Datamining bei Meldungen von Sicherheitssystemen

Guter Griff

Christoph Puppe

Sim City kennt fast jeder, SIM-Tools noch nicht: Security Information Management soll Netzwerkverantwortlichen das Leben erleichtern und aus den kaum mehr überschaubaren Meldungen der verschiedenen Sicherheitssysteme nur die wirklich relevanten Vorkommnisse extrahieren.

Wenn es um die Meldungen von Firewalls, Virenscannern, Intrusion-Detection- und anderen sicherheitsrelevanten Systemen im Netz geht, sieht auch der motivierteste Administrator bald den Wald vor lauter Bäumen nicht mehr – in größeren Netzen sind mehrere Millionen pro Tag die Regel. Und selbst in kleineren Netzen reicht die Anzahl aus, um den menschlichen Analysten zu überfordern. Abhilfe schaffen soll das Datamining bei Sicherheitsmeldungen – genannt Security Information Management (SIM) oder auch Security Event Management (SEM).

SIM-Tools sind im weitesten Sinne vergleichbar mit Trouble-Ticketing-Systemen wie Tivoli, Remedy oder OpenView, die schon seit Jahren das Problemmanagement in puncto Unternehmenshardware unterstützen. Sie sammeln Meldungen über deren Betriebszustand und informieren den Administrator. Ein Ausfall verursacht oft eine ganze Reihe von Meldungen, die ein Ticketing-System zusammenfasst und als ein Ereignis meldet. Darauf kann der Administrator nun reagieren, nach dem Bearbeiten des Vorfalls wird das Ticket geschlossen.

Bei den Meldungen, die die Sicherheitsanwendungen erzeugen, ist das nicht so einfach. Eine Meldung kann zum Beispiel den Fund eines Virus auf einem Arbeitsplatz anzeigen. Der Virenscanner hat darauf bereits reagiert, menschliches Eingreifen ist nicht mehr erforderlich. Oder die Firewall meldet verbotene Verbindungsversuche, die Verbindung kam jedoch nicht zustande. Eine Bearbeitung des Vorfalls ist ebenso unnötig wie ein durch das Intrusion Detection System (IDS) angezeigter Angriffsversuch.

Potenzielle Spuren bewahren

Dennoch kann man all diese Meldungen nicht ignorieren oder löschen. Der Sicherheitsverantwortliche muss sie zumindest für wenige Monate archivieren, damit er einen Einbruch oder Virenausbruch im Nachhinein analysieren oder den Beweis für eine Täterschaft finden kann. Da es nicht möglich ist, diese Informationen auf den Geräten, die sie produzieren, zu sammeln, ist eine zentrale Speicherung notwendig. Nur so kann man sicherstellen, dass etwa ein Einbrecher nicht die Logfiles des übernommenen Systems vernichtet und damit seine Spuren beseitigt.

Der zweite wichtige Aspekt bei der Bearbeitung der Daten ist die Suche nach schwerwiegenden Vorfällen, die zwingend menschliches Eingreifen erfordern. Zwar ist ein einziger entdeckter Virus noch kein Grund zur Sorge, aber eine von Minute zu Minute steigende Zahl von Viren kann ein Hinweis auf einen Ausbruch sein, den die Systeme nicht mehr beherrschen. Oder es wird ein Einbruchsversuch auf einem Server der DMZ gemeldet – an sich kein Problem. Wenn dieser Server allerdings kurze Zeit später Angriffe auf Systeme im Intranet startet, sollten die Alarmglocken laut schrillen.

Die Schwierigkeit, die die Verwaltung dieser Meldungen mit sich bringt, ist also ihre sinnvolle Verknüpfung, um aus den Millionen Meldungen diejenigen herauszufiltern, die auf einen gravierenden Sicherheitsvorfall hinweisen. Dazu müssen die Benachrichtigungen aller Systeme miteinander verglichen, Gemeinsamkeiten ausgemacht und Warnungen an den Administrator ausgegeben werden. Diese nicht gerade geringe Aufgabe sollen die SIM-Tools meistern.

