h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Hochschule Darmstadt

- Fachbereich Informatik -

SIEM für mobile Endgeräte

Abschlussarbeit zur Erlangung des akademischen Grades

Master of Science (M.Sc.)

vorgelegt von Patrick Burkard

Referent:	Prof. Dr. Harald Baier
Korreferent:	Prof. Dr. Alois Schütte

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig erstellt und keine anderen als die angegebenen Hilfsmittel benutzt habe. Soweit ich auf fremde Materialien, Texte oder Gedankengänge zurückgegriffen habe, enthalten meine Ausführungen vollständige und eindeutige Verweise auf die Urheber und Quellen. Alle weiteren Inhalte der vorgelegten Arbeit stammen von mir im urheberrechtlichen Sinn, soweit keine Verweise und Zitate erfolgen. Mir ist bekannt, dass ein Täuschungsversuch vorliegt, wenn die vorstehende Erklärung sich als unrichtig erweist.

Babenhausen den 22. August 2013

Patrick Burkard

Zusammenfassung

Die Art der Geräte, die zur Datenverarbeitung in Unternehmen verwendet werden, hat sich in den letzten Jahren verändert. Von klassischen Arbeitsplatzsystemen entwickelte sich der Trend hin zum mobilen Arbeiten. Beginnend mit dem Einsatz von Laptops, bis heute zum Einsatz von Smartphones und Tablets. Die Risiken, die sich damit für die IT-Systeme eines Unternehmens ergeben, haben sich durch diesen Trend verändert.

Im Rahmen dieser Arbeit wurden diese Risiken analysiert und ein plattformunabhängiges Konzept zur Behandlung dieser Risiken mithilfe von Security Information und Event Management Systemen, kurz SIEM-Systemen, entwickelt. Das Konzept berücksichtigt wichtige Sicherheitsfragen, enthält Hinweise zur Speicheroptimierung bei der Erhebung von Log-Daten auf mobilen Endgeräten, sowie Optimierungsvorschläge für die Übertragung der Daten an ein SIEM-System.

Zur Überprüfung der Realisierbarkeit dieses Konzeptes wurden, am Beispiel des Betriebssystems Android, einige Versuche und Analysen durchgeführt. Diese zeigten das Potenzial der im Konzept beschriebenen Methoden. Es konnte festgestellt werden, dass sich Android für eine SIEM-Integration eignet, da bereits mit einfachen Mitteln den bestehenden Risiken begegnet werden konnte.

Abstract

The kind of devices, that are used in the information technology of enterprises, has changed in the last years. From classical desktop systems the trend is developing to mobile working. Starting with the usage of Laptops, and today the use of smartphones and tabets. The risks for IT-Systems that enterprises experience have changed through this trend.

Within the following document the risks will be analyzed and a platform independant concept to deal with these risks, using a Security Information an Event Managament System, in short SIEM-System, will be developed. Questions about security will be considered within the concept, details to optimize the storage while collecting Log-Data on the device and proposals to optimize the data transfer to a SIEM-System will be given.

To proof the possibility to realize the concept some experiments, on the basis of the Android operating system, will be realised and discussed. Those experiments will show the capability of the methods that are discussed in the concept. It was ascertained that Android is applicable for an integration into a SIEM-System, because it was possible to deal with the existing risks by only using simple instruments.

Inhaltsverzeichnis

Erklärung ii

Zusammenfassung iii

Abstract iv

Abbildungsverzeichnis viii

Tabellenverzeichnis ix

1 Einleitung 1

1.1 Aktuelle Situation . . . 1
1.2 Fragestellungen und Ziele . . . 3
1.3 Ergebnisse . . . 4

2 Grundlagen 5

2.1 Mobile Endgeräte . . . 5
2.2 Security Information and Event Management . . . 6
2.2.1 Log Management . . . 7
2.2.2 Einhaltung von IT-Richtlinien . . . 7
2.2.3 Ereigniskorrelation . . . 8
2.2.4 Aktive Reaktionen . . . 9
2.2.5 Endpunktabsicherung . . . 9
2.3 Mobile Device Management . . . 10
2.3.1 Device Management . . . 10
2.3.2 Security Management . . . 11
2.3.3 Application Management . . . 11
2.4 Analyse der Risiken . . . 12
2.4.1 Datenschwund durch Verlust oder Diebstahl . . . 13
2.4.2 Unsachgemäßes Stilllegen . . . 13
2.4.3 Ungewollte Datenpreisgabe . . . 13
2.4.4 Phishing . . . 14
2.4.5 Spyware . . . 14
2.4.6 Netzwerk Spoofing Angriffe . . . 15
2.4.7 Überwachung . . . 15
2.4.8 Dialler Schadsoftware . . . 15

2.4.9 Finanzielle Schadsoftware . . . 15
2.4.10 Netzwerk Überlastung . . . 15

3 SIEM-Konzept für mobile Endgeräte 16
3.1 Herausforderungen für die Integration mobiler Endgeräte in ein SIEM-System . . . 18
3.1.1 Technische Herausforderungen . . . 18
3.1.2 Datenschutzaspekte . . . 20
3.2 Datenübertragung . . . 20
3.2.1 Protokolle . . . 21
3.2.2 Sicherheit . . . 22
3.2.3 Übertragungszeitpunkt . . . 22
3.2.4 Datenreduktion . . . 24
3.3 Datenspeicherung . . . 26
3.3.1 Zugriffsschutz . . . 27
3.4 Relevante Daten und Risikobehandlung . . . 27
3.4.1 Datenschwund durch Verlust oder Diebstahl . . . 27
3.4.2 Unsachgemäßes Stilllegen . . . 29
3.4.3 Ungewollte Datenpreisgabe . . . 30
3.4.4 Phishing . . . 31
3.4.5 Spyware . . . 32
3.4.6 Netzwerk Spoofing Angriffe . . . 34
3.4.7 Überwachung . . . 35
3.4.8 Dialler Schadsoftware . . . 37
3.4.9 Finanzielle Schadsoftware . . . 37
3.4.10 Netzwerküberlastung . . . 38
3.4.11 Zusammenfassung . . . 39

4 Praktische Prüfung des Konzeptes 41
4.1 Aufbau des Testsystems . . . 41
4.1.1 Logging auf Androidgeräten . . . 45
4.2 Erläuterung der Datenbasis . . . 47
4.2.1 Prioritäten der Log-Daten . . . 48
4.2.2 Zählen häufig auftretender Zeilen . . . 49
4.2.3 Einige einfache Operationen . . . 51
4.3 Anwendung von Korrelationsszenarien . . . 53
4.3.1 Erkennen eines Diallers . . . 54

4.3.2 Erkennen von Überwachung 56

5 Fazit **59**

6 Ausblick **60**

Literatur **61**

Abbildungsverzeichnis

1 SIEM Umfeld . . . 17
2 Prioritätsbasiertes Message-Scheduling . . . 24
3 Samsung Galaxy Nexus Systemdaten . . . 42
4 NXLog Konfiguration . . . 44
5 Rechte NXLog . . . 45
6 Splunk Datenquelle . . . 45
7 Android Logs mit LogCat . . . 46
8 Android Log Puffer . . . 47
9 Android Logs mit dd . . . 47
10 Verteilung der Log-Prioritäten . . . 48
11 Verteilung der Log-Zeilen auf die Prozesse . . . 49
12 Ersparnis je Zeitraum . . . 51
13 Senden einer SMS . . . 51
14 Anrufablauf im Log . . . 52
15 Erstellen eines Fotos . . . 53
16 Gesendete SMS je Host . . . 55
17 Erstellen eines Alarms für ungewöhnliche SMS-Häufung . . . 55
18 Beispiel Dialler Alarmmeldung . . . 56
19 Ereignisse Dialler Alarmmeldung . . . 56
20 Kamera Aktivierung während Inaktivität . . . 58
21 Alarmmeldung bei Kameraaktivierung . . . 58

Tabellenverzeichnis

1 Risiken für mobile Endgeräte von Angestellten (nach [HD10]) 12
2 Neue Risikobewertung: Datenschwund durch Verlust oder Diebstahl 28
3 Neue Risikobewertung: Unsachgemäßes Stilllegen 29
4 Neue Risikobewertung: Ungewollte Datenpreisgabe 31
5 Neue Risikobewertung: Phishing 32
6 Neue Risikobewertung: Spyware 33
7 Neue Risikobewertung: Netzwerk Spoofing 35
8 Neue Risikobewertung: Überwachung 36
9 Neue Risikobewertung: Dialler Schadsoftware 37
10 Neue Risikobewertung: Finanzielle Schadsoftware 38
11 Neue Risikobewertung: Netzwerk Überlastung 39
12 Neueinschätzung der Risiken 40
13 NXLog und Android Log-Prioritäten 48
14 Verhältnis Zählzeitraum zu Log-Zeilenanzahl 50

1 Einleitung

Die Verwendung von Smartphones, Tablets und anderen mobilen Geräten hat sich in den letzten Jahren verändert. Die Geräte sind leistungsfähiger und die Möglichkeiten für ihren Einsatz umfangreicher geworden. Für den Anwender birgt dies viele praktische Anwendungsfälle und für die Verantwortlichen in einem Unternehmen neue Herausforderungen mit Blick auf die Unternehmenssicherheit.

Eine Schlüsselrolle nimmt dabei die starke Verbreitung von Anwendungen für mobile Endgeräte - sogenannte Apps - ein. Diese erlauben dem Benutzer ihr Gerät voll auf die eigenen Bedürfnisse anzupassen. Aus der Perspektive eines Sicherheitsverantwortlichen entstehen dadurch neue Wege zur Verbreitung von Schadsoftware. In [Sch12] wird mit Blick auf Apps gar vom Besten, durch Menschen entwickelten Verteilungssystem für Malware gesprochen.

Durch den Einsatz von Smartphones und Tablets in Unternehmen, sowie deren mobilen Einsatz auch außerhalb der Unternehmensgrenzen, entstehen so eine ganze Reihe neuer Risiken für die Sicherheit der IT-Infrastruktur und neue Gefährdungspotenziale für sensible Daten eines Unternehmens.

Eine etablierte Technik zur Reaktion auf Risiken für IT-Systeme in einem Unternehmen sind sogenannte SIEM-Systeme. SIEM steht als Abkürzung für Security Information und Event Management. Eine detaillierte Erklärung befindet sich in Abschnitt 2.2. Für Arbeitsplatzrechner oder Serversysteme ist die Verwendung von SIEM bereits etabliert und wird in der einschlägigen Literatur bereits ausführlich diskutiert. Im Bereich mobiler Endgeräte ist diese Form des Schutzes bislang nicht verbreitet.

1.1 Aktuelle Situation

Die European Network and Information Security Agency (ENISA) veröffentlichte im Dezember 2010 einen Bericht mit dem Titel: “Smartphones: Information security risks, opportunities and recommendations for users”. “Der Report analysiert 10 Risiken der Verwendung von Smartphones und 7 Möglichkeiten Sicherheit zu gewährleisten. Es werden 20 Empfehlungen gegeben, wie den Risiken begegnet werden kann.” (Übersetzt aus [HD10])

Nur kurze Zeit vorher, im November 2010, erschien in der Zeitung Technology Review ein Artikel mit dem Titel “Smart oder sicher?”. Dort heißt es im Bezug auf Smartphones: “Mit solchen Geräten können sie im Web surfen, E-Mails lesen, Anwendungen für

die verschiedensten Aufgaben installieren – und problemlos auf das interne Firmennetz zugreifen. Mit den Möglichkeiten steigt auch das Missbrauchspotenzial." ([Sch10])

In [Sch10] wird darüber hinaus eine der ersten Datenpannen erwähnt, die in der Historie der Smartphones im Jahr 2004 auftrat. "Ein 17-jähriger Computerfreak brach in (Paris [Anm. des Autors]) Hiltons Account beim Handy-Dienst Sidekick ein" ([Sch10]). Bis heute hat sich das Angebot an Smartphones massiv weiterentwickelt.

In [HD10] ist von weltweit 80 Millionen verkauften Smartphones allein im dritten Quartal 2010 die Rede. Die Technik hat sich inzwischen ebenfalls weiterentwickelt. Dies zeigt sich beispielsweise mit Blick auf die Rechenleistung. Insbesondere hat die Anzahl verfügbarer Anwendungen für Smartphones stark zugenommen. Zum Beispiel enthält Googles Play Store nach Aussage des Statistikportals Statista (`http://de.statista.com/statistik/daten/studie/74368/umfrage/anzahl-der-verfuegbaren-apps-im-google-play-store/`) im April 2013 insgesamt 850000 Anwendungen. Zwei Jahre zuvor im April 2011 waren es lediglich 200000.

Die Risiken, die in [HD10] von der ENISA gezeigt werden, stellen jedoch weiterhin eine Bedrohung dar. Wird heute über die Absicherung der mobilen Endgeräte eines Unternehmens gesprochen, werden häufig sogenannte Mobile Device Management (MDM) Lösungen in den Fokus gerückt. Diese werden inzwischen von vielen verschiedenen Unternehmen angeboten. Das New Yorker Unternehmen Tekserve veröffentlichte dazu 2012 eine Marktstudie, die von Forrester Research Inc. durchgeführt wurde. (siehe [GK12]).

Nach der Studie bieten alle 17 getesteten Produkte Monitoringfunktionen und das Auslösen von Alarmen an. Weitere Funktionsmerkmale zur Gewährleistung mobiler Sicherheit sind in unterschiedlichen Ausprägungen in den getesteten Produkten integriert. Es entsteht hierbei der Eindruck, dass die Produkte aus [GK12] im Bezug auf Monitoringfunktionen gut ausgestattet sind. Als Definition für die Monitoringfähigkeiten steht dort: "Jedes Unternehmen hat ein einzigartiges Systemumfeld und eigene Anforderungen für die Überwachung der Compliance und Gerätenutzung. Die Fähigkeit anpassbare Alarmmeldungen zu generieren ermöglicht den Verantwortlichen den direkten Zugriff auf benötigte Informationen" (Übersetzt aus [GK12]).

Einen Leitfaden, welche Ereignisse bei einem Smartphone besondere Relevanz besitzen, sucht man jedoch vergeblich. Welche der sicherheitsrelevanten Informationen über ein MDM-System zugänglich sind und welche nur direkt auf dem Telefon erfasst werden können ist ebenfalls eine offene Frage. Die in [GK12] getesteten Produkte bieten zwar alle Monitoring und Alarmfunktionen, die Qualität und der Umfang dieser Funktionen geht aus der Studie jedoch nicht hervor.

Bereits 2008 wurde in [SPL+08] die Möglichkeit analysiert durch Überwachung von bestimmten Kernfunktionen bei Mobiltelefonen auf Basis des Betriebssystems Symbian Anomalien zu identifizieren. Dies gelang durch den Einsatz lernender Algorithmen, wobei Merkmalsvektoren an einen Server versendet wurden und dort die Anomaliedetektion durchgeführt wurde.

