Konsolidierung von Metadaten zur Erhöhung der Unternehmenssicherheit

Prof. Dr. Kai-Oliver Detken[1] · Dennis Dunekacke[1] · Ingo Bente[2]

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

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

Zusammenfassung

Eine sichere und korrekt funktionierende IT-Infrastruktur ist mittlerweile für fast jedes Unternehmen unabdingbar. Auch Unternehmen, die nicht aus dem IT-Bereich kommen, haben hohe Anforderungen an ihre IT Infrastruktur, da hier unternehmenskritische Anwendungen laufen. Die rasant gestiegene Nutzung von mobilen Geräten (speziell Smartphones) im Unternehmenseinsatz und mangelnde Sicherheitskonzepte für diese neue Geräteklasse machen Unternehmensnetze zu einem attraktiven Angriffsziel. Trotz zahlreicher Möglichkeiten das Netzwerk abzusichern wie z.B. 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. Und selbst wenn 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. Zentrales Element dabei ist die IF-MAP-Spezifikation der Trusted Computing Group (TGC), die verwendet wird um Daten zentral abzulegen und den Sicherheitssystemen den Zugriff auf die Daten zu ermöglichen.

1 Einleitung

Der erste grundlegende Schritt innerhalb des ESUKOM-Projekts war die Definition von Szenarien für den Einsatz von mobilen Endgeräten. Als Arbeitsgrundlage für die Szenarios wurde dabei zuerst betrachtet, welche mobilen Geräte zum Einsatz kommen können, aus welchen Komponenten die 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 ergeben und betrachtet wie eine zentrale IF-MAP-Struktur die Sicherheit oder Verwaltbarkeit weiter verbessern könnte. Aus diesen fachlichen Szenarios ergaben sich die Bedrohungen, die für das mobile Gerät oder das Firmennetzwerk entstehen. Die Definition der Szenarios und Bedro-

hungen war wichtig für die Ableitung von Kernanforderungen für das ESUKOM Projekt. Die Kernanforderungen stellen die Ziele das ESUKOM Projektes dar, die möglichst vollständig erfüllt werden sollen. Sie zeigen klar die vielfältigen Vorteile einer zentralen IF-MAP-Struktur 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 Mobiler Zugriff auf das Unternehmensnetz

Im ESUKOM-Projekt wurden sechs verschiedene reale Szenarien beschrieben, die die beteiligten Firmen aus Kundenprojekten gewonnen haben. Dabei wurden Logistik-, Krankenhäuser- oder Unternehmensanwendungen betrachtet. Gemeinsamer Nenner der 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, das die Autoren von Schadsoftware zunehmend professioneller und zielgerichteter agieren. Ein Beispiel, welches vor kurzem für großes Aufsehen sorgte, ist dabei der sogenannte „Stuxnet“-Wurm, welcher sich vor allem durch seine hohe Komplexität und das für die Erstellung nötige Insider-Wissen auszeichnet: Zur unerkannten Verbreitung des Wurms bedienten sich die Autoren unterschiedlicher, bis zu diesem Datum unbekannter „Zero-Day-Exploits“ sowie gestohlener Zertifikate zur Installation eigener, signierter Treiber. Darüber hinaus zeichnet sich „Stuxnet“ durch seine sehr zielgerichteten Attacken aus (das Ziel der Infizierung und Manipulation sind bestimmte industrielle Steuerungsanlagen). Insgesamt wird der Aufwand, welcher zur Erstellung von „Stuxnet“ notwendig war, als sehr hoch eingeschätzt, die Autoren müssen dabei über sehr viel Insider-Wissen und Ressourcen verfügt haben [FSEC10].

Im Mittelpunkt dieses Szenarios stehen zunächst einmal alle mobilen Endgeräte, mit denen Mitarbeiter auf das Unternehmensnetz zugreifen können. Der Fokus liegt hier jedoch auf die Geräteklasse der mobilen Smartphones: Durch deren hohe Portabilität erhöht sich gleichzeitig das Risiko eines Verlustes oder Diebstahls. Zusätzlich verstärkt wird dies durch den zunehmenden Einsatz solcher Endgeräte in immer mehr Bereichen des privaten und beruflichen Umfeldes, wobei es in vielen Fällen auch zu einer Überschneidung der beiden Bereiche kommen kann: Viele Mitarbeiter nutzen ihr Firmen-Smartphone zum Teil auch für private Zwecke, beispielsweise für Privatgespräche, Fotoaufnahmen oder den Abruf von ortbezogenen Diensten (Location Based Services) auf Dienstreisen. Zwar verfolgen einige Unternehmen dabei strenge Richtlinien für die Nutzung von Firmen-Smartphones, allerdings kann deren Durchsetzung nicht immer gewährleistet werden, da sich deren Einhaltung in manchen Fällen nur sehr schwer oder gar nicht kontrollieren lässt. Zusätzlich zeichnet sich diese Geräteklasse durch den Einsatz von noch relativ neuen Betriebssystemen aus (iOS, Android, etc.), welche einen zunehmenden Funktionsumfang und eine dementsprechend wachsende Komplexität aufweisen. Dieser Umstand führt wiederum dazu, dass auch diese Betriebssysteme vermehrt Ziele von Schadsoftware-Autoren werden.

Das hier beschriebene Szenario setzt zunächst keine spezifische Infrastruktur voraus. Es wird lediglich davon ausgegangen, dass das Unternehmen seinen Mitarbeitern die Möglichkeit bietet, auch außerhalb des Firmensitzes auf das Unternehmensnetz zuzugreifen. Um dieses zu realisieren kann dabei z.B. eine VPN Lösung zum Einsatz kommen, über welches die Mitarbeiter mit Hilfe ihrer mobilen Endgeräte zugreifen können.