Der erste Schritt besteht darin, alle Meldungen zu sammeln. Das betrifft zunächst die Intrusion-Detection-Systeme, Firewalls, Virenscanner und sonstige zur Absicherung eingesetzte Systeme wie Screening-Router. Allerdings können auch die Logfiles von Servern und physikalischen Zutrittssystemen spannende Informationen liefern: So kann zum Beispiel eine hohe Last auf dem Mailserver ein Indiz für einen sich verbreitenden Wurm sein.

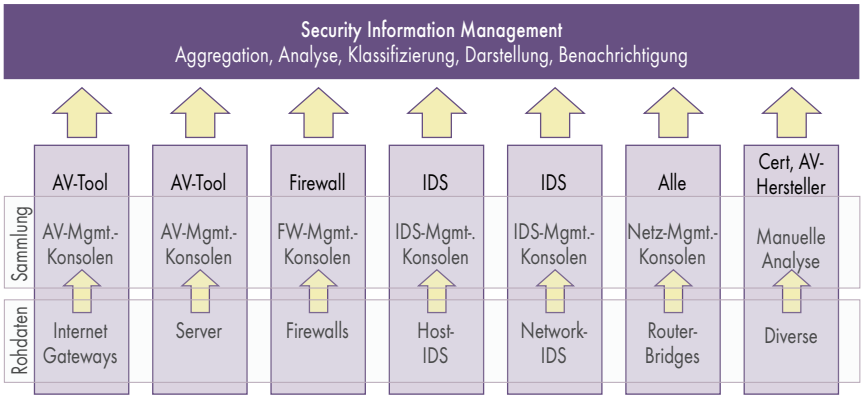
In der Praxis bedeutet das, dass die Software eines SIM-Herstellers in der Lage sein muss, die Daten von allen im Zielnetz eingesetzten Geräten zu importieren. Zwar bietet jedes der meldenden Produkte die Möglichkeit, alle Benachrichtigungen zentral in einer Managementkonsole zu sammeln und

teilweise auch bereits zusammenzuführen, eine tiefergehende Analyse ist meistens jedoch nicht durchführbar. Zudem kocht fast jeder Hersteller sein eigenes Süppchen.

Einige gehen so weit, dass sie keine verbreiteten Standards einsetzen, sondern eigene Protokolle benutzen, um die Meldungen zu versenden. In der Praxis werden die Daten aber meistens über Syslog oder SNMP übertragen – ohne Authentifizierung oder gar Verschlüsselung. Syslog transportiert die Daten überdies in UDP-Paketen durch das hoffentlich vom Produktivnetz getrennte Managementnetz.

Alle SIM-Anbieter halten eine lange Liste mit Soft- und Hardware bereit, die ihr Produkt unterstützt. Manche Hersteller sehen auch die Erstellung eigener Module vor, die unübliche Geräte anbinden. Wer sich nicht sicher ist, ob ein SIM-Tool die eingesetzte Version unterstützt, sollte sich das beim Hersteller direkt bestätigen lassen.

Die Exportfunktionen zu nutzen ist eine der Möglichkeiten, an die gesammelten Daten zu kommen – die neben den genannten Sicherheitsbedenken beim Transport auch andere unerwünschte Effekte erzielen kann. So startet IBMs Tivoli für jede neue Meldung, die aus ihm exportiert wird, einen neuen Prozess, was zu erheblicher Last auf dem System führt. Alternativ hat der Administrator bei einigen Produkten auch die Option, einen Agenten zu installieren, der auf den Systemen die Meldungen sammelt und



Die SIM-Software importiert die Daten der sicherheitsrelevanten Systeme in einem Netz, analysiert sie in Abhängigkeit voneinander und schlägt bei bedenklichen Ereignissen Alarm (Abb. 1).

über meist gut verschlüsselte, propietäre Protokolle an das SIM-Tool schickt. Dabei muss man die verbesserte Sicherheit allerdings mit einem stark erhöhten Installationsaufwand für die zusätzliche Software auf allen meldenden Systemen bezahlen.

Die entstehenden Datenmengen können schnell beträchtliche Ausmaße annehmen, nicht zuletzt, weil die Meldungen für Nachweiszwecke komplett abzuspeichern sind. Die gesetzlichen Anforderungen an Speicherfristen – Stichwort Basel II, Sorbanes-Oaxley und die Vorschriften der ordentlichen Buchhaltung – sowie Branchenstandards wie ISO 17799 sehen nicht unerhebliche Aufbewahrungszeiträume vor. Diese Aspekte müssen Anwender bei der Kapazitätsplanung der von den SIM-Tools genutzten Datenbanken bedenken.

Auch für den Transport der Daten ist die Menge der zu erwartenden „Events pro Sekunde“ (eps) zu berücksichtigen. Besonders während eines Wurmausbruchs können die übertragenen Datenmengen schnell die vorhandene Leitungskapazität ausreizen und so zum Stillstand der WAN-Strecken führen.

Um das Sammeln der Informationen aus vielen unterschiedlichen Segmenten des Intranets zu unterstützen, bieten fast alle Produkte die Möglichkeit, die Meldungen pro Intranet-Segment auf ein System zu schicken, das diese dann über eigene Protokolle verschlüsselt und komprimiert an die Zentrale weiterleitet. So kann man vermeiden, dass SNMP und Syslog beispielsweise aus der DMZ zum SIM erlaubt werden müssen. Auch muss die Firewall zwischen den Segmenten lediglich einen offenen Port von einem System zum SIM zulassen.

Wenn die Meldungen im SIM angekommen sind, beginnt die eigentliche Arbeit. Wie beim klassischen Datamining werden nun alle Daten in Relation zueinander untersucht. Ziel ist es, Meldungen zu finden, die auf eine gemeinsame Ursache zurückzuführen und damit zu einem Ereignis (Event) zusammenzufassen sind. Ein Beispiel ist der Wurm, der auf mehreren hundert Systemen aktiv ist. Er erregt durch seine Suche nach weiteren verwundbaren Systemen die Aufmerksamkeit der Firewalls und Intrusion-Detection-Systeme, die diese Aktivität melden. Nun ist es die Aufgabe des SIM, die gemeinsame Ursache zu identifizieren und ein Ereignis zu präsentieren, das eine Liste aller betroffenen Systeme enthält. Der Administrator ist damit in der Lage, das Ereignis zu bearbeiten und die Systeme vom Netz zu trennen. Ohne das SIM wäre er allein mit der manuellen Analyse der IDS-Daten Stunden beschäftigt gewesen.

Individuelle Anpassung erfolgsentscheidend

Alle SIM-Tools haben eine eingebaute Logik, die der Benutzer meist mehr oder weniger einfach um eigene Filter und Regeln erweitern kann. Wie bei einem IDS entscheidet auch hier über den Erfolg der Installation, wie gut man Letztere auf das Netz anpasst. Wer mit einem Security Information Management liebäugelt, sollte sich vor dem Kauf das Benutzerinterface zum Erstellen der Regeln ansehen und dabei die Mitarbeiter einbeziehen, die diese im laufenden Betrieb ergänzen sollen.

Grob kann man zwei Arten der Analyse unterscheiden: die Trendanalyse, die die Ereignisse eines Zeitraums untersucht und nach Entwicklungen forscht, die sich währenddessen

iX-TRACT

- Damit Systemverantwortliche der vielen tausend sicherheitsrelevanten Meldungen in der Firmen-IT Herr werden, bieten immer mehr Hersteller Produkte aus der neuen Kategorie der Security-Information-Management-Tools an.
- Richtig eingesetzt und geplant entlastet ein Management der Security-Meldungen Administratoren sowie Mitarbeiter und dient im Ernstfall dem Nachweis sicherheitsrelevanter Vorfälle.
- Den Kinderschuhen sind die Produkte zwar entwachsen, an der Zusammenarbeit mit Schwachstellen- und Patchmanagementsystemen müssen die Hersteller allerdings noch arbeiten.

ergeben haben, und die Echtzeit-Analyse, die die Daten im Augenblick des Eintreffens bewertet. Beide haben ihren Platz im Sicherheitsmanagement. Der Trend ist ein guter Indikator für langsam ablaufende Vorgänge. Wenn etwa ein Angreifer sich sehr langsam dem Netzwerk nähert, sollten alle Meldungen, die sein Vorgehen erzeugt, in einer solchen Analyse einem Täter zugeordnet werden können. Oder wenn zum Beispiel in einer Filiale immer wieder ähnliche Probleme auftauchen, kann man die Häufung erst durch die langfristige Beobachtung erkennen.

Bei der Echtzeitanalyse dagegen steht die schnelle Reaktion auf gerade passierende Ereignisse im Vordergrund. Das SIM verbindet beispielsweise die bis jetzt ignorierte IDS-Meldung von gestern über den eventuellen Angriff gegen ein System mit den eben stattfindenden Versuchen, sich als Administrator an diesem System anzumelden. Erst durch die Verbindung der beiden Meldungen kommt es zum Erstellen eines hoch priorisierten Vorfalls, der dem Administrator zur Bearbeitung vorgelegt wird. Bis das SIM wie ein Intrusion Prevention System (IPS) reagiert und die Verbindungen des Angreifers auf der Firewall automatisch unterbindet, dauert es allerdings noch eine Weile.

Klassifizierung der Meldungen

Jedes System muss eine Meldung zunächst als meldenswert oder nicht klassifizieren, bevor es sie an das SIM weitergibt. Der Administrator kann beispielsweise einstellen, dass nur Meldungen ab der Stufe „warn“ auf den als Syslog-Host eingetragenen Sammler des SIM geschickt werden. Die zweite Klassifizierung der Meldung erfolgt durch das SIM, im Zusammenhang mit allen weiteren über das jeweilige System vorliegenden Meldungen. Die zweite Klassifikation ist letztlich entscheidend dafür, ob der aus vielen Meldungen zusammengestellte Vorfall die Alarmkette in Gang setzt.

Wie schnell oder langsam der Alarm ausgelöst wird, hängt zum Teil von der Bewertung der Systeme durch den Administrator ab. Diese Option bieten leider nicht alle Hersteller, obwohl es den Betrieb des SIM enorm unterstützen könnte – etwa in der Entscheidung, ob ein Ereignis ein kritisches System betrifft. Ein Angriff auf ein wichtiges E-Commerce-Portal würde in dem Fall schneller Alarm auslösen als der gleiche Angriff auf ein Testsystem ohne echte Daten.

Eine weitere Möglichkeit ist die Klassifizierung nach Relevanz: Wenn ein Angriff auf ein nicht verwundbares System entdeckt wird, ist beispielsweise die Priorität deutlich niedriger anzusetzen als wenn ein verwundbares System das Ziel ist. Die dafür notwendigen Daten aus dem Schwachstellen- und Patch-Management sind jedoch nicht immer verfügbar, und eine direkte Verbindung dieser Managementsysteme ist eher noch die Ausnahme.

Ein SIM ist eine integrative Instanz im Netzmanagement, die nicht nur viele Quellen hat, sondern auch viele Empfänger für die Ergebnisse. Die wichtigste Gruppe ist die der Mitarbeiter, die die erkannten Vorfälle bearbeiten. Daneben gibt es jedoch noch Vorstände, Revisoren und die Administratoren der Intrusion-Detection-, Firewall-, Antiviren- und sonstigen Systeme. Für jede dieser Gruppen muss eine eigene Sicht auf die Daten beziehungsweise Aufbereitung vorhanden sein. Je nach Intensität und Häufigkeit der Arbeit mit den SIM-Daten empfiehlt sich die Installation der Software auf dem eigenen Rechner oder ist ein Webbrowser ausreichend.

Wer solche Datenmengen verarbeiten muss, ist auf die Hilfe von Grafiken angewiesen. So kann man besser den Überblick behalten, wenn alle Rechenzentren als Symbole auf einer Karte angezeigt sind, deren Farbe sich der aktuellen Situation anpasst. Ein rot blinkender Server zieht schneller die Aufmerksamkeit auf sich als eine rote Zeile in einem Fenster, in dem ständig Meldungen durchlaufen.

Gleiches gilt für statistische Auswertungen und Trends. Wenn ein Tool die Entwicklung bestimmter Meldungen als Zahlenkolonne darstellt, ist der Mitarbeiter, der einen Ausreißer entdecken soll, überfordert. Auch hier hilft die Darstellung als Grafik, in der sich die Meldungen einer Art, eines Systems, eines Sensors oder von einem Ausgangspunkt optisch aufbereitet fin-

Entscheidungshilfen für ein Security Information Management

Vor der Einführung eines solchen nicht gerade preiswerten Produktes sollten die folgenden Fragen zufriedenstellend beantwortet sein:

- Sind alle beteiligten Personen (inkl. Betriebsrat) der betroffenen Abteilungen involviert?
- Gibt es ausreichende Motivation beim Management, das Projekt durchzuführen?
- Sind klare Ziele und realitätsnahe Erwartungen an das Projekt gestellt worden?
- Sind die meldenden Systeme identifiziert?
- Sind die Orte und Netzsegmente aller meldenden Systeme bekannt?
- Kann jeder im Unternehmen vorhandene Typus eines meldenden Systems an einem Pilotprojekt teilnehmen?
- Bietet das SIM Import-Module für diese Systeme?
- Welche Auswirkungen auf die Last der meldenden Systeme und Netze hat das SIM?
- Ist die ungefähre Zahl der zu verarbeitenden Meldungen bekannt?
- Gibt es für die Aussagen der Hersteller Referenzkunden, die das Produkt auf die genannte Weise einsetzen?
- Werden die Daten revisionssicher gespeichert und sind alle gesetzlichen Anforderungen erfüllt?
- Kann man aus den gesammelten Daten einen Tatbeweis ableiten?
- Existieren Schnittstellen zu vorhandenen Problemmanagementsystemen oder genügt das eingebaute?
- Lassen sich eigene Regeln einstellen?
- Wie ist im Alarmfall die Benachrichtigung der Mitarbeiter organisiert?
- Welche Gruppen und Funktionen gibt es in der Organisation und welche Auswertungen sollen sie erhalten?
- Sind Ansichten für jede Gruppe vorhanden und wie einfach kann das System neue erstellen?

den. Wenn in der Anzeige etwas Auffälliges erscheint, kann der Bediener bei fast allen Produkten durch einen Klick mehr über die jeweilige Meldungen erfahren.

Sich aus der Grafik oder der Anzeige eines Events hinunter bis zu den einzelnen Meldungen zu arbeiten, dabei neue, temporäre Filter zu definieren und das Level der Details stufenweise zu erhöhen (Drill-Down), gehört zum Standard bei allen Produkten. Ob sich das eher intuitiv mit der rechten Maustaste oder umständlich durch Menüs erledigen lässt, entscheidet stark über die Praxistauglichkeit der Produkte.

Eine weitere Unterscheidung, die auch Aussagen über die Ausgereiftheit des SIM zulässt, ist die Zahl und Qualität der mitgelieferten Berichte und Auswertungen. Bis zu mehrere hundert unterschiedliche Auswertungen sind bei guten Systemen üblich. Hier gilt das Gleiche wie bei den Analyseregeln: Vor dem Kauf sollten sich die damit befassten Mitarbeiter mit dieser Funktion beschäftigen und sie ausgiebig auf Unternehmensbedürfnisse hin testen.

Alarm an die richtige Instanz

Was hilft die beste Analyse in Echtzeit, wenn sich niemand um den Vorfall kümmert? Die schnelle und zuverlässige Benachrichtigung der Mitarbeiter kann Schlimmeres verhindern. Fast alle auf dem Markt erhältlichen Produkte lassen die Integration in ein vorhandenes Ticket-System zu. Einige bringen zusätzlich ihr eigenes mit, damit Mitarbeiter sicherheitsrelevante Ereignisse kontrolliert abarbeiten können und gleich ein Nachweis darüber vorhanden ist.

Wer sich den 24/7-Betrieb eines „Security Operations Center“ (SOC) sparen möchte und die Mitarbeiter lieber auf Bereitschaftsdienst mit Fernzugang nach Hause schickt, sollte gleich die Anschaffung eines entsprechenden Systems zur Benachrichtigung erwägen, denn dieses ist in den seltensten Fällen im Lieferumfang eines SIM-Tools enthalten. Es sollte in der Lage sein, Benachrichtigungen per Mail, Fax, SMS und Anruf weiterzuleiten.