Es steht damit ausser Frage, dass es möglich ist illegitime Aktivitäten auf einem Smartphone zu erkennen. Die Verwendung einer spezialisierten Software zu Generierung der Merkmalsvektoren sowie der Einsatz lernfähiger Algorithmen für die Anomaliedetektion erfordert jedoch viel Expertenwissen und systemnahe Implementierungen auf den Endgeräten. SIEM-Systeme dagegen sind bereits in vielen Unternehmen im Einsatz und Möglichkeiten Log-Daten[1] von Smartphones zu diesen zu transportieren existieren ebenfalls.

Der Frage, wie große Mengen Log-Daten zu verwalten und auszuwerten sind, wird in der einschlägigen Literatur vielfach nachgegangen zum Beispiel in [MHH+10], [FN09] und [CS12]. Viele der Informationen aus diesen Werken lassen sich auch auf mobile Endgeräte übertragen. Besondere Aspekte, die durch den Einsatz mobiler Endgeräte relevant werden, sind jedoch noch nicht mit dieser Intensität untersucht worden.

1.2 Fragestellungen und Ziele

Aufgrund der neuartigen Risiken, die sich für Unternehmen durch den Einsatz mobiler Endgeräte ergeben, stellt sich die Frage ob es möglich ist bereits etablierte Schutzmechanismen zur Risikohandhabung auf diese neue Klasse von Endgeräten zu übertragen. Die Frage: "Ist es sinnvoll mobile Endgeräte in ein SIEM-System einzubinden?" wird daher als Leitfrage dieser Thesis betrachtet.

Damit ergeben sich die folgenden Eckpunkte:

- Wie kann eine sinnvolle Log-Datenverwaltung auf einem mobilen Endgerät umgesetzt werden?
- Lassen sich die größten Risiken, die bei der Verwendung mobiler Endgeräte entstehen, durch ein SIEM-System minimieren und wie ist das möglich?
- Ist eine SIEM-Integration praktisch umsetzbar?

Diesen Fragen soll in den folgenden Kapiteln nachgegangen werden. Die praktische Umsetzbarkeit soll am Beispiel des Betriebssystems Android überprüft werden.

[1] Log-Daten oder kurz Logs bezeichnet die Gesamtheit der System- und Applikationsereignisse (vgl. [MHH+10])

1.3 Ergebnisse

Das Ergebnis dieser Arbeit ist ein Konzept zur Log-Datenverwaltung und Risikominimierung bei mobilen Endgeräten. Die Theorien, die im Rahmen des Konzeptes zur Speicherplatzoptimierung und zur Minimierung des Bandbreitenbedarfs bei der Log-Datenverwaltung aufgestellt wurden, konnten in einem praktischen Versuch mit dem Betriebssystem Android auf ihre Wirksamkeit überprüft werden.

Als Basis für die Risikoanalyse diente eine Veröffentlichung der ENISA, die die zehn häufigsten Risiken beim Einsatz mobiler Endgeräte beschreibt und mit Blick auf ihre Eintrittswahrscheinlichkeit und Auswirkungen quantifiziert. Diese Risiken wurden analysiert und unter der Voraussetzung der konsequenten Umsetzung von SIEM-Techniken neu bewertet.

Abschließend wurde, am Beispiel eines Android-Smartphones und der SIEM-Software Splunk, ein mobiles Endgerät in ein SIEM-System integriert. Die Log-Daten und das Logging-System von Android wurden mit Blick auf die Umsetzbarkeit des Konzeptes analysiert. Auch ohne den Einsatz einer neuen Software auf dem mobilen Endgerät war es möglich Beispiele für die Risikoerkennung durch ein SIEM-System abzubilden.

Durch eine Übertragung der Log-Daten an Splunk war es möglich, beispielhaft Indizien für den Befall mit einer Dialler Schadsoftware und für eine Überwachung durch das Endgerät zu erheben und entsprechende Warnmeldungen zu generieren.

2 Grundlagen

Im folgenden Abschnitt werden die nötigen Grundlagen zum Verständnis der Arbeit vorgestellt. Dies umfasst eine abstrakte Definition des Begriffs mobile Endgeräte. Eine Erklärung des Funktionsumfangs moderner SIEM- und MDM-Systeme. Weiterhin wird eine aktuelle Analyse der Risiken für mobile Endgeräte vorgestellt.

2.1 Mobile Endgeräte

Ein mobiles Gerät ist in [Fri10] definiert als: "Ein typischerweise elektronisches Gerät, dass große Mengen Informationen speichern kann und ohne übermäßigen Aufwand oder Kosten von einem Ort zum Anderen transportiert werden kann" (übersetzt aus [Fri10]).

Während die Definition eines mobilen Gerätes in [Fri10] sehr weit gefasst ist und beispielsweise auch USB-Sticks umfasst soll in dieser Arbeit der Begriff enger gefasst und von mobilen Endgeräten gesprochen werden. Ein mobiles Endgerät im Sinne dieser Arbeit besitzt zusätzlich zu den Eigenschaften die in [Fri10] definiert wurden noch vier weitere Eigenschaften.

1. Ein mobiles Endgerät besitzt die Fähigkeit Daten aktiv zu verarbeiten. Diese Eigenschaft schließt passive Geräte wie USB-Sticks aus der Betrachtung dieser Arbeit aus.

2. Ein mobiles Endgerät kann ohne ständige Stromversorgung betrieben werden. Diese Einschränkung bedeutet nicht, dass ein mobiles Endgerät ohne Energiequelle betrieben werden kann. Der Betrieb eines mobilen Endgerätes ist jedoch unabhängig von einem dauerhaften Anschluss an das Stromnetz möglich. Andernfalls würden auch kleinere stationäre Geräte (z.B. Desktop PCs) unter die Ausgangsdefinition aus [Fri10] fallen.

3. Ein mobiles Endgerät hat die Möglichkeit, Daten über drahtlose Kommunikationswege zu empfangen und zu versenden. Dies grenzt die Geräteauswahl weiter ein und schließt Geräte aus, die Daten vorhalten und verarbeiten können, jedoch keine Möglichkeit zur aktiven Kommunikation besitzen. Solche Geräte sind beispielsweise Navigationsgeräte. Es werden Daten vorgehalten (Kartenmaterial), Daten verarbeitet (Berechnung von Routen) und sogar empfangen (Positionsdaten per GPS). Ein einfaches Navigationsgerät ist jedoch nicht in der Lage die Daten drahtlos an andere Geräte zu übermitteln.

Bis zu diesem Punkt ist die Definition immernoch weit gefasst, denn nach ihr würde ein Navigationsgerät mit integrierter Bluetooth-Freisprecheinrichtung und Adressbuchsynchronisation weiterhin als mobiles Endgerät gewertet werden. Dies genügt für viele Aspekte der Diskussion über Sicherheit von mobilen Endgeräten bereits, da ein Navigationsgerät mit gespeicherten Firmenkontakten ebenso Sicherheitsrelevant sein kann wie ein Mobiltelefon (sofern sich in dessen Speicher neben den Kontakten keine weiteren mobilen Daten befinden).

Dennoch verfehlt die Definition, bis zu diesem Punkt, den Kern der aktuellen Verwendung von mobilen Endgeräten. So schreibt das BSI in einer Eischätzung über Sicherheitsgefährdungen und Schutzmaßnahmen mobiler Endgeräte: "Jedes mobile Endgerät stellt heute einen leistungsfähigen Computer dar, dessen Struktur grundsätzlich dem eines herkömmlichen Arbeitsplatzrechners entspricht" ([BSI06]).

Eine große Gemeinsamkeit ist, dass sowohl beim klassischen Arbeitsplatzrechner, als auch bei mobilen Endgeräten, Funktionsumfang und Einsatzzweck durch den Anwender bestimmt werden. Daraus ergibt sich der dritte wichtige Punkt der Definition mobiler Endgeräte.

4. Die Fähigkeiten eines mobilen Endgerätes können durch einen Benutzer, ohne technische Expertise, mit Hilfe von Software verändert werden. Dieser letzte Faktor schließt eine ganze Reihe weiterer Geräte von der Betrachtung aus. Zum Beispiel das bereits beschriebene Navigationsgerät oder einfache Mobiltelefone.

Im Wesentlichen trifft diese Definition heute auf Smartphones, Tablets und tragbare Computer zu. Der Fokus dieser Arbeit liegt dabei auf dem Einsatz von Smartphones, da die Integration von klassischen PC-Systemen in ein SIEM-System bereits hinreichend behandelt wurden. Die Grenzen zwischen tragbaren Computern und Smartphones verschwimmen jedoch immer weiter, weshalb alle unter diese Definition fallenden Geräte von den gewonnenen Erkenntnissen profitieren können.

2.2 Security Information and Event Management

Ein funktionierendes Security Information and Event Management (SIEM) umfasst laut [MHH+10] fünf grundlegende Aufgaben. Zur Erfüllung dieser Aufgaben werden in einem SIEM-System Daten gesammelt, korreliert und für spätere Analysen bereitgestellt.

Typische Datenquellen für ein SIEM-System nach [MHH+10] sind: Syslog, Alerts (z.B. aus SNMP-Traps), Network Flow Data und Schwachstellen Prüfungen.

Die Aufgaben eines SIEM-Systems sind nach [MHH+10]: Log Management, Einhaltung von IT-Richtlinien, Ereigniskorrelation, Aktive Reaktionen und Endpunkt Absicherung. Ein SIEM-System ist dabei nicht als eine einzelne Software zu verstehen, die nach einmaliger Installation diese Aufgaben erfüllt. "Ein SIEM-System ist eine komplexe Sammlung von Technologien um eine übersichtliche Ansicht über ein IT-System als ganzes zur Verfügung zu stellen, die für Analysten und Administratoren gleichermaßen Vorteile bietet" (Übersetzt aus [MHH+10]).

In den folgenden Unterabschnitten sind die fünf Aufgaben eines SIEM-Systems genauer definiert.

2.2.1 Log Management

Der Begriff "Log Management" verleitet zu der Annahme, dass es sich dabei lediglich um eine Datensammlung handelt. Die Definition ist jedoch etwas weiter gefasst: "Log Management in einem SIEM-System beginnt mit der Konfiguration der Systeme, ihre relevanten System- und Applikationsereignisse (Logs) an eine zentrale Datenbank zu senden, die vom SIEM-System verwaltet wird. Dabei wird mit den kritischen Systemen begonnen. Generell gilt, je mehr Systeme diese Daten liefern umso akkurater die Sicht auf das ganze System." (Übersetzt aus [MHH+10]).

Dieser Definition folgend gehört eine der wichtigsten Fragen der Planung eines SIEM-Systems in den Bereich Log Management. Die Frage, welche Logs am Wichtigsten sind und welche Logs Berücksichtigung im SIEM-System finden sollen.

Ein gängiges Vorgehen, dass in [CS12] beschrieben wird, beantwortet diese Frage mit der Aussagen, dass erst alle Log-Daten gespeichert werden sollten. Diese Aussage ist mit der Tatsache begründet, dass es nicht möglich ist alle Fälle in denen die Logs möglicherweise gebraucht werden vorher zu sehen. Daher sollten alle Log-Daten erfasst und erst anschließend zur Auswertung gefiltert werden. Werden die Daten vor der Speicherung bereits gefiltert können Vorfälle möglicherweise nicht nachträglich aufgearbeitet werden. (vgl. [CS12]).

2.2.2 Einhaltung von IT-Richtlinien

"Nach der Erfassung der Logs können diese Anhand von Regeln auf die Einhaltung von Richtlinen überwacht werden. Zum Beispiel die Aktualität von Virenscannern oder die rechtzeitige Installation von Patches." (Übersetzt aus [MHH+10])

Dabei kommt es nicht darauf an, dass die Logs mit diesen Informationen auch von dem jeweils betroffenen System stammen. Lediglich die Zuordnung zu einem System muss korrekt sein.

Zum Beispiel werden die Virenscanner in Unternehmen in der Regel über ein zentrales Managementsystem verwaltet. Für ein SIEM-System ist es dabei unerheblich ob die Information, dass ein Virenscanner mit aktuellen Signaturen arbeitet, von einem zentralen Managementsystem oder von dem Virenscanner des Systems selbst kommt.

Es ist auch möglich, dass solche periodisch generierbaren Informationen wie die Systemaktualität nicht in Form von Logs an ein SIEM gesendet werden. Wie zu Beginn dieses Abschnitts erwähnt, ist ein SIEM-System eine komplexe Sammlung von Technologien, sodass es zum Beispiel möglich ist solche Informationen bei Bedarf aus einer Datenbank abzufragen.

2.2.3 Ereigniskorrelation

"Mit der Ereigniskorrelation kommt ein höherer Grad der Intelligenz in das System. Es kommt dann nicht mehr darauf an, auf ein einzelnes Ereignis zu reagieren. Bei der Korrelation lernt das System mehrere Bedingungen zu berücksichtigen, bevor ein Alarm ausgelöst wird." (Übersetzt aus [MHH+10])

Ein einfaches Beispiel für diese Art des Vorgehens ist die Verarbeitung fehlgeschlagener Anmeldeversuche an einem System.

Einzelne fehlerhafte Anmeldeversuche sind völlig normal. Wenn ein SIEM-System bei jedem fehlerhaften Anmeldeversuch einen Alarm generiert, wird dies zu einer großen Zahl Meldungen führen, die lediglich dadurch zustande kommen, dass ein Mitarbeiter bei der Eingabe seines Passworts einen Fehler gemacht hat.

Viele fehlerhafte Anmeldeversuche innerhalb kurzer Zeit hingegen sind ein Indiz für den Versuch, ein Passwort mit einer Software zu erraten (sog. Brute Force).

Finden viele fehlerhafte Anmeldeversuche in kurzer Zeit statt und steht an deren Ende eine einzelne erfolgreiche Anmeldung ist es möglich, dass das System kompromittiert und das Passwort durch einen Angreifer erraten wurde. Dieser letzte Fall ist ein guter Grund für eine Alarmmeldung und eine genauere Untersuchung des Systems.

Der Sicherheits- und Monitoringexperte Markus Ranum schreibt dazu: "Die Anzahl, wie oft etwas uninteressantes passiert, ist etwas interessantes" (Übersetzt aus [Ran05]).

2.2.4 Aktive Reaktionen

Nachdem die Systeme ihre Log-Daten an das SIEM-System liefern, Filter definiert sind und Regeln für die Ereigniskorrelation erstellt wurden, stellt sich die Frage ob das SIEM-System aktiv auf bestimmte Korrelationsereignisse reagieren sollte. Dies kann den Analysten und den IT-Verantwortlichen viel Arbeit abnehmen (vgl. [MHH+10]).

Übertragen auf das Beispiel mit den fehlgeschlagenen Anmeldungen ist ein Szenario denkbar, in dem lediglich für den dritten Fall (viele fehlgeschlagene Anmeldungen gefolgt von einer erfolgreichen) eine Alarmmeldung erzeugt wird. Auf den zweiten Fall (viele fehlgeschlagene Anmeldungen) könnte das SIEM durch das Setzen einer Firewallregel reagieren und die Verbindung des potenziellen Angreifers unterbrechen.