Um die Kontrolle über ein mobiles Endgerät und dessen Daten und Funktionen zu erlangen, ist ein Angreifer nicht darauf beschränkt, dieses auch physikalisch in seinen Besitz zu bringen (z.B. um unbemerkt Schadsoftware auf das Gerät zu installieren). Ebenso ist es möglich, sich durch unterschiedliche Sicherheitslücken einen unerlaubten Fernzugriff auf solche Geräte zu verschaffen. Neben den Angriffsmöglichkeiten, welche durch den Einsatz unsicherer Schnittstellen geschaffen werden (z.B. Bluetooth, siehe auch [Oste08]), rückt dabei vor allem die Möglichkeit der Kompromittierung der mobilen Endgeräte durch das Ausnutzen von bestehenden Sicherheitslücken innerhalb des Betriebssystems und den darauf laufenden Programmen zunehmend in den Mittelpunkt. Hierbei bieten sich durch die zunehmende Komplexität der installierten Anwendungen unterschiedliche Angriffsvektoren an, welche für eine Kompromittierung durch Schadsoftware ausgenutzt werden können. Einige mögliche Wege für eine Infektion des Endgerätes mit einer solchen Software sind dabei:

1. Ausnutzen von Sicherheitslücken innerhalb der installierten Anwendungen und des darunter liegenden Betriebssystems. Vor allem bei den noch recht jungen Smartphone-Betriebssystemen häufen sich die Berichterstattungen über zunehmend auftretende Sicherheitslücken, einige Beispiele für Apples iPhone-OS oder Googles Android Plattform können unter [Goeb10] und [Schw10] gefunden werden. Zu den bekanntesten Lücken gehören dabei der Einsatz von manipulierten Dateien (Bild-Dateien, PDF-Dokumente etc.) oder das Ausnutzen von mobilen Webdiensten, beispielsweise um durch absichtlich herbeigeführte Pufferüberläufen (Buffer Overflows) unbemerkt eigenen Code auf das Gerät einzuschleusen [Teuf10].
2. Des Weiteren bringt die Möglichkeit, nachträglich eigene Anwendungen auf diesen Geräten zu installieren, zusätzliche Risiken mit sich, beispielsweise durch als Applikation getarnte Schadsoftware. Zwar bieten viele Geräte-Hersteller wie z.B. Apple mit den Konzept ihrer „App-Stores“ mittlerweile eine gewisse Prüfung vor der Veröffentlichung einer Anwendung, jedoch können aus unterschiedlichen Gründen meistens nicht alle sicherheitsrelevanten Aspekte betrachtet werden. So sind bereits mehrere Fälle bekannt geworden, in welchen als Applikation getarnte Schadsoftware über den offiziellen „App-Store“ auf Endgeräte gelangen konnte [Seri10].
3. Darüber hinaus existieren auch Möglichkeiten, diese Prüfung technisch zu umgehen und Anwendungen auch aus „unsicheren“ Quellen zu beziehen und auf dem Endgerät zur Ausführung zu bringen. Als Beispiel sei an dieser Stelle der sogenannte „Jailbreak-Hack“ für das iPhone OS genannt [HEIS10a]. Hierbei handelt es sich um ein Programm, welches viele der Einschränkungen des iPhones (Installieren von ungeprüften Anwendungen, freie Wahl des Mobilfunk-Betreibers etc.) aushebelt, dabei aber weitere potentielle Sicherheitslücken für eine Kompromittierung des Endgerätes öffnet. Mittlerweile wird das „Jailbreaking“ auch über eine Webseite angeboten, welche das einfache Entsperren des aufrufenden Gerätes ermöglicht. Hierbei bedienen sich die Betreiber der Webseite einer Sicherheitslücke in der PDF-Funktion des mobilen Safari-Webbrowsers. Außerdem erlauben einige Gerätehersteller auch die Installa-

tion von potentiell unsicheren Anwendungen, welche keiner vorherigen Prüfung unterzogen wurden, wie zum Beispiel Googles Android-Betriebssystem [Weig10].

Abb. 1 zeigt die verschiedenen Möglichkeiten zur Kompromittierung eines mobilen Endgerätes schematisch auf. Durch die Mobilität solcher Geräte erhöht sich auch gleichzeitig das Risiko des Verlustes oder des Zugriffs bzw. Diebstahls des Gerätes durch unbefugte Personen. Wenn unzureichende Sicherheitsvorkehrungen durch den eigentlichen Besitzer des Endgerätes getroffen wurden, wie z.B. der Einsatz von „schwachen" PIN-Codes und Passwörtern oder das Speichern von Zugangsdaten auf dem Gerät, haben unbefugte Personen die Möglichkeit Daten auszuspähen oder sich mit Hilfe des Endgerätes selbst Zugang in das Netz des Unternehmens zu verschaffen. Darüber hinaus besteht die Möglichkeit einer vom Besitzer unbemerkten Manipulation des Gerätes, beispielsweise durch die Installation von Schadsoftware, welche als Grundlage für weitere Angriffe dienen kann.

