulung und Implementierung	24.000 USD	24.000 USD
Einführungskosten sind oben enthalten		
Implementierungsgebühr für verwaltetes SIEM • Einrichtung des Daten-Upstreaming an SOC • 1.000 USD wenn < 3 Jahre		0 USD
Investitionskosten insgesamt Jahr 1	**269.000 USD**	**24.000 USD**
Betriebskosten (laufende Kosten)	**Selbstverwaltetes SIEM**	**Verwaltetes SIEM**
Verwalteter SIEM-Dienst		64.000 USD
Systemadministration	0 USD*	
Systemadministrationsdienst • Gesundheitscheck durch Trustwave		10.900 USD
Wartung und Support (Hardware und Software)	8.320 USD	
Compliance- und Überwachungsanalysten	578.819 USD	
SIEM Bedrohungs- und Korrelationsspezialist	130.340 USD	
Verwaltete Compliance- und Bedrohungsanalysedienste		428.930 USD
Behebung eskalierter Vorfälle durch interne Mitarbeiter**	0 USD	69.458 USD
Anwerbung von Mitarbeitern	89.232 USD	
Jährliche Schulung und Zertifizierung	21.000 USD	
Jährliche Betriebskosten insgesamt	**842.582 USD**	**573.288 USD**
GESAMTKOSTEN JAHR 1	**1.111.582 USD**	**597.288 USD**

* Null Kosten aufgrund der Annahme, dass die Aufgaben des Systemadministrators durch die zusätzliche Zeit des fünften Sicherheitsanalysten wahrgenommen werden.

**Für selbstverwaltet: Null Kosten wegen der angenommenen Aufteilung der Arbeitszeit des fünften Sicherheitsanalysten.
Für verwaltetes SIEM: Diese Berechnung entspricht dem Stundensatz für einen erfahrenen IT-Mitarbeiter multipliziert mit den Stunden, die für Pannenbehebung aufgewendet werden. Dies geschieht in Kooperation mit den Fachleuten, Analysten und SOC-Teams der Trustwave Managed Security Services. Die veranschlagte Zeit basiert auf durchschnittlich 6 Vorfällen pro Woche mit durchschnittlich 4 Stunden pro Vorfall.

Kosten im Verlauf eines 3-Jahres-Abonnements*

	Jahr 1	Jahr 2	Jahr 3	Gesamtkosten
Selbstverwaltetes SIEM	1.114.120 USD	845.120 USD	845.120 USD	**2.804.359 USD**
Verwaltetes SIEM	597.288 USD	573.288 USD	573.288 USD	**1.743.865 USD**

*Veranschlagt keine Inflation der Gehälter oder Kosten, die in den meisten Organisationen Standard sind.

MITTELSTÄNDISCHER BETRIEB

Dieses Szenario geht von einem typischen mittelständischen Betrieb mit 1.000 oder mehr Mitarbeitern aus. Das wesentliche Attribut für diese Analyse ist die Anzahl der IT-Geräte, die für die Größenbestimmung des Systems und die Preisgestaltung der Dienstleistung herangezogen wird. Die Anzahl der Arbeitsplatzrechner hängt mit der Anzahl an Mitarbeitern zusammen, ist aber nicht mit ihr identisch. Einige Organisationen haben aufgrund ihrer Branchenzugehörigkeit oder der dort verrichteten Arbeit mehr Mitarbeiter als Arbeitsplatzrechner.

