Automatisches Erkennen mobiler Angriffe auf die IT-Infrastruktur

Prof. Dr. Kai-Oliver Detken[1] · Dr. Dirk Scheuermann[2] · Ingo Bente[3] · Jürgen Westerkamp[4]

[1]DECOIT GmbH, Fahrenheitstr. 9, D-28359 Bremen
detken@decoit.de

[2]Fraunhofer SIT, Rheinstrasse 75, D-64295 Darmstadt
dirk.scheuermann@sit.fraunhofer.de

[3]Hochschule Hannover, Ricklinger Stadtweg 120, D-30459 Hannover
ingo.bente@fh-hannover.de

[4]macmon secure gmbh, Bülowstraße 66, D-10783 Berlin
juergen.westerkamp@mikado.de

Zusammenfassung

Eine sichere und korrekt funktionierende IT-Infrastruktur ist mittlerweile unabdingbar. Die rasant gestiegene Nutzung von mobilen Geräten (speziell Smartphones) im Unternehmenseinsatz und mangelnde Sicherheitskonzepte für diese neue Geräteklasse machen aber Unternehmensnetze zu einem attraktiven Angriffsziel. Trotz zahlreicher Möglichkeiten das Netzwerk abzusichern wie z.B. durch Firewalls oder VPNs haben diese Lösungen oft das Problem, dass sie isoliert voneinander arbeiten und viele Angriffe nur durch die Kombination von Daten verschiedenster Systeme erkannt werden können. Selbst wenn heute ein Angriff erkannt wird, erfolgen Gegenmaßnahmen oft zu spät und der Angreifer hat bereits den Betrieb wichtiger Systeme gestört oder sensible Informationen erlangt. Dieser Bericht beschreibt die innerhalb des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Verbundprojektes ESUKOM bisher erreichten Ziele. Das ESUKOM-Projekt versucht die beschriebene Sicherheitsproblematik zu beheben, indem Informationen verschiedener Sicherheitssysteme zentral gespeichert, ausgewertet und abgerufen werden können. Damit wird den beteiligten Systemen Zugriff auf den aktuellen Sicherheitsstand des gesamten Netzwerkes ermöglicht. Als zusätzliches Sicherheitsinstrument soll eine automatisierte Reaktion möglich sein, um zeitnah auf Bedrohungen des Netzwerkes reagieren zu können. Als technologische Basis wird das durch die Trusted Computing Group (TCG) spezifizierte IF-MAP Protokoll verwendet.

1 Einleitung

Der erste grundlegende Schritt innerhalb des ESUKOM-Projekts war die Definition von Szenarien für den Einsatz von mobilen Endgeräten. Als Arbeitsgrundlage wurde dabei zuerst betrachtet, welche mobilen Geräte zum Einsatz kommen können, aus welchen Komponenten die

P. Schartner · J. Taeger (Hrsg.) · DACH Security 2012 · syssec (2012) pp-pp.

Infrastruktur besteht, über die die Geräte Zugriff erhalten, und auf welche Ressourcen diese Geräte zugreifen. Von den beteiligten KMUs wurden dazu fachliche Szenarien geliefert, die sich aus praktischen Kundenprojekten bzw. Kundenanfragen ergaben. Zudem wurde betrachtet wie eine zentrale IF-MAP-Struktur die Sicherheit und Verwaltbarkeit weiter verbessern könnte. Aus diesen fachlichen Szenarien ergaben sich Bedrohungen, die für das mobile Gerät oder das Firmennetzwerk entstehen. Die Definition der Szenarien und Bedrohungen war wichtig für die Ableitung von Kernanforderungen für das ESUKOM-Projekt. Die Kernanforderungen zeigten klar die vielfältigen Vorteile einer zentralen IF-MAP-Struktur auf und wirken den definierten Bedrohungen entgegen. Abschließend wurde innerhalb der Anforderungsanalyse genauer betrachtet, welche Komponenten zusätzlich notwendig sind und wie die Kommunikation zwischen den Komponenten ablaufen muss, um die Kernanforderungen erfüllen zu können.

2 IF-MAP-Spezifikation

Die Trusted Computing Group (TCG) hat im Mai 2008 die erste Version der IF-MAP-Spezifikation veröffentlicht, welche später in zwei Teile aufgespalten wurde. Seit Mai 2012 liegen neue Versionen vor ([TCG12-1], [TCG12-2]). IF-MAP ist ein offenes, Hersteller-unabhängiges Protokoll zum Austausch von beliebigen Daten innerhalb eines Netzwerkes in Echtzeit. IF-MAP ist ein integraler Bestandteil des Trusted Network Connect Frameworks der TCG. Die TNC-Architektur ist in Abb. 1 dargestellt.

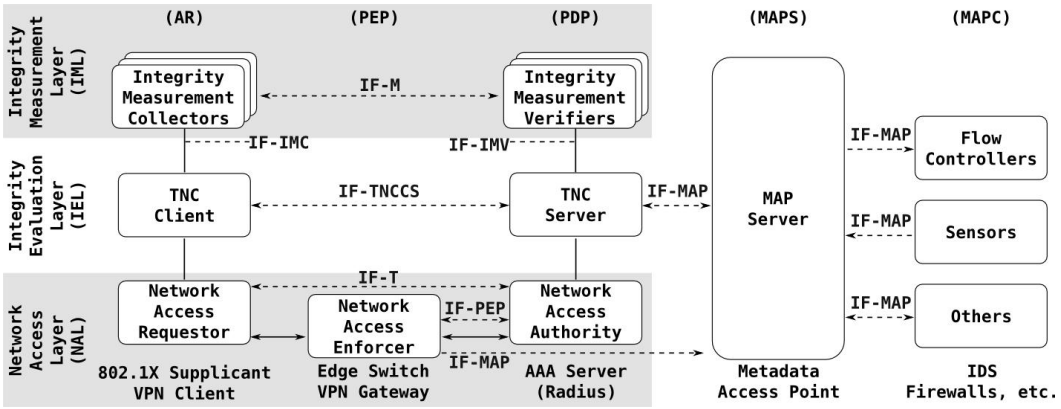

Abb. 1: TNC-Architektur in der Version 1.4 [TCG09]

Die Architektur ist in fünf verschiedene Spalten unterteilt, die jeweils eine Rolle definieren, die Komponenten in einem Netzwerk übernehmen können. Die Bedeutung der Rollen wird im Folgenden kurz beschrieben.