Dass ein solches Vorgehen möglich ist zeigt die Software Fail2Ban. Wie beschrieben wertet Fail2Ban die Log-Daten eines Systems aus und schaltet beim Erkennen von schädlichen Aktivitäten (z.B. sehr viele Anmeldeversuche) temporär entsprechende Firewallregeln, die einen weiteren Angriff verhindern. (siehe [F2B11])

Ein solches Vorgehen kann von einem SIEM-System als aktive Reaktion auf bestimmte Angriffe adaptiert werden. Sind die Regeln für aktive Reaktionen fehlerhaft konfiguriert kann dies jedoch zu Störungen im Betriebsablauf führen. Richtig geplant werden sie zu einem mächtigen Werkzeug bei der Absicherung einer Unternehmensinfrastruktur.

2.2.5 Endpunktabsicherung

"Die Meisten SIEM-Systeme können die Sicherheit der Endpunkte feststellen um den Sicherheitszustand des Gesamtsystems zentral zu überwachen." (Übersetzt aus [MHH+10])

Da mobile Endgeräte aufgrund ihrer zunehmenden Anwendungsmöglichkeiten immer enger in die IT-Infrastruktur von Unternehmen eingebunden werden, können sie inzwischen ebenfalls als Endpunkte betrachtet werden. Laut [MHH+10] gehören zum Beispiel die Patchlevel der installierten Anwendungen und die Aktualität der Virensignaturen zu typischen Schlüsselwerten für die Endpunktabsicherung.

Diese Parameter können gut aus zentralen Verwaltungsschnittstellen der verwendeten Antivirussoftware oder einem Mobile Device Management System gewonnen werden. Andere Informationen, die zum Beispiel als Indizien für eine gezielte Überwachung des Nutzers durch ein mobiles Endgerät verwendet werden können, lassen sich ohne Daten von den Geräten selbst nur schwer erheben.

2.3 Mobile Device Management

Das Mobile Device Management oder kurz MDM bezeichnet eine Klasse von Management Systemen, die zur zentralen Verwaltung einer großen Menge mobiler Endgeräte im Unternehmen eingesetzt werden kann. Durch die wachsende Anzahl mobiler Endgeräte in den Unternehmen, wird die Verwendung von MDM-Lösungen immer wichtiger. Einer Studie des Marktforschungsunternehmes Forrester Research folgend, gliedert sich die Funktionalität einer guten MDM-Lösung in vier Untergruppen (siehe [GK12]).

Da die vierte Gruppe keine Fragen des Funktionsumfangs behandelt sondern Kriterien, wie die unterstützten Plattformen und die Verfügbarkeit, ist diese im Rahmen dieser Arbeit nicht relevant und wird daher nicht weiter behandelt. Die drei verbleibenden Kategorien, sollen in den folgenden Abschnitten definiert werden.

- Kernfunktionen: Mobile Device Management
- Sicherheitsfunktionen: Mobile Security Management
- Anwendungskontrolle: Mobile Application Management

2.3.1 Device Management

Die Kernfunktionen des Mobile Device Management sind laut [GK12]:

- Konfiguration des Geräts, unabhängig von dessen Aufenthaltsort (Over-the-Air)
- Geplante oder ereignisbasierte Aktionen zur Fehlerbehandlung und Nutzerunterstützung
- Echtzeitinformationen über die Konfiguration (z.B. installierte Anwendungen, Sicherheitseinstellungen)
- Fernwartungsfunktionen
- Serviceportal für die Anwender (z.B. zur Erstellung von Backups)
- Monitoring und Alarmierungsfunktionen
- Vorlagen für die Erstellung von Berichten

Diese Informationen bilden die Grundlage der Geräteverwaltung und der aktiven Gerätenutzung in einem Unternehmen. Durch diese Funktionen sind die Verantwortlichen in der Lage die Geräte zentral zu konfigurieren und Wartungsaufgaben durchzuführen. Ebenso bilden die Daten die Grundlage für eine Einbettung in ein SIEM-System. Fernwartungs und Konfigurationsfähigkeiten können darüber hinaus die Grundlage für die Konfiguration aktiver Reaktionen auf Gefahrensituationen bilden.

2.3.2 Security Management

In [GK12] werden die folgenden Fähigkeiten für ein mobiles Sicherheitsmanagement genannt:

- Erzwingen von Passwortrichtlinien
- Selektives (z.B. nur Unternehmensdaten) Löschen von Dateien
- Erkennung von Jailbreaks / Device Rooting
- Verschlüsselung sensibler Daten
- Virtual Private Networking (VPN) Unterstützung. Beispielsweise zentrale Verwaltung der Zertifikate
- Data Leak Prevention Funktionen
- Restriktive Behandlung von ActiveSync Verbindungen

Sind Mobile Security Funktionen verfügbar, behandeln diese bereits Sicherheitskritische Aufgaben. Wird eine Warnung von einer dieser Funktionen erzeugt, zum Beispiel wenn ein Nutzer einen Jailbreak durchführt, handelt es sich mit hoher Wahrscheinlichkeit um einen sicherheitsrelevanten Vorfall.

2.3.3 Application Management

Die dritte Kategorie relevanter Funktionen für MDM-Systeme aus [GK12] umfasst die folgenden Funktionen:

- Ferngesteuerte Softwareverteilung und Aktualisierungen für unternehmensspezifische Software
- White- / Blacklisting Fähigkeiten für Applikationen
- Restriktionen für die App-Store-Verwendung
- Unternehmensspezifischer App-Store

Die Verwaltungsfunktionen dieser Kategorie betreffen ausschließlich Applikationen. Der Begriff “App-Store” bezeichnet hier stellvertretend die Anwendungsverteilung aller Anbieter.

2.4 Analyse der Risiken

Trotz der Verwendung von MDM-Lösungen entstehen für Unternehmen durch die steigende Verwendung mobiler Endgeräte neue Risiken und Herausforderungen für die Unternehmenssicherheit. In einer Studie ermittelte die ENISA zehn gängige Bedrohungen, die in [HD10] erläutert sind und deren Risikopotenzial für drei Anwendergruppen quantifiziert wird. Da sich diese Arbeit auf den Einsatz von SIEM in Unternehmen bezieht, werden im Folgenden die Bewertungen für Angestellte zu Grunde gelegt.

Dies bedeutet: "Das mobile Endgerät wird von einem Angestellten eines Unternehmens oder einer Regierungsorganisation verwendet. Das mobile Endgerät wird für geschäftliche Telefonate, Surfen im Internet, geschäftliche E-Mails, Kostenmanagement, Verwaltung von Kundenkontakten, Reiseunterstützung, Kontaktverwaltung und geschäftliches Social Networking, Video Konferenzen, Terminplanung und zum Lesen von Dokumenten verwendet. In manchen Fällen werden Workflow-Applikationen auf dem mobilen Endgerät betrieben um beispielsweise Formulare, die Teil einer Aufgabe sind, auszufüllen. Die Benutzung unterliegt den IT (Sicherheits) Richtlinen der Verantwortlichen Stellen im Unternehmen" (Übersetzt aus [HD10]).

Eine Übersicht der Einschätzung der ENISA gibt Tabelle 1. Erläuterungen zu den Risiken finden sich in den Folgeabschnitten 2.4.1 - 2.4.10.

Bedrohung	Wahrscheinlichkeit	Auswirkungen
Datenschwund durch Verlust oder Diebstahl	Mittel	Hoch
Unsachgemäßes Stilllegen	Hoch	Hoch
Ungewollte Datenpreisgabe	Hoch	Mittel
Phishing	Mittel	Hoch
Spyware	Mittel	Hoch
Netzwerk Spoofing Angriffe	Mittel	Hoch
Überwachung	Niedrig	Hoch
Dialler Schadsoftware	Mittel	Mittel
Finanzielle Schadsoftware	Niedrig	Hoch
Netzwerk Überlastung	Niedrig	Niedrig

Tabelle 1: Risiken für mobile Endgeräte von Angestellten (nach [HD10])

2.4.1 Datenschwund durch Verlust oder Diebstahl

"Das Smartphone wurde gestohlen oder verloren und der interne oder austauschbare Speicher ist ungeschützt, was Angreifern Zugriff auf die darauf gespeicherten Daten erlaubt" (Übersetzt aus [HD10]).

Geschäftlich genutzte Smartphones enthalten häufig unternehmensbezogene E-Mails und Dokumente, die sensible Informationen enthalten können. Die Wahrscheinlichkeit für Datenschwund ist bei Angestellten als Mittel eingestuft, da den Nutzern die Risiken eines Verlustes klarer sind als bei rein privater Nutzung des Gerätes. Darüber hinaus ergreifen die Verantwortlichen im Unternehmen in der Regel Schutzmaßnahmen gegen Datenschwund bei Verlust oder Diebstahl und aktivieren beispielsweise die Speicherverschlüsselung oder erzwingen die Verwendung der automatischen Gerätesperre bei Nichtbenutzung (vgl. [HD10]).

2.4.2 Unsachgemäßes Stilllegen

"Das Smartphone wurde nicht korrekt stillgelegt, was einem Angreifer den Zugriff auf Daten des Gerätes erlaubt" (Übersetzt aus [HD10]).

Immer mehr Smartphones werden für die Wiederverwendung recycled. Im Jahr 2012 waren dies nach Schätzungen des Marktforschungsunternehmens ABI Research über 100 millionen Geräte. Dennoch wird bei der Stillegung noch nicht in jedem Fall auf eine sichere Löschung der Daten geachtet (vgl. [HD10]).

2.4.3 Ungewollte Datenpreisgabe

"Der Nutzer gibt ungewollt Daten mit seinem Smartphone preis" (Übersetzt aus [HD10]).

"Benutzer sind sich der Fähigkeiten von Smartphone Apps nicht in jedem Fall vollumfänglich bewusst. Auch wenn sie ihre Zustimmung explizit geben kann es sein, dass der Benutzer es nicht wahrnimmt wenn eine App Daten sammelt und veröffentlicht" (Übersetzt aus [HD10]).

So findet man bei [Sul13] einen Artikel über Anwendungen, die für ihren Zweck nicht benötigte Daten übertragen. Beispielsweise ist dort von einer Taschenlampen-App die Rede, welche die Position des Smartphones an unbekannte Dritte übermittelt.

Dieses Risiko tritt ein, wenn eine Anwendung mehr Rechte vom Nutzer verlangt als erforderlich, diese Rechte durch den Benutzer gewährt bekommt und für ein Weiterleiten der Informationen an unberechtigte Dritte missbraucht.

2.4.4 Phishing

"Ein Angreifer sammelt Nutzerdaten (wie Passwörter und Kreditkartennummern) durch betrügerische Anwendungen oder (SMS, E-Mail) Nachrichten, die vertrauenswürdig wirken" (Übersetzt aus [HD10]).

Phinshing Angriffe sind eine bekannte Gefahr. Besondere Beachtung sollte ihnen bei Smartphones zukommen, da es auf kleinen Displays leichter ist eine vertrauenswürdige Quelle vorzutäuschen oder eingeschränkte Fähigkeiten eines Smartphone-Browsers möglicherweise nicht vor einem falschen Zertifikat warnen (vgl. [HD10]).

Eine auf mobile Endgeräte zugeschnittene Art des Phishings ist durch Applikationen möglich, die als App für einen bestimmten Dienst beworben werden und eingegebene Daten unberechtigt weitergeben. In [Hyp10] wird beispielsweise beschrieben, dass durch eine illegitime Banking-App Benutzerdaten an unberechtigte Dritte gesendet werden.

2.4.5 Spyware

"Auf dem Smartphone ist Spyware installiert, die es einem Angreifer erlaubt auf persönliche Daten zuzugreifen oder auf sie zu schließen. Spyware beschreibt eine ungezielte Sammlung persönlicher Daten im Gegensatz zu einer gezielten Überwachung" (Übersetzt aus [HD10]).

Mobile Endgeräte enthalten viele persönliche Daten und bieten viele Möglichkeiten diese an unberechtigte Dritte zu übertragen (vgl. [HD10]).

"Zum Beispiel könnte eine Wetter-App die Berechtigung einfordern den Standort abzufragen und sich mit dem Internet zu verbinden, was zur Abfrage aktueller standortspezifischer Wetterdaten legitim ist. Die App könnte diese Rechte jedoch auch missbrauchen und Standortdaten zu Marketingzwecken an einen Anzeigenserver versenden" (Übersetzt aus [HD10]).

In Abgrenzung zur ungewollten Datenpreisgabe (siehe Abschnitt 2.4.3), handelt es sich bei einer Spyware um eine Anwendung mit legitimen Rechten. Die unberechtigte Weitergabe von Daten bleibt eine Gemeinsamkeit dieser beiden Risiken.

2.4.6 Netzwerk Spoofing Angriffe

"Ein Angreifer stellt einen Access Point (WiFi oder GSM) auf und Benutzer verbinden sich mit diesem. Der Angreifer kann daraufhin die Netzwerkkommunikation unterbrechen (oder Verändern) um weitere Angriffe wie Phishing durchzuführen" (Übersetzt aus [HD10]).

2.4.7 Überwachung

"Ein Angreifer hält einen bestimmten Benutzer unter Beobachtung durch sein Smartphone" (Übersetzt aus [HD10]).

Durch die Sensoren eines mobilen Endgerätes wie zum Beispiel Mikrofon, Kamera und GPS, sowie den Fakt, dass mobile Endgeräte häufig in der Nähe eines Nutzers sind, können mobile Endgeräte zu Spionagewerkzeugen werden (vgl. [HD10]).

2.4.8 Dialler Schadsoftware

"Ein Angreifer stiehlt Geld von einem Benutzer durch Schadsoftware, die im Verborgenen Premium SMS-Dienste oder Nummern verwendet" (Übersetzt aus [HD10]).

2.4.9 Finanzielle Schadsoftware

"Das Smartphone ist mit einer Schadsoftware infiziert, die speziell für das Stehlen von Kreditkartendaten, Zugangsdaten zum Online Banking oder zur Unterminierung von Online Banking oder E-Commerce Transaktionen erstellt wurde" (Übersetzt aus [HD10]).

"Finanzielle Schadsoftware kann ein Key-Logger sein, der Kreditkartendaten mitliest oder sie kann eine ausgeklügelte Software zum Eingriff in die SMS-Kommunikation sein um Online Banking Anwendungen anzugreifen" (Übersetzt aus [HD10]).

2.4.10 Netzwerk Überlastung

"Die zusätzliche Last auf dem Netzwerks durch die Benutzung von Smartphones kann zu einer Überlastung und dadurch zu Einschränkungen der Verfügbarkeit für den Endnutzer führen" (Übersetzt aus [HD10]).

3 SIEM-Konzept für mobile Endgeräte

Mobile Endgeräte stellen eine neue Geräteklasse in Unternehmen dar. Der Definition mobiler Endgeräte in Abschnitt 2.1 können die grundlegenden Eigenschaften entommen werden. Bislang werden SIEM-Systeme jedoch nicht zur Überwachung mobiler Endgeräte eingesetzt. Der Sicherheitsaspekt wird jedoch zunehmend wichtiger, wie durch die Entwicklung von Sicherheitsfunktionen in MDM-Systemen (siehe Abschnitt 2.3.2) und die Risikoanalyse der ENISA (siehe Abschnitt 2.4) ersichtlich wird.