Größenbestimmung der Plattform: Anzahl und Art der Geräte

- 1.000 Arbeitsplatzrechner
- 18 Schutzeinrichtungen (IDS, Firewall usw.)
- 25 Server
- 1.500 bis 3.000 Ereignisse pro Sekunde (~130 bis 260 Mio. Ereignisse pro Tag)

Vorrangige Verwendung der Sicherheitseinrichtungen

- Sicherung des Netzwerks
- Erfüllung der Auflagen zur Compliance
- Bedrohungs- und Risikoanalyse

Beschreibung der selbstverwalteten Lösung

- SIEM-Plattform: Trustwave SIEM Enterprise (SIEM-E)
- Software- und Hardware-Support und Wartung: 3 Jahre

Beschreibung der von Trustwave verwalteten SIEM-Lösung

- Laufzeit des Abonnements: 3 Jahre
- Plattform-Managementdienste (Systemadministration)
  - Von Trustwave verwalteter Gerätedienst
  - Gesundheitscheck von Trustwave (vierteljährliche Analyse der Systemleistung und Aktualisierungen)
- Compliance-Dienste: Von Trustwave verwaltete Dienste zur Compliance-Überwachung für die Arbeitsplatzrechner
- Bedrohungsanalysedienste: Von Trustwave verwalteter Überwachungsdienst zur Bedrohungsanalyse für IDS, Firewalls und Server
  - Der verwaltete Überwachungsdienst zur Bedrohungsanalyse umfasst auch Compliance-Berichte für diese Geräte

Schulung und Implementierung: 5-tägige Schulung zu Anwendung und Implementierung

- Trustwave bietet eine Schulung zu Anwendung und Implementierung am Standort. Die Dauer der Schulung richtet sich nach Umfang und Komplexität der Einrichtung.

MITTELSTÄNDISCHER BETRIEB

Hinweis: Es handelt sich um ein Fallbeispiel aus den USA.

Investitionskosten		
	Selbstverwaltetes SIEM	**Verwaltetes SIEM**
SIEM-Gerät	86.500 USD	
Schulung der Endnutzer • 5-tägige Schulung und Implementierung	13.900 USD	13.900 USD
Einführungskosten sind oben enthalten		
Implementierungsgebühr für verwaltetes SIEM • Einrichtung des Daten-Upstreaming an SOC • 1.000 USD wenn < 3 Jahre		0 USD
Investitionskosten insgesamt Jahr 1	**100.400 USD**	**13.900 USD**
Betriebskosten	**Selbstverwaltetes SIEM**	**Verwaltetes SIEM**
Verwalteter SIEM-Dienst		38.000 USD
Systemadministration	14.870 USD	
Systemadministrationsdienst • Gesundheitscheck durch Trustwave		10.900 USD
Wartung und Support (Hardware und Software)	8.320 USD	
Compliance- und Überwachungsanalyst • „fast“ rund um die Uhr Support durch SOC*	347.292 USD	
SIEM Bedrohungs- und Korrelationsspezialist	130.340 USD	
Verwaltete Compliance- und Bedrohungsanalysedienste		102.920 USD
Behebung eskalierter Vorfälle durch interne Mitarbeiter**	0 USD	34.729 USD
Anwerbung von Mitarbeitern	71.824 USD	
Jährliche Schulung und Zertifizierung	14.000 USD	
Jährliche Betriebskosten insgesamt	**581.689 USD**	**185.144 USD**
GESAMTKOSTEN JAHR 1	**682.089 USD**	**199.044 USD**

* Es wird angenommen, dass ein mittelständischer Betrieb ein „partielles“ Securities Operations Center (SOC) mit 3 vollzeitäquivalenten Mitarbeitern für eine angemessene Dienstgüte zur Verwirklichung der Risikomanagementziele akzeptiert. „Partielles SOC“ bedeutet, dass das SOC zu gewissen Zeiten nicht besetzt ist. Auf die Woche gerechnet wird das SOC bei 8-Stunden-Schichten technisch gesehen 48 Stunden lang (d. h. ca. 7 Stunden pro Tag) „unbesetzt“ sein. Ausgehend von durchschnittlich 48 Arbeitswochen pro Jahr pro VZÄ ist das SOC für rund ein Drittel des Jahres zu 66 % gedeckt.

**Für selbstverwaltet: Diese Position ist ein SIEM-Sicherheitsspezialist in Vollzeit. Je nach Arbeitsbelastung wird diese Person ungefähr 50–70 % der Zeit mit Analyse und Korrelierungen und 20–30 % mit der Reaktion auf Vorfälle und deren Behebung verbringen.