1. Als **Access Requestor (AR)** wird ein Endgerät bezeichnet, das Zugriff auf ein durch TNC geschütztes Netzwerk erhalten möchte.
2. Ein **Policy Decision Point (PDP)** befindet sich innerhalb des zu schützenden Netzwerkes. Basierend auf dem Integritätszustandes des Access Requestors entscheidet der PDP, in welchem Umfang Zugriff auf ein geschütztes Netzwerk gewährt wird.
3. Ein **Policy Enforcement Point (PEP)** befindet sich „am Rand“ des zu schützenden Netzwerkes. Dabei handelt es sich in der Regel um Wireless Access Points oder kabelgebundene Switche. Ein PEP setzt die Zugriffsentscheidung die ein PDP getroffen hat um.

4. Ein Server innerhalb des zu schützenden Netzwerkes, der so genannte **Metadata Access Point (MAP)**, ist dafür verantwortlich, den aktuellen Zustand des Netzwerkes abzubilden. Dieser Zustand wird anhand eines vorgegebenen Formates für Metadaten beschrieben und kann (sicherheitsrelevante) Informationen wie angemeldete Benutzer, verwendete IP-Adressen oder erkannte Anomalien enthalten.
5. Die letzte der definierten Rollen wird als **MAP-Client (MAPC)** bezeichnet. Über die standardisierte Schnittstelle **IF-MAP** können MAP-Clients Metadaten von einem MAP-Server abfragen oder neue Metadaten veröffentlichen.

Die Rolle eines MAPC kann von verschiedenen Komponenten übernommen werden. Insbesondere auch von Komponenten die schon als PDP oder als PEP fungieren. Zum Beispiel kann ein PDP nach erfolgreicher Authentisierung eines Benutzers sowie der Integritätsüberprüfung des verwendeten Endgerätes Metadaten in dem MAP-Server veröffentlichen. Diese Metadaten werden in der Regel den erfolgreichen Zugriff des Access Requestors auf das Netzwerk widerspiegeln. Die einzelnen Rollen sind nochmals in einzelne, logische Komponenten unterteilt. Insgesamt drei Schichten kapseln wiederum Komponenten mit ähnlicher Funktionalität. Gestrichelte Linien zeigen standardisierte Schnittstellen und Protokolle zwischen den einzelnen Komponenten an.

IF-MAP ist ein solches Standard-Protokoll im Sinne des TNC Frameworks. MAP-Clients (MAPC) können Metadaten von einem MAP-Server abfragen oder neue Metadaten veröffentlichen. Innerhalb des MAP-Servers werden die veröffentlichten Metadaten in Form eines Graphen verwaltet. Damit bietet sich die Möglichkeit, an zentraler Stelle eine Gesamtsicht auf den aktuellen Status eines Netzwerkes zu etablieren. Durch Korrelation der vorhandenen Metadaten können außerdem sicherheitsrelevante Informationen abgeleitet werden.

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:

1. Durch die **Publish-Operation** kann ein MAPC neue Metadaten veröffentlichen, vorhandene Metadaten ändern oder sogar löschen.
2. Ein MAPC kann per **Search-Operation** nach vorhandenen Metadaten suchen.
3. Über die **Subscribe-Operation** kann sich ein MAPC über Änderungen der im MAPS gespeicherten Metadaten informieren lassen. Dabei wird seitens des MAPC spezifiziert, welche Art von Metadatenänderungen relevant ist. Nur solche Änderungen haben eine Benachrichtigung durch den MAPS zur Folge.

Technologisch setzt IF-MAP auf eine Reihe von etablierten Standardtechnologien. 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 Netzwerkes austauschen.

3 Der Ansatz des ESUKOM-Projektes

Basierend auf den fachlichen Szenarien sowie den Bedrohungsaspekten wurden im ESUKOM-Projekt Kernanforderungen abgeleitet, welche die Basis für die weiteren Arbeiten bildeten: Anomalie-Erkennung, Smartphone Awareness, Single-Sign-Off, Secure Evidence,

Identity Awareness, Location-based Services, Erkennen von Malapp-basierten Angriffen und Real-time Enforcement. Diese Kernanforderungen bestehen aus einer Menge von Anwendungsmöglichkeiten, deren technologische Grundlage der Austausch von Metadaten über das IF-MAP-Protokoll ist. Sie ermöglichen es, den identifizierten Bedrohungen effektiv entgegenzuwirken. Durch diese Abstraktion ließen sich die erforderlichen Kern-Funktionen unabhängig von einer konkreten Fachlichkeit benennen. Auf diese Weise kann den universellen Einsatzmöglichkeiten des IF-MAP-Protokolls Rechnung getragen werden. Die Auswahl der nachfolgend beschriebenen Kernanforderungen, haben sich bei den späteren Überlegungen als besonders relevant für das in Kapitel 4 beschriebene Anwendungsszenario herausgestellt.