Folgend soll daher ein Konzept für die Möglichkeit erörtert werden mobile Endgeräte in ein SIEM-System zu integrieren. Dies soll die neu entstandenen Risiken besser beherrschbar zu machen.

Abbildung 1 zeigt eine vereinfachte Darstellung eines SIEM-Systems. Klassische Arten von Log-Daten, die in einem SIEM-System erfasst werden können, sind in der Abbildung bereits benannt. Log-Daten die durch mobile Endgeräte neu hinzukommen sind mit Fragezeichen und einem roten Pfeil gekennzeichnet.

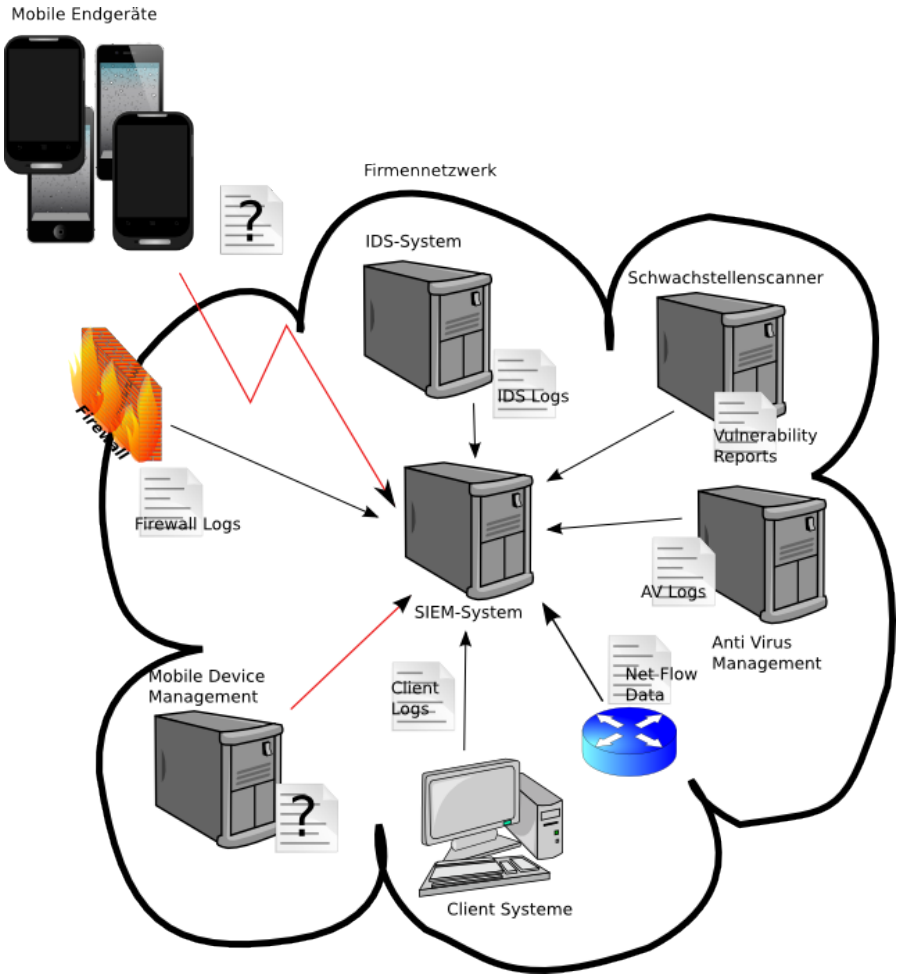

Abbildung 1: SIEM Umfeld

Wie in Abbildung 1 ersichtlich, bringt die Integration mobiler Endgeräte in ein SIEM-System zwei neue Perspektiven mit sich. Zum Einen das Mobile Device Management, zum Anderen die mobilen Endgeräte selbst.

Mobile Device Management Systeme werden dabei wie andere zentrale Systeme im Unternehmen integriert. Bei mobilen Endgeräten entstehen, aufgrund ihrer Verwendung und ihrer Eigenschaften, einige Herausforderungen bei der Integration, die in Abschnitt 3.1 näher erläutert werden.

Darauf folgend werden fragen der Datenübertragung und Speicherung besprochen, da auch hier die besonderen Eigenschaften mobiler Endgeräte zu Unterschieden gegenüber klassischen Systemstrukturen führen.

Abschließend wird gezeigt, wie die Sammlung von Log-Daten in einem zentralen SIEM-System dazu verwendet werden kann das Sicherheitsniveau zu erhöhen. Dazu werden die von der ENISA analysierten Risiken für mobile Endgeräte (siehe Abschnitt 2.4) erneut aufgegriffen und analysiert, wie mit Hilfe eines SIEM-Systems ein verbesserter Umgang mit diesen Risiken möglich ist.

3.1 Herausforderungen für die Integration mobiler Endgeräte in ein SIEM-System

Wie kann ein mobiles Endgerät in ein SIEM-System integriert werden? Soll eine Lösung auf diese Frage gefunden werden, sind sicher viele Ansätze mit unterschiedlichen Fokussierungen denkbar. Es gibt jedoch einige Herausforderungen, denen sich alle Implementierungen stellen müssen.

Aus der Perspektive der Verantwortlichen in einem Unternehmen stellt sich für eine solche Neueinführung häufig die Frage nach dem Datenschutz. Priorität im Rahmen dieses Konzepts besitzen jedoch die technischen Herausforderungen. Beide Perspektiven werden im folgenden besprochen.

3.1.1 Technische Herausforderungen

Aus einer technischen Sichtweise leiten sich die Herausforderungen für ein SIEM-Konzept für mobile Endgeräte aus den Zuständen ab, die mobile Endgeräte einnehmen können. Zu berücksichtigen ist, dass sich die Zustände in beliebiger Reihenfolge und beliebig schnell ändern können.

1. Ein mobiles Endgerät ist aktiv und befindet sich im Unternehmensnetz, zum Beispiel im WLAN eines Büros.
2. Das Gerät ist aktiv, befindet sich außerhalb des Unternehmensnetzwerks, ist jedoch vollständig darin integriert. Beispielsweise durch eine VPN-Verbindung.
3. Ein mobiles Endgerät ist aktiv und agiert außerhalb des Unternehmensnetzwerks. Dies geschieht beispielsweise beim einfachen Gebrauch als mobiles Telefon. Allgemeiner ausgedrückt bezeichnet dieser Zustand den Gebrauch des mobilen Endgerätes ohne direkte Integration in das Unternehmensnetzwerk.
4. Das mobile Endgerät ist zwar aktiv, kann aber keine Daten an das SIEM-System liefern. Dies geschieht dann, wenn eine Internetverbindung nicht möglich ist. Im

einfachsten Fall bedeutet dies, dass das Gerät kurze Zeit keinen Empfang hat. Da die Log-Daten an ein SIEM über das Internet geliefert werden kann dies jedoch auch durch das Deaktivieren des Datenroamings im Ausland der Fall sein. In solchen Fällen kann dieser Zustand auch über mehrere Wochen anhalten obwohl das mobile Gerät möglicherweise rege verwendet wird.

5. Das mobile Endgerät ist ausgeschaltet.

Am einfachsten lässt sich Zustand eins handhaben. Die Ablieferung von Log-Daten kann mit hoher Bandbreite erfolgen und erfolgt über das eigene Netzwerk. Die Wahrscheinlichkeit für Angriffe auf die Datenübertragung sinkt. Anfragen an das Gerät können schnell abgesetzt, empfangen und umgesetzt werden. Gleichzeitig sind hier die Risiken für ein Unternehmen am höchsten wenn das mobile Endgerät kompromittiert ist, da der Zugriff auf Unternehmensresourcen direkt erfolgen kann.

In Zustand zwei treten wie in Zustand eins keine Probleme mit der Erreichbarkeit des Endgeräts auf. Je nach Geschwindigkeit der Verbindung können jedoch Engpässe der Bandbreite auftreten. Eine Software zur Erfassung der Logs auf einem mobilen Endgerät muss mit langsamen Verbindungen arbeiten können und sollte die Bandbreite nach Möglichkeit schonen um andere Applikationen nicht zu beeinträchtigen. Die Absicherung der Datenübertragung erfolgt dabei durch die Übertragung per VPN auf dem unsicheren Teil des Netzwerkes.

Im dritten Zustand nimmt der Sicherheitsbedarf zu. Sollen Kommandos an das Endgerät gesendet werden, muss es eine Authentifizierung geben und die Kommunikation muss verschlüsselt erfolgen. Ebenso muss die Ablieferung der Log-Daten an das SIEM-System sicher verschlüsselt werden, da das Netzwerk nun nicht mehr als Sicher bewertet werden kann. Ist das mobile Endgerät nicht in das Unternehmensnetz integriert, müssen auf der Seite des SIEM und auch des MDM sichere Zugänge über das Internet möglich sein. Bezüglich der Bandbreite gelten die gleichen Einschränkungen wie in Zustand zwei.

Zustand vier liefert eine eigene Klasse von Herausforderungen. Können die gesammelten Log-Daten nicht direkt abgeliefert werden, müssen diese auf dem Endgerät zwischengespeichert und in einem anderen Zustand übertragen werden. Dabei muss der begrenzte Speicherplatz auf mobilen Endgeräten berücksichtigt werden. Wird später in einen Zustand mit Verbindung zum SIEM-System gewechselt, darf die Übertragung der gespeicherten Log-Daten nicht über lange Zeit die komplette Bandbreite beanspruchen.

In den Zuständen vier und fünf gibt es abschließend noch eine weitere Herausforderung. Soll das mobile Endgerät Kommandos empfangen, müssen diese auf der Seite der Server

ebenfalls zwischengespeichert werden, bis das Gerät wieder Informationen empfangen kann.

3.1.2 Datenschutzaspekte

Der Datenschutz ist, gerade für deutsche Unternehmen, ein sehr wichtiges Thema mit vielen Fallstricken. Bei der Einführung eines SIEM-Konzeptes für mobile Endgeräte muss auch dieser Aspekt berücksichtigt werden. Bei der Verwendung eines SIEM-Systems auf klassischen Arbeitsplatzsystemen sind die Fragen des Datenschutzes geklärt und die Sammlung der Log-Daten ist in vielen Unternehmen Alltag.

Die organisatorischen Schritte, zum Beispiel eine Abstimmung mit dem Betriebsrat, werden bei einer Einführung von SIEM bei mobilen Endgeräten zu klären sein. Der Unterschied bei mobilen Engeräten ist, dass der Mitarbeiter das mobile Endgerät auch im privaten Rahmen bei sich haben kann.

Im Rahmen dieser Arbeit wurde davon ausgegangen, dass ein mobiles Endgerät nur für den dienstlichen Gebrauch verwendet wird und damit keine persönlichen Daten des Nutzers enthält. Weiterhin wurde auf die Verwendung von Informationen verzichtet, die die Privatsphäre des Benutzers beeinträchtigen wenn er das Gerät bei sich hat. Es wird beispielsweise nicht auf Ortungsdaten zugegriffen und bei Telefonaten oder SMS lediglich die Häufigkeit ausgewertet und keine Daten wie angerufene Telefonnummern oder gar Kommunikationsinhalte.

Bei einer Nutzung eines privaten Gerätes zu dienstlichen Zwecken ist die Rechtslage wesentlich komplexer. Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) hat dazu einen Leitfaden für Unternehmen entwickelt (Siehe [BIT13]).

3.2 Datenübertragung

Für die fünf Zustände, die sich für die Log-Datenübertragung von mobilen Endgeräten ausmachen lassen sind zwei Gruppen von Herausforderungen identifizierbar. Erstens ist es nötig die verfügbare Bandbreite so zu nutzen, dass eine optimale Ausnutzung ohne Überlastung gegeben ist. Zweitens muss die Übertragung hohen Sicherheitsansprüchen genügen.

Da es ein sehr weit verbreitetes Protokoll ist und in der aktuellen Protokollversion hohe Sicherheitsstandards vorausgesetzt werden, kann die Datenübertragung mithilfe des Sys-

logprotokolls nach [Ger09] beziehungsweise [MMS09] durchgeführt werden. Aufgrund der starken Verbreitung des Protokolls, entsteht der Vorteil, dass die Daten durch jedes SIEM-System interpretiert werden können.

Einige Funktionen bietet eine native Verwendung von Syslog jedoch nicht. So wird in der Syslogstandardisierung beispielsweise keine Regelung für eine zeitversetzte Übertragung der Daten getroffen. Eine Datenreduktion zur Bandbreiten- und Speicherplatzoptimierung ist ebenfalls nicht vorgesehen. Soche Funktionen müssen für eine Verwendung implementiert werden.

Im folgenden werden einige Grundlagen des Syslogprotokolls erläutert und die Sicherheitsmerkmale besprochen. Anschließend werden die Möglichkeiten zur Änderung des Übertragungszeitpunktes und der Datenreduktion besprochen.

3.2.1 Protokolle

Jede Syslognachricht besteht aus einem Header und der eigentlichen Nachricht. Die Nachricht ist UTF-8 kodiert (vgl. [Ger09]).

Der Header umfasst die Priorität, die verwendete Protokollversion, einen Timestamp, den Hostnamen, den Namen der sendenden Anwendung, eine PROCID und eine MSGID. PROC- und MSGID sind nicht standardisiert und können durch die sendende Anwedung einen, dem Anwendungsfall entsprechenden, sinnvollen Wert erhalten.

Wichtig ist, für die Korrelation von Ereignissen, der Timestamp, sowie die Berechnung der Priorität. Die Priorität ist ein Wert zwischen 0 und 191, wobei 0 die höchste Priorität darstellt. Oftmals wird die Priorität aus der Facility und der Severity berechnet. Dies ist jedoch kein Bestandteil des Standards, wird dort jedoch aufgrund der häufigen Verwendung erklärt (vgl [Ger09]). Dort heißt es:

“Die Priorität wird berechnet, indem zuerst der Facility-Wert mit 8 multipliziert wird und dann der numerische Wert der Severity addiert wird. Zum Beispiel, eine Kernel-Nachricht (Facility=0) mit einer Notfall (Emergency) Severity (Severity=0) würde eine Priorität von 0 erhalten. Eine local4 Nachricht (Facility=20) mit einer Severity von 5 (Notice) würde eine Priorität von 165 erhalten” (Übersetzt aus [Ger09]).

In der Standardeinstellung werden Syslognachrichten unverschlüsselt per UDP an Port 514 übertragen. (vgl. [Okm09])

3.2.2 Sicherheit

Die inzwischen obsolete Version des RFC zum Syslog Protokoll (RFC 3164) sieht keine Verschlüsselungsmaßnahmen für Syslog vor. Der Standard in [Ger09] hingegen besagt: "Alle implementierungen dieser Spezifikation müssen eine TLS basierte Übertragung unterstützen" (Übersetzt aus [Ger09]).

Die Standardisierung für Syslog über TLS kann in [MMS09] eingesehen werden.