Für verwaltetes SIEM: Diese Berechnung entspricht dem Stundensatz für einen erfahrenen IT-Mitarbeiter multipliziert mit den Stunden, die für Pannenbehebung aufgewendet werden. Dies geschieht in Kooperation mit den Fachleuten, Analysten und SOC-Teams der Trustwave Managed Security Services. Die veranschlagte Zeit basiert auf durchschnittlich 3 Vorfällen pro Woche mit durchschnittlich 4 Stunden pro Vorfall.

Kosten im Verlauf eines 3-Jahres-Abonnements*

	Jahr 1	Jahr 2	Jahr 3	Gesamtkosten
Selbstverwaltetes SIEM	682.089 USD	581.689 USD	581.689 USD	**1.845.468 USD**
Verwaltetes SIEM	199.044 USD	185.144 USD	185.144 USD	**569.332 USD**

*Veranschlagt keine Inflation der Gehälter oder Kosten, die in den meisten Organisationen Standard sind.

KLEINBETRIEB

Dieses Szenario geht von einem typischen Kleinbetrieb mit 250 bis 500 Mitarbeitern aus. Das wesentliche Attribut ist die Anzahl der IT-Geräte, die für die Preisgestaltung der Dienstleistung herangezogen wird. Die Anzahl der Arbeitsplatzrechner hängt mit der Anzahl an Mitarbeitern zusammen, ist aber nicht mit ihr identisch. Einige Organisationen haben aufgrund ihrer Branchenzugehörigkeit oder der dort verrichteten Arbeit mehr Mitarbeiter als Arbeitsplatzrechner.

Größenbestimmung der Plattform: Anzahl und Art der Geräte

- 250 Arbeitsplatzrechner
- 6 Schutzeinrichtungen (IDS, Firewall usw.)
- 8 Server
- 1.000 Ereignisse pro Sekunde (~86 Mio. Ereignisse pro Tag)

Vorrangige Verwendung der Sicherheitseinrichtungen

- Protokollierung und Verwaltung
- Compliance-Berichte
- Bedrohungsanalyse auf IDS

Beschreibung der selbstverwalteten Lösung

- SIEM-Plattform: Trustwave Log Management Enterprise (LME)
- Software- und Hardware-Support und Wartung: 3 Jahre

Beschreibung des von Trustwave verwalteten SIEM

- Laufzeit des Abonnements: 3 Jahre
- Plattform-Managementdienste (Systemadministration)
  - Von Trustwave verwalteter Gerätedienst
  - Gesundheitscheck von Trustwave (vierteljährliche Analyse der Systemleistung und Aktualisierungen)
- Compliance-Dienste: Von Trustwave verwalteter Dienst zur Compliance-Überwachung für die Arbeitsplatzrechner
- Bedrohungsanalysedienste: Von Trustwave verwalteter Überwachungsdienst zur Bedrohungsanalyse für IDS, Firewalls und Server
  - Der verwaltete Bedrohungs-Überwachungsdienst umfasst auch Compliance-Berichte für diese Geräte

Schulung und Implementierung: 3-tägige Schulung zu Anwendung und Implementierung im Haus durch Trustwave

- Die Dauer der Schulung richtet sich nach dem Umfang der Einrichtung und nach der Komplexität des Produkts.
- Die Schulung umfasst sowohl Unterricht als auch die Implementierung des erworbenen SIEM-Systems. Die Unterrichtskosten verstehen sich pro Lehrgang, nicht pro Teilnehmer.

Bereitschaft und Reaktion auf Vorfälle

- Trustwave bietet weitreichende Bereitschafts- und Reaktionsdienste, die auf die Ziele, Branche und interne Umgebung des Kunden zugeschnitten und in einem individuellen Reaktionsprogramm zusammengestellt werden können. Dieser Sicherheitsservice ist nicht Bestandteil dieser Kostenanalyse.