3.1 Anomalie-Erkennung

Zur Anomalie-Erkennung werden möglichst viele Informationen, die möglicherweise auch unabhängig von diesem Einsatzszenario gesammelt worden sind, beobachtet, so dass sich Normalverhalten und Grenzverhalten identifizieren lassen. Wird dann eine Grenzwertüberschreitung festgestellt, so kann dies durch Korrelation mit dem sonstigen Systemverhalten eingeordnet werden. Insbesondere mehrere, gleichzeitige Grenzüberschreitungen könnten dabei interessant sein. Die Stärke von IF-MAP gegenüber einer IDS Anomalie-Erkennung liegt in der Diversität der Daten.

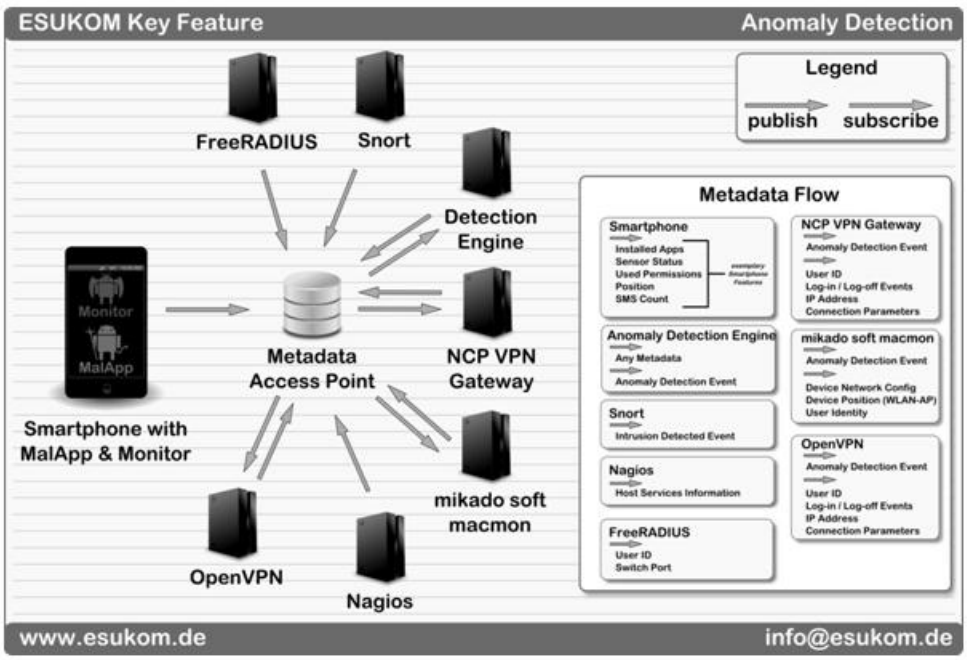

Abb. 2: Relevante Komponenten der Anomalie-Erkennung

Die Anomalie-Erkennung könnte auf verschiedene Metadaten angewandt werden. Dies sind beispielsweise die Network-Security-Metadaten wie Access-Request, IP, MAC oder Location-Information. Zusätzlich wäre es hilfreich, die Persistierung der entsprechenden Metadaten gewährleisten zu können. Zwar ermöglicht es IF-MAP, veröffentlichte Metadaten permanent in dem MAP-Server zu speichern (d.h. unabhängig von der aktuellen Session eines Clients). Diese Metadaten können später aber auch wieder gelöscht werden. Im Kontext von IF-MAP ist dieser Zustand der gleiche, als wenn die Metadaten nie veröffentlicht worden wären. Für die geplante Anomalie-Erkennung kann es allerdings erforderlich sein, sowohl das Veröffent-

lichen als auch das Löschen der Metadaten zu persistieren. Darüber hinaus können bei IF-MAP-Metadaten auch an die Laufzeit einer Session gebunden werden. Beendet der MAP-Client die Session, werden die entsprechenden Metadaten gelöscht. Auch in diesem Fall ist eine Persistierung der Metadaten zur Anomalie-Erkennung erforderlich. Andernfalls wäre es zum Beispiel nicht möglich, das Normalverhalten des Clients bzgl. der Anzahl der Logins zu bestimmen.

Für die Anomalie-Erkennung können nun folgende Daten gesammelt werden: Login-Count eines Useraccount (ID) oder eines Geräts (MAC), Zeit des Logins im System, Anwesenheit erfasst z. B. durch ein Arbeitszeiterfassungssystem, Anzahl der MAC-Adressen, die mit einer UserID verbunden sind sowie die Anzahl messbarer Aktionen im System (z.B. Zugriffe auf Patientendatenbank).

3.2 Smartphone Awareness

Für das Erkennen von Angriffen auf Unternehmensnetze und die Einleitung entsprechender Gegenmaßnahmen sind auch die Typen der eingesetzten Geräte von Bedeutung. Bestimmte Geräte können gesonderte Schutzmaßnahmen erfordern oder aus Sicherheitsgründen auch gleich von der Verwendung für bestimmte Funktionen ausgeschlossen sein. Für den mobilen Datenzugriff spielen Smartphones eine besondere Rolle, weshalb gerade hier besondere Sicherheitsaspekte zu beachten sind. So ist es beispielsweise denkbar, dass in Unternehmensnetzen auf bestimmte Daten und Dienste ein Zugriff über Smartphones gar nicht zulässig ist, sondern ausschließlich über besondere unternehmenseigene Geräte erfolgen darf. Zu diesem Zweck wurde im Rahmen von ESUKOM die Kernanforderung Smartphone Awareness definiert. Sie dient dazu, ein Gerät zweifelsfrei als zur Kategorie Smartphone zugehörig zu erkennen um aufgrund dieser Status-Meldung entsprechend Maßnahmen einleiten zu können.

