Mappen von Sicherheitsereignissen

Einsatz von IF-MAP als Integrationsprotokoll zur Konsolidierung von Systemmeldungen

Kai-Oliver Detken

Heute sind in Unternehmen diverse Sicherheitssysteme wie Firewalls, Virenscanner, Spamfilter und VPN-Gateways im Einsatz, nur arbeiten diese oft isoliert voneinander. Viele Angriffe können jedoch erst durch die Kombination von Daten verschiedener Systeme erkannt werden. Zudem findet meist keine kontinuierliche und vorausschauende Überwachung von IT-Systemen sowie von Vorgängen und Ereignissen im Netz statt. Dies können aber sog. SIEM-Lösungen (Security Information and Event Management) leisten, die Meldungen und Warnungen einzelner Sicherheitskomponenten zusammenführen und auswerten. Der Nachteil: Diese Systeme sind oftmals noch sehr komplex, kostspielig und durchaus nicht fehlerfrei. Der hier vorgestellte SIEM-Ansatz basiert auf IF-MAP und soll eine Datenkorrelation effektiver machen und einfacher umsetzen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Die meisten Hersteller von Sicherheitskomponenten sehen ihre Produkte als Insellösungen und bieten sie entsprechend am Markt an. Als Schnittstelle zum IT-Administrator existiert i.d.R.11 ein Konfigurations- und Reporting-Portal. Die Informationen werden hier für den IT-Administrator aufbereitet, aber nicht in einen unternehmensweiten Kontext gestellt. Dies obliegt dem IT-Administrator selbst, der die verschiedenen Events sinnvoll analysieren muss, was je nach Größe des Netzes sehr zeitintensiv werden kann.

Zudem konzentrieren sich traditionelle Sicherheitslösungen ausschließlich auf die Abbildung ihrer eigenen Leistungsmerkmale. Andere Bereiche innerhalb des Unternehmens (z.B. Serversysteme, Applikationen, Facility Management, Zugriffskontrolle, Inventarisierungsverwaltung) werden nicht mit einbezogen. Dabei beinhalten diese Bereiche die eigentlich zu schützenden Unternehmenswerte. Doch in die Betrachtung der IT-Sicherheit fließen sie bisher nicht mit ein.

Problematisch ist weiterhin, dass die unterschiedlichen Sicherheitskomponenten verschiedener Hersteller nicht über die gleichen Protokolle und Schnittstellen verfügen. Daher ist es, selbst wenn eine Kombination der unterschiedlichen Logdateien geplant ist, nicht immer möglich, die Informationen einheitlich zusammenzubringen. Erschwert wird dies, wenn Hersteller proprietäre Lösungen verwenden. Das IF-MAP-Protokoll bietet eine Möglichkeit an, um die unterschiedlichen Datenformate zusammenzubringen, so dass es auch als gemeinsamer Nenner im Simu-Projekt verwendet wird.

Die Simu-Architektur

Das Simu-Projekt (www.simu-project.de) ist ein vom BMBF gefördertes Forschungsprojekt mit einer Laufzeit von zwei Jahren. Sein Ziel ist die Entwicklung eines SIEM-artigen Systems zur Verbesserung der IT-Sicherheit und der Kontrollmöglichkeiten in Unternehmensnetzen. Das Simu-System wird Unternehmensnetze überwachen und – wo sinnvoll – automatisiert Maßnahmen zur Verbesserung der Sicherheit einleiten.

Der Begriff SIEM wurde von Mark Nicolett und Amrit Williams von Gartner im Jahr 2005 geprägt, indem beide die SIEM-Produktfähigkeit als eine Sammlung, Analyse und Darstellung von Informationen aus Netz- und Sicherheitsgeräten beschrieben, um Sicherheitslücken effektiver auf die Spur zu kommen und Identity- sowie Access-Managementanwendungen für Unternehmensnetze zu ermöglichen. Dadurch würde man externe Bedrohungen eher oder überhaupt erst wahrnehmen. Der Schwerpunkt eines SIEM-Systems ist demnach die Überwachung und Verwaltung von Benutzerdiensten und -privilegien, Verzeichnisdiensten und Änderungen der Systemkonfiguration sowie die Bereitstellung zur Auditierung und Überprüfung der Vorfälle (siehe Amrit Williams Blog: Observations of a Digitally Enlightened Mind: The Future of SIEM – The Market Will Begin to Diverge, Januar 2007). Es geht damit einen Schritt weiter, als herkömmliche Monitoring-Systeme und bezieht explizit die IT-Sicherheit mit ein.

Die SIEM-Architektur des Simu-Projektes stellt das IF-MAP-Protokoll als zentrales Protokoll zum Austausch von Metadaten in den Mittelpunkt (s.a. NET 6/2014, S. 40, Bild 4). Neben den Open-Source-Tools, die schwerpunktmäßig integriert werden, sind die Lösungen NCP-VPN und macmon NAC ebenfalls Teil der Architektur.

Die Simu-Architektur teilt sich in zwei Schichten, die durch das IF-MAP-Pro-

tokoll miteinander verbunden werden:

- Simu-Kollektoren- und Flow-Controller-Schicht: verantwortlich für Datensammlung und Enforcement;
- Simu-Engine: enthält den zentralen Wissens- und Datenspeicher, Komponenten zur Korrelation, Aggregation und Darstellung von Daten sowie Protokollschnittstellen.

Die Simu-Engine muss u.a. die Ergebnisse der Datenanalyse durch die Simu-GUI entsprechend aufbereitet darstellen. Die grafische Oberfläche muss dafür mit der Detection Engine (enthält die intelligente Analyse der MAP-Serverdaten) und VisITMeta (enthält die grafische Darstellung des IF-MAP-Graphens) direkt sowie indirekt mit dem I/O-Tool (enthält die Erhebung der Daten der IT-Infrastruktur) kommunizieren. Sie muss Events eindeutig anzeigen und ensprechende Mitteilungen an die IT-Administration schicken. Dieser Simu-GUI kommt damit eine zentrale Bedeutung zu.

Flow-Controller und Kollektoren stellen die Schnittstelle zwischen der Simu-Engine und den Diensten, Sicherheits- und Infrastrukturkomponenten des Netzes dar. Aktuell sind die folgenden Kollektoren für die Integration in Simu vorgesehen:

- DHCP-Kollektor: extrahiert Metadaten zu aktuellen IP-Leases des DHCP-Servers aus dem Lease-File von DHCP-Servern;
- Radius-Kollektor: liefert Metadaten zu Benutzeranmeldungen sowie Metadaten zu den Benutzern selbst (Gruppen, Berechtigungen);
- Syslog-Kollektor: stellt voraggregierte Metadaten zum Zustand von Hosts und Diensten (CPU-Last, fehlgeschlagene Logins) zur Verfügung;
- Nagios-Kollektor: veröffentlicht aus Nagios extrahierte Metadaten zum Zustand von Hosts und Diensten (u.a. Netzverfügbarkeit);
- Snort-Kollektor: übersetzt Snort-Alarme in IF-MAP-Metadaten;
- Logfile-Kollektor: generischer Kollektor zur Auswertung beliebiger Log-Dateien und Transformation in IF-MAP-Metadaten.

Zusätzlich sind die IF-MAP-Kollektoren Android, Icinga REST, LDAP und WMI (Windows Management Instrumentation) enthalten. Die Berücksichtigung von Android wurde notwendig, da es auch möglich sein sollte, mobile Endgeräte mit in die SIEM-Betrachtung einbeziehen zu können. So können über diesen Kollektor u.a. Firmware, Kernel-Version, Build-Nummer und SMS/E-Mail-Informationen weitergeleitet werden. Der Nagios-Fork Icinga kann als Alternative zu Nagios über die REST-Schnittstelle verwendet werden und Anfragen bei Bedarf durchführen. Der LDAP-Kollektor soll eine Verbindung zum vorhandenen Verzeichnisdienst herstellen, während der WMI-Client auch die Windows-Clients mit einbezieht.

Des Weiteren ist die Integration folgender Flow-Controller-Komponenten vorgesehen, die zum Teil auch Kollektorenfunktionalität besitzen:

- Iptables-Flow-Controller: ermöglicht das automatische Anlegen von Firewall-Regeln für Hosts als Reaktion auf bestimmte Metadaten und veröffentlicht diese als Enforcement-Reports im MAP-Server;
- macmon NAC: publiziert verschiedene Daten zu aktiven Endgeräten im Netz, vor allem Autorisierungsinformationen zu bekannten Endgeräten, deren Standort im Netz und weitere Gerätecharakteristika wie Betriebssysteminformationen und offene Ports;
- NCP-VPN: stellt eine Reihe relevanter Metadaten auf dem MAP-Server zur Verfügung, insbesondere Informationen über angemeldete Benutzer sowie die IP-Adresse der Geräte, mit denen die Benutzer im VPN angemeldet sind, Datendurchsatz und Verbindungszeit der jeweiligen Benutzer; es wird ein Enforcement auf VPN-Ebene ermöglicht.

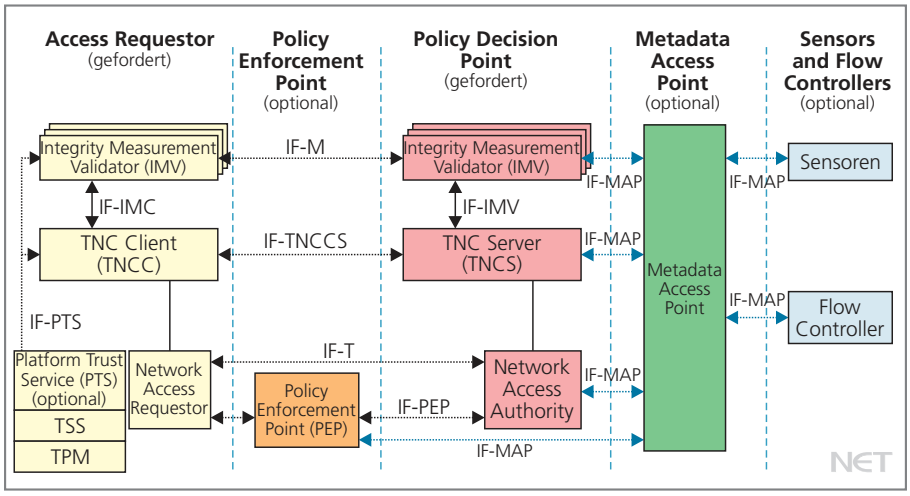

Bild 1: TNC-Architektur mit IF-MAP
(Quelle: TCG Specification: Architecture Overview, Specification, Revision 1.4, August 2007)

Zusätzlich ist der Flow-Controller/Kollektor OpenVPN in der Entwicklung, um zusätzlich eine SSL-basierte Alternative zur ausschließlich auf IPsec basierenden Herstellerlösung von NCP anbieten zu können.

IF-MAP-Protokoll

Für den Austausch von Informationen zwischen Simu-Engine und den Kollektoren und Flow-Controllern wird das IF-MAP-Protokoll der Trusted Computing Group (TCG) eingesetzt. IF-MAP ist ein offen spezifiziertes, herstellerunabhängiges Protokoll zum Austausch von Metadaten innerhalb eines Netzes in Echtzeit. Es ist zudem ein integraler Bestandteil des TNC-Frameworks (Trusted Network Connect) der TCG (*Bild 1*), kann jedoch auch wie im Simu-Projekt losgelöst von TNC verwendet werden.

IF-MAP definiert im Wesentlichen zwei Rollen:

- Ein Server, der Metadata Access Point (MAP), dient als zentraler Zugriffspunkt und Sammelstelle für beliebige Metadaten.
- MAP-Clients (MAPCs) können über das IF-MAP-Protokoll auf den MAP-Server zugreifen, um Metadaten zu veröffentlichen, sie zu durchsuchen

oder Abonnements auf Metadaten zu registrieren.

Welche Art von Metadaten mit IF-MAP transportiert und gesammelt werden, kann durch die Definition eines Metadatenschemas auf die jeweilige Anwendungsdomäne angepasst werden. Die TCG schlägt u.a. ein Schema speziell für die Anwendung im Bereich der Netzsicherheit vor.

- Ein MAPC kann per Search nach vorhandenen Metadaten suchen.
- Über Subscribe kann sich ein MAPC über Änderungen der im MAPS gespeicherten Metadaten informieren lassen. Dabei spezifiziert der MAPC, welche Art von Metadatenänderungen relevant ist. Nur solche Änderungen haben eine Benachrichtigung durch den MAPS zur Folge.

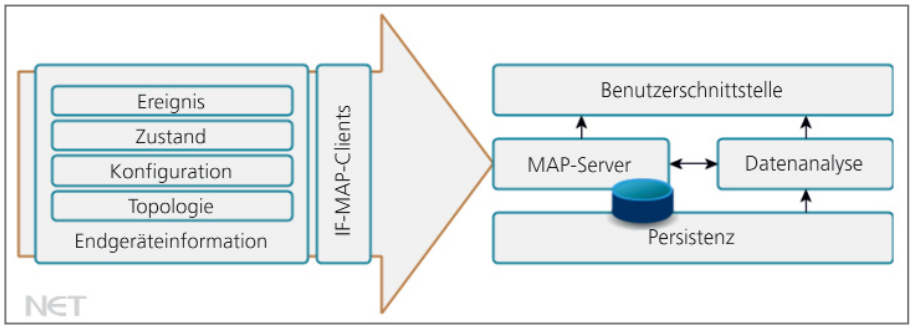

Bild 2: Informationsfluss im Simu-System

Die Rolle eines MAPC kann von verschiedenen Komponenten übernommen werden. Beispielsweise kann ein Policy Decision Point (PDP) nach erfolgreicher Authentifizierung eines Benutzers die Ergebnisse einer etwaigen Integritätsüberprüfung des verwendeten Endgerätes in Form von Metadaten im MAP-Server veröffentlichen. Diese Metadaten spiegeln i.d.R. den erfolgreichen Zugriff des Access Requestors (AR) auf das Netz wider.

Im MAP-Server werden Metadaten in Form eines Graphen verwaltet. Damit bietet sich die Möglichkeit, an zentraler Stelle eine Gesamtsicht auf den aktuellen Status eines Netzes zu etablieren. Die Modellierung als Graphstruktur hat den Vorteil, dass Beziehungen und die Semantik dieser Beziehungen direkt in den Daten abgebildet werden können. Durch Korrelation der vorhandenen Metadaten sind zusätzliche sicherheitsrelevante Informationen ableitbar.

Die Kommunikation zwischen einem MAPC und dem MAPS basiert auf einem Publish-Search-Subscribe-Modell, bei dem sowohl synchron als auch asynchron MAP-Daten ausgetauscht werden können:

- Mit Publish kann ein MAPC neue Metadaten veröffentlichen, vorhandene Metadaten ändern oder löschen.

Technisch setzt IF-MAP auf eine Reihe von etablierten Standardtechniken. Als Framework zur Übertragung der Metadaten kommt das SOAP-Protokoll in Kombination mit HTTP(S) zum Einsatz. Das Format der Metadaten ist durch XML-Schemata beschrieben. Auf diese Weise können etablierte Sicherheitssysteme, die um MAP-Client-Funktionen erweitert worden sind, beliebige Metadaten über den aktuellen Status des Netzes austauschen. Das Simu-Projekt wird aber auch den Einsatz von CBOR (Concise Binary Object Representation) nach RFC-7049 prüfen, um eine schlankere Kommunikation zu ermöglichen.

Fazit

SIEM-Lösungen sind komplexe Systeme und bestehen aus unterschiedlichen Modulen, Sicherheitskomponenten und Schnittstellen. Mit dem Einsatz eines großen, kommerziellen SIEM-Systems sind hohe Erstinstallations- und Wartungsaufwände und folglich Kosten verbunden. Somit sind SIEM-Lösungen bei kleinen und mittelständischen Unternehmen bisher wenig verbreitet.

Das SIMU-Projekt integriert Informationen beliebiger Endgeräte; relevant sind hierbei insbesondere Topologiedaten (DHCP-Logs, Asset-Managementinformationen usw.), Konfigurations- und Zustandsdaten (NAC-Endgeräteinformationen, Dienstprotokolle usw.) sowie Ereignisdaten (u.a. IDS-Meldungen). Diese werden von den jeweiligen Infrastrukturkomponenten, Diensten und Endgeräten gewonnen und mittels des IF-MAP-Protokolls an den MAP-Server versendet (*Bild 2*). Der MAP-Server dient als zentraler Zugriffspunkt für Analyseverfahren, deren Ergebnisse grafisch aufbereitet den Anwendern zur Verfügung gestellt werden.

Die Abbildung auf das IF-MAP-Datenformat, die von den IF-MAP-Clients vorgenommen wird, dient vor allem der Homogenisierung der Informationen für eine spätere Weiterverarbeitung. Darüber hinaus findet während dieser Transformation durch die Verbindung von Einzelinformationen zu einer Graphenstruktur eine semantische Einbettung in den Gesamtkontext der Endgeräteinformationen statt. Diese erleichtert automatisierte Analysen und sorgt darüber hinaus für eine bessere Nachvollziehbarkeit von Zusammenhängen bei manuellen Analysen seitens des Sicherheitspersonals.

Die Analyseverfahren greifen direkt auf die Graphenstruktur im MAP-Server zu und haben somit eine Datenbasis, die eine Gesamtsicht auf die IT-Infrastruktur ermöglicht. Unerlaubte Zustände im Netz lassen sich leicht anhand der Topologie des Graphen und, in einer geeigneten Regelsprache formuliert, mittels Pattern-Matching automatisiert feststellen. Darüber hinaus können unbekannte, schadhafte Zustände anhand von Abweichungen des Normalzustandes des Graphen festgestellt werden. Der Normalzustand kann anhand der persistierten MAP-Daten dynamisch ermittelt werden.

Durch den Einsatz von IF-MAP als Integrationsprotokoll ist es somit möglich, herstellerübergreifend eine Vielzahl von Komponenten an das Simu-System anzubinden, was Anpassungen bestehender Netzinfrastrukturen auf ein Minimum reduziert und die verfügbare Datenbasis maximiert. Dies erhöht das Sicherheitsniveau von Unternehmen entscheidend. *(bk)*