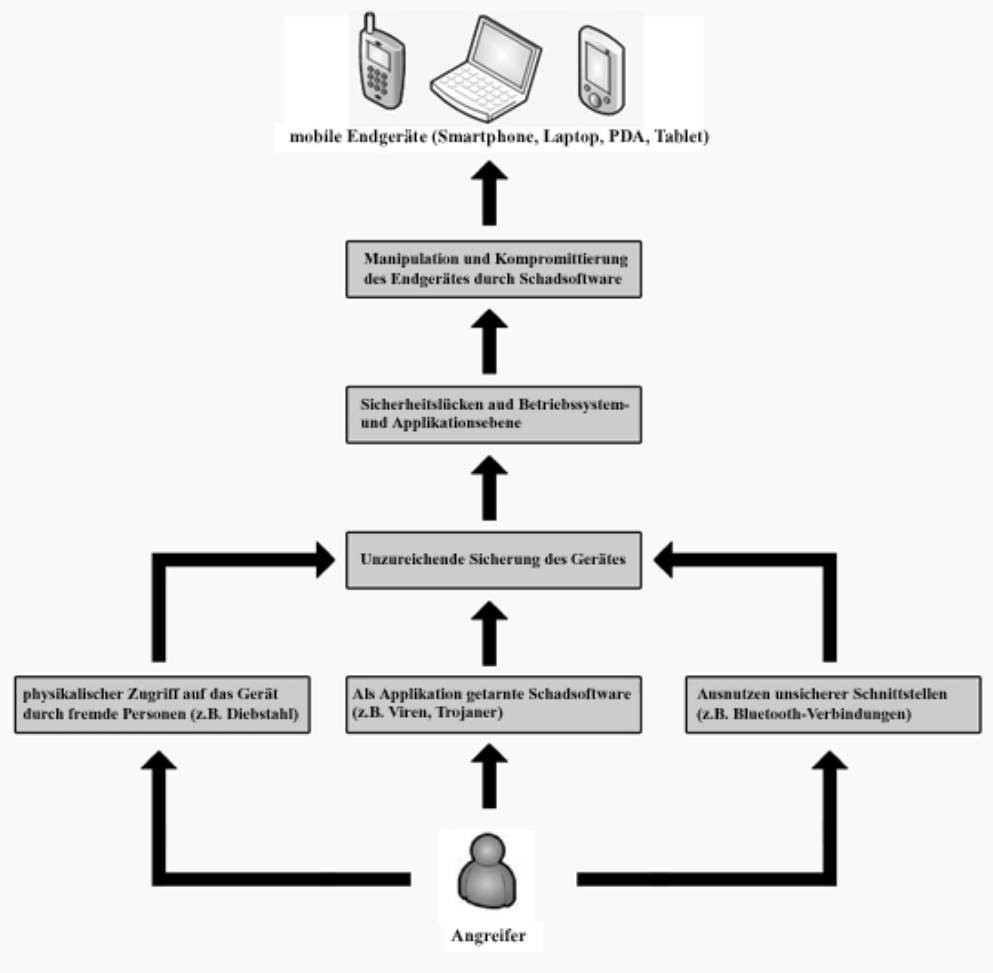

Abb. 1: Möglichkeiten zur Kompromittierung mobiler Endgeräte durch fremde Personen [DeDu11]

Durch den immer höheren Funktionsumfang und der damit einhergehenden Komplexität steigen auch die potentiellen Möglichkeiten diese Geräte zu kompromittieren um sich Zugriff auf deren sicherheitsrelevante Funktionen zu verschaffen. Gerade bei den noch recht jungen Geräteklassen, wie den eingangs erwähnten Smartphones, haben die Entwickler der eingesetzten Betriebssysteme und Anwendungen aufgrund der wachsenden Anforderungen an deren Funktionalität zunehmend mit kritischen Sicherheitslücken zu kämpfen.

Sollte ein kompromittiertes Endgerät den Zugriff auf das Unternehmensnetz erlangen, entstehen vielfältige Möglichkeiten, die Sicherheit des Unternehmens und dessen Datenbestands zu gefährden. Einige dieser Möglichkeiten sind in Abb. 2 dargestellt. [DeDu11]

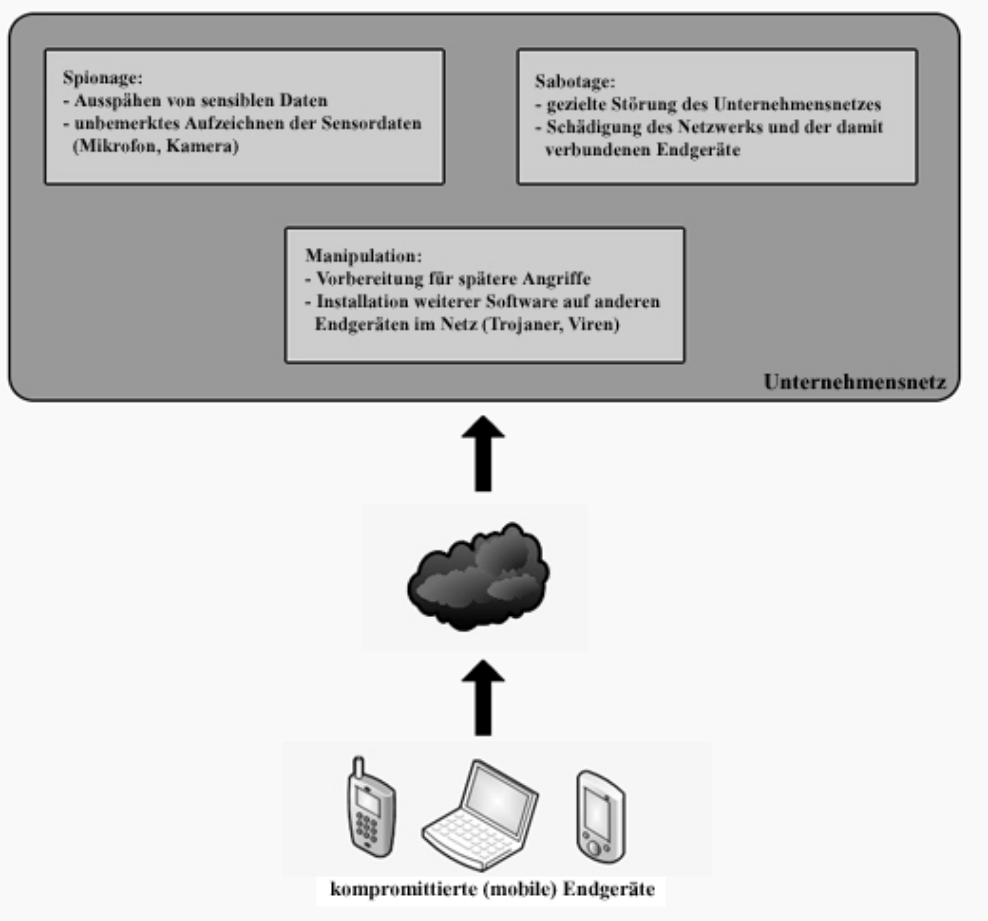

Abb. 2: Gefahren beim Zugriff durch kompromittierte Endgeräte

Die in Abb. 2 dargestellten Angriffsszenarien werden nachfolgend noch einmal detailliert ausgeführt:

1. Ausspähen von sensiblen Daten wie z.B. Nutzerdaten oder interne Unternehmensdaten. Zusätzliche Gefahren ergeben sich dabei auch außerhalb des Unternehmensnetzwerks, bedingt durch die verschiedenen Sensoren und Schnittstellen heutiger mobiler Endgeräte: Wenn diese unter die Kontrolle von unbefugten Benutzern gelangen, können mit Hilfe des eingebauten Mikrofons vertrauliche Gespräche von Fremden aufgezeichnet und mitgehört werden, die momentane Position eines Endgerätes kann ausgelesen oder die Kamera unbemerkt ausgelöst werden („Spionage“).
2. Ein mobiles Endgerät kann zum Beispiel als Überträger von Schadsoftware eingesetzt werden um einen weiteren Angriff auf das Unternehmensnetz vorzubereiten („Manipulation“).
3. Schädigung des Unternehmensnetzes oder der damit verbundenen Endgeräte. Gerade durch die zunehmend wichtige Rolle des Zugriffs auf das Unternehmensnetzes in allen Geschäftsbereichen kann ein Stillstand des Netzes für Unternehmen ein großes, finanzielles Risiko darstellen („Sabotage“).

3 ESUKOM-Projekt

Das Gesamtziel des ESUKOM[1]-Vorhabens ist die Konzeption und Entwicklung einer Echtzeit-Sicherheitslösung für Unternehmensnetze, die basierend auf der Konsolidierung von Metadaten arbeitet. Dabei soll insbesondere der durch mobile Endgeräte wie Smartphones erzeugten Bedrohungslage Rechnung getragen werden. ESUKOM setzt auf die Integration vorhandener Sicherheitslösungen (kommerziell und Open Source) basierend auf einem einheitlichen Metadatenformat gemäß der IF-MAP-Spezifikation der Trusted Computing Group (TCG). Das bedeutet konkret, dass man als Grundlage für die Arbeitsweise eine gemeinsame Datenbasis verwenden wird, die den gesamten, aktuellen Zustand eines Unternehmensnetzes abbildet. Dabei sollen alle vorhandenen Sicherheitstools die Möglichkeit besitzen, aus dieser Datenbasis die für ihre Funktionsweise relevanten Daten zu beziehen und selbst neue Daten zu veröffentlichen. Erst dadurch wird es möglich, auf verschiedenste Bedrohungen in Echtzeit zu reagieren. Das ESUKOM-Vorhaben verfolgt hinsichtlich der Integration verschiedener Sicherheitsmechanismen den Ansatz ein wohl definiertes Modell zur Beschreibung von Metadaten zu erstellen, das nicht alleine auf der Analyse von Logdateien beruht.

Das Ziel des Vorhabens ist die Konzeption und prototypische Entwicklung einer ganzheitlichen Sicherheitslösung, die durch die Integration vorhandener Sicherheitstools und die Konsolidierung von Metadaten die Sicherheit eines Netzwerkes in Echtzeit gewährleistet. Als technologische Basis dient die IF-MAP Spezifikation der Trusted Computing Group (TCG).

3.1 IF-MAP-Spezifikation

Die technologische Basis für das ESUKOM Projekt ist das IF-MAP (Interface for Metadata Access Point) Protokoll der TCG. Dabei handelt es sich um ein offenes, Hersteller-unabhängiges Client-Server Netzprotokoll zum Austausch von beliebigen, in XML codierten Metadaten. IF-MAP ist ein substantieller Bestandteil des Trusted Network Connect (TNC) Frameworks. Die ursprüngliche Motivation für IF-MAP war die Integration von vorhandenen, sicherheitsrelevanten Infrastrukturdiensten wie Firewalls, Virtual Private Networks und Intrusion-Detection-Systemen. Durch die Integration dieser Dienste erhält man eine ganzheitliche Sicht auf den aktuellen Status eines Netzwerkes, was Vorteile bei der Administration und der Erkennung von Bedrohungen verspricht. Die erste Version (1.0) von IF-MAP erschien im Mai 2008. Die aktuelle Version der Spezifikation (2.0 Revision 36) wurde im Juli 2010 veröffentlicht[2].

Die grundlegende Architektur von IF-MAP ist in Abb. 3 dargestellt. Die zentralen Komponenten unterteilen sich in einen MAP-Server und eine Menge von MAP-Clients. Der MAP-Server innerhalb des zu schützenden Netzwerkes 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.

Über die standardisierte IF-MAP Schnittstelle können Metadaten von diesem Server abgefragt oder neue Metadaten veröffentlicht werden. Innerhalb des MAP-Servers werden die

[1] URL: http://www.esukom.de

[2] URL: http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification

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.

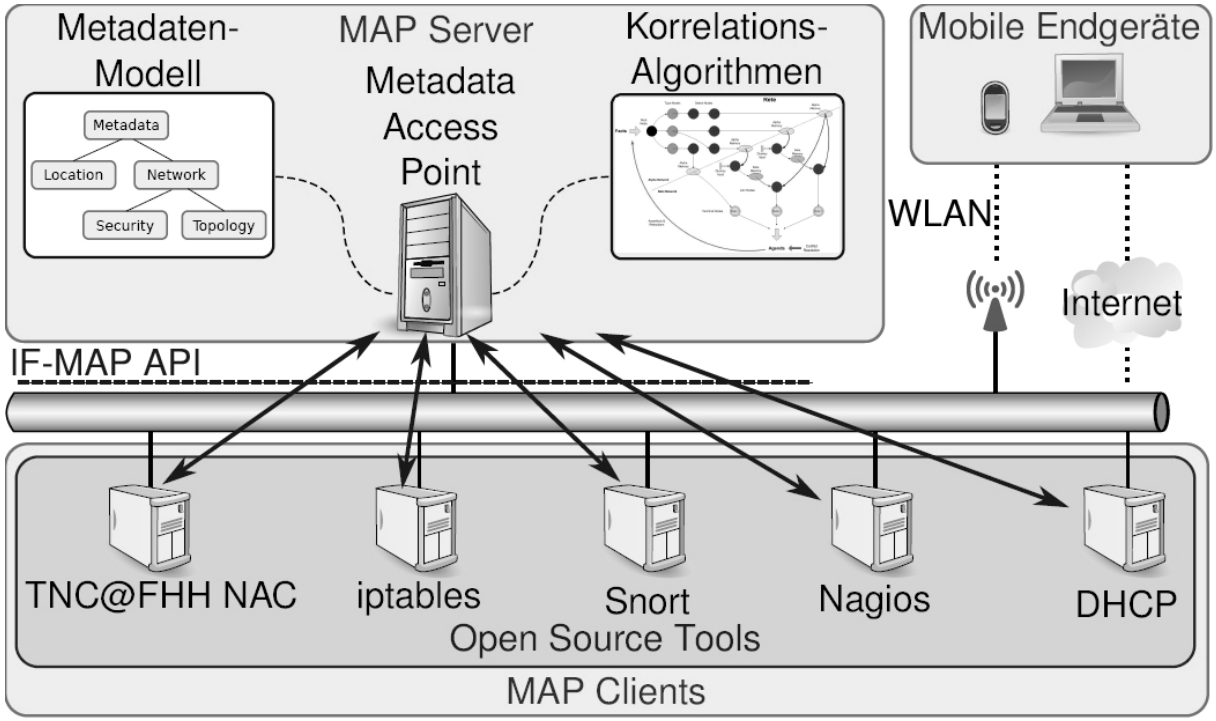

Abb. 3: IF-MAP-Architektur

Systeme, die mit dem MAP-Server kommunizieren, werden als MAP-Clients bezeichnet. Die Kommunikation basiert auf einem Publish-Search-Subscribe Modell, bei dem sowohl synchron als auch asynchron Metadaten ausgetauscht werden können:

1. Neue Metadaten werden über die Publish-Operation veröffentlicht.
2. Nach vorhandenen Metadaten kann per Search-Operation gesucht werden.
3. Über die Subscribe-Operation können sich MAP-Clients asynchron über Änderungen der im MAP-Server gespeicherten Metadaten informieren lassen. Dabei wird seitens des MAP-Clients spezifiziert, welche Art von Metadatenänderungen relevant ist. Nur solche Änderungen haben eine Benachrichtigung durch den MAP-Server zur Folge.

Technologisch basiert IF-MAP auf einer 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. In der Abbildung ist dies u.a. für die Systeme iptables, DHCP und Snort dargestellt. Auf diese Weise können ansonsten isolierte Daten (IDS Events, DHCP Lease Informationen) verknüpft werden.

Durch den Einsatz der IF-MAP-Architektur in dem geschilderten Szenario wäre es möglich, kompromittierte Endgeräte gezielt aufzuspüren und ggf. weitere Maßnahmen einzuleiten.

Dies kann beispielsweise die Sperrung oder Isolierung dieser Geräte sein. Ein wichtiger Aspekt hierbei ist, dass durch den Einsatz der IF-MAP-Architektur ein kompromittiertes Endgerät auch nach den Authentifizierungs- und Autorisierungsvorgang anhand seines Verhaltens erkannt und somit flexibel auf die jeweilige Bedrohungslage reagiert werden kann.

3.2 Mehrwert durch IF-MAP-Einsatz

Durch die zunehmende Professionalisierung und Komplexität von Schadsoftware, insbesondere in den Bereichen der Industrie- und Wirtschaftsspionage, wird es zunehmend schwerer, eventuell manipulierte Endgeräte bereits bei der Authentifizierung korrekt zu erkennen und zu isolieren, z.B. wenn die entsprechende Schadsoftware erst nach einen erfolgreichen Anmeldevorgang aktiv wird. Die Autoren solcher Schadsoftware bedienen sich dabei zunehmend ausgefeilter Mechanismen, welche eine Erkennung der Manipulation zusätzlich erschwert. Als Beispiel sei an dieser Stelle nochmal der eingangs erwähnte „Stux-Net"-Schädling zu nennen, der sich dabei unterschiedlicher Mechanismen bedient, welche zum Teil so ausgeklügelt sind, das selbst die Analyse des Schadsoftware mit einen sehr hohen Aufwand verbunden ist [HEIS10b].

Nachfolgend soll Stichpunktartig ein möglicher Ablauf dargestellt werden, in welchem ein zunächst unentdecktes, manipuliertes Endgerät aufgrund seiner Aktivitäten aufgespürt und gesperrt bzw. isoliert wird. Hierbei soll vor allem der Mehrwert aufgezeigt werden, der durch den Einsatz eine IF-MAP-Architektur entsteht.

a. Das kompromittierte Endgerät erbittet Zugang zum Unternehmens-Netzwerk. Die auf dem Gerät befindliche Schadsoftware ist dabei noch inaktiv und wird während der Authentifizierung/Autorisierung und Überprüfung der Integrität des Endgerätes (beispielswiese durch den Einsatz von TNC) nicht korrekt erkannt. Das Gerät erhält demzufolge Zugang. Die entsprechenden Verbindungsdaten (MAC/IP-Adresse des Endgerätes, Zeitpunkt des Zugriffes, Nutzerrollen und Berechtigung, etc.) werden an den MAP-Server übertragen und in den entsprechenden Meta-Daten-Graphen eingetragen.

b. Nach einem gewissen Zeitraum aktiviert sich die Schadsoftware und beginnt damit ihre Tätigkeit aufzunehmen. Einige mögliche Beispiele für solche Aktivitäten wurden bereits im vorhergehenden Abschnitt geschildert.

c. Die eingeleiteten Aktivitäten des manipulierten Endgerätes werden von einem MAP-Client (z.B. ein Intrusion-Detection-System wie Snort) bemerkt. Dieses veröffentlicht die entsprechende Meldung und Daten an den MAP-Server („Publish").

d. Der MAP-Server nimmt die entsprechenden Daten entgegen und fügt diese zum jeweiligen Metadaten-Graphen hinzu. Anschließend werden die MAP-Clients, welche 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.

e. Die benachrichtigten MAP-Clients können daraufhin weitere Maßnahmen einleiten, welche wiederum von den jeweiligen Informationen abhängig sind. Beispiele hierfür sind unter anderem die Blockierung des Datenstroms durch eine Firewall, Sperrung des Zugriffes auf das Unternehmensnetz durch einen Policy Enforcement Point (PEP), z.B. in Form eines Switches oder eines VPN-Gateways, Isolierung des Endgerätes in eine Quarantänezone etc. Hierbei müssen die entsprechenden MAP-Clients ihre Ent-

scheidung 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 wird vom Unternehmensnetz isoliert. Abschließend können auf Grundlage der gesammelten Informationen die unterbundenen Aktivitäten sowie deren Details protokolliert und entsprechende Meldungen an die verantwortlichen Systemadministratoren generiert werden.

3.3 Ableitung von Kernanforderungen für ESUKOM

Basierend auf den fachlichen Szenarien sowie den Bedrohungsaspekten wurden Kernanforderungen im ESUKOM-Projekt abgeleitet, welche die Basis für die weiteren Arbeiten bilden:

1. **Anomalie-Erkennung:** Normalverhalten und Grenzverhalten muss sich über das Sammeln möglichst viele Daten identifizieren lassen. Grenzüberschreitungen lassen sich dann durch Korrelation mit dem sonstigen Systemverhalten ins Verhältnis setzen.
2. **Smartphone Awareness:** Durch Smartphone-Awareness soll gewährleistet werden, dass Komponenten und Dienste innerhalb der IT-Infrastruktur eines Unternehmens erkennen können, ob es sich bei angebundenen Geräten um ein Smartphone handelt. Darüber hinaus soll ebenfalls ermittelt werden können, ob die angebundenen Smartphones hinsichtlich Verwendung und Softwarezustand den Vorgaben des Unternehmens genügen.
3. **Single-Sign-Off:** Darunter versteht man infrastrukturseitige Komponenten, welche die unabhängige Authentifizierung eines Nutzers gegenüber verschiedener Anwendungen und Diensten durch eine einmalige, zentrale Authentifizierung ersetzen. Dem Anwender bleibt es somit erspart, verschiedenste Daten zur Authentifizierung, wie Kombinationen aus Benutzernamen und Passwörtern oder Zertifikaten, vorzuhalten
4. **Secure Evidence:** Darunter versteht man die Erzeugung eines möglichst gerichtsfesten Beweises über einen Vorgang. Dazu ist es notwendig, den Zustand des Erzeugers des Beweises, im folgenden Evidence Generator (EG) genannt, sicher zu erfassen. Dafür kann IF-MAP als Publish-Subscribe basiertes System zur Verbreitung von Metainformationen im Netzwerk eingesetzt werden.
5. **Identity Awareness:** Der Begriff bezeichnet die Fähigkeit von Netzwerkkomponenten, ihre Funktionsweise abhängig von der Identität des anfragenden Benutzers anzupassen. Das Ziel ist die Konfiguration von Komponenten flexibler gestalten zu können. Über IF-MAP soll auch eine identitätsbasierte Konfiguration unterstützt werden.
6. **Location-based Services:** Darunter versteht man Dienste und Anwendungen, die den aktuellen Aufenthaltsort des Benutzers für die Bereitstellung und Verarbeitung von Daten nutzen. Anhand des Aufenthaltsortes kann dann auch auf den regulären Zugriff geschlossen werden (z.B. wenn ein WLAN-Zugang außerhalb des Firmennetzes genutzt wird).
7. **Erkennen von MalApp-basierten Angriffen:** Im Rahmen der Bedrohungsanalyse haben sich Malicious Application (MalApps) als Ursache für viele der beschriebenen

Bedrohungen herausgestellt. Im Rahmen des ESUKOM-Projektes sollen deshalb MalApps erkannt und so den Bedrohungen entgegen gewirkt werden können.

8. **Real-time Enforcement:** Bei dieser Anwendung handelt es sich um die automatisierte Umsetzung von reaktiven Maßnahmen, die durch den Metadata Access Point (MAP) kommuniziert werden und möglicherweise auch mit Hilfe von IF-MAP-Anwendungen ausgelöst werden können.

Diese Kernanforderungen bestehen aus einer Menge von Anwendungsmöglichkeiten, deren technologische Grundlage der Austausch von Metadaten über das IF-MAP-Protokoll ist. Diese Anwendungen können (einzeln oder kombiniert) in den dargestellten fachlichen Szenarien einen Mehrwert bringen. Zudem ermöglichen sie es, den identifizierten Bedrohungen effektiv entgegenzuwirken. Durch diese Abstraktion der ESUKOM-Anwendungen lassen 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 Beschreibung, der definierten ESUKOM-Anwendungen unterteilt sich in vier Abschnitte:

1. Als erstes wurde ein Überblick über die generelle Idee der ESUKOM-Anwendung im Projekt seitens der Partner gegeben.
2. Anschließend wurde dargestellt, welche Art von Metadaten für die Realisierung der Anwendung erforderlich ist. So konnte herausgearbeitet werden, welche der im Konsortium existierenden Sicherheitslösungen die entsprechenden Metadaten bereitstellen könnten und welche Metadaten darüber hinaus erzeugt werden müssten.
3. Weiterhin wurde exemplarisch dargestellt, wie die jeweilige ESUKOM-Anwendung in den fachlichen Szenarien eingebettet werden können. Es wurde insbesondere untersucht, auf welche Weise Metadaten gesammelt und verknüpft werden können und welche Rückschlüsse sich aus den so korrelierten Metadaten schließen lassen.
4. Abschließend wurde untersucht und skizziert, wie die dem Konsortium zur Verfügung stehenden Sicherheitslösungen in diesem Anwendungsfall Einsatz finden können und welche der Metadaten von diesen Tools erzeugt werden können.

Es soll dabei jedoch beachtet werden, dass es sich um eine repräsentative Teilmenge der möglichen Zielanwendungen von IF-MAP in ESUKOM handelt, die im Laufe eines iterativen Prozesses während der Laufzeit des Projekts erweitert werden kann. In diesem Bericht wird exemplarisch nur auf die Anomalie-Erkennung eingegangen, da sie letztendlich die Basis für die Szenarien darstellt.

3.4 Anomalie-Erkennung

Zur Anomalie-Erkennung sollen möglichst viele Informationen, die möglicherweise auch unabhängig von diesem Einsatzszenario gesammelt werden, beobachtet werden, 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-basierten Anomalie-Erkennung liegt in der Diversität der Daten (siehe Abb. 4).

Die Anomalie-Erkennung könnte auf verschiedene Metadaten angewandt werden. Dies sind einerseits die schon bekannten Network-Security Metadaten wie Access-Request, IP, MAC oder Location-Information. Jedoch wäre es hier hilfreich, die Persistierung der entsprechenden Metadaten zu gewährleisten. 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 Veröffentlichen 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. Die für die Persistierung nötigen IF-MAP-Erweiterungen sind noch zu entwickeln.

Beispielsweise könnten folgende Daten gesammelt werden:

- Login-Count eines User Account (ID) oder eines Geräts (MAC)
- Zeit des Logins im System
- Anwesenheit erfasst z. B. durch ein Arbeitszeiterfassungssystem
- Anzahl der MAC-Adressen, die mit einer User ID verbunden sind
- Anzahl messbarer Aktionen im System (z.B. Zugriffe auf Patientendatenbank)

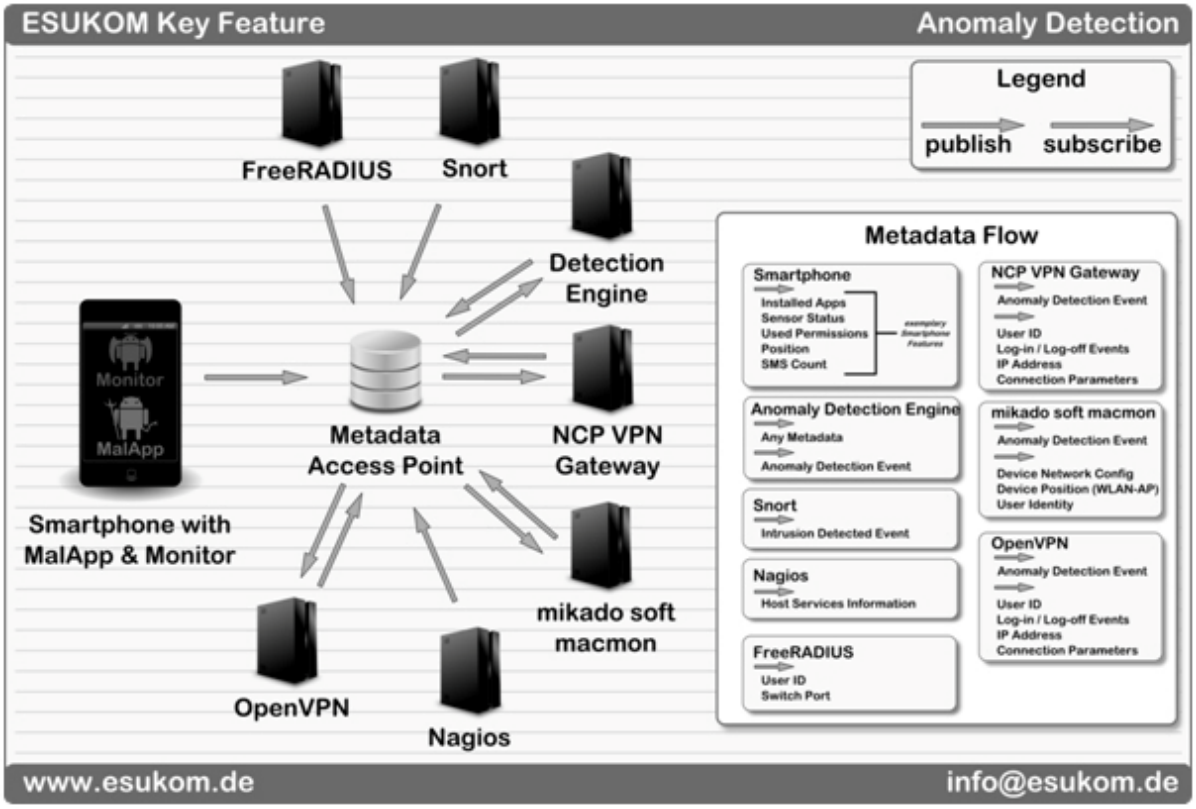

Abb. 4: Anomalie-Erkennung

Durch die Feststellung von übermäßig vielen Zugriffen auf das Netzwerk mit unterschiedlichen MAC-Adressen, aber jeweils der gleichen User-ID-Passwort-Kombination, könnte sich eine Warnung ergeben, durch die erkannt würde, dass das Passwort eines Benutzers einer Gruppe nicht-legitimierter Personen zugängig gemacht wurde. Diese könnten dann über den User-Account, mit grundsätzlich hinreichend sicheren Geräten ohne Erlaubnis auf Ressourcen im Netzwerk zugreifen.

Ein weiteres Beispiel wäre die User-ID eines Arztes, unter der a) besonders häufige Anmeldungen, b) besonders lange Arbeitszeit c) unterschiedliche MAC-Adressen der Geräte, d) ungewöhnliche Orte bei Login und e) besonders viele Zugriffe auf die Akten unterschiedlicher Patienten festgestellt werden könnten. Dies kann eine Ausnahme im Arbeitsverhalten des Arztes sein, jedoch wäre auch Missbrauch des User-Accounts möglich. Um False-Positives zu verhindern wäre hier eine Warnung mit anschließender Untersuchung angebracht, die schnell zu verifizieren wäre.

4 Fazit

Dieser Bericht beschreibt die innerhalb des ESUKOM-Projektes bisher erzielten Ergebnisse. Das 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. Als einleitende Untersuchung wurde im Projekte zunächst definiert welche Gerätehardware innerhalb des Projektes relevant ist. Da mobile Endgeräte betrachtet werden sollen, haben sich hier die Klassen der Smartphones, der mobilen Geräte in der Produktion und der Notebooks herausgestellt. Dabei wird innerhalb des Projektes besonders die Klasse der Smartphones betrachtet. Zusätzlich wurde betrachtet, welche Dienste und Infrastrukturen für diese Geräte notwendig sind. Dazu wurden sowohl Netzzugangsmöglichkeiten wie WLAN betrachtet, als auch funktionelle Komponenten wie z.B. Firewalls. Ergänzend wurde definiert, welche speziellen Anforderungen an Smartphones im Unternehmenseinsatz gestellt werden, damit sich diese problemlos in eine bestehende IT-Umgebung integrierten lassen und den Anforderungen der Unternehmen an die IT Infrastruktur genügen.

Anschließend wurden verschiedene Szenarien beschrieben, die aktuelle Anforderungen oder Anfragen aus Kundenprojekten widerspiegelten oder bereits umgesetzte Projekte, in denen die Sicherheit weiter verbessert werden sollte. Neben grundlegenden Szenarien wurden noch die Bedrohungen und Gefahren betrachtet, die beim Zugriff mit kompromittierten Endgeräten für das zentrale Firmennetzwerk entstehen können. Innerhalb dieser Szenarien wurde bereits betrachtet, welchen Mehrwert in dem Szenario durch den Einsatz von IF-MAP entstehen könnte.

Es folgte eine detaillierte Analyse welche Bedrohungen für das Firmennetzwerk oder für Smartphones aktuell vorliegen und wie diese initiiert werden könnten. Die Vielzahl der hier gefundenen Bedrohungen zeigt wie stark gefährdet Smartphones aktuell sind und dass hier viele bisher vorhandene Sicherheitsmechanismen wie Virenscanner noch fehlen, bzw. komplett neue Bedrohungen entstanden sind, denen noch nicht entgegengewirkt werden kann.

Durch die Anforderungen in den Szenarien und die aktuell vorliegenden Bedrohungen des Unternehmensnetzwerkes durch Smartphones wurden insgesamt acht Kernforderungen definiert, die die Anforderungen an das ESUKOM Projektes darstellen und durch das Projektergebnis möglichst vollständig abgedeckt werden sollen. Die Kernanforderungen betrachten

dabei eine große Bandbreite an möglichen Einsatzzwecken und spiegeln so auch die vielfältigen Möglichkeiten des IF-MAP Protokolls wider. Bedingt durch diese große Bandbreite wird das ESUKOM-Projekt wahrscheinlich nicht alle Kernanforderungen in der beschrieben Form komplett abdecken können, auch wenn es weiterhin das Ziel bleibt, alle diese so vollständig wie möglich zu erfüllen.

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), mikado soft gmbh, NCP Engineering GmbH sowie die Forschungseinrichtungen Fraunhofer SIT und FH Hannover dran beteiligt. Daher gilt der Dank den Partnern des Projektes, die durch ihre Beiträge und Arbeiten diesen Bericht erst ermöglicht haben.

Literatur

[DeDu11] K.-O. Detken, D. Dunekacke: Verhängnisvolle Isolierung – IT-Sicherheit ist mehr als die Summe aller Einzelteile. NET 05/11, NET Verlagsservice GmbH, Woltersdorf 2011

[FSEC10] F-Secure Labs: Fragen und Antworten zu Stuxnet. Info-Point-Security GmbH, 10/2010, München 2010

[Goeb10] M. Göbel: Deutsche Datenschützer warnen vor iPhone Sicherheitslücken. Macnews.de, ECONA Internet AG, 08/2010, Berlin 2008

[HEIS10a] Heise Online: Erneut iPhone Jailbreak via Safari (Update). 08/2010, Heise-Online-Verlag, Hannover 2010

[HEIS10b] Heise Online: 27C3 – Hacker analysieren Stuxnet-Maschinencode, 12/2010, Heise-Online-Verlag, Hannover 2010

[Oste08] A. Osterhues: Bluetooth Sicherheit. ESCRYPT – Embedded Security, 09/2008

[Schm09] P. Schmitz: Datendiebstahl ist ein lukratives Geschäft – fünf Tipps gegen Datendiebstahl und Datenhandel. 14.08.09, SearchSecurity.de, Vogel IT-Medien GmbH, Augsburg 2009

[Schw10] B. Schwarz: Große Android Sicherheitslücken offengelegt, 11/2010, PCMasters, www.pcmasters.de

[Seri10] N. Seriot: iPhone Privacy, Black Hat DC, Virginia/USA 2010

[Teuf10] P. Teufel: Sicherheitsanalyse iPhone. 04/2010, Zentrum für sichere Informationstechnologie – Österreich, Version 1.0.2, Wien 2010

[Weig10] M. Weigert: Android Quantität vor Qualität?, 07/2010, netzwertig.com, Blogwerk AG, Zürich 2010