Verhängnisvolle Isolierung

IT-Sicherheit – mehr als die Summe aller Einzelteile

Kai-Oliver Detken,
Dennis Dunekacke

Alle Unternehmen sollten hohe Anforderungen an ihre IT-Infrastruktur haben, da hier alle unternehmenskritischen Anwendungen zusammenlaufen. Zusätzlich machen die rasant gestiegene Nutzung mobiler Geräte sowie mangelnde Sicherheitskonzepte für diese Geräteklasse die Unternehmensnetze zu einem attraktiven Angriffsziel. Trotz zahlreicher Möglichkeiten zur Absicherung des Netzes wie z.B. durch Firewall-Systeme oder Antivirenlösungen arbeiten diese Einzelkomponenten oft isoliert voneinander. Viele Angriffe sind aber erst durch die Kombination von Daten verschiedenster Systeme zu erkennen bzw. können, selbst wenn sie erkannt werden sollten, nicht rechtzeitig über Gegenmaßnahmen verhindert werden. Das Forschungsprojekt Esukom will dem begegnen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH, Dennis Dunekacke ist Software-Entwickler bei der Decoit GmbH

Zentraler Zugriffspunkt heutiger Unternehmensnetze ist die Firewall, die den Datenverkehr zwischen dem sicheren internen und dem unsicheren externen Netz reglementiert. Häufig eingesetzt werden sog. Paketfilter, die anhand von IP-Adresse und Port der Quelle bzw. des Ziels des anfallenden Datenverkehrs entscheiden, ob dieser gestattet wird oder nicht. Komplexere Firewall-Systeme untersuchen auch den durchgelassenen Datenverkehr und führen auf Applikationsebene Sicherheitsreglementierungen durch. Neben der Firewall existieren häufig sog. VPN-Gateways, die Außenstandorte und -dienstmitarbeiter in das Unternehmensnetz sicher einbinden sollen. So können durch virtuelle private Netze sichere Verbindungen zwischen einem Benutzer und einem Netz (End to Site) oder zwischen zwei Netzen (Site to Site) bereitgestellt werden. Die Verbindung erfolgt in der Regel über ein unsicheres Netz.

Für den Fall, dass ein Angreifer sich bereits im internen Netz befindet bzw. dass Anomalien im sicheren Netz auftauchen, wurden Intrusion-Detection-Systeme (IDS) entwickelt, die den Datenverkehr innerhalb des eigenen Unternehmensnetzes ständig überwachen, mögliche Angriffe erkennen und diese entsprechend dokumentieren. Teilweise unterstützen einige IDS-Produkte auch die Integration mit anderen Sicherheits-Tools. So ist es z.B. möglich, das IDS-System Snort (www.snort.org) über das Plugin Snortsam mit verschiedenen Firewall-Produkten zu integrieren. Bei einer Anomalie kann so automatisch die Konfiguration der Firewall angepasst werden.

Der NAC-Ansatz (Network Access Control) soll zusätzlich die Bedrohung, die von dynamisch eingebunden Endgeräten für das eigene Netz ausgeht, verringern. Dazu wird, bevor der Netzzugriff gewährt wird, neben der Identität des Benutzers auch die Integrität bzw. die Konfiguration des verwendeten Endgerätes überprüft. Je nachdem, wie gut die Richtlinien des Unternehmens erfüllt werden, kann der Zugriff auf das Netz gewährt oder nur ein Teilzugriff auf ein Quarantänenetz beschlossen werden. Erst wenn das Endgerät alle Richtlinien erfüllt, darf es auf das Unternehmensnetz zugreifen.

Diese beispielhaften Sicherheitsmechanismen erhöhen den Sicherheitsgrad eines Unternehmensnetzes signifikant. Allerdings arbeiten sie im Normalfall isoliert voneinander. Die erwähnte Integration von Snort mit einigen Firewall-Produkten stellt eine Ausnahme dar. Ein herstellerübergreifender, interoperabler Ansatz zur Integration mehrerer, verschiedener Sicherheitsmechanismen ist momentan nicht als Produkt verfügbar.

IF-MAP-Spezifikation

Eine Möglichkeit, verschiedene Datenbasen zusammenzuführen, stellt die IF-MAP-Spezifikation (Interface – Metadata Access Point) der Trusted Computing Group (www.trustedcomputinggroup.org) dar. Sie ist ein Bestandteil der Trusted-Network-Connect-Architektur (TNC) und wird von der gleichnamigen Arbeitsgruppe der TCG entwickelt. Die erste Version der Spezifikation erschien im April 2008.

In der IF-MAP-Terminologie wird die zentrale Metadatenbasis eines Netzes als MAP-Server bezeichnet. MAP-Clients können über eine standardisierte Schnittstelle mit dem MAP-Server kommunizieren:

- Über die Search-Funktion werden basierend auf den vorhandenen Metadaten komplexe Suchoperationen durchgeführt;
- über die Subscribe-Funktion können MAP-Clients veranlassen, dass sie über Änderungen an vorhandenen Metadaten informiert werden;

- über die Publish-Funktion werden Metadaten im MAP-Server hinzugefügt, verändert oder gelöscht.

Vorhandene Sicherheits-Tools agieren daher als MAP-Client. Die Kommunikation kann sowohl synchron als auch asynchron erfolgen. Das bedeutet, dass ein MAP-Client über Subscribe Interesse an einer bestimmten Art von Metadaten „anmelden" kann. Sobald neue Metadaten dieser Art veröffentlicht werden oder sich die vorhandenen Metadaten dieser Art ändern, wird der entsprechende MAP-Client durch den MAP-Server informiert.

Neben dem Kommunikationsmodell und der dazugehörigen Schnittstelle wird in der Spezifikation auch ein rudimentäres, erweiterbares Format für die Beschreibung von Metadaten basierend auf XML-Schemata definiert. Die zwingend notwendige Interoperabilität über Herstellergrenzen hinweg ist somit prinzipiell gewährleistet. Das definierte Format ermöglicht es, Metadaten in Form eines Graphen zu modellieren. Auf diese Weise können die veröffentlichten Metadaten einzelner MAP-Clients miteinander konsolidiert werden. So wird es möglich, die bislang isoliert voneinander existenten Sichten der einzelnen Sicherheits-Tools miteinander zu kombinieren.

Obwohl die IF-MAP-Spezifikation bereits 2008 vorgestellt wurde, und viele Hersteller ihr Interesse an dem ihr zugrunde liegenden Konzept bekundeten, existieren bis heute nur wenige Implementierungen bzw. Produkte. So hat Juniper Networks (**www.juniper.net**) als erster kommerzieller Hersteller IF-MAP-Funktionen in seine Produkte integriert. Im Juniper-Anwendungsszenario ist die Integration eines SSL-VPN und einer NAC-Lösung enthalten. Ziel ist es, dass Benutzer, die sich über die VPN-Lösung authentifiziert haben, transparent auf Ressourcen des Netzes zugreifen können. Das muss insbesondere auch dann möglich sein, wenn für die entsprechenden Ressourcen Richtlinien gelten, die von der NAC-Lösung überwacht und durchgesetzt werden.

Inzwischen hat Infoblox (**www.infoblox.com**) nachgezogen und bietet weltweit den ersten kommerziellen MAP-Server an. Für das Unternehmen stellt der IF-MAP-Standard eine Möglichkeit zur Vereinheitlichung verschiedener Monitoring-Protokolle dar.

Obwohl Juniper in IF-MAP-Hinsicht eine Vorreiterrolle einnimmt, erschöpft die bislang vorhandene Integration die potenzielle Funktionsfähigkeit von IF-MAP nur ansatzweise. Bei den vorgestellten Produkten wurde IF-MAP primär dazu verwendet, um die Handhabbarkeit bei der Nutzung von SSL-VPNs und NAC-Lösungen aus dem eigenen Haus zu verbessern. Eine Analyse von sicherheitsrelevanten Metadaten über Herstellergrenzen hinweg, um fortgeschrittene Bedrohungen schnell erkennen und diesen entgegenwirken zu können, findet bislang allerdings nicht statt. Auch Infoblox steckt noch in der eigenen Forschung. So ist man relativ einfach dazu in der Lage, entsprechende Metadaten zu veröffentlichen, aber die Konsolidierung der unterschiedlichen Daten für eine einheitliche Analyse bereitet noch Probleme. Hier soll das Forschungsprojekt Esukom (**www.esukom.de**) neue Erkenntnisse bringen und neue Impulse setzen.