Dort werden die folgenden drei Ziele für die TLS verschlüsselte Übertragung der Syslognachrichten genannt:

- "Vertraulichkeit um das öffentlich werden der Nachricht zu verhindern" (Übersetzt aus [MMS09]).
- "Integritätstest um Modifikationen einer Nachricht zwischen den Hops (z.B. zwischen mehreren Sammelstationen [Anm. des Autors]) zu verhindern" (Übersetzt aus [MMS09]).
- "Serverseitige oder gegenseitige Authentifizierung um das Vortäuschen einer falschen Identität zu verhindern" (Übersetzt aus [MMS09]).

3.2.3 Übertragungszeitpunkt

Eine der großen Herausforderungen bei der Integration mobiler Endgeräte in ein SIEM-System ist der Übertragungszeitpunkt. Mobile Endgeräte sind nicht immer mit dem Internet verbunden, weswegen eine verzögerte Übertragung als Regelfall angesehen werden kann. Dies betrifft nicht nur Zustände in denen das mobile Endgerät keine Verbindung zum Internet herstellen kann sondern auch gleichermaßen Engpässe der Bandbreite, bei denen eine Verzögerung der Übertragung nötig wird.

Zur Verwaltung dieses Aufwandes kann ein Message-Scheduling eingesetzt werden. Der Scheduler kann dabei zwei Funktionen erfüllen. Das Überprüfen der verfügbaren Bandbreite, die Reduzierung der Übertragungsgeschwindigkeit bei geringer Bandbreite und eine Auswahl der nächsten zu sendenden Nachricht nach Priorität. Bei der Wahl der Übertragungspriorität kann die Klassifikation des Syslog Standards verwendet werden (siehte 3.2.1).

Der Begriff Scheduler taucht in der Informatik häufig im Zusammenhang mit der Prozessverwaltung des Betriebssystems auf. Während dort der Scheduler für das Verteilen

der CPU-Zeit an die Prozesse verantwortlich ist sollen im Zusammenhang mit mobilen Endgeräten Übertragungszeitpunkte für Nachrichten verwaltet werden. Diese sind grundsätzlich unterschiedliche Aufgaben, dennoch kann bei der Idee für einen Message-Scheduler auf Techniken des Prozess-Schedulings eines Betriebssystems zurückgegriffen werden.

Klassische Ansätze sind beispielsweise “FCFS” (First-Come-First-Serve), “RR” (Round-Robin), “SJF” (Shortest-Job-First), “PS” (Priority-based-Scheduling).

Beim FCFS-Scheduling wird der Prozess, der als Erster CPU-Zeit anfragt, zuerst abgearbeitet. Dieses ist vergleichbar mit einer Schlange an der Supermarktkasse. Bei der Übertragung von Log-Daten wird dieses Prinzip ebenfalls angewandt. Die Log-Daten werden in der Reihenfolge ihrer Entstehung an ein SIEM-System oder ein beliebiges Syslog-System gesendet.

RR und SJF basieren auf Zeitschlitzen, in denen Prozesse ihre Arbeit verrichten. Da die Übertragung einer Nachricht nicht zeitintensiv ist eignen sich diese Verfahren nicht für die Anwendung als Message-Scheduler für mobile Endgeräte.

Das Prioritätsbasierte Scheduling (PS) bietet jedoch einige Vorteile bei der Anwendung des Prinzips auf die Übertragung der Log-Daten mit Zeitverzögerung. Die Prozesse bekommen beim PS eine Priorität zugeordnet. Die Prozesse mit der höchsten Priorität werden dabei zuerst bearbeitet. Gibt es mehrere Prozesse mit der gleichen Priorität wird wiederum das FCFS-Prinzip auf diese Prioritätsgruppe angewendet.

Das Grundprinzip für ein prioritätenbasiertes Message-Scheduling ist in Abbildung 2 dargestellt.

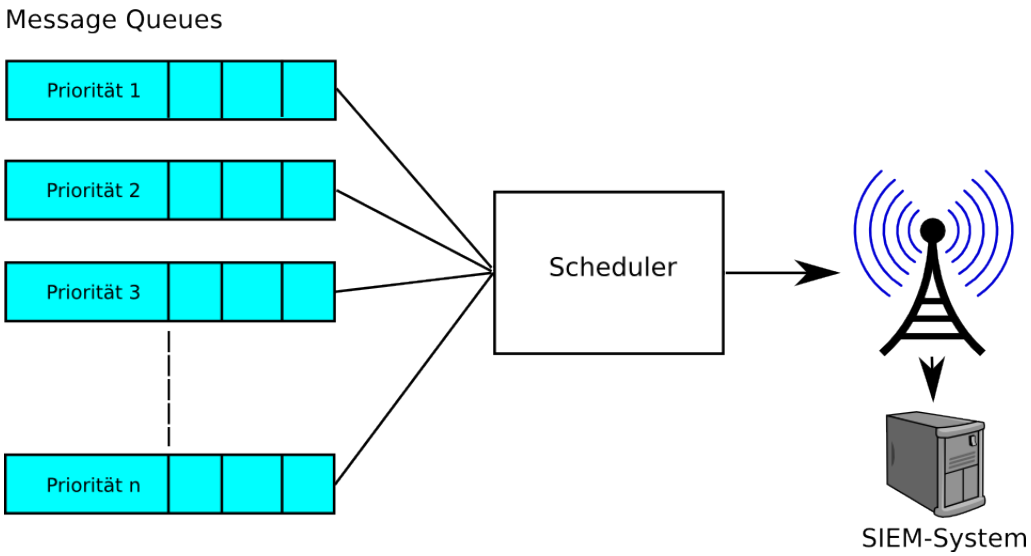

Abbildung 2: Prioritätsbasiertes Message-Scheduling

Die einzelnen Log-Zeilen werden dafür direkt nach ihrer Priorität in die Message Queues einsortiert. Eine Möglichkeit die Priorität zu bestimmen ist bereits in Abschnitt 3.2.1 über das Syslog Protokoll beschrieben, weitere Möglichkeiten sind denkbar. Der Scheduler arbeitet die Queues dann nach ihrer Priorität ab. Dazu prüft er die Verfügbarkeit des Netzwerks und passt die Übertragungsgeschwindigkeit entsprechend an.

Eine andere Methode zur Abstufung der Übertragungsgeschwindigkeit kann die Art der aktuellen Verbindung sein. Bei einer schnellen WLAN- oder Mobilfunkverbindung können alle Daten direkt übertragen werden. Ist nur eine langsame Verbindung über das Mobilfunknetz möglich, können die Nachrichten mit geringerer Priorität zurückgehalten werden, bis wieder eine schnelle Verbindung möglich ist.

Wichtig bei dieser Art des Vorgehens ist die korrekte Speicherung des Entstehungszeitpunktes der einzelnen Log-Zeilen. Durch das zeitversetzte Versenden wird eine spätere Korrelation mit zeitlichem Ablauf ansonsten unmöglich.

3.2.4 Datenreduktion

Generell wird in [CS12] eine Filterung vor der Sammlung der Daten als Fehler bezeichnet. In [CS12] wird daher ein Vorgehen mit sechs Abstufungen empfohlen. Die ersten drei Stufen können unter der Berücksichtigung einiger Besonderheiten auf mobile Endgeräte

übertragen werden. Die drei weiteren Prinzipien stellen für sich genommen eher Hinweise für die Handhabung von Log-Daten in SIEM-Systemen dar.

Die Verwendung dieser Prinzipien zur Datenreduktion stellen eine Möglichkeit dar die zu übertragende Datenlast zu reduzieren um somit Bandbreite und Speicherplatz zu sparen.

Alles loggen

Diese Stufe nach [CS12] sagt aus, dass alle verfügbaren Log-Daten, ohne nähere Betrachtung erfasst werden sollten. Dies gilt auch für die Datenerfassung bei mobilen Endgeräten. Da die Übertragung der Daten bei mobilen Endgeräten anders als bei Arbeitsplatzsystemen eine Herausforderung sein kann (siehe Abschnitt 3.1), können hierzu weitere Einschränkungen vorgenommen werden.

Das meiste behalten

Da mobile Endgeräte nicht immer Online sein können, müssen Daten vor der Übertragung zwischengespeichert werden. Nach einem längeren Auslandsaufenthalt und einer Sperrung des Internetzugriffs bei Roaming kann die anschließend zu übertragende Datenmenge groß sein, womit der Speicherplatz des Gerätes beansprucht wird.

Die Aussage von Marcus Ranum: "Die Anzahl, wie oft etwas uninteressantes passiert, ist etwas interessantes" (Übersetzt aus [Ran05]) bietet hierzu einen interessanten Ausweg. Wenn für eine definierte Menge häufig auftretender, bekannter und normalerweise irrelevanter Meldungen definiert wird, dass lediglich deren Auftrittshäufigkeit gespeichert wird, kann die Datenmenge reduziert werden. Dies führt dazu, dass die enthaltenen Informationen erhalten bleiben. Es entfällt jedoch die Möglichkeit den exakten Zeitpunkt für jedes einzelne Auftreten festzuhalten.

Um dennoch einen Zeitraum bestimmen zu können sollten die gezählten Ereignisse in einem festen Intervall als eigene Log-Zeilen übertragen werden. Ungewöhnliche Häufungen je Intervall lassen sich auf diesem Weg sehr schnell entdecken. Welche Meldungen häufig auftreten und im Normalfall irrelevant sind muss vorher im Einzelfall analysiert und regelmäßig an Neuerungen angepasst werden.

Hinreichend analysieren

Die verbleibenden Daten können, weiterhin auf dem mobilen Endgerät, im Anschluss noch grob vorab klassifiziert werden. Dies ermöglicht ein prioritätsbasiertes Vorgehen

wie beispielsweise wie in Abschnitt 3.2.3 über den Übertragungszeitpunkt beschrieben.

3.3 Datenspeicherung

Das Thema Datenspeicherung bezieht sich im Rahmen dieser Arbeit nicht auf die Speicherung der Log-Daten im SIEM-System. Die gängigen SIEM-Systeme bringen hierzu ihre eigenen Implementierungen mit und die Themen Speicherung, Indizierung und Korrelation sind in der gängigen Literatur behandelt (siehe zum Beispiel [MHH+10]).

Interessanter ist die Frage wie die Log-Daten auf den mobilen Endgeräten gespeichert werden können, bevor sie an ein SIEM-System versendet werden. Wie sollen Daten, die für einen Message-Scheduler bereitgestellt werden, abgelegt werden?

Generell existieren nach [CS12] vier Möglichkeiten zur Speicherung von Log-Daten. Die Speicherung in Textdateien, in Binärdateien, in Datenbanken, sowie das Speichern der Daten in einer Cloudlösung.

Die Speicherung von Log-Daten in Text- oder Binärdateien hat den Vorteil, dass das Schreiben sehr einfach und schnell möglich ist. Eine Aufteilung der Daten in separate Message-Queues zur Abarbeitung durch einen Message-Scheduler ist effizient möglich. Da die Daten jedoch nicht längerfristig auf dem mobilen Endgerät archiviert werden sollen müssen einzelne Zeilen nach der Abarbeitung auch wieder gelöscht werden. Dies ist mit einfachen Dateien nur mit erhöhtem Implementierungsaufwand möglich.

Das Speichern von Log-Daten in der Cloud ist sicher eine naheliegende Lösung für mobile Endgeräte. Die Ideen für die Verwendung eines Message-Schedulers und die Datenreduktion sollen jedoch den Bandbreitenbedarf reduzieren. Dies ist mit einem ständigen Datenfluss der Log-Daten in die Cloud nicht möglich.

Die Verwendung einer Datenbank ist daher empfehlenswert. Nach [CS12] liegen die größten Nachteile für die Log-Daten-Verwaltung mit Datenbanken im größeren Rechenaufwand für die Verwaltung von Indizes und dem höhere Speicherbedarf. Da die Log-Daten nicht über größere Zeiträume auf den mobilen Endgeräten aufbewahrt werden sollen stellt der erhöhte Speicherplatz keine Schwierigkeit dar. Die Verwaltung von Indizes ist auch bei der Speicherung in Dateien nötig um das effiziente Löschen einzelner Datensätze zu ermöglichen und die Daten nach Prioritäten zu sortieren.

3.3.1 Zugriffsschutz

Werden die Log-Daten in einer lokalen Datenbank auf dem mobilen Endgerät gespeichert, sollte diese gegen unberechtigte Zugriffe geschützt sein. Da Verlust oder Diebstahl eines mobilen Endgerätes explizit als Risiko für die Geräteklasse gesehen wird (siehe Abschnitt 2.4.1), kann hier ein höherer Schutzbedarf als Maßstab angelegt werden.

Wird der Empfehlung, eine Datenbank zur Verwaltung der Log-Daten auf dem mobilen Engerät zu verwenden, entsprochen können Datenbanktreiber zur verschlüsselten Ablage der Datenbank verwendet werden. Ein Beispiel, das für eine große Anzahl Endgeräte benutzbar ist, ist das Projekt SQLCipher (siehe `http://sqlcipher.net/about`). Dieses bietet eine vollständige Datenbankverschlüsselung von SQLite Datenbanken an.

Da die Verschlüsselung von Datenbanken auf mobilen Endgeräten im genannten Beispiel symmetrisch abläuft muss es einen bekannten Schlüssel zur Öffnung der Datenbank geben. Dieser sollte, für den Fall des Diebstahls, nicht unverschlüsselt auf dem Gerät hinterlegt sein. Wird beim Starten des mobilen Gerätes eine "Single Sign On" Strategie verwendet und ein Passwort für die Entsperrung verschlüsselter Speicherbereiche etc. abgefragt, ist es sinnvoll dies mit der Entschlüsselung und Aktivierung des Log-Datensystems zu verknüpfen. Dies verhindert, dass der Nutzer beim Starten seines Gerätes viele Passworte eingeben muss, erhöht die Transparenz für den Nutzer und steigert so die Benutzbarkeit.

3.4 Relevante Daten und Risikobehandlung

Welche der Daten aus dem SIEM-Umfeld (siehe Abbildung 1) zur Behandlung der Risiken aus Abschnitt 2.4 eine besondere Relvanz besitzen wird im Folgenden diskutiert. Dazu werden die Risiken in ein neues Licht gerückt, relevante Daten zur Behandlung des Risikos besprochen, Schutzmöglichkeiten erläutert und abschliessend die Risikoquantifizierung aus Tabelle 1 angepasst.

3.4.1 Datenschwund durch Verlust oder Diebstahl

Einen Datenschwund durch Verlust oder Diebstahl zu identifizieren ist durch ein SIEM-System im Grunde unmöglich. Im Umfeld von MDM-Systemen gibt es einige Funktionen zur Behandlung dieses Szenarios. Zum Beispiel das Löschen wichtiger Daten oder das Orten des Gerätes nachdem ein Benutzer es als verloren oder gestohlen gemeldet hat.

Es ist dennoch möglich in diesem Szenario Vorteile aus dem Einsatz eines SIEM-Systems zu ziehen. Solange das mobile Endgerät nicht ausgeschaltet wurde werden weiterhin Log-

Daten produziert und können ausgewertet werden. Dadurch kann beispielsweise nachvollzogen werden ob das Gerät nach dem Verlust noch verwendet wurde.