KLEINBETRIEB

Hinweis: Es handelt sich um ein Fallbeispiel aus den USA.

Investitionskosten		
	Selbstverwaltetes SIEM	**Verwaltetes SIEM**
SIEM-Gerät	18.500 USD	
Schulung der Endnutzer • 3-tägige Schulung und Implementierung	7.500 USD	7.500 USD
Einführungskosten sind oben enthalten		
Implementierungsgebühr für verwaltetes SIEM • Einrichtung des Daten-Upstreaming an SOC • 1.000 USD bei Abonnement < 3 Jahre		0 USD
Investitionskosten insgesamt Jahr 1	**26.000 USD**	**7.500 USD**
Betriebskosten	**Selbstverwaltetes SIEM**	**Verwaltetes SIEM**
Verwalteter SIEM-Dienst		12.456 USD
Systemadministration	9.914 USD	
Systemadministrationsdienst • Gesundheitscheck durch Trustwave		10.900 USD
Wartung und Support (Hardware und Software)	2.960 USD	
Compliance- und Überwachungsanalyst	115.764 USD	
Verwaltete Compliance- und Bedrohungsanalysedienste		33.873 USD
Anwerbung von Mitarbeitern • 20 % des Gehalts der angeworbenen VZÄ	23.153 USD	
Jährliche Schulung und Zertifizierung	3.500 USD	
Behebung eskalierter Vorfälle durch interne Mitarbeiter*	0 USD	11.596 USD
Jährliche Betriebskosten insgesamt	**166.886 USD**	**68.825 USD**
GESAMTKOSTEN JAHR 1	**192.886 USD**	**76.325 USD**

* Es wird 1 eskalierter Vorfall pro Woche mit durchschnittlich 4 Arbeitsstunden pro Vorfall veranschlagt.

Für selbstverwaltet: Es wird angenommen, dass Kleinbetriebe aufgrund von Ressourcenzwängen mit ihren vorhandenen Mitarbeitern auf Vorfälle reagieren werden; die Kosten werden daher von den obigen Posten erfasst und hier mit Null wiedergegeben.

Für verwaltetes SIEM: Diese Berechnung entspricht dem Stundensatz für einen erfahrenen IT-Mitarbeiter multipliziert mit den Stunden, die für Pannenbehebung aufgewendet werden. Stellt die Opportunitätskosten zur Umlage der Mitarbeiter von ihren Vollzeitbeschäftigungen dar. Dies geschieht in Kooperation mit den Fachleuten, Analysten und SOC-Teams der Trustwave Managed Security Services. Die veranschlagte Zeit basiert auf durchschnittlich 3 Vorfällen pro Woche mit durchschnittlich 4 Stunden pro Vorfall.

Kosten im Verlauf eines 3-Jahres-Abonnements*

	Jahr 1	**Jahr 2**	**Jahr 3**	**Gesamtkosten**
Selbstverwaltetes SIEM	192.886 USD	166.886 USD	166.886 USD	**526.659 USD**
Verwaltetes SIEM	76.325 USD	68.825 USD	68.825 USD	**213.974 USD**

*Veranschlagt keine Inflation der Gehälter oder Kosten, die in den meisten Organisationen Standard sind.

VERWALTETE SICHERHEITSDIENSTE: NICHT ALLES ODER NICHTS

Obwohl diese Szenarien einen Entweder-Oder-Vergleich abbilden, ist Trustwave nicht der Ansicht, dass die Entscheidung zwischen selbstverwaltetem und verwaltetem SIEM absolut ist. Jede Organisation hat unterschiedliche Ressourcen, IT-Umgebungen und Sicherheitsstrategien. Wenn Organisationen eine SIEM-Lösung in Betracht ziehen, sollten sie überlegen, ob und wie die Dienste auf ihre IT-Strategie, Organisation und Umgebung zugeschnitten werden können. Trustwave gestaltet ihre verwalteten Sicherheitsdienste und Bereitstellungsmodelle so, dass Kunden die Dienste auswählen können, die ihrem Bedarf entsprechen. Dieser Ansatz resultiert in einer Mischform für verwaltete SIEM-Dienste (gemeinsame Verwaltung). Ein Kunde möchte zum Beispiel nur Compliance-Reportingdienste für seine Arbeitsplatzrechner und will alle anderen Bedrohungsanalysen selbst ausführen. Dieser Ansatz erlaubt dem Kunden die Auswahl der Komponenten für den SIEM-Dienst fast wie aus einem Menü.