3.3 Location-based Services

Bei der Nutzung von Diensten in mobilen Netzen spielt auch der Aufenthaltsort des Benutzers bzw. seines verwendeten Endgerätes eine Rolle. Bestimmte sicherheitskritische Dienste sollen nur von bestimmten Orten (z.B. ein abgegrenzter Bereich innerhalb eines Unternehmens) nutzbar sein, oder die Nutzung aus größerer Entfernung unterliegt besonderen Sicherheitsvorkehrungen. Im Rahmen von ESUKOM dient die Kernanforderung dazu, verlässliche Informationen über den Aufenthaltsort eines Benutzers bzw. den Standort eines Endgerätes zu bekommen und bei bestimmten Systemzuständen oder Zugriffsversuchen auf Dienste in Abhängigkeit der Ortsinformationen reagieren zu können.

3.4 MalApp-Erkennung

Im Rahmen der Bedrohungsanalyse haben sich MalApps als Ursache für viele Bedrohungen herausgestellt. Im Rahmen des ESUKOM-Projektes werden deshalb MalApps erkannt und so den Bedrohungen entgegengewirkt. Verschiedene Ansätze, um MalApps zu erkennen, werden dabei verfolgt:

1. Eine Möglichkeit ist es, auf Ergebnissen der Anomalie-Erkennung aufzusetzen. Wird eine Anomalie für ein Smartphone festgestellt, soll darauf aufbauend untersucht werden, ob eine auf dem Smartphone installierte App dafür die Ursache sein könnte.

2. Eine weitere Möglichkeit besteht in der Analyse, der auf den Smartphones vorhandenen Apps. Basierend auf Parametern wie Urheber und gewährten Rechten kann das Bedrohungspotential der App für die IT-Infrastruktur zumindest grob ermittelt werden.

Ob die MalApps für Sensor-basierte Angriffe, DoS-Angriffe oder für das Abgreifen von (lokal) vorhandenen Daten eingesetzt werden, ist dabei für die Erkennung des Angriffes nicht relevant. Um das Bedrohungspotential von verwendeten Apps serverseitig bewerten zu können, müssen möglichst viele Parameter über IF-MAP gesammelt werden. Dafür ist eine Monitoring-Komponente auf den Smartphones erforderlich, die die erforderlichen Daten sammelt und zum MAP-Server überträgt. Folgende Metadaten wären in diesem Kontext wichtig: eine Liste der installierten Apps pro Smartphone, der Urheber einer App, die Quelle aus der die App bezogen worden ist oder die Berechtigungen die die App auf dem Gerät hat.

Ein konkretes Beispiel kann anhand der Android-Plattform aufgezeigt werden. Dort geben Apps in einer Art Manifest an, welche System-Berechtigungen (so genannte Permissions) sie benötigen, um korrekt zu funktionieren. Der Benutzer muss diese Berechtigungen akzeptieren, bevor die App installiert und genutzt werden kann.

3.5 Real-time Enforcement

Die Kernanforderung Real-time Enforcement spielt eine übergeordnete Rolle. Sie behandelt die Reaktion auf Ereignisse, welche ggf. bei anderen Kernanforderungen erkannt wurden. Die Kernanforderung Real-time Enforcement ist deshalb auch für alle später im Anwendungsszenario betrachteten Anwendungsfälle relevant (siehe Kapitel 4).

Die vielleicht größte Herausforderung beim Real-time Enforcement, welches vollautomatisch durchgeführt wird, ist das Verhindern von falschen Entscheidungen (sog. False Positives). Hierzu kann zum Beispiel eine strikte Policy bzgl. der Rechte zur Veröffentlichung solcher Informationen eingesetzt werden. Je nachdem an welcher Stelle die Entscheidung für das Real-time Enforcement getroffen wird, werden unterschiedliche Metadaten benötigt. Im einfachsten Fall liegt die Auswertung der Metadaten bei den einzelnen MAP-Clients, die auch die Entscheidung über das Enforcement anhand einer Policy treffen. Um die Vorteile der Korrelation von Metadaten nutzen zu können, müssen spezielle Metadaten veröffentlicht werden, auf die die einzelnen Clients reagieren können. Diese Metadaten enthalten Werte, die anhand einer Warnstufe oder einer Aktion den Clients vorgeben, welche Aktion durchgeführt werden soll.

Ein Beispiel für das IF-MAP gestützte Real-time Enforcement ist die Reaktion eines Paketfilters auf erkannte Anomalien. Anomalien können in diesem Zusammenhang klassische, durch ein Intrusion Detection System (IDS) erzeugte Events sein, die auf eine Verletzung der Unternehmens-Policy hindeuten (z.B. die Nutzung von peer2peer-Programmen). Darüber hinaus können Anomalien natürlich auch von der vorher beschriebenen Anomalie-Erkennungs-Anwendung erzeugt werden. Als Reaktion auf erkannte Anomalien wird es oft erforderlich sein, den Zugriff des verursachenden Endgerätes auf das Netzwerk zu limitieren. Ein über IF-MAP an den MAP-Server angebundener Paketfilter kann sich über solche Events informieren lassen und seine Konfiguration entsprechend anpassen, beispielweise um den vom verursachenden Endgerät ausgehenden Datenverkehr zu blockieren. Dies ist insbesondere auch für verteilte Firewall-Umgebungen leicht umsetzbar.

4 Generisches Anwendungsszenario

Im ESUKOM-Projekt wurde aus sechs verschiedenen realen Szenarien ein generischer Anwendungsfall beschrieben, der für die Entwicklung als Vorgabe genutzt wurde. Gemeinsamer Nenner aller Szenarien war der mobile Mitarbeiter, weshalb die Manipulation und Kompromittierung mobiler Endgeräte durch Schadsoftware speziell betrachtet wurde. Hierbei ergeben sich Risiken, welche durch die unbemerkte Installation von Schadsoftware auf mobilen Endgeräten entstehen können. Daraus ergeben sich wiederum für die Administratoren von Unternehmensnetzen zahlreiche neue Herausforderungen und Gefährdungen, welche es zu bewältigen gilt. Auf der anderen Seite werden Übergriffe auf Unternehmensnetze und deren Daten für Angreifer ein zunehmend lukrativer Geschäftsbereich [SCHM09], was wiederum dazu führt, dass die Autoren von Schadsoftware zunehmend professioneller und zielgerichteter agieren.

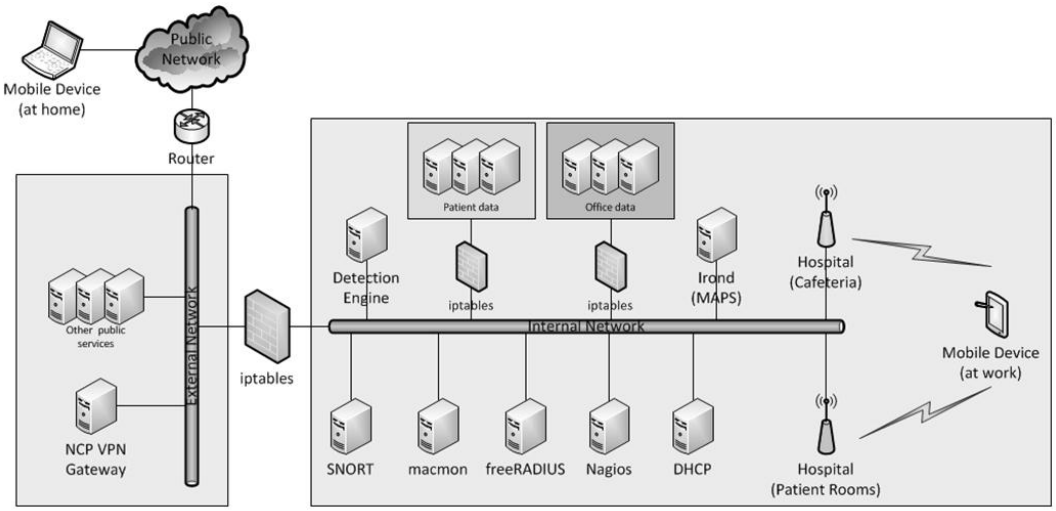

Abb. 3: IT-Infrastrukturübersicht des generischen Krankenhaus-Szenarios

Das generische Anwendungsszenario bezieht sich auf die IT-Umgebung in einem Krankenhaus. In diesem Krankenhaus werden zur Erleichterung der ärztlichen Tätigkeit mobile Endgeräte verwendet. Die mobilen Endgeräte können von der medizinischen Belegschaft verwendet werden, um mobile Patientendaten abzurufen und zu bearbeiten. Zusätzlich kann das Personal aber mobile Geräte nutzen, um über eine externe Verbindung auf ihre persönlichen Daten wie E-Mails, Kontakte oder Termine zuzugreifen.

Als Sicherheitsrichtlinien können genannt werden:

a. Aufgrund der Sensibilität von Patientendaten, darf der Zugriff auf diese nur
   - aus dem internen Netzwerk erfolgen. Hierbei wird bei mobilen Geräten eine VPN-Verbindung benötigt,
   - während des Aufenthalts im Patientenbereich erfolgen. Hierzu müssen die Geräte sich geographisch in diesem Bereich befinden.

b. Ausschließlich mobile Geräte von Ärzten dürfen auf die Patientendaten zugreifen. Pflege- und Verwaltungspersonal darf ausschließlich persönliche Bürodaten abrufen.

c. Die Anwendung zum Zugriff auf die Patientendaten, sowie der Office-Zugang erfordern eine Authentifizierung des Benutzers.

d. Alle mobilen Geräte, die Zugriff auf das interne Netzwerk erhalten, verfügen ausschließlich über Software, die durch den Administrator freigegebenen wurde.

Abb. 3 zeigt eine Übersicht der IT-Infrastruktur im Krankenhaus. Folgende Netzwerksegmente sind hierbei zu unterscheiden:

a. **Internal Network:** Das interne Netzwerk enthält alle IF-MAP-Clients (ESUKOM-Sicherheitslösungen) und den IF-MAP-Server (irond), sowie die Server mit Patienten- und Bürodaten. Das interne Netzwerk ist durch eine Firewall (iptables) vom externen Netzwerk getrennt. Zusätzlich bietet das interne Netzwerk ein WLAN für den mobilen Zugriff auf Patienten- und Bürodaten. Das WLAN ist logisch durch die Position der WLAN Access Points unterteilt. Hierbei werden WLAN-APs im Patientenbereich des Krankenhauses und WLAN-APs im öffentlichen (Cafeteria) Bereich unterteilt.

b. **External Network:** Das externe Netzwerk (DMZ) enthält alle Dienste, die vom Internet erreichbar sind. Im Szenario ist ausschließlich das NCP VPN-Gateway um Verbindungen in das interne Netzwerk aufzubauen, von Bedeutung. Zusätzlich ist ein Router an das externe Netzwerk angebunden, welcher die Verbindung zum Internet herstellt.

c. **Public Network:** Das Internet (Public Network) wird von Mitarbeitern verwendet, um mit Ihren mobilen Geräten von zu Hause aus zu arbeiten.