Werden Ereignisse erkannt, die auf ein erraten des Passwortes für die Displaysperre hinweisen, Anwendungen gestartet oder der Status der Funktechnologien verändert deutet dies auf eine Weiterbenutzung des Gerätes durch Dritte hin. Dies birgt potenziell eine größere Gefahr für ein Unternehmen, als ein ausgeschaltetes Gerät.

Für Datenschwund durch Verlust oder Diebstahl sind andere Schutzmaßnahmen, wie eine Speicherverschlüsselung, effektiver.

Daten:

Alle Daten die nach der Meldung eines Verlustes oder Diebstahls eingehen können Hinweise auf eine weitere Benutzung des Gerätes geben. Besonders interessant können unter anderem Informationen über eine Deaktivierung bzw. Deaktivierungsversuche der Displaysperre sein.

Schutz:

Viele MDM-Systeme bieten eine Möglichkeit zum Löschen von kritischen Daten auf mobilen Endgeräten. Weiterhin sollten kritische Daten im Speicher des mobilen Engerätes verschlüsselt sein. Dies verringert die Wahrscheinlichkeit, dass nach einem Geräteverlust die Daten an unberechtigte Dritte gelangen.

Risiken:

Die Eintrittswahrscheinlichkeit für einen Verlust oder Diebstahl kann durch ein SIEM-System nicht gesenkt werden. Die Auswirkungen können jedoch durch Verschlüsselung und eine Löschung kritischer Daten reduziert werden. Die Möglichkeit Spuren für eine weitere Benutzung zu sehen oder die Falsifizierung des Verdachts auf eine weitere Benutzung mit einem SIEM-System, macht die Planung der nächsten Schritte einfacher.

Für die Auswirkungen wird eine Einstufung als mittel vorgenommen, da die Möglichkeiten für ein SIEM-System begrenzt sind, wenn das Gerät ausgeschaltet oder die SIM-Karte entfernt wird. Bleibt das mobile Endgerät in das SIEM-System eingebunden können die Auswirkungen jedoch reduziert werden.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Mittel	Hoch
Nachher	Mittel	Mittel

Tabelle 2: Neue Risikobewertung: Datenschwund durch Verlust oder Diebstahl

3.4.2 Unsachgemäßes Stilllegen

Ob ein mobiles Endgerät unsachgemäß stillgelegt wurde kann durch ein SIEM-System nur in einem Fall erkannt werden. Ist ein Gerät offiziell als stillgelegt klassifiziert und liefert weiterhin Log-Daten, so wurde die Stilllegung nicht ordnungsgemäß durchgeführt.

Daten:

Alle Daten, die nach einer offiziellen Stillegung des Gerätes erfasst werden, geben Hinweise auf eine unsachgemäße Stilllegung des Geräts.

Soll ein SIEM-System automatisch auf eine unsachgemäße Stilllegung reagieren muss die Information über eine Gerätestilllegung für das SIEM-System zugänglich sein.

Schutz:

Viele MDM-Systeme bieten eine Möglichkeit zum Löschen von kritischen Daten auf mobilen Endgeräten. Weiterhin sollten kritische Daten im Speicher des mobilen Engerätes verschlüsselt sein. Dies verringert die Wahrscheinlichkeit, dass nach einer unsachgemäßen Stilllegung Daten an unberechtigte Dritte gelangen.

Ist die Information über die Stilllegung eines Gerätes für ein SIEM-System zugreifbar kann die Löschung automatisch ausgelöst werden. Dies garantiert eine optimale Reaktionszeit.

Risiken:

Ist erst ein Prozess definiert, der die Stilllegung vorsieht und die Information über die stillgelegten Geräte einem SIEM-System zur Verfügung stellt, sinkt auch die Wahrscheinlichkeit für eine unsachgemäße Stilllegung. Die Auswirkungen einer unsachgemäßen Stilllegung ist durch die zeitnahe automatische Löschung relevanter Daten und eine Verschlüsselung ebenfalls niedriger.

Wird ein unsachgemäß stillgelegtes Gerät ausgeschaltet und ohne SIM-Karte weitergegeben ist dies durch ein SIEM-System nichtmehr erkennbar. Daher verbleibt ein Restrisiko.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Hoch	Hoch
Nachher	Mittel	Mittel

Tabelle 3: Neue Risikobewertung: Unsachgemäßes Stilllegen

3.4.3 Ungewollte Datenpreisgabe

Zur Erkennung, ob durch eine installierte Anwendung ungewollt Daten preisgegeben werden, können zwei Quellen herangezogen werden. Die Informationen eines MDM-Systems über die installierten Anwendungen und deren Rechte und die Einstufung der Anwendung durch eine Antivirus Software. Im Optimalfall wird die Installation schadhafter Software bereits durch einen eingeschränkten App-Store, der nur geprüfte Software enthällt, verhindert.

Da die Verwendung eines eingeschränkten App-Stores den Benutzer in seinen Möglichkeiten einschränkt wird dieses Vorgehen nicht in jedem Fall verwendet. Für ein SIEM-System gewinnen daher die Log-Daten der Virenscanner auf den mobilen Endgeräten an Relevanz. Wird eine Anwendung als schadhaft klassifiziert und dies durch den Virenscanner an das SIEM gemeldet sollte dies einen Alarm auslösen.

Alternativ zum völlig eingeschränkten App-Store und ergänzend zum Virenschutz können auch Blacklistingdatenbanken von Anwendungstestern, wie zum Beispiel Mediatest Digital (`http://www.mediatest-digital.com/`) hinzugezogen werden.

Daten:

Befindet sich das Gerät ausserhalb des Unternehmensnetzwerks, sind die Daten eines installierten Virenscanners und eine Überprüfung der installierten Apps auf schadhafte Anwendungen durch ein MDM-System besonders wichtig. Bei der ungewollten Datenpreisgabe kann ein regelmäßiges Audit der App-Rechte helfen, Gefährdungen zu erkennen.

Wird das Gerät innerhalb des Unternehmensnetzwerks verwendet gibt es weitere Quellen. Dort sind Logs der Firewall, von IDS-Systemen und auch NetFlow-Daten von Interesse. Diese können auf ungewöhnliche Aktivitäten, wie den Datenversand an bekannte schadhafte IP-Adressen, prüfen.

Schutz:

Wird durch den Virenscanner eine schadhafte Anwendung erkannt sollte diese deinstalliert werden. Weiterführend sollte die Anwendung zu einer Blacklist hinzugefügt und durch das MDM von allen Geräten entfernt werden.

Ist das mobile Endgerät innerhalb des Unternehmensnetzwerkes kann der Datenversand an illegitime Empfänger vom SIEM-System durch setzen einer Firewallregel verhindert werden.

Wird bei einem mobilen Endgerät ein Befall durch eine schadhafte Software festgestellt, die Daten an unberechtigte Dritte sendet, sollten mehrere Schritte automatisch erfolgen. Die Entschlüsselung der Unternehmensdaten auf dem Gerät sollte deaktiviert werden, der Zugriff auf das Unternehmensnetz (z.B. durch einen VPN-Zugang) sollte gesperrt werden und die Verantwortlichen sollten eine Alarmmeldung erhalten um den Vorgang schnell klären zu können. Auch der Nutzer muss schnellstmöglich über diesen Vorgang informiert werden.

Risiken:

Wird die Installation von externen Softwarepaketen erlaubt und kein eingeschränkter App-Store verwendet, indem die Installation schadhafter Software grundsätzlich ausgeschlossen wird, besteht die Möglichkeit, dass ein Nutzer eine solche Anwendung installiert. Durch den Einsatz eines Virenscanners und von Blacklists sinkt jedoch die Eintrittswahrscheinlichkeit für dieses Risiko.

Wird trotz der Schutzmechanismen eine Anwendung installiert, die Daten unberechtigt an Dritte leitet, sind die Auswirkungen jedoch identisch zum Ausgangsszenario.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Hoch	Mittel
Nachher	Mittel	Mittel

Tabelle 4: Neue Risikobewertung: Ungewollte Datenpreisgabe

3.4.4 Phishing

Wird der Phishingangriff mit einer betrügerische Anwendungen betrieben, bieten Virenscanner, Einschränkungen des App-Stores oder App-Blacklisting, ebenso wie bei der ungewollten Datenpreisgabe (Abschnitt 3.4.3), einen Schutz.

Phishing E-Mails können möglicherweise auf den Mail-Servern des Unternehmens erkannt und entfernt werden.

Befindet sich ein System innerhalb des Unternehmensnetzwerks ist die Erkennung am Internetübergang des Unternehmens, zum Beispiel durch ein Blockierung bekannter Phishing-Domains an der Firewall, sinnvoll. Da bei mobilen Endgeräten dieser Schutz nicht vorausgesetzt werden kann ist eine Erkennung nur auf dem Gerät selbst möglich.

Daten:

Die Firewall- und Virenscannerlogs können Hinweise auf Phishing enthalten.

Schutz:

Meldet ein Virenscanner eine Phishing-Applikation auf einem mobilen Endgerät, kann durch das MDM-System eine Löschung und ein Blacklisting der App erfolgen. Wenn die App auf einer Blacklist steht, sollte sie über das MDM von allen Geräten auf denen sie noch installiert ist, ebenfalls entfernt werden.

Bei der Erkennung des Datenversands an illegitime Empfänger (zum Beispeil an bekannte Phsihing-Domains), während sich das mobile Endgerät im Unternehmensnetz befindet, kann das SIEM-System durch setzen einer Firewallregel ein weiteres Abfließen der Daten verhindern.

Der Nutzer sollte schnellstmöglich über diesen Vorgang informiert werden. Diese Maßnahme kann den Nutzer weiter sensibilisieren und damit einen besserern Schutz gegen Phishing bieten, als dies durch technische Mittel möglich wäre.

Risiken:

Die Wahrscheinlichkeit für einen erfolgreichen Phishing-Angriff kann zum Beispiel durch automatisches Blacklisting von Phishing-Apps gemindert werden. Der Erfolg von Phishing ist jedoch in den meisten Fällen von der Aufmerksamkeit der Nutzer abhängig und nicht von einem technischen Schutz. Reagiert ein Nutzer auf eine Phishing-Mail oder wird eine Phishing-App nicht als solche erkannt und verwendet, bleiben die Auswirkungen hoch.

Die Möglichkeiten eines SIEM-Systems zur Verringerung der Eintrittswahrscheinlichkeit und zur Reduzierung der Auswirkungen reichen im Fall des Phishings nicht aus, um eine Veränderung der Einstufung vorzunehmen.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Mittel	Hoch
Nachher	Mittel	Hoch

Tabelle 5: Neue Risikobewertung: Phishing

3.4.5 Spyware

Eine Spyware versendet, ebenso wie der beschriebene Anwendungstyp zur ungewollten Datenpreisgabe aus Abschnitt 3.4.3, Daten an unberechtigte Dritte. Entsprechend ist ein Schutz durch Firewallüberwachung, Virenschutz und Anwendungsblacklisting möglich.

Daten:

Die Firewall- und Virenscannerlogs können Hinweise auf Spyware enthalten.

Schutz:

Wird durch den Virenscanner eine schadhafte Anwendung erkannt, sollte diese deinstalliert werden. Weiterführend sollte die Anwendung zu einer Blacklist hinzugefügt und durch das MDM von allen Geräten entfernt werden.

Bei der Erkennung des Datenversands an illegitime Empfänger, während sich das mobile Endgerät im Unternehmensnetz befindet, kann das SIEM-System durch setzen einer Firewallregel ein weiteres Abfließen der Daten verhindern.

Wird bei einem mobilen Endgerät ein Befall durch eine schadhafte Software festgestellt die Daten an unberechtigte Dritte sendet, sollten mehrere Schritte automatisch erfolgen. Die Entschlüsselung der Unternehmensdaten auf dem Gerät sollte deaktiviert werden, der Zugriff auf das Unternehmensnetz (z.B. durch einen VPN-Zugang) sollte gesperrt werden und die Verantwortlichen sollten eine Alarmmeldung erhalten um den Vorgang schnell klären zu können. Auch der Nutzer sollte schnellstmöglich über diesen Vorgang informiert werden.

Risiken:

Wird kein eingeschränkter App-Store verwendet, wodurch die Installation schadhafter Software grundsätzlich ausgeschlossen wird, besteht die Möglichkeit, dass ein Nutzer eine solche Anwendung installiert. Durch den Einsatz von Virenscannern und Blacklists sinkt die Eintrittswahrscheinlichkeit für dieses Risiko etwas. Durch den legitim wirkenden Zweck einer Spyware kann jedoch noch nicht von einer niedrigen Wahrscheinlichkeit ausgegangen werden.

Wird trotz der Schutzmechanismen eine Anwendung installiert, die Daten unberechtigt an Dritte sendet, können die Auswirkung durch verschlüsseln relevanter Daten und Sperren von Zugriffen verringert werden.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Mittel	Hoch
Nachher	Mittel	Mittel

Tabelle 6: Neue Risikobewertung: Spyware

3.4.6 Netzwerk Spoofing Angriffe

Es existieren zwei Arten von Netzwerk Spoofing Angriffen. Eine besteht darin einen ungesicherten WLAN-Accesspoint aufzustellen und Daten von angemeldeten Geräten abzufangen. Diese WLANs werden gezielt so angelegt, dass sie wie das WLAN eines Hotels oder Restaurants aussehen und bieten einen kostenlosen Internetzugang an.

Erst kürzlich wurde ein Angriff gegen ein bekanntes Authentifizierungsprotokoll mittels gefälschten WLAN-Accesspoints bekannt. Für Details kann das zugehörige Microsoft Security Advisory unter `http://technet.microsoft.com/en-us/security/advisory/2876146` eingesehen werden.

Die zweite Spoofingvariante sind sogenannte IMSI-Catcher (siehe [Str07] und [MW04]). Diese geben sich als Mobilfunkstation aus und greifen so Daten von Personen ab, deren Smartphones sich in der Reichweite des IMSI-Catchers aufhalten und sich über den Catcher ins Netz einbuchen.

Daten:

Spoofing durch Monitoring zu erkennen ist eine große Herausforderung. Ein Hinweis auf einen IMSI-Catcher kann es sein, dass die Verschlüsselung der GSM-Verbindung deaktiviert ist.

Ein gefälschter Firmen-Accesspoint kann über geschickte Korrelation der verfügbaren Daten im SIEM-System erkannt werden. Der Zugriff auf ein WLAN wird in den Systemlogs der mobilen Endgeräte festgehalten. Wird auf ein WLAN mit dem Namen des Firmen-WLANs zugegriffen kann durch Überprüfung der Logs von internen Systemen festgestellt werden, ob das Endgerät wirklich mit einem Zugang der Firma verbunden ist.

Bei der Verwendung öffentlicher WLAN-Zugänge hilft nur ein grundsätzliches Misstrauen. Durch die Offenheit können ungesicherte, öffentliche Netzzugänge immer abgehört werden.

Schutz:

Grundsätzlich sollte die Kommunikation mobiler Endgeräte mit Systemen eines Unternehmens immer verschlüsselt sein, zum Beispiel durch die erzwungene Verwendung eines VPN-Tunnels.

Ist diese erzwungene VPN-Nutzung nicht erwünscht, sollte wenigstens immer dann, wenn ein Gerät über einen unverschlüsselten Zugang kommuniziert (egal ob GSM oder WLAN-Netz), die VPN-Nutzung erzwungen sein.

Der Zugriff auf ein WLAN, das den Zugang zur Firma fälscht, sollte dazu führen, dass die Verbindung unterbrochen wird und sicherheitsrelevante Daten verschlüsselt werden. Sicherer ist lediglich eine zertifikatsbasierte Authentifizierung der Accesspoints, wie auch Microsoft im oben genannten Advisory empfiehlt.

Risiken:

Die genannten Schutzmöglichkeiten sind zu einem großen Teil keine spezifischen SIEM-Mechanismen. Die Wahrscheinlichkeit für einen Zugriff auf einen Accesspoint von dem Daten durch Dritte abgefangen werden lässt sich durch ein SIEM-System nicht senken. Setzt man SIEM-Korrelation für die Erkennung von Accesspoints ein, die sich fälschlich als Firmen-Zugänge ausgeben, lassen sich jedoch einige der schwerwiegenderen Auswirkungen verhindern.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Mittel	Hoch
Nachher	Mittel	Mittel

Tabelle 7: Neue Risikobewertung: Netzwerk Spoofing

3.4.7 Überwachung

Eine Überwachung durch das mobile Endgerät muss durch eine Schadsoftware durchgeführt werden. Daher gelten auch hier die Hinweise aus Abschnitt 3.4.3 zur Verwendung eines Virenscanners und zum Schutz vor schadhaften Anwendungen mit Hilfe von Blacklists.

Als Überwachungsszenario wird häufig von einer Verwendung des Mikrofons oder der Kamera des Geräts gesprochen. Die Zustände der jeweiligen Sensorfunktion in Verbindung mit der aktuellen Verwendung des Geräts können im SIEM-System Hinweise auf eine Überwachung geben.

Wird beispielsweise das Mikrofon aktiviert obwohl kein Telefonat stattfindet oder ist die Kamera aktiv obwohl das Display gesperrt ist, sind dies Hinweise auf eine Überwachung des Nutzers durch eine Schadsoftware auf dem mobilen Endgerät.

Daten:

Eine Korrelation des Gerätestatus mit den Zuständen der Sensorfunktionen.

Wird im SIEM-Umfeld von schadhafter Software gesprochen, die Daten an unberechtigte Dritte sendet, wird in [MHH+10] von “Phoning Home” (nach Hause telefonieren) gespro-

chen. Um Hinweise auf solche schadhaften Aktivitäten zu erlangen sind in [MHH+10] vier Möglichkeiten aufgeführt: Eine Veränderung der Startseite des Browser, Datenverkehr an bekannte schadhafte IP-Adressen, Datenverkehr an nicht allokierte IP-Adressen, ungewöhnlicher Datenverkehr an legitime IP-Adressen.

Die Browserstartseite wird von einer Schadsoftware zur heimlichen Nutzerüberwachung wahrscheinlich nicht verändert. Da die Daten der Überwachung, beispielsweise Audio oder Videodateien jedoch an den Überwachenden übertragen werden müssen, können die anderen genannten Punkte Hinweise auf den Befall bieten.

Schutz:

Wird durch den Virenscanner eine schadhafte Anwendung erkannt, sollte diese deinstalliert werden. Weiterführend sollte die Anwendung zu einer Blacklist hinzugefügt und durch das MDM von allen Geräten entfernt werden.

Werden Daten an bekannte schadhafte IP-Adressen versendet, sollte dieser Datenverkehr durch die Firewall unterbunden werden.

Da die Korrelation des Gerätestatus mit den Sensorfunktionen lediglich Hinweise liefert und die Aktivitäten auch einen legitimen Zweck haben können, ist es nicht zweckmäßig bei Erkennen der Aktivität automatisch einzuschreiten. Sollten sich die Indizien jedoch häufen, ist eine Warnung für die Verantwortlichen im Unternehmen sinnvoll, die dann genauer untersuchen können ob das Gerät zur heimlichen Überwachung des Nutzers eingesetzt wird.

Risiken:

Die Wahrscheinlichkeit für eine Überwachung durch ein mobiles Endgerät wird bereits von der ENISA als niedrig eingestuft. Da es durch das SIEM-System eine Möglichkeit gibt Hinweise auf eine Überwachung zu sammeln und darauf zu reagieren, können jedoch die Auswirkungen reduziert werden.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Niedrig	Hoch
Nachher	Niedrig	Mittel

Tabelle 8: Neue Risikobewertung: Überwachung

3.4.8 Dialler Schadsoftware

Der Befall durch einen Dialler kann durch Virenscanner oder durch einen eingeschränkten App-Store mittels Blacklists verhindert werden (wie auch in Abschnitt 3.4.3 erläutert). Schlägt dieses Vorgehen fehl, gibt es weitere Hinweise auf die Anwesenheit eines Diallers im System, die durch ein SIEM-System erkannt werden können.

Daten:

Zum Beispiel kann durch das Versenden vieler Kurznachrichten in kurzer Zeit, möglicherweise ohne Inhalt, auf die Anwesenheit eines Diallers geschlossen werden. Ein anderes Szenario wäre eine Häufung besonders kurzer oder langer Telefonate und dies eventuell zu ungewöhnlichen Uhrzeiten.

Schutz:

Wird durch den Virenscanner eine schadhafte Anwendung erkannt sollte diese deinstalliert werden. Weiterführend sollte die Anwendung zu einer Blacklist hinzugefügt und durch das MDM von allen Geräten entfernt werden.

Da das Versenden vieler Kurznachrichten oder das führen langer Telefonate - auch ins Ausland - durchaus legitim sein können ist eine automatische Unterbindung nicht sinnvoll. Es sollte jedoch eine Warnung an die verantwortlichen Personen im Unternehmen generiert werden.

Risiken:

Durch eine Diagnose des SIEM-Systems wird es möglich, noch vor der Abrechnung, Spuren auf eine schadhafte Verwendung zu entdecken. Dies kann die Auswirkungen eines Diallers reduzieren.

Auch die Infektionswahrscheinlichkeit nimmt durch die Schutzmöglichkeiten von Anwendungsblacklisting und der Verwendung von Virenscannern ab.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Mittel	Mittel
Nachher	Niedrig	Niedrig

Tabelle 9: Neue Risikobewertung: Dialler Schadsoftware

3.4.9 Finanzielle Schadsoftware

Da es sich bei finanzieller Schadsoftware um eine dediziertere Art von Spyware handelt, kann diese wie bei Spyware (siehe Abschnitt 3.4.5), durch Firewallüberwachung, Virens-

canner und Anwendungsblacklisting erkannt werden.

Manipuliert die Schadsoftware bekannte Programme, zum Beispiel eine Banking App, können die Anwendugslogs dieser Anwendung Unregelmäßigkeiten aufweisen.

Daten:

Auf dem mobilen Endgerät erzeugte Anwendungslogs können Hinweise auf finanzielle Schadsoftware enthalten. Weitere Hinweise bieten die Logs der Virenscanner und eine Firewallüberwachung.

Schutz:

Wird durch den Virenscanner eine schadhafte Anwendung erkannt, sollte diese Deinstalliert werden. Weiterführend sollte die Anwendung zu einer Blacklist hinzugefügt und durch das MDM von allen Geräten entfernt werden.

Wenn Kontakt zu einer schadhaften IP-Adresse aufgenommen wird, kann dieser Kontakt unterbunden und so ein weiteres Abfließen von Daten verhindert werden.

Unregelmäßigkeiten in Anwendungen können aus vielen unterschiedlichen Gründen auftreten. Werden diese festgestellt, müssen diese vor einer weiteren Aktion in jedem Fall von einem Analysten untersucht werden.

Risiken:

Da die Wahrscheinlichkeit für eine Infektion mit finanzieller Schadsoftware bereits von der ENISA als niedrig eingestuft wird, ist durch die genannten Schutzmethoden keine weitere Senkung möglich. Durch die Möglichkeiten zur frühzeitigen Erkennung einer Infektion können die Auswirkungen jedoch eingedämmt werden.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Niedrig	Hoch
Nachher	Niedrig	Mittel

Tabelle 10: Neue Risikobewertung: Finanzielle Schadsoftware

3.4.10 Netzwerküberlastung

Eine Überlastung des Netzwerks kann durch ein SIEM-System nicht verhindert werden. Durch die Übertragung der Log-Daten zum SIEM-System steigt letztlich die Belastung des Netzwerks. Durch die Möglichkeiten Schadsoftware zu erkennen, kann jedoch eine illegitime Benutzung des Netzes unterbunden werden.

Daten:

Je weniger Daten übertragen werden desto weniger wird das Netzwerk belastet, daher gibt es keine relevanten Daten zur Verhinderung der Netzwerküberlastung.

Schutz:

Zur Reduzierung der Datenlast auf dem Netzwerk können die Hinweise aus Abschnitt 3.2.4 zur Datenreduktion herangezogen werden. Ist die Kapazität des Netzes erschöpft, hilft die temporäre Drosselung der Datenlast durch einen Message Scheduler (siehe Abschnitt 3.2.3) dabei, einen kompletten Ausfall zu verhindern.

Risiken:

Ein Restrisiko, dass das Netzwerk den wachsenden Anforderungen nicht genügt, besteht nach wie vor. Die Wahrscheinlichkeit ist jedoch niedrig. Durch geeignete Maßnahmen, kann dem Risiko weiter entgegen gewirkt werden. Um eine wachsende Geräteanzahl zu bewältigen, muss in einigen Fällen ein Ausbau der Infrastruktur in Betracht gezogen werden.

	Wahrscheinlichkeit	Auswirkungen
Vorher	Niedrig	Niedrig
Nachher	Niedrig	Niedrig

Tabelle 11: Neue Risikobewertung: Netzwerk Überlastung

3.4.11 Zusammenfassung

Abschließend, zur Erläuterung der Risiken und der Möglichkeiten diese durch ein SIEM-System besser zu beherrschen, zeigt Tabelle 12 wie sich durch den Einsatz eines SIEM-System für mobile Endgeräte die Risiken verändern können. Die relevanten Daten, Schutzmaßnahmen und eine Begründung zur Veränderung des Risikos können den vorangehenden Abschnitten entnommen werden.

In den Spalten Wahrscheinlichkeit und Auswirkungen steht jeweils zuerst die Einschätzung der ENISA aus [HD10] und nach einem Schrägstrich die neue Einschätzung nach der Etablierung der genannten Schutzmaßnahmen.

Risiko	Wahrscheinlichkeit	Auswirkungen
Datenschwund durch Verlust oder Diebstahl	Mittel / Mittel	Hoch / Mittel
Unsachgemäßes Stilllegen	Hoch / Mittel	Hoch / Mittel
Ungewollte Datenpreisgabe	Hoch / Mittel	Mittel / Mittel
Phishing	Mittel / Niedrig	Hoch / Hoch
Spyware	Mittel / Mittel	Hoch / Mittel
Netzwerk Spoofing Angriffe	Mittel / Mittel	Hoch / Mittel
Überwachung	Niedrig / Niedrig	Hoch / Mittel
Dialler Schadsoftware	Mittel / Niedrig	Mittel / Niedrig
Finanzielle Schadsoftware	Niedrig / Niedrig	Hoch / Mittel
Netzwerk Überlastung	Niedrig / Niedrig	Niedrig / Niedrig

Tabelle 12: Neueinschätzung der Risiken

4 Praktische Prüfung des Konzeptes

Das vorangegangene Konzept behandelt die Möglichkeit für Unternehmen, ihre mobilen Endgeräte in ein zentrales SIEM-System einzubinden. Dies soll die Möglichkeit schaffen, die Risiken, die durch den Einsatz mobiler Endgeräte entstehen, besser beherrschen zu können.

Theoretisch wurden diese Möglichkeiten besprochen. Praktisch soll dies im Folgenden Abschnitt am Beispiel des Betriebssystems Android erprobt werden. Dazu sollen die Systemlogs eines Android Smartphones betrachtet und ihre Verwendbarkeit für die beschriebenen Methoden zur Risikominimierung überprüft werden. Ebenso sollen die erläuterten Möglichkeiten zur Bandbreiteneinsparung und Speicherplatzoptimierung auf ihre Umsetzbarkeit geprüft werden.

Die Wahl des Betriebssystems Android ist dabei überwiegend aus zwei Gründen getroffen worden.

1. Android besitzt mit einem Marktanteil von 79,3% derzeit die größte Verbreitung (Stand 2. Quartal 2013, siehe [Köl13]).
2. Android bringt die Möglichkeit, Systemlogs an ein Analysesystem zu senden, zum größten Teil bereits mit.

Da die Möglichkeiten, mit den Systemlogs eines Android Smartphones zu arbeiten, bereits gegeben sind, wird für die praktische Prüfung keine eigene Anwendung implementiert. Dies bietet die Möglichkeit, alle Ergebnisse mit einfachen Mitteln nachvollziehen zu können. Es entsteht jedoch der Nachteil, dass keine Versuche mit einer vollständigen Umsetzung des Konzeptes durchgeführt werden können.

Analysen über die Auswirkungen auf die Akkulaufzeit und Beobachtungen des Bandbreitenbedarfs in einem realen Szenario mit vielen Endgeräten können auf diese Weise nicht durchgeführt werden. Stattdessen wird ein tiefer Einblick in die Log-Daten von Androidsystemen gegeben.

4.1 Aufbau des Testsystems

Alle Tests wurden mit einem “Samsung Galaxy Nexus” durchgeführt. Auf diesem wird die Android Version 4.3 mit der Kernelversion 3.0.72 betrieben, wie in Abbildung 3 gezeigt. Dies entspricht dem aktuellen Patchlevel für diesen Gerätetyp.

Abbildung 3: Samsung Galaxy Nexus Systemdaten

Auf dem Gerät wird die Software NXLog (http://nxlog.org/) betrieben, die die Systemlogs an einen Syslog-Server bzw. ein SIEM-System senden kann. Diese Anwendung kann einfach über den Google Play Store installiert werden. Die Konfiguration der Anwendung erfolgt in Form einer XML-Konfigurationsdatei. In Abbildung 4 kann die verwendete Testkonfiguration eingesehen werden.

NXLog bietet dazu drei Funktionsklassen: Eingabe, Verarbeitung, Ausgabe. In den beiden Inputbereichen ist definiert, dass die Module im_internal und im_android zum Erfassen der Log-Daten verwendet werden sollen. Entsprechend der NXLog Dokumentation (siehe [Edi13]), fragt das im_android Modul die von Android zur Verfügung gestellten Systemlogs ab. Das Modul im_internal wird hauptsächlich zur Konfiguration und Fehlerbehebung benötigt, es erfasst die von NXLog selbst generierten Nachrichten.

Zur Verarbeitung dient die Konfigurationssektion “Processor”. Für diese wird zusätzlich das Modul xm_syslog als Erweiterung des Basisfunktionsumfanges eingesetzt. Dort wird die Log-Zeile in eine Syslognachricht gewandelt und das Feld, das den Hostnamen enthällt, überschrieben. Dies ist nötig, da Android als Hostname sonst immer “localhost” verwendet und eine spätere Unterscheidung mehrerer Geräte im SIEM-System nicht mehr möglich wäre. In der Praxis wäre dieses Vorgehen umständlich und sollte

auf andere Art und Weise gelöst werden. Bei einem Versuchsaufbau entsteht so eine maximale Flexibilität für die Wahl der Identifikationskriterien. Abschließend wird die Funktion "to_syslog_bsd()" erneut aufgerufen um die Daten, inklusive dem geänderten Hostnamen, zu einer standardkonformen Syslog Log-Zeile zu formatieren.

In der Outputsektion der Konfiguration ist das empfangende System definiert. In diesem Fall werden die Log-Daten per TCP an Port 1514 des SIEM-Systems gesendet. NXLog bietet auch noch weitere Ausgabemöglichkeiten an. Dies sind zum Beispiel Eintragungen in Datenbanken, Weitergabe der Log-Zeilen an externe Kommandos, Übertragung per UDP, verschlüsselte Übertragung per SSL. Eine vollständige Aufzählung kann in [Edi13] eingesehen werden.

Die Route-Sektion verknüpft abschließend die drei Funktionsklassen. Hier werden die Eingabedaten mit einem oder auch mehreren Prozessoren verknüpft und anschließend an ein Ausgabemodul weitergegeben. So können beispielsweise die Quellen an verschiedene Ziele gesendet werden oder ein Pufferspeicher (diese werden als Prozessormodul behandelt) definiert werden.

NXLog könnte auch die Logs des Kernels auswerten. Dies erfordert jedoch Root-Rechte auf dem Smartphone. Daher wird davon im Rahmen dieser Versuche abgesehen, da Unternehmen in der Regel keine derart manipulierten Geräte betreiben möchten. Für das Erfassen und Versenden der anderen Log-Daten werden lediglich die Berechtigungen aus Abbildung 5 benötigt.

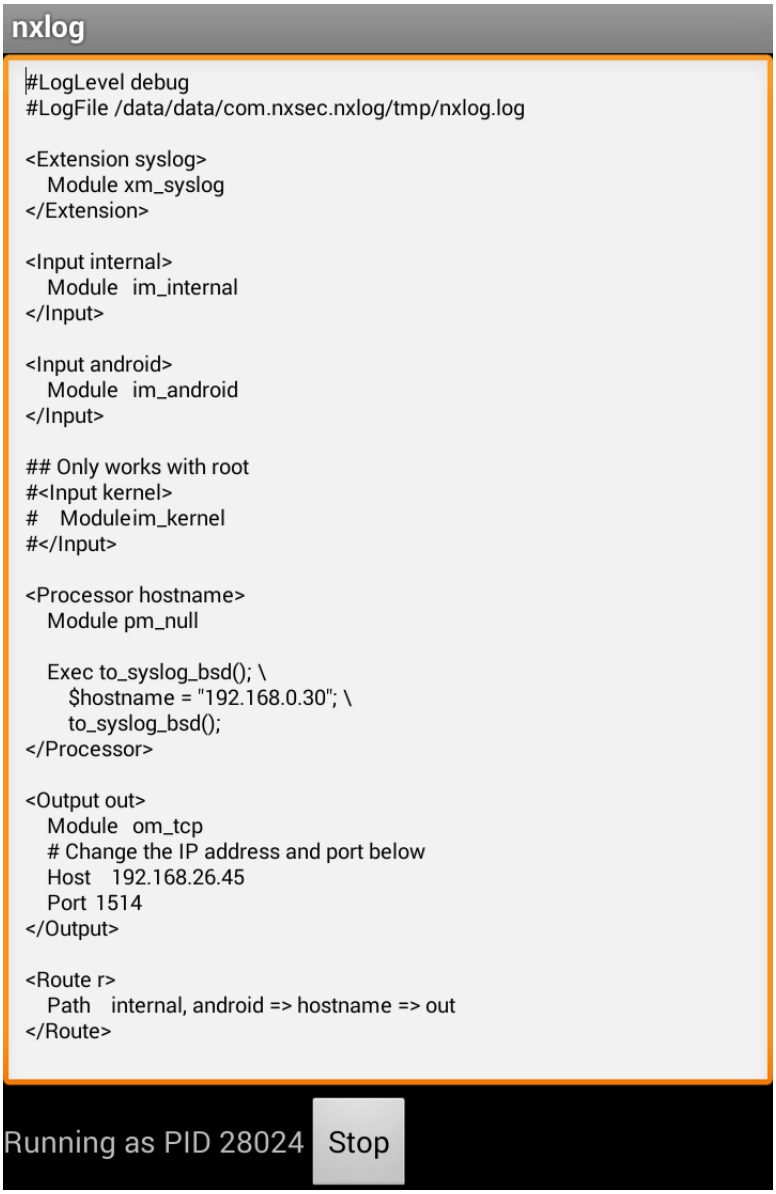

Abbildung 4: NXLog Konfiguration

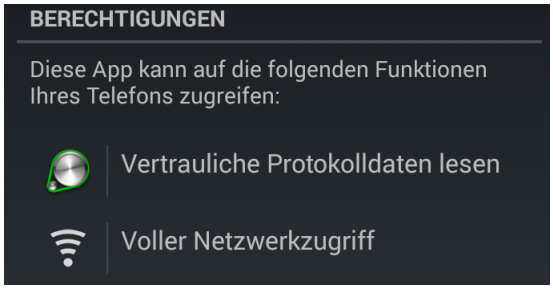

Abbildung 5: Rechte NXLog

Auf dem Zielsystem wird zur Auswertung und zum Log-Empfang ein Debian Squeeze (Version 6.0.7) betrieben. Darauf arbeitet die SIEM-Software Splunk (`http://de.splunk.com/`) und nimmt die Daten entgegen.

Splunk unterstützt die Einrichtung verschiedener Datenquellen, die aus der Perspektive des mobilen Endgeräts als Ziele verwendet werden können. Die Splunk-Konfiguration für diesen Versuchsaufbau ist in Abbildung 6 dargestellt.

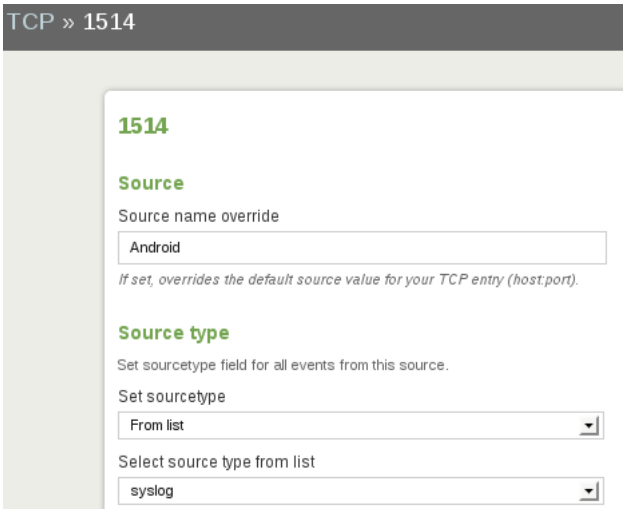

Abbildung 6: Splunk Datenquelle

4.1.1 Logging auf Androidgeräten

Im erklärten Aufbau für die Überprüfung des Konzeptes werden die Log-Daten des Galaxy Nexus mit der Anwendung NXLog an das SIEM-System gesendet. NXLog bedient sich dabei eines Input-Moduls für die Erfassung der Log-Daten. Die spezifische Funktionalität des Input-Moduls konnte leider nicht eingesehen werden. Im Hintergrund werden

die Log-Daten jedoch von Android in Form von Pufferspeichern verwaltet. Diese bieten eine einheitliche Schnittstelle, das Tool LogCat, zum Abfragen der Log-Daten.

In der Dokumentation heisst es: “Im Android Logging-System werden mehrere zirkulierende Pufferspeicher gehalten” (Übersetzt aus [Docb]). Diese Pufferspeicher können alle mit LogCat ausgelsen werden. Damit gibt es auf den Android Geräten zwei Möglichkeiten die Log-Daten zu lesen.

Die erste Möglichkeit ist die Verwendung von LogCat. Um LogCat auf dem System auszuführen kann beispielsweise die Android Debug Bridge (ADB) verwendet werden (siehe [Doca]). Die ADB erlaubt es, Befehle direkt auf dem Zielgerät auszuführen. Ein Beispiel für den Einsatz von LogCat mit der ADB, ist in Abbildung 7 zu sehen. Neben den ersten fünf Einträgen im Pufferspeicher wird in der Abbildung zusätzlich die Größe des Haupt- und des System-Log-Pufferspeichers angezeigt. Durch den Parameter “-b” wird definiert, dass nur der Haupt-Pufferspeicher gelesen wird. Dies ist gleichermaßen für die anderen Pufferspeicher möglich.

```
[redacted]:~/Android/platform-tools$ ./adb logcat -g
/dev/log/main: ring buffer is 256Kb (255Kb consumed), max entry is 5120b, max payload is 4076b
/dev/log/system: ring buffer is 256Kb (255Kb consumed), max entry is 5120b, max payload is 4076b
[redacted]:~/Android/platform-tools$ ./adb logcat -b main | head -n 5
D/n.h.a.w.r.ClockRenderer( 1519): scale=2.0,spad=4.0
D/dalvikvm(  675): GC_FOR_ALLOC freed 1371K, 27% free 14211K/19292K, paused 29ms, total 29ms
D/dalvikvm( 1519): GC_FOR_ALLOC freed 472K, 6% free 11114K/11808K, paused 20ms, total 20ms
D/GCM     (  713): Ignoring attempt to send heartbeat on dead connection.
D/n.h.a.w.r.ClockRenderer( 1519): scale=2.0,spad=4.0
[redacted]:~/Android/platform-tools$
```

Abbildung 7: Android Logs mit LogCat

Die Pufferspeicher können im Dateisystem des Gerätes im Verzeichnis /dev/log gefunden werden. Insgesamt gibt es dort vier Speicher, die in der Standardeinstellung alle auf die Maximalgröße 256Kb festgelegt sind. Eine Liste ist in Abbildung 8 zu sehen.

Dort ist ebenfalls ersichtlich, dass die gelisteten Dateien nicht der genannten Puffergröße entsprechen. Dieses Verhalten kommt dadurch zustande, dass es sich um typische Unix Gerätedateien handelt. “Gerätedateien (engl. device files) sind im Dateisystem unterhalb von /dev untergebrachte Dateien, die eine Hardwarekomponente repräsentieren. Dabei kann eine solche Hardwarekomponente entweder real vorhanden oder nur virtueller Natur sein” ([PW08]).

```
shell@maguro:/dev/log $ ls -l
crw-rw-rw- root     log       10,  42 2013-08-07 21:30 events
crw-rw-rw- root     log       10,  43 2013-08-07 21:30 main
crw-rw-rw- root     log       10,  41 2013-08-07 21:30 radio
crw-rw-rw- root     log       10,  40 2013-08-07 21:30 system
shell@maguro:/dev/log $
```

Abbildung 8: Android Log Puffer

Die zweite Möglichkeit die Log-Daten zu erhalten ist das Auslesen der rohen Log-Daten aus den Pufferspeichern. Über einen direkten Zugriff auf das System mit der ADB ist dieses Vorgehen sehr unkomfortabel, da die Log-Daten in den Pufferspeichern in einer binären Form abgelegt werden und nicht darstellbare Zeichen beinhalten. Ein Programm wie NXLog oder eine eigene SIEM-Lösung könnte die Daten jedoch auch auf diese Weise weiter verarbeiten. Ein Beispiel zeigt Abbildung 9.

```
shell@maguro:/dev/log $ dd if=main count=5
Tamem
R  alvikvmGC_CONCURRENT freed 405K, 6% free 9356K/9908K, paused 3ms+3ms, total 26msTamem
R x alvikvmGC_CONCURRENT freed 371K, 6% free 9372K/9908K, paused 4ms+3ms, total 24msTamem
R  N alvikvmGC_CONCURRENT freed 404K, 6% free 9356K/9908K, paused 3ms+3ms, total 27msTamem
R x alvikvmGC_CONCURRENT freed 371K, 6% free 9372K/9908K, paused 4ms+3ms, total 22msTamem
Rg  alvikvmGC_CONCURRENT freed 403K, 6% free 9356K/9908K, paused 2ms+2ms, total 23ms0+5 records in
1+1 records out
520 bytes transferred in 0.001 secs (520000 bytes/sec)
```

Abbildung 9: Android Logs mit dd

Auf der Basis dieser Erkenntnisse ist es möglich eigene Entwicklungen für eine Software zur Sammlung der Log-Daten zu realisieren. Für das Lesen der Log-Daten wird die Berechtigung “android.permission.READ_LOGS” benötigt. Eine Ausnahme ist die Androidversion 4.1, die das Lesen der Logs auf die Daten der jeweiligen Anwendung beschränkt.

Mit einem Samsung Galaxy S3 und installiertem Android 4.1 konnte dieses Verhalten reproduziert werden. Das Galaxy Nexus mit Android 4.3 weist diese Eigenheit nicht auf.

4.2 Erläuterung der Datenbasis

Werden die Log-Daten erfasst und ausgewertet wird ersichtlich, dass die Datenmenge umfangreich ist und eine Vielzahl von Informationen enthällt. Im folgenden werden einige Rahmeninformationen zu den gesammelten Daten gegeben.

Die Anzahl der Einträge im Log variiert sehr stark, je nach Intensität der Benutzung. Der Höchstwert lag im Laufe der Tests bei 88367 Zeilen an einem Tag. Im Verlaufe

einer Woche, die sowohl Tage mit sehr aktiver Nutzung als auch Tage mit schwächerer Benutzung enthielt, wurde eine durchschnittliche Zeilenanzahl von 16354,14 pro Tag gemessen.

4.2.1 Prioritäten der Log-Daten

Die Prioritäten der Log-Daten sind, wie in Abbildung 10 gezeigt, verteilt. Die Daten stammen von zwei exemplarisch gewählten, sehr aktiven Tagen. Bei Tagen ohne starke Aktivität verändert sich die Abstufung kaum, lediglich die niedrigste Priorität (höchster numerischer Wert) 15, sinkt dann auf ein Minimum.

Abbildung 10: Verteilung der Log-Prioritäten

Die numerische Staffelung der Prioritäten stammt dabei von der Syslog-Konvertierung der Daten durch NXLog. Sie korrelieren mit den Kritikalitätswerten aus [Docb] und werden lediglich in eine nummerische Entsprechung geändert. Tabelle 13 gibt eine Übersicht.

NXlog	Android
<15>	Verbose
<14>	Debug
<13>	Info
<12>	Warning
<11>	Error
<10>	Fatal

Tabelle 13: NXLog und Android Log-Prioritäten

Dieses Ergebnis zeigt, dass die in Abschnitt 3.2.3 entwickelte Idee zur Wahl des Übertragungszeitpunktes auf Androidgeräten umgesetzt werden könnte. Es ist möglich während Bandbreitenengpