Log-Wächter

Christoph Puppe

Kein Administrator kann die Flut an sicherheitsrelevanten Daten mehr manuell bewältigen. Unterstützung leisten hier sogenannte SIEM-Werkzeuge. Die Marktübersicht stellt neun Stand-alone-Produkte im Detail vor.

iX-TRACT

- In jedem Unternehmen fallen Log-Meldungen der verschiedenen IT-Systeme so zahlreich an, dass ein einzelner Verantwortlicher sie ohne automatisierte Hilfe durch Software nicht mehr auswerten kann.
- SIEM-Systeme unterstützen den Verantwortlichen: Sie sammeln sämtliche Logdaten, korrelieren, interpretieren und speichern sie und schlagen bei relevanten Ereignissen Alarm. Kleinen Unternehmen nützen auch die teilweise vorhandenen Systemmanagementfunktionen.
- Die Grundfunktionen beherrschen alle auf dem Markt erhältlichen Systeme. Für den Nutzer ist es am wichtigsten, dass sich die Software an seine IT-Landschaft anpassen lässt und die vordefinierten Regeln schon so viele eigene Anforderungen wie möglich abdecken.

SIEM steht für „Security Information and Event Management“. Gemeint ist das Sammeln und Auswerten sämtlicher Meldungen von IT-Systemen und der zugehörigen Metadaten. Vom Syslog-Eintrag des Webservers über die Meldung eines erfolgreich gelöschten Virus bis hin zur Information, welches IT-System welchen Wert für die Organisation hat, lässt sich alles sammeln und verknüpfen. Der IT-Betrieb kann durch dieses Datamining Probleme teilweise schon vor dem Eintritt des Schadens identifizieren oder zumindest schnell und gut informiert auf kritische Situationen reagieren.

Auch im Zusammenhang mit dem allgegenwärtigen Schlagwort „Compliance“ entsteht zunehmend das Bedürfnis nach Kontrolle der eigenen Systeme. Gut archiviert, dienen die mit SIEM-Werkzeugen gewonnenen Informationen dem Nachweis, dass die Verantwortlichen Sicherheitsanforderungen umsetzen.

Erste Produkte kamen schon vor einigen Jahren auf den Markt, damals allerdings häufig noch getrennt nach SIM (Security Information Management) und SEM (Security Event Management): Erstere verarbeiteten die gesammelten Log-Informationen zu Reports und stellten Trends fest, Letztere korrelierten in Echtzeit Daten aus verschiedenen Systemen und schlugen bei sicherheitsrelevanten Ereignissen Alarm. Die heutigen Produkte sind weitaus komplexer und erfüllen beide Aufgaben.

Integriert oder „Einzelspieler“

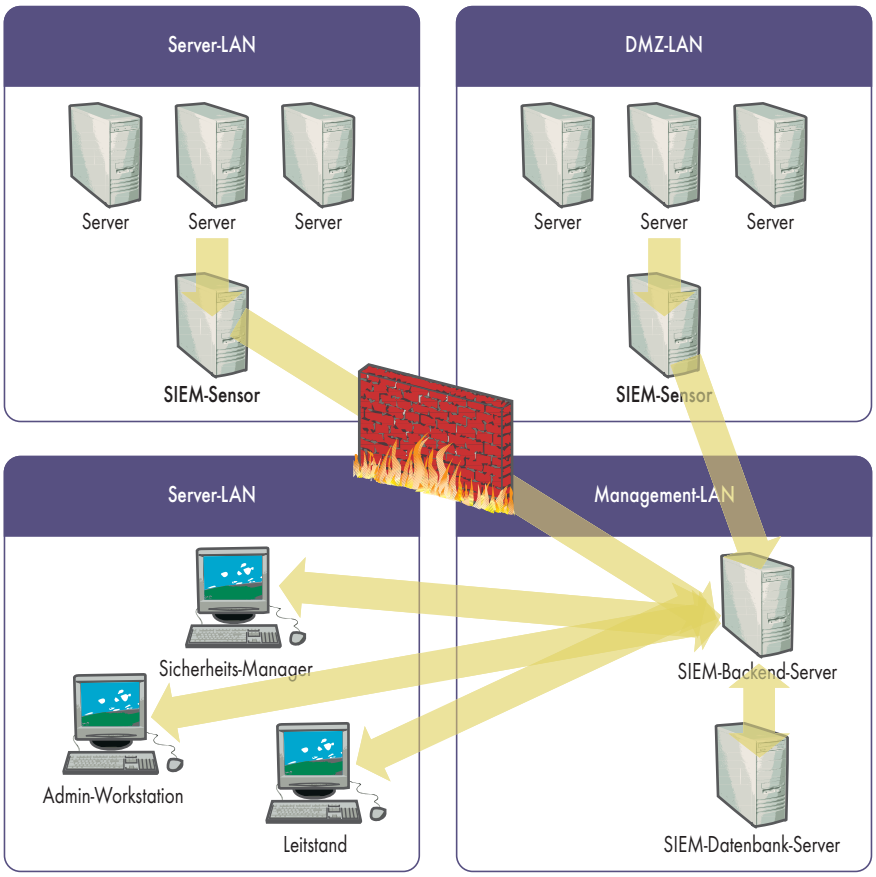
Eine differenzierte Darstellung der Produkte mit ihren Gemeinsamkeiten und spezifischen Eigenheiten ist nicht immer einfach, denn die Herangehensweise an das Thema SIEM unterscheidet sich stark. So integrieren etwa die Hersteller bekannter Systemmanagement-Software SIEM-Funktionen in ihre Software, was eine Nutzung als Standalone-Produkt in der Regel erschwert oder zumindest sehr teuer macht. Ihre Produkte finden sich nicht in der Tabelle, sondern im Kasten „Produkte mit integrierter SIEM-Funktion“. Ein anderer Hersteller, Cisco, hat sich nach dem Kauf eines SIEM-Produkts aus diesem Markt zurückgezogen und nutzt es nur noch für die eigenen Anwendungen. Auch er findet sich im erwähnten Kasten, nicht in der Marktübersicht.

Werkzeuge für Security Information and Event Management (SIEM)