ZUSAMMENFASSUNG

Auf der Grundlage dieser Analyse erweist sich die verwaltete SIEM-Option als die kostengünstigere Lösung in allen drei Szenarien. Die Entscheidung einer Organisation sollte jedoch nicht nur von Kosten geleitet werden. Es sind auch die strategischen Kompromisse zwischen den Optionen für selbstverwaltete und verwaltete Sicherheitsdienste zu beurteilen. Die verwaltete SIEM-Option greift folgende Bedenken im Zusammenhang mit der Prüfung der in diesem White Paper genannten Kompromisse auf:

- **Kostenumlage:** Die Steuerstrategien der meisten Firmen bewerten Betriebskosten über Investitionskosten, was das verwaltete SIEM-Modell begünstigt.
- **Kontrolle:** Organisationen sollten einen erfahrenen Diensteanbieter mit klar definierten Aufgaben und Verfahrensweisen und einer Lösung wählen, die den SIEM-Betrieb transparent macht. Ein verwalteter Dienstanbieter, der diese Probleme aufgreift, wird Ihre Kontrolle nicht behindern.
- **Bindung erfahrener Mitarbeiter:** Mit der Wahl eines Anbieters mit einem flexiblen Servicemodell können Firmen ihr Serviceportfolio individuell zusammenstellen und Mittel für die internen Mitarbeiter schonen, deren Erfahrung als strategisch wichtig gilt.

Diese Strategie- und Kostenüberlegungen schaffen den Rahmen für die Wahl eines Bereitstellungsmodells. Firmen, die die Technologien von Anbietern prüfen (oder sich die Auffrischung eines bestehenden SIEM überlegen), sollten sich auf Anbieter konzentrieren, die nicht nur Erfahrung mit den hier besprochenen Bereitstellungsmodellen haben, sondern auch die notwendige Flexibilität bieten, damit die Dienste auf ihren spezifischen Bedarf zugeschnitten werden können. Sie sollten ferner die Migration von einfachen SIEM-Diensten auf anspruchsvollere Kompetenzen ermöglichen.

ANHÄNGE

Anhang 1: Szenario-Berechnungen und Datenquellen

Die Tabelle zeigt die Formeln und Datenquellen, die zur Berechnung der Kosten für das Szenario in Kleinbetrieben herangezogen wurden.

Alle Preisangaben für die Produkte von Trustwave entsprechen unseren üblichen Listenpreisen in den USA zum Zeitpunkt der Erstveröffentlichung dieses Dokuments. Preisänderungen vorbehalten. Aufgrund des Preismodells für die Produkte und Dienstleistungen von Trustwave unterscheiden sich die Preisangebote an Kunden nach den unterschiedlichen Dienstleistungstypen und der Anzahl an überwachten Geräten.