Des Weiteren ist eine Alarmierungskette, ein so genannter Call-Tree festzulegen: Man definiert verschiedene Rollen, wer für die Behandlung welches Vorfalls zuständig ist. Dies kann je nach betroffenem System variieren, bei einem Einbruch in einen Server ist nicht zwingend derselbe Mitarbeiter zu informieren wie bei einem Wurmausbruch auf den Arbeitsplätzen. Für jede Rolle werden Mitarbeiter bestimmt und ihre Kontaktdaten hinterlegt. Unerlässlich ist die Gewissheit, dass die Benachrichtigung wirklich bei der richtigen Person angekommen ist und nicht nur als Mail fehlerfrei zugestellt wurde. Wenn der erste für eine Rolle definierte Mitarbeiter nicht erreichbar ist, sollte das System so lange weitere Zuständige kontaktieren, bis jemand den Empfang bestätigt.

Der technischen Wirksamkeit bei Einführung eines SIM sind allerdings noch einige organisatorische Hürden vorangestellt. Zum einen in Form des Betriebsrats, der nicht zu Unrecht befürchtet, dass diese Technik zur Überwachung von Mitarbeitern eingesetzt werden kann. Ihn möglichst früh einzubinden und genau über die gesammelten Daten und Abläufe zu informieren kann helfen, Widerstände gar nicht erst aufkommen zu lassen.

Ein weiteres Problem ist, dass die sicherheitsrelevanten Systeme oft in unterschiedliche Abteilungen gepflegt werden. Dort überwachen eigene Mitarbeiter die Systeme und analysieren die Meldungen. Ein SIM-Projekt zentralisiert und übernimmt Teile ihrer Aufgaben. Die betreffenden Mitarbeiter und Vorgesetzten sollte man in die Planung des Projekts einbeziehen, um sich ihrer Unterstützung zu versichern.

Richtig geplant und eingesetzt kann ein Security Information Management Administratoren und Mitarbeiter entlasten, die Sicherheit der Systeme erhöhen und Nachweise über alle relevanten Vorfälle in der Organisation bereithalten. (ur)

CHRISTOPH PUPPE

ist Security Consultant bei der Hisolutions AG in Berlin und CISSP-zertifiziert.

Security-Information-Management-Tools

Der größte Teil der Anbieterfirmen sind Neugründungen, die sich auf SIM-Tools spezialisiert und nichts anderes im Angebot haben. Doch auch die großen Softwarehersteller, die schon ähnliche Produkte vertreiben, sind mittlerweile auf den Zug aufgesprungen und haben SIM-Funktionen in ihre Netzmanagementprogramme integriert. Die Open-Source-Gemeinde steuert ebenfalls ihren Teil dazu bei: Das Open Source SIM (OSSIM) steht kurz vor der Version 1.0. Nicht extra aufgeführt sind in der folgenden Übersicht die Anbieter so genannter Managed Security Services, die statt Hard- oder Software die Überwachung und Analyse der Meldungen als Dienstleistung anbieten.

Hersteller	SIM-Tool	Webadresse
ArcSight	ArcSight ESM	www.arcsight.com/product_esm_3.0.htm
Cisco	Cisco SIM (netForensics 3.1)	www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html
Computer Associates	CA eTrust Security Command Center	www3.ca.com/Solutions/Product.asp?ID=4351
e-Security	eSecurity Sentinel 5	www.esecurityinc.com/Software/index.asp
GuardedNet	GuardedNet neuSecure	www.guarded.net/
IBM	Tivoli Security Event Management	www.ibm.com/software/tivoli/solutions/securityevent/
Intellitactics	Intellitactics Network Security Manager	www.intellitactics.com/
NetForensics	netForensics nFX Open Security Platform	www.netforensics.com/nfxosp.asp
Network Intelligence	Network Intelligence EX-, HA-, LS-Serien	www.network-intelligence.com/
Protego Networks	Protego Networks PN-MARS	www.protegonetworks.com/products/products.htm
Symantec	Symantec Security Management System	http://enterprisesecurity.symantec.com/products/products.cfm?productid=45
Symantec	Symantec DeepSight Analyzer	enterprisesecurity.symantec.com/products/products.cfm?productid=159
Open-Source-Tool:	Open Source Security Information Management (OSSIM)	www.ossim.net/
Nützliche Hilfestellung:	Internet Storm Center	isc.sans.org/ und www.dshield.org/