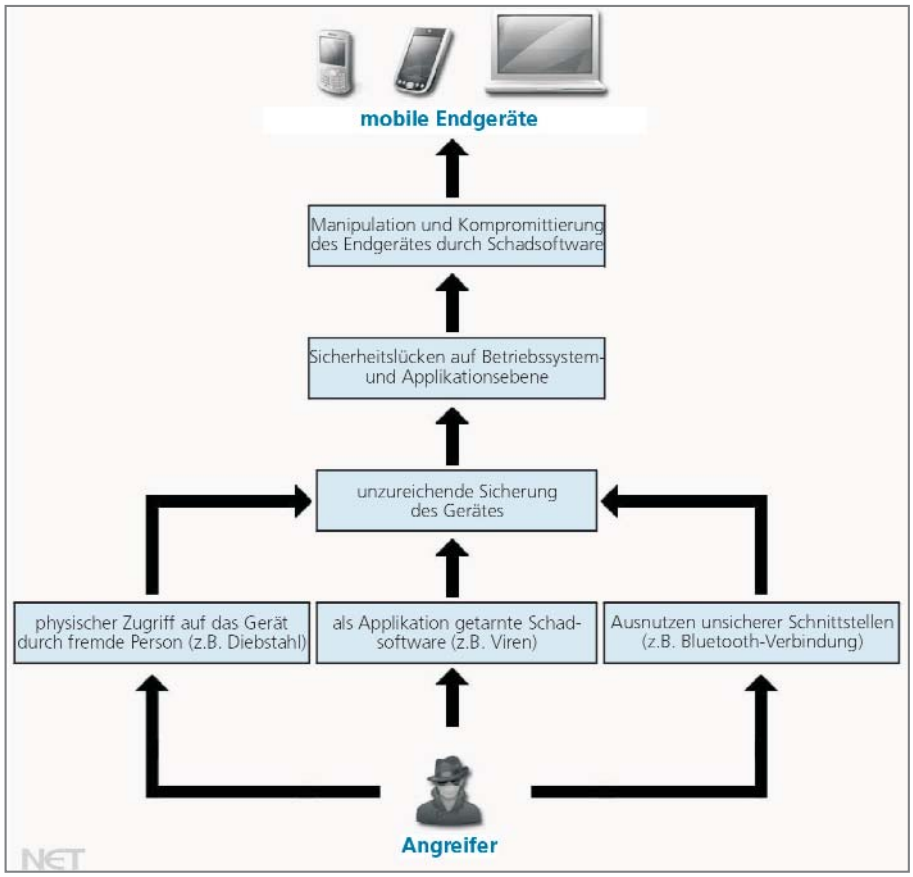

Bild 1: Möglichkeiten zur Kompromittierung mobiler Endgeräte

Das ESUKOM-Projekt

Das vom BMBF geförderte Forschungsprojekt Esukom ist auf zwei Jahre ausgelegt und beinhaltet die Konzeption und Entwicklung einer Echtzeitsicherheitslösung für Unternehmensnetze, basierend auf der Konsolidierung von Metadaten. Das Projekt startete im Oktober 2010 und weist bereits erste Lösungsansätze vor.

Esukom erweitert aktuelle IT-Infrastrukturen um Komponenten, deren primäres Ziel die Schaffung und Einhaltung eines hohen Sicherheitsniveaus der jeweiligen Umgebung ist. Durch den verteilten Ansatz der verwendeten IF-MAP-Spezifikation, in der Metadaten aus verschiedenen Quellen in einer zentralen Datenbank aggregiert werden, können prinzipiell alle gängigen IT-Systeme von dem erhöhten Sicherheitsniveau profitieren. Insbesondere mobile Endgeräte werden im Rahmen von Esukom berücksichtigt. Die Szenarien umfassen z.B. den Schutz des Unternehmensnetzes vor dynamisch angebundenen, mobilen Endgeräten mittels IF-MAP.

Des Weiteren kann IF-MAP in Verbindung mit mobilen Endgeräten auch die Verwaltbarkeit und Überprüfbarkeit von IT-Infrastrukturen erhöhen. Der MAP-Server hält in realen Umgebungen eine immense Menge an sicherheitskritischen Daten vor. Diese Datenbasis kann im Ernstfall auch für forensische Untersuchungen herangezogen werden. Durch die Anbindung mobiler Endgeräte als MAP-Clients, die primär auf das Konsumieren von Metadaten ausgerichtet sind, steht diese Datenbasis dezentral auf einer Vielzahl von Endgeräten zur Verfügung. So könnten z.B. Administratoren mit Smartphones ausgestattet werden, die via IF-MAP über sämtliche, sicherheitsrelevanten Vorfälle in Echtzeit informiert werden.

Im Rahmen der ersten Projektphase wurden unterschiedliche Einsatzszenarien definiert, aus denen sich dann die Funktionen ableiten ließen. Ein wichtiges Szenario stellt dabei der Zugriff auf das Unternehmensnetz durch kompromittierte Endgeräte dar. Dabei ergeben sich für die Administratoren von Unternehmensnetzen zahlreiche neue Herausforderungen und Gefährdungen. Gleichzeitig werden Übergriffe auf Unternehmensnetze und deren Daten für Angreifer ein zunehmend lukrativer Geschäftsbereich, was wiederum dazu führt, das die Autoren von Schadsoftware immer professioneller und zielgerichteter agieren.

Um die Kontrolle über ein mobiles Endgerät und dessen Daten und Funktionen zu erlangen, ist ein Angreifer nicht darauf beschränkt, dieses auch physisch in seinen Besitz zu bringen. Ebenso ist es möglich, sich durch unterschiedliche Sicherheitslücken einen unerlaubten Fernzugriff auf solche Geräte zu verschaffen. Neben den Angriffsmöglichkeiten, die durch den Einsatz unsicherer Schnittstellen geschaffen werden, rückt vor allem die Möglichkeit der Kompromittierung der mobilen Endgeräte durch Ausnutzen bestehender Sicherheitslücken innerhalb des Betriebssystems und den darauf laufenden Anwendungen zunehmend in den Mittelpunkt. Hierbei bieten sich durch die zunehmende Komplexität dieser Anwendungen unterschiedliche Angriffsvektoren an, die für eine Kompromittierung durch Schadsoftware ausgenutzt werden können. Mögliche Wege für eine Infektion des Endgerätes mit Software sind (*Bild 1*):

- Ausnutzen von Sicherheitslücken innerhalb der installierten Anwendungen und des darunter liegenden Betriebssystems;
- nachträgliches Installieren eigener Anwendungen auf den Geräten über Herstellerportale;
- Installieren von Anwendungen ohne technische Prüfung aus „unsicheren" Quellen.

Für alle drei Fälle gibt es Negativbeispiele. Jüngster Fall ist die Entdeckung von Trojaner-infizierten Apps von Google, die über den Android-Market auf die Endgeräte gelangten. Experten sind sich sicher, dass dies kein Einzelfall bleiben wird und auch nicht alle Trojaner gefunden wurden.

Durch den Einsatz der IF-MAP-Architektur innerhalb des Esukom-Projektes wäre es möglich, kompromittierte Endgeräte gezielt aufzuspüren und ggf. weitere Maßnahmen einzuleiten, z.B. das Sperren oder Isolieren dieser Geräte. Ein wichtiger Aspekt hierbei ist, dass durch den Einsatz der IF-MAP-Architektur ein kompromittiertes Endgerät auch nach dem Authentifizierungs- und Autorisierungsvorgang anhand seines Verhaltens zu erkannt werden kann.

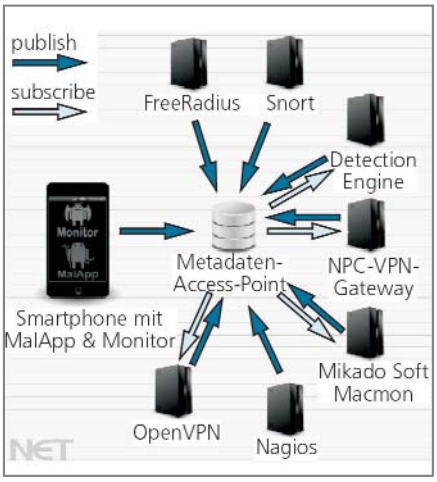

Bild 2: Anomaly-Detection-Szenario im Esukom-Projekt.

Tabelle 1: Fluss der Metadaten beim Szenario in Bild 2

	publish	subscribe
Smartphone (typische Smartphone-Features)	installierte Apps, Sensorstatus, genutzte Genehmigungen, Position, SMS-Zähler	
Anomaly Detection Engine	Anomaly Detection Event	alle Metadaten
Snort	Intrusion Detection Event	
Nagios	Host Services Information	
FreeRadius	User-ID, Switch-Port	
NCP-VPN-Gateway	User-ID, Login/Logoff-Events, IP-Adresse, Verbindungsparameter	Anomaly Detection Event
Micado Soft Macmon	Device Network Configuration, Geräteposition, User-ID	Anomaly Detection Event
OpenVPN	User-ID, Login/Logoff-Events, IP-Adresse, Verbindungsparameter	Anomaly Detection Event

Mehrwerte durch IF-MAP

Nachfolgend wird ein möglicher Ablauf dargestellt, in dem ein zunächst unentdecktes, manipuliertes Endgerät aufgrund seiner Aktivitäten auf-gespürt und gesperrt bzw. isoliert wird:

- Das kompromittierte Endgerät erbittet Zugang zum Unternehmensnetz. Die auf dem Gerät befindliche Schadsoftware ist dabei noch in-aktiv und wird während der Authentifizierung/Autorisierung und Überprüfung der Integrität des Endgerätes nicht korrekt erkannt. Das Gerät erhält Zugang. Die entsprechenden Verbindungsdaten werden an den MAP-Server übertragen und in den entsprechenden Metadaten-Graphen eingetragen.
- Nach einem gewissen Zeitraum aktiviert sich die Schadsoftware.
- Die eingeleiteten Aktivitäten des manipulierten Endgerätes werden von einem MAP-Client bemerkt. Dieser veröffentlicht die entsprechende Meldung und Daten an den MAP-Server (Publish).
- Der MAP-Server nimmt die entsprechenden Daten entgegen und fügt

diese zum jeweiligen Metadaten-Graphen hinzu. Anschließend werden die MAP-Clients, die sich für eine Benachrichtigung beim Ändern bestimmter Metadaten beim MAP-Server registriert haben (Subscribe), von diesen Ereignissen in Kenntnis gesetzt und erhalten die entsprechenden Informationen.

- Die benachrichtigten MAP-Clients können daraufhin weitere Maßnahmen einleiten, die von den jeweiligen Informationen abhängig sind. Hierbei müssen die entsprechenden MAP-Clients ihre Entscheidung nicht nur anhand der eingehenden Informationen treffen, sondern können zusätzliche Daten vom MAP-Server abfragen (Search) und zur Entscheidungsfindung hinzuziehen.

Nach diesen Vorgängen wird die unerlaubte Aktivität des Endgerätes unterbunden und das Endgerät vom Unternehmensnetz isoliert. Abschließend können auf Basis der gesammelten Informationen die unterbundenen Aktivitäten sowie deren Details protokolliert und entsprechende Meldungen an die verantwortlichen Systemadministratoren generiert werden.

Fazit

Basierend auf den fachlichen Szenarien, die innerhalb des Esukom-Projektes definiert wurden, sowie den analysierten Bedrohungsaspekten, konnten Kernanforderungen abgeleitet werden (siehe unten stehender *Kasten*). Sie bilden die Basis für die weiteren Arbeiten innerhalb des Esukom-Projektes und bestehen aus einer Menge von Anwendungsmöglichkeiten, deren technische Grundlage der Austausch von Metadaten über das IF-MAP-Protokoll ist. Diese Anwendungen können (einzeln oder kombiniert) in den definierten fachlichen Szenarien einen Mehrwert bringen. Zudem ermöglichen sie es, den Bedrohungen effektiv entgegenzuwirken. Durch diese Abstraktion der Esukom-Anwendungen lassen sich die erforderlichen Kernfunktionen leicht bedienen.

ESUKOM-Kernmerkmale

- Anomalieerkennung (s. *Bild 2* und *Tabelle 1*);
- Smartphone-Awareness;
- Single Sign-off;
- Secure Evidence;
- Identitäts-Awareness;
- Location-based Services;
- Erkennung von Mal-App-basierten Angriffen;
- Echtzeit-Enforcement.

Für jede Kernanforderung wurde betrachtet, welche grundlegenden Metadaten notwendig sind, um die bestehenden Anforderungen erfüllen zu können. Das Esukom-Projekt wird im nächsten Schritt an der Realisierung der MAP-Clients und eines MAP-Servers arbeiten. Die ersten Prototypen sind dabei bereits umgesetzt worden, so dass eine Testphase bald erfolgen kann. Hersteller wie Juniper, Infoblox oder Enterasys Networks sind ebenfalls an diesen Ergebnissen interessiert, weshalb eine enge Partnerschaft zu dem Forschungsvorhaben besteht.

Es bleibt zu wünschen, dass zukünftig möglichst viele Hersteller auf IF-MAP setzen werden, damit die Datenkonsolidierung zwischen verschiedenen IT-Sicherheitskomponenten nicht nur eine Vision bleibt. *(bk)*