Investitionskosten		
	Selbstverwaltetes SIEM	**Verwaltetes SIEM**
SIEM-Gerät und Datenspeicherung	Produktpreis	
Schulung der Endnutzer • 5-tägige Schulung und Implementierung	Übliche Preisgestaltung für Dienstleistungen	Übliche Preisgestaltung für Dienstleistungen
Einführungskosten sind oben enthalten		
Implementierungsgebühr für verwaltetes SIEM • Einrichtung des Daten-Upstreaming an SOC • 1.000 USD bei Abonnements von einem Jahr und kürzer		Keine Einrichtungsgebühr, wenn der Kunde die Dienste für mehr als ein Jahr abonniert.
Investitionskosten insgesamt Jahr 1		
Betriebskosten		
	Selbstverwaltetes SIEM	**Verwaltetes SIEM**
Verwalteter SIEM-Dienst		Übliche Preisgestaltung für Dienstleistungen
Systemadministration	10 % der Standard-Systemadministration mit einem Gesamtgehalt von 99.136 USD und einem Gemeinkostenzuschlag von 33 %. Angaben zum Grundgehalt aus der IT-Gehaltsumfrage 2015 von ComputerWorld. Die Kosten für die Systemadministration in Großunternehmen ist mit Null angesetzt, weil die Kosten teilweise im fünften Informationssicherheitsanalysten unter „Compliance- und Überwachungsanalyst“ enthalten sind.	
Systemadministrationsdienst • Gesundheitscheck durch Trustwave		Übliche Preisgestaltung für Dienstleistungen

Wartung und Support (Hardware und Software)	Abonnementpreis	
Compliance- und Überwachungsanalyst	Komplettes Gehalt von 115.764 USD für einen Informationssicherheitsanalysten Angaben zum Grundgehalt aus der IT-Gehaltsumfrage 2015 von ComputerWorld. Vollzeitäquivalente Mitarbeiter (VZÄ): • Kleinbetrieb: 1 VZÄ • Mittelständischer Betrieb: 3 VZÄ • Großunternehmen 5 VZÄ	
Analyst für Sicherheits- und Bedrohungskorrelierung	Analyst für Sicherheits- und Bedrohungskorrelierung mit komplettem Gehalt von 130.340 USD und einem Gemeinkostenzuschlag von 33 %. Legt 10 % Aufschlag über einfachem Überwachungsanalysten zugrunde. Angaben zum Grundgehalt aus der IT-Gehaltsumfrage 2015 von ComputerWorld.	
Verwalteter Compliance- + Sicherheitsdienst • Compliance und Überwachung • Bedrohungskorrelierung		Übliche Preisgestaltung für Dienstleistungen
Behebung eskalierter Vorfälle durch interne Mitarbeiter	Anforderungen durch Überwachungs- und Bedrohungskorrelierungsanalysten gedeckt	Kosten für die Zeit von IT-Spezialisten zur Koordinierung mit den Sicherheitsdiensten von Trustwave und Behebung von Pannen am Standort. Zeit basiert auf durchschnittlicher Anzahl an Vorfällen pro Woche im Jahr multipliziert mit der durchschnittlichen Dauer der Behebung eines Vorfalls (4 Stunden). Szenario-Vorfälle: • Kleinbetrieb: 1 Vorfall pro Woche • Mittelständischer Betrieb: 3 Vorfälle pro Woche • Großunternehmen: 6 Vorfälle pro Woche Bei der Pannenbehebung mit verwaltetem SIEM wird vorhandenes Personal zugrunde gelegt. Dies sind zwar keine neuen direkten Lohnkosten, aber Opportunitätskosten für IT zur Beziehung von Ressourcen aus anderen IT-Projekten und -Funktionen.

Anwerbung von Mitarbeitern	Die Kosten für die Anwerbung von Mitarbeitern werden konservativ mit 20 % des ersten Jahresgehalts berechnet. Die Kosten für die Einstellung eines neuen Mitarbeiters werden mit zwischen 10 % und 100 % des ersten Jahresgehalts veranschlagt.	
Jährliche Schulung und Zertifizierung	Hier werden Kosten von 3.500 USD pro Mitarbeiter pro Jahr für Schulungen und die entsprechenden Zertifizierungen angesetzt. Dabei handelt es sich nur um die direkten Kosten dieser Maßnahmen (z. B. Lehrgangskosten, Reisen, Zertifizierungen); die Opportunitätskosten für die Zeit des Mitarbeiters sind nicht inbegriffen.	
Jährliche Betriebskosten insgesamt		
GESAMTKOSTEN JAHR 1		

Trustwave®

Smart security on demand