Die verschiedenen IF-MAP-Clients, Server und Endgeräte sind wie folgt konfiguriert:

a. **Mobile Endgeräte:** Die mobilen Endgeräte der Mitarbeiter sind mit *NCP VPN-Clients* und dem *DECOIT IF-MAP-Android-Client* ausgestattet.

b. **Datenserver:** Die Server mit den Patientendaten bzw. den Bürodaten sind durch einen eigenen Authentifizierungsmechanismus geschützt.

c. **NCP VPN-Gateway:** Das *NCP VPN-Gateway* nimmt Verbindungen von den mobilen Geräten der Mitarbeiter an und leitet diese in das internen Netzwerk weiter.

d. **iptables:** Gibt den Zugang nur für Verbindungen vom VPN-Gateway vom externen Netzwerk in das interne Netzwerk frei. Verbindungen vom internen in das externe Netzwerk unterliegen keiner Beschränkung. Zusätzlich existieren zwei iptables Firewalls, welche die Patienten- und Bürodaten schützen. Diese geben den Zugriff ausschließlich für IP-Adressen frei, welche im MAPS von einem bekannten IF-MAP-Client autorisiert sind. Es wird der *DECOIT IF-MAP-Client* verwendet.

e. **SNORT:** Snort scannt das Netzwerk auf sicherheitskritische Ereignisse und publiziert diese als IF-MAP-Events. Damit wird jedes erkannte Ereignis als Event in MAPS für andere IF-MAP-Clients veröffentlicht. Es wird der *DECOIT IF-MAP-Client* verwendet.

f. **macmon NAC:** Der *macmon NAC* scannt das interne und externe Netzwerk und publiziert alle autorisierten Geräte in IF-MAP. Bei Erkennung von unautorisierten oder nicht mehr sicher konfigurierten Geräten, werden diese Geräte vom Netzwerk getrennt (falls möglich). Zusätzlich werden diese Ereignisse per IF-MAP-Event publiziert.

g. **FreeRADIUS:** Der FreeRADIUS-Server veröffentlicht die Profile von externen mobilen Teilnehmern, welche sich über WLAN mit 802.1X authentifiziert haben. Es wird der *DECOIT IF-MAP-Client* verwendet.

h. **Nagios:** Das Nagios-System fragt kontinuierlich den Zustand der im Netzwerk aktiven Hosts und Services ab. Statuswechsel werden an den MAPS publiziert. Es wird der *DECOIT IF-MAP-Client* verwendet.

i. **MAP-Server:** Der MAP-Server *irond* von der Hochschule Hannover stellt die zentrale MAP-Serverkomponente (MAPS) dar.

j. **Detection Engine:** Die Detection Engine *irondetect* von der Hochschule Hannover kontrolliert die Daten des MAPS und analysiert diese auf bekannte Signaturen oder das Auftreten von Anomalien.

k. **DHCP:** Der ISC DHCP-Server ist mit der IF-MAP-Erweiterung *irondhcp* von der Hochschule Hannover ausgestattet und veröffentlicht alle IP- zu MAC-Adressen-Zuordnungen an den MAPS.

Im ersten Anwendungsfall versucht ein Angreifer vom öffentlichen Netzwerk direkt auf Ressourcen im internen Netzwerk zuzugreifen. Der Angreifer verwendet dabei ein unbekanntes mobiles Gerät. Bei diesem Angriff scheitert der Angreifer direkt an der iptables-Firewall, da diese ausschließlich Geräte zulässt, welche vom VPN-Gateway autorisiert wurden. Das *NCP VPN-Gateway* weist jedem verbundenen Endgerät eine eigene IP-Adresse zu und veröffentlicht diese per IF-MAP. Der *DECOIT IF-MAP-Client* der Firewall übernimmt alle vom VPN-Gateway veröffentlichen IP-Adressen in seine interne Liste mit autorisierten Adressen. Dieser Anwendungsfall ist ausschließlich für die Kernanforderung Real-time-Enforcement relevant.

Beim zweiten Anwendungsfall verbindet sich ein Mitarbeiter über einen WLAN-AP in der Cafeteria mit dem internen Netzwerk und versucht auf die Patientendaten zuzugreifen. In diesem Fall scheitert der Mitarbeiter an der iptables-Firewall, welche den Zugriff auf die Patientendaten steuert. Das Endgerät des Mitarbeiters wird von allen IF-MAP-Clients im Netzwerk autorisiert. Zusätzlich wird von *macmon NAC* die Position des Endgerätes (AP im Cafeteria-Bereich) publiziert. Von der Detection Engine *irondetect* wird dadurch ein Event ausgelöst, welches die Firewall veranlasst, die IP-Adresse des Endgerätes zu sperren. Neben dem Real-time-Enforcement spielen hier die Kernanforderungen Smartphone Awareness und Location-based-Services eine Rolle: das Endgerät könnte z.B. aufgrund seiner besonderen Eigenschaft als Smartphone oder aufgrund seiner erkannten Position zurückgewiesen werden.

In einem weiteren Anwendungsfall versucht ein Mitarbeiter mit einem mobilen Endgerät, welches von schadhafter Software befallen ist, auf die Datenserver zuzugreifen. In diesem Fall scheitert der Mitarbeiter ebenfalls an der iptables Firewall vor den Datenservern oder an der Verbindung zum *NCP VPN-Gateway*, falls eine Verbindung von außerhalb des internen Netzwerks aufgebaut wird. Das Endgerät des Mitarbeiters wird auch in diesem Anwendungsfall von allen IF-MAP-Clients ordnungsgemäß im MAPS *irond* als autorisiertes Gerät gemeldet. Der *DECOIT IF-MAP-Android-Client* veröffentlicht bei der Verbindung zum Netzwerk die installierten Anwendungen des Endgerätes an den MAPS. Die Detection Engine *irondetect* analysiert die Daten im MAPS und veröffentlicht ein Event zum Befall des Endgerätes mit einer MalApp. Die Firewalls sowie das VPN-Gateway sperren daraufhin das Endgerät aus dem internen Netzwerk aus. Unter den Kernanforderungen spielt hier die Malapp-Detection eine besondere Rolle.

Im letzten Anwendungsfall versucht ein Angreifer mit einem gestohlenen mobilen Endgerät an sensible Daten zu gelangen. Der Angreifer verbindet sich hierbei mit einem WLAN-AP aus dem Patientenbereich. In diesem Fall scheitert der Angreifer wieder an der Firewall vor den Datenservern. Das Endgerät wird vorerst von den Sicherheitssystemen ordnungsgemäß autorisiert. Der Angreifer kann dadurch ohne Einschränkungen auf alle Daten zugreifen. Im Hintergrund werden Nutzungsdaten vom *DECOIT IF-MAP-Android-Client* an den MAPS *irond* gesendet. Von der Detection Engine werden die Nutzungsdaten analysiert und mit dem Normalverhalten des eigentlichen Besitzers des Endgerätes vergleichen. Das mehrfache und frequentierte Zugreifen des Angreifers auf beliebige Patientendaten wird hierbei als Anomalie erkannt. Die Detection Engine *irondetect* publiziert daraufhin ein Event im MAPS, welches zur Folge hat, dass alle Sicherheitssysteme das Endgerät des Angreifers sperren. Besonders relevant für diesen Anwendungsfall ist die Kernanforderung Anomalie-Erkennung, da sich ein gestohlenen Endgerät typischerweise durch die dabei betrachteten Anomalien auszeichnet.

5 Detection Engine

Durch die Integration verschiedener Netzwerkkomponenten stehen sicherheitsrelevante Informationen an einer zentralen Stelle zur Verfügung. Innerhalb des MAP-Servers werden die Daten durch einen ungerichteten Graphen strukturiert. In praktischen Einsatzszenarien können diese Metadatengraphen sehr komplex werden. Zudem sind sie ständigen Änderungen unterworfen. Durch diese Komplexität und Dynamik der vorhandenen Daten ist ihre sinnvolle Auswertung allerdings schwierig.

Die sinnvolle Erkennung und Abwehr von Angriffen kann sich nicht auf die alleinige Erkennung illegaler Systemzustände oder unerwünschter Ereignisse beschränken. Viel mehr bewirkt ein Angriffsszenario häufig eine ungewöhnliche Kombination von Systemzuständen oder eine ungewöhnliche zeitliche Abfolge von Ereignissen welche für sich genommen in Ordnung sind. Man könnte den Ansatz verfolgen, das Datenmodell mit zugehörigen Policys gleich im Hinblick auf abzuwehrende Angriffsszenarien zu gestalten, welche dann zu illegalen System-Zuständen führen. Zur Berücksichtigung neuer Angriffs-Szenarien wäre dann aber jedes Mal eine Anpassung erforderlich.

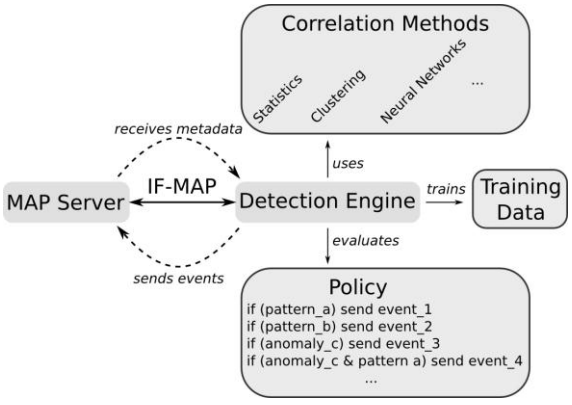

Abb. 4: Übersicht der Detection-Engine-Architektur

Im Rahmen des ESUKOM-Projektes wird der Ansatz verfolgt, eine Analyse des MAP-Graphen über einen speziellen MAP-Client, die so genannte Detection Engine, durchführen zu lassen. Das Ziel ist es, sowohl eine Muster- als auch eine Anomalie-Erkennung basierend auf den in Echtzeit gesammelten und vorliegenden Metadaten durchführen zu können. Durch

eine Mustererkennung können zum Beispiel Signaturen, von in einem Unternehmen nicht zugelassenen Apps, auf einem Smartphone leicht erkannt werden. Über Anomalie-Erkennung sollen verdächtige Abweichungen im Verhalten eines Smartphones erkannt werden, da diese auf einen Sicherheitsvorfall hindeuten können. Als Reaktion auf erkannte Signaturen und Anomalien kann die Detection Engine ein entsprechendes Event in dem MAP-Server publizieren. Durch diese Rückkopplung wird es dann anderen Systemen ermöglicht, gemäß ihrer Policys auf die erkannten Vorfälle zu reagieren (z.B. im Rahmen eines Real-time Enforcements).

Die Detection Engine ist wie erwähnt als MAP-Client realisiert. Über passende Subscriptions können so sämtliche Metadaten, die im MAP-Server veröffentlicht werden und quasi in Echtzeit bezogen werden. Policys für die Detection Engine definieren, nach welchen Mustern bzw. Anomalien gesucht werden sollen und mit welchen Events auf erkannte Fälle reagiert werden kann. Zur Mustererkennung reicht ein einfacher Vergleich, der in der Detection Engine Policy definierten Muster, mit den empfangenen Metadaten aus. Wenn ein bestimmtes Angriffsmuster erkannt wird, durch eine so definierte Regel der Policy, wird direkt ein entsprechender Event veröffentlicht. Der Versuch mit laut Signatur nicht zugelassenen Apps unbefugter Weise auf Daten zuzugreifen ist dann ein Beispiel für ein Angriffsszenario das man über die Mustererkennung recht einfach abwehren kann.

Die Erkennung von Anomalien (d.h. eine „zu große“ Abweichung vom erwarteten Normalverhalten) ist dagegen komplexer. Voraussetzung dafür ist, dass das Normalverhalten vorher entweder trainiert oder basierend auf Expertenwissen festgelegt worden ist. Beispiele für hiermit abzuwehrende Angriffe sind die im letzten Anwendungsfall betrachteten Zugriffsversuche mit einem gestohlenen Gerät. Hier gilt es beispielsweise zu erkennen, dass Login-Versuche außergewöhnlich häufig fehlgeschlagen sind, dass ungewöhnlich häufig auf bestimmte Daten zugegriffen wird oder dass eine Verbindung zu einer Datenbank ungewöhnlich lange aufrechterhalten bleibt. Um Anomalien zu erkennen soll die Detection Engine eine Vielzahl von verschiedenen Verfahren aus dem Bereich der Statistik (Mittelwert, Median, Clustering) und des maschinellen Lernens (Neuronale Netze) unterstützen. Neben der flexiblen Anbindung einer Vielzahl von Verfahren ist eine besondere Herausforderung festzustellen, mit welchen Verfahren sich welche Anomalien am zuverlässigsten erkennen lassen. Hierzu wird im Rahmen des ESUKOM-Prototypens aktuell eine entsprechende Evaluierung durchgeführt. Vergleichbare Ansätze zur Erkennung von Anomalien auf Smartphones haben vielversprechende Resultate geliefert [SKEGW12]. Im Gegensatz zu dem ESUKOM-Vorhaben konnten bisherige Ansätze allerdings nicht verschiedene Metadaten verschiedener Messkomponenten integrieren, sondern waren in der Regel auf Messungen nur einer Komponente beschränkt. Eine Rückkopplung von Auswerteergebnissen in Form von Events war ebenfalls bislang nicht möglich.

6 Fazit

Das IF-MAP-Protokoll stellt eine ideale Basis für die Erfüllung der Anforderungen des ESUKOM-Projektes dar. Eine Integration verschiedener Netzkomponenten hätte man grundlegend auch über alternative Ansätze realisieren können. Denkbar wäre zum Beispiel die Nutzung eines zentralen Dienstes zum Sammeln von Log-Meldungen in einem wohldefinierten Format. Die Kombination aus der Menge der unterstützten Funktionen, der Erweiterbarkeit und der durch die offene Spezifikation gegebenen Interoperabilität ist bei alternativen Ansät-

zen in der Form allerdings nicht vorhanden. Zudem wird IF-MAP von der TCG stark vorangetrieben und ist inzwischen auch bei den Netzwerkherstellern wie Juniper Networks, Enterasys Networks und Cisco Systems angekommen, wodurch eine weite Verbreitung zukünftig wahrscheinlich ist.

Das ESUKOM-Projekt hat zum Ziel mit Hilfe der IF-MAP-Spezifikation die Sicherheit von Unternehmensnetzen zu steigern, gerade im Hinblick auf mangelnde Konzepte zur Sicherheit von Smartphones. Die bisher erarbeiteten Konzepte zeigen ein hohes Potential zur Verbesserung der IT-Sicherheit moderner Infrastrukturen. Die ersten funktionsfähigen Prototypen des Projektes können bereits erfolgreich Metadaten über IF-MAP austauschen, was auch auf einem internationalen PlugFest der Trusted Computing Group (TCG) im März 2012 in Darmstadt nachgewiesen werden konnte. Auf diese Weise ist jetzt schon eine Integration von zwei kommerziellen und fünf Open-Source-Produkten über IF-MAP erfolgreich umgesetzt worden.

Die größte Herausforderung ist aktuell die Umsetzung der Detection Engine. Es ist eine offene Forschungsfrage, mit welchen Methoden welche Metadaten am geeignetsten auszuwerten sind, um bestimmte Anomalien zu erkennen. Die Detection Engine wird daher so ausgelegt, dass diese Konfiguration flexibel über entsprechende Policys gesteuert werden kann. Hinzu kommt, dass eine generische Schnittstelle zur Anbindung beliebiger Analyseverfahren (Correlation Methods) geschaffen wurde. Darüber hinaus wird gerade eine Komponente entwickelt, die es erlaubt, über einen definierten Zeitraum die erforderlichen Trainingsdaten zu sammeln. Bis zum Ende des Projektes will man auch diesen letzten Meilenstein erfolgreich gemeistert haben.

7 Danksagung

Das ESUKOM-Projekt (http://www.esukom.de) ist ein gefördertes BMBF-Projekt mit einer Laufzeit von zwei Jahren, das im Oktober 2010 seine Arbeiten begonnen hat und im September 2012 endet. An dem Projekt sind die Firmen DECOIT GmbH (Projektleitung), macmon secure gmbh, NCP Engineering GmbH sowie die Forschungseinrichtungen Fraunhofer SIT und Hochschule Hannover beteiligt. Daher gilt der Dank den Partnern des Projektes, die durch ihre Beiträge und Arbeiten diesen Bericht erst ermöglicht haben.

8 Literaturverzeichnis

[SCHM09] Schmitz, Peter: *Datendiebstahl ist ein lukratives Geschäft – fünf Tipps gegen Datendiebstahl und Datenhandel*. 14.08.09, SearchSecurity.de, Vogel IT-Medien GmbH, Augsburg 2009

[SKEGW12] Shabtai, Kanonov, Elovici, Glezer, Weiss: *"Andromaly": a behavioral malware detection framework for android devices*. Journal of Intelligent Information Systems, Volume 38 Issue 1, February 2012

[TCG09] Trusted Computing Group: *TNC Architecture for Interoperability*. Specification Version 1.4, Revision 4, Mai 2009

[TCG-12-1] Trusted Computing Group: *TNC IF-MAP Binding for SOAP*. Specification Version 2.1, Revision 15, Mai 2012

[TCG-12-2] Trusted Computing Group: *TNC IF-MAP Metadata for Network Security*. Specification Version 1.1, Revision 8, Mai 2012