Produkt	ArcSight Enterprise Security Manager (ESM)	enVision	EventsManager 2011	LogLogic Security Event Manager
Hersteller	ArcSight LLC (HP)	RSA (EMC)	GFI Software	LogLogic
Webseite	www.arcsight.com	www.rsa.com/envision	www.gfisoftware.de	www.loglogic.com
Whitepaper	www.arcsight.com/collateral/ArcSight_ProducTByterief_ESM.pdf	k. A.	www.gfisoftware.de/eventsmanager/esmpapers.htm	www.loglogic.com/sites/default/files/datasheets/360_insight_-_all-in-one_datasheet.pdf
Größe und Performance				
Größe der Live-Daten	> 1 TByte	bis 15 TByte	1,7 GByte	bis zu 8 TByte
Größe des Archivs	> 500 GByte	bis 15 TByte	1,7 GByte	bis zu 8 TByte
Ereignisse [1]	4 kEPS	7,5 kEPS (Appliance)	1,6 kEPS	150 kEPS (Appliance)
Geräte und Tickets	Geräte und Tickets	Geräte und Tickets	Geräte und Tickets	Geräte und Tickets
Datenbank der Systeme enthalten	✓	✓	–	✓
Wert der Systeme	✓	✓	–	✓
Tickets	✓	✓	–	–
Tickets exportieren	✓	✓	✓, per E-Mail und SNMP	✓
Mandanten				
mehrere Mandanten möglich	✓	✓	–	✓
Merkmale				
vordefinierte Regeln zur Korrelation	245	< 200	1240	70 generische, die herstellerunabhängig sind
Standardreporte	621 (zusätzliche erhältlich)	> 1400	152	> 100
eigene Reporte	✓	✓	✓	✓
Aktionen	SNMP, E-Mail, CLI, SOAP-Call, Start des ArcSight Threat Response Manager (TRM)	E-Mail, SNMP, CLI, SNPP, AIM, Beobachtungsliste	E-Mail, SNMP, CLI, VB-Skripte, SMS	E-Mail, SNMP, Syslog, CLI
vordefinierte Warungen	ESM und Logger zusammen ca. 100	< 200	1240	> 100, weitere erhältlich
eigene Warnungen	✓	✓	✓	✓
Abgleich mit Standards	ISO-27002- und Compliance-Pakete erhältlich für: PCI, SOX, IT-Governance, HIPAA, NERC	✓, z. B. SOX, PCI, ISO 27002, BASEL II, SAS 70, HIPAA, FISMA, Bill 198, NISPOM, NERC, Memo 22, GLBA	PCI DSS, HIPAA, GLBA, SOX, GCSx	SOX/COBIT, HIPAA, ITIL, FISMA, ISO, NERC, PCI
Quellen				
eigene Quellen	✓	✓, GUI	✓	✓, GUI
Syslog	✓	✓	✓	✓
Windows Event Log	✓	✓	✓	✓
SNMP Traps (v1/v2/v3)	✓, kein v3	✓, kein v3	✓	✓
W3C	✓	✓	✓	✓
Datenbanken	✓, per JDBC	✓	✓ (Oracle und MS-SQL)	✓ (5)
Firewalls	✓	✓	✓	✓ (32)
andere Quellen ohne Agenten	✓ (41)	✓ (ca. 230)	–	✓ (> 340)
andere Quellen mit Agenten	✓ (die meisten mit oder ohne Agent möglich)	–	–	✓ (5)
andere Netzwerk- und Systemmanagement-Tools				
Vulnerability Assessment	eEye REM, eEye Retina, Harris STAT, ISS Internet Scanner, Foundscan, nCircle IP360, Nmap, OVAL, Qualys Guard, NeXpose, NetRecon, Nessus, Visionael Security Audit, Saint	Foundscan, nCircle IP360, Nessus, QualysGuard, SiteProtector	–	Nessus, QualysGuard u. a.
NetFlow	✓	✓	–	✓
NetMRTG	–	–	–	✓
Verfügbarkeitsüberwachung	–	✓	✓	✓
Überwachung von Antwortzeiten	–	–	–	✓
Host Intrusion Detection System	–, Anbindung an Drittanbieter	–, Anbindung an Drittanbieter	–	✓
Network Intrusion Detection System	–, Anbindung an Drittanbieter	–, Anbindung an Drittanbieter	–	–, Anbindung an Drittanbieter
sonstige Aspekte				
aktuelle Version	V 5	V 4.0 SP4	2011	3.5
auf dem Markt seit	2002	1999	2003	2004
deutscher Support/Niederlassung	✓	✓	✓, deutsche Firma	✓, allerdings nicht aus Deutschland
eigene Software für die Bedienung [2]	✓	✓	✓	–
Managed Service	✓	✓, durch Partner	–	✓, durch Partner
erhältlich als Software	✓	–	✓	✓
erhältlich als Appliance	✓	✓	–	✓
Preise (netto)	ab 48 000 € plus Support und Wartung ab 15 % des Nettopreises	k. A.	pro Asset bei 250–499 €; 85 € pro Server (inkl. Switch, Router, Firewall, DB); 11 pro Workstation (Microsoft Windows 2000, XP, Vista, 7)	k. A.
Lizenzmodell	System, Benutzer und Kerne	Appliance	System	Appliance

✓ = ja/vorhanden/trifft zu, – = nein/nicht vorhanden/trifft nicht zu, k. A. = keine Angabe, [1] pro Sekunde in tausend (Dual Xeon 3,2 GByte wie XSERIES 346 oder Appliance), [2] nicht Web

	NitroView Enterprise Security Manager (ESM)	QRadar Security Intelligence Platform	Smart Event Software Blade	Unified SIEM	VIA – Log Center
	NitroSecurity	Q1 Labs	CheckPoint	AlienVault	Tripwire
	www.nitrosecurity.com	q1labs.com	www.checkpoint.com	www.alienvault.com	www.tripwire.com
	www.nitrosecurity.com/SIEM/?LinkServID=0B9A87D6-E533-5A1B-5D6C375321DC5C4A&showMeta=0	q1labs.com/resource-center/white-papers.aspx	www.checkpoint.com/products/downloads/datasheets/SmartEvent-software-blade-datasheet.pdf	www.alienvault.com/docs/AlienVault_Solution_Datasheet.pdf	www.tripwire.com/register/?resourceId=9855&cat=Log-Management&type=wp
	bis zu 7 TByte	6 TByte	unbeschränkt	0,5 TByte	unbeschränkt
	unbeschränkt	6 TByte	unbeschränkt	0,5 TByte	unbeschränkt
	bis zu 25 kEPS (Appliance)	10 kEPS	2,3 kEPS	5 kEPS	1 kEPS
	Geräte und Tickets	Geräte und Tickets	Geräte und Tickets	Geräte und Tickets	Geräte und Tickets
	✓	✓	✓	✓	✓
	✓	✓	✓	✓	–, für 2011 geplant
	✓	–	✓	✓	✓
	nur beim Produkt Remedy	✓	✓	✓	✓
	✓	✓	✓	✓	–
	ca. 150	mehrere Hundert	> 100	> 600	ca. 100
	600	> 1300	> 80	> 1800	> 100
	✓	✓	✓	✓	✓
	Datei, SNMP, E-Mail, Syslog (ab 9.0 CLI und Ticket)	E-Mail, SNMP	E-Mail, SNMP, CLI	E-Mail, SNMP, SQL, WMI-Befehle, CLI	E-Mail, CLI, Syslog, *wall*
	– (ab 9.0 enthalten)	mehrere Hundert	> 100	> 700	> 100
	✓	✓	✓	✓	✓
	HIPAA, PCI-DSS, PA-DSS, NERC CIP, SOX, BASEL II, EU 8th, GLBA, GIODO, and ISO 17799	mehrere Hundert inkl. PCI DSS, NERC/FERC, SOX, NIST, FISMA, HIPPA, GPG-13, FSA, Code of Connections	ISO 17799, COBIT, PCI-DSS, SOX and HIPAA	PCI, ISO27001, HIPAA, SOX etc.	> 200, inkl. PCI, CIS, NIST, DISA, NERC, ISO 27001
	✓	✓	✓	✓, GUI	✓, GUI
	✓	✓	✓	✓	✓ (130)
	✓	✓	✓	✓	✓ (9)
	✓	✓	✓	✓	✓ (5)
	✓	✓	k. A.	✓	–
	✓, Logs und Transaktionsüberwachung	✓	✓	✓	✓ (Oracle)
	✓	✓ (5)	✓	✓	✓ (26)
	✓ (> 700)	✓ (8)	✓, Symantec, TrendMicro, Blue Coat, Cisco, Fortinet, Juniper etc.	> 2395	✓ (32)
	eigener Agent, Snare, Adiscon	–	✓, Windows Events in Syslog-Meldungen übersetzt	> 2395	MS Windows NT, MS Windows XP, MS Windows Vista, MS Windows 7, MS Windows 2000, MS Windows 2003, MS Windows 2008
	Nessus, Foundstone, eEye Retina, Lumension, nCircle, QualysGuard, Rapid7, Saint	eEye REM, Foundscan, Juniper NSM Profiler, nCircle IP360, Nessus, Nmap, Patchlink Scan, QualysGuard, NeXpose, Saint, SecureScout	–	Nessus, openVAS, Nikto	Retina REM Console, GFI Languard, Harris STAT, SiteProtector, NeXpose, Nmap, QualysGuard, Nessus
	✓	✓	–	✓	✓, Drittanbieter per Syslog
	✓	✓	–	✓	✓, Drittanbieter per Syslog
	✓	✓	✓	✓	–
	teilweise	✓	–	✓	–
	–, Anbindung an Drittanbieter	–, Anbindung an Drittanbieter	–	✓	Datei-Integritätstests
	–, Anbindung an Drittanbieter	–, Anbindung an Drittanbieter	✓	✓	–
	8.5	7.0	R75	3.0	6.2
	2007	2005	2005	2003	2004
	–, London	✓	✓	✓	✓
	–	–	✓	–	✓
	–	✓, durch Partner	✓	✓	✓
	teilweise, Receiver ✓, ESM nur Appliance	✓	✓	✓	✓
	✓	✓	✓	✓	–
	ab 21 995 €	ab 17 900 US-$	ab 4000 US-$ (SmartEvent Intro blade)	8420 € Appliance inkl. 0,5 kEPS Sekunde; 28 100 € Appliance inkl. 5 kEPS/Sekunde	pro Asset und Jahr: Server: 127 US-$, 25 US-$ Wartung, Network Devices: 192 US-$, 38 US-$ Wartung, Security Devices: 319 US-$, 64 US-$ Wartung
	Appliance	Appliance	System	EPS	System



Eine typische Architektur eines SIEM nutzt pro Netzsegment einen Sensor, der die Meldungen an den Backend-Server weiterleitet, auf den wiederum die Benutzer zugreifen. So können auch aus abgeschotteten Umgebungen die Meldungen zum SIEM gelangen. Die Verbindungen zwischen Sensor und SIEM-Backend sind üblicherweise stark verschlüsselt und authentifiziert.

In Artikel und Tabelle werden Standalone-Werkzeuge vorgestellt, die hierzulande erhältlich sind. Von 16 angeschriebenen Herstellern füllten neun einen detaillierten Fragebogen aus, die anderen – samt und sonders amerikanische Hersteller – scheinen den deutschen Markt nicht zu bedienen.

Die Standardfeatures sind bei allen Produkten vorhanden und daher nicht in der Tabelle aufgeführt. So archivieren etwa alle Produkte die gesammelten Daten für den Bedarfsfall einer forensischen Analyse. Als Beweis dafür, dass sie nicht manipuliert wurden, sind sie mit kryptografischen Prüfsummen versehen. Ob ein Gericht sie als Beweis anerkennt, hängt allerdings von vielen Faktoren ab, etwa dem Schutz der Daten und der Systeme. Sind sie nicht hinreichend gesichert, könnte ein Administrator oder ein Angreifer auf einem kompromittierten System die Daten verändern und ihre Prüfsummen fälschen. Hier könnte das Einbinden eines externen Stempeldienstes hilfreich sein, denn dieser ist kaum zu manipulieren. Diese Option bietet jedoch kein Produkt.

Wer im Unternehmen mit dem SIEM arbeiten soll, ist meistens klar – in der Regel die Sicherheitsverantwortlichen, oder, falls diese nicht explizit vorhanden sind, die Systemadministration. Zudem werden die Warnungen oft auf Leitständen angezeigt. Allerdings ist besonders bei einer Software mit so weitreichenden Einblicken und teilweise auch Rechten ein abgestuftes Rollenkonzept erforderlich. Dieses Grundfeature ist in allen Produkten umgesetzt und daher nicht in der Tabelle aufgeführt. Ebenso wenig wie die unumgängliche Nutzung von Verschlüsselung zur Kommunikation mit der Software oder für die Verbindungen zwischen den auf den Systemen eingesetzten Agenten und der Zentrale.

Nicht ohne Verschlüsselung

Einfach zu vergleichen sind auch die Funktionen für die Suche nach Details wie einzelne Ereignisse, Systeme, Uhrzeit et cetera, die Zusammenfassung der Meldungen etwa zu einem sicherheitsrelevanten Ereignis und das Navigieren aus der Zusammenfassung heraus zu Details. Sie sind gleichermaßen bei allen Produkten vorhanden. Unterschiedlich ist allerdings die Anzahl der vordefinierten Regeln für die Korrelation der einzelnen Ereignisse.

Die bloße Anzahl der Regeln ist jedoch nur bedingt aussagekräftig. Manches Produkt enthält eine Regel pro Datenquelle und damit insgesamt sehr viele. Andere verarbeiten in einem ersten Schritt die Meldungen dergestalt, dass das SIEM Meldungen eines Typs, zum Beispiel fehlgeschlagene Anmeldeversuche, bereits in verallgemeinerter Form einträgt. Dann reichen nur wenige Regeln für die gleichen Funktionen. Beide Ansätze haben ihre Vor- und Nachteile, und insgesamt gilt immer, dass für jeden Datenlieferanten auch eine Regel zum Import vorhanden sein muss.

Wer ein SIEM auswählt, sollte zuallererst darauf achten, dass es alle im eigenen Unternehmen betriebenen IT-Systeme erfasst. Oder anders ausgedrückt: Das Produkt sollte zu von diesen Systemen stammenden Meldungen vordefinierte Regeln zur Entgegennahme und Speicherung enthalten. Fehlende Regeln selbst zu erstellen oder erstellen zu lassen, sollte die Ausnahme sein. So wie der Hersteller die Regeln für die Normalisierung der Meldungen möglichst aller eingesetzten Systeme mitliefern sollte, sollten auch die Regeln für die Korrelation möglichst umfangreich im Preis enthalten sein. Die Einführung eines SIEM ist immer ein Projekt mit vielen Anpassungen an die eigene Systemlandschaft. Daran ändert sich nicht viel, selbst wenn die Software umfangreiche Regelwerke mitbringt. Aber sie können den Aufwand, bis der Leitstand die erste Meldung sieht, teilweise erheblich reduzieren.

Alles unter einem Hut

Viele Korrelationen sind in den meisten Umgebungen gleich oder ähnlich. Fehlerhafte Anmeldungen, unautorisierte Zugriffe, Fehler in der Hardware, Meldungen von NIDS und HIDS (Network Intrusion Detection System/Host Intrusion Detection System) und so weiter sind meist einen Alarm wert. Wenn noch nicht beim ersten Auftreten, so doch zu-

mindest, wenn die Meldungen die eingestellten Schwellwerte von Ereignissen pro Zeiteinheit überschreiten. Daraus resultiert auch die Frage an die Hersteller, wie viele vordefinierte Warnungen er bereits mit der Software ausliefert.

Für die Berichte gilt das Gleiche. Die Software sollte einen umfangreichen Satz mitbringen. Hier ist die Besonderheit, dass es oft notwendig ist, die Umsetzung von Standards der IT-Sicherheit nachzuweisen. Mithin liefert dies meist den Grund für die Einführung eines SIEM, und es existiert ein entsprechendes Budget. Die Tabelle gibt eine Übersicht darüber, welche Berichtsoptionen in den Produkten enthalten sind und welche Standards sie abdecken.

Wünschenswert ist auch, dass die Software bei Berichten, Eingangs-, Korrelations- sowie Alarmierungsregeln benutzbare und praxiserprobte Standards mitbringt. Allerdings scheitert das Projekt, wenn Administratoren diese nicht an den eigenen Betrieb anpassen können. Jedes der vorgestellten Softwareprodukte bietet die Möglichkeit, die Regeln dieser vier Kernfunktionen selbst zu erstellen. Nur bei den eigenen Quellen, also den Regeln für den Dateneingang, gab es bei den Antworten der Hersteller Unterschiede, da hier manche eine grafische Oberfläche anbieten, während die meisten einen Texteditor für Skripte, reguläre Ausdrücke und Ähnliches verlangen.

Teil des Systemmanagements

Neben den Berichten und Warnungen bieten SIEM-Produkte verschiedene Möglichkeiten, auf Ereignisse automatisiert zu reagieren. Die Unterschiede sind jedoch erheblich. Während manche nur E-Mails und Meldungen als Reaktion vorsehen, bieten andere die Option, per Kommandozeile oder SNMP (Simple Network Management Protocol) in Millisekunden auf Probleme, Angriffe oder anderes zu reagieren.

Da solche Reaktionen auf Ereignisse durch Regeln ausgelöst werden, ist im IT-Betrieb ein hohes Maß an Automatisierung möglich. Und nicht nur, was die Sicherheit betrifft. Das SIEM kann neben der Überwachung auch als aktiver Bestandteil eines Systemmanagements agieren. Da dies jedoch einige Risiken mit sich bringt und eine sehr genaue Analyse der Ursachen von Meldungen und der möglichen Reaktionen voraussetzt, setzt es kaum ein IT-Betrieb dafür ein. Beispielsweise wäre es zwar möglich, auf einen speicherfressenden Prozess durch einen Befehl auf der Kommandozeile zu reagieren, aber das will gut durchdacht sein. Es könnte sonst passieren, dass man den falschen Prozess oder den richtigen Prozess zur falschen Zeit erwischt oder aus Versehen den Switch-Port des Standard-Gateways abschaltet und somit das ganze Netz lahmlegt.

Zentrale Ticket-Systeme verschaffen Übersicht

Die meisten Produkte ermöglichen für die Integration in ein Systemmanagement den Export von Tickets. Die Alarme und Warnungen wandern so in ein zentrales Ticket-System, mit dessen Hilfe der Leitstand einen zentralisierten Blick auf alle Vorkommnisse hat. Hier

unterscheiden sich die Produkte leicht voneinander, manche bieten ein eingebautes Ticket-System, andere können nur zu einem exportieren.

Teilweise gehen die Hersteller bei der Zusammenfassung unterschiedlicher Aspekte des Systemmanagements noch einen Schritt weiter, indem sie auch die Verfügbarkeits- und Auslastungsüberwachung integrieren. Die Produkte übernehmen teilweise die Auswertung des Monitoring-Tools NetMRG und von Netflow sowie die Abfrage von Antwortzeiten. Für einen kleineren Betrieb ist dies ungemein praktisch. Denn diese haben meistens nicht in ein umfangreiches Projekt zur Kontrolle der Verfügbarkeit investiert. Wo ein Systemmanagement mit diesen Funktionen bereits eingesetzt wird, ist diese Funktion des SIEM nicht erforderlich.

Für den Bearbeiter einer Warnung von entscheidender Bedeutung ist die Relevanz der Meldung und der Wert des betroffenen Systems für die Organisation. Daher können alle bis auf ein SIEM verdeutlichen, wie hoch sich dieser Wert bemisst. Die Funktion erreicht im besten Fall die eines kompletten Asset-Management-Systems.

Weitere Lieferanten von Daten, die die Hersteller mit in die Datenbasis aufgenommen haben, sind sogenannte Verwundbarkeitsscanner. Der Vorteil ist hier, dass das SIEM Meldungen mit den Ergebnissen des letzten Schwachstellenscans vergleichen kann. Entweder automatisiert, was nicht einfach ist, oder zumindest manuell, bei der Analyse eines Ereignisses. So kann der Bearbeiter sich innerhalb einer Oberfläche ansehen, ob die Meldung von einem System kommt, das eine Schwachstelle hat. Ähnlich sieht es mit den Meldungen von Intrusion-Detection-Systemen aus. Das SIEM bildet hier die zentrale Konsole, die die Daten von beiden zusammengefasst anzeigt – eine Funktion, die nicht unbedingt im Zusammenhang mit den aktuell eingehenden Meldungen steht. So ist dies bei den Anbietern, die gleich mit einem SIEM auf den Markt kamen, üblicherweise stärker ausgeprägt als bei denen, die von der reinen Meldungsanalyse kommen.

Geschwindigkeit und Hexerei

Das wohl am schwierigsten zu vergleichende und für die Entscheidung wesentliche Kriterium ist die Architektur der Sensoren, Agenten und zentralen Systeme. Sie beeinflusst zusammen mit der Geschwindigkeit jedes einzelnen Sensors die insgesamt zu erreichende maximale Anzahl von Ereignissen pro Sekunde, die das SIEM entgegennehmen und verarbeiten kann. Bis auf einen Hersteller können alle eine beliebige Zahl von Sensoren kaskadiert aufstellen. Da jeder Sensor bereits Verarbeitungsschritte durchführt, können die Produkte eine fast beliebige Menge an Meldungen entgegennehmen. Eine Ausnahme bildet hier enVision von RSA mit einem Limit von 3 SIEM-Geräten pro „Site“ (so nennt RSA eine Installation). Die Sites sind bei enVision voneinander getrennt, Suchen gehen aber über alle Sites hinweg.

Die von den Herstellern genannten Geschwindigkeiten pro Sensor beziehen sich – bis auf die Appliances – auf das Referenz-Modell (Dual Xeon 3,2 GByte wie ein XSERIES 346). Ähnlich schwierig ist die Angabe der maximalen Datenmengen. Die Angaben sind entweder auf die Größe einer Appliance bezogen oder auf typische Einsatzszenarien. Da alle mit Datenbanken für die Live-Daten und Dateisystem für das Archiv arbeiten, sind die maximalen Zahlen im Prinzip nur von der bereitgestellten Festplattengröße abhängig.

Für die Kaufentscheidung insbesondere kleiner Unternehmen ist sehr wichtig, in welcher Form das SIEM angeboten wird. Kann man die Software auf eigenen Servern installieren oder muss man eine Appliance kaufen? Wem selbst die Appliance noch zu viel Belastung für die eigene Mannschaft ist, der kann bei fast allen Herstellern einen Managed Service erstehen. Die Lizenzmodelle unterscheiden sich gravierend. Drei Ansätze verfolgen hier die Hersteller: Entweder nach Meldungen pro Sekunde, nach Anzahl der überwachten Systeme oder nach betriebenen SIEM-Servern. Ein Hersteller nimmt gleich alle drei Kennzahlen und errechnet daraus einen Preis. Den eigenen Bedarf vor dem Kauf durchzurechnen, spart bei einem kleinen Unternehmen den einen oder anderen Euro.

Fazit

Ohne Hilfe kann heutzutage kaum jemand mehr die Fluten an Sicherheits- und anderen Meldungen seiner Systeme bewältigen. SIEM-Produkte leisten hier hervorragende Unterstützung – insbesondere, wenn Unternehmen nach gesetzlichen Regularien spezielle Sicherheitsmaßnahmen nachweisen müssen oder wenn diese Produkte in kleineren Betrieben gleichzeitig Systemmanagementfunktionen übernehmen. Wichtig vor dem Kauf ist eine Analyse der eigenen Systeme und deren Unterstützung durch das infrage kommende Produkt, desgleichen eine Analyse der vordefinierten Regelsätze. Denn alles, was das SIEM nicht mitbringt, muss man selbst anpassen – was aber zwingend möglich sein sollte. (ur)

Produkte mit integrierter SIEM-Funktion

Tivoli Security Operations Manager	www-01.ibm.com/software/tivoli/products/security-operations-mgr
Symantec Security Information Manager	www.symantec.com/business/security-information-manager
CA Total Defense	www.ca.com/us/products/category/it-security-solutions/Threat-Management.aspx
Novell Sentinel	www.novell.com/de-de/products/sentinel/
Cisco Security Monitoring, Analysis and Response System (MARS)	www.cisco.com/en/US/products/ps6241/index.html

CHRISTOPH PUPPE

ist leitender Sicherheitsberater bei der HiSolutions AG in Berlin.

Literatur

[1] Christoph Puppe; SIM; Logfeuerwehr; Systemlogs auswerten und Netzwerk überwachen mit OSSIM; *iX* Special Sicher im Netz 3/2010, S. 74

[2] Christoph Puppe; Log-Auswertung I; Guter Griff; Datamining bei Meldungen von Sicherheitssystemen; *iX* Special Sicher im Netz 2008, S. 106

[3] Stefan Middendorf; Log-Auswertung II; Ereignis-Reich; Möglichkeiten und Grenzen von SIEM-Tools; *iX* Special Sicher im Netz 2008, S. 110

Alle Links: www.ix.de/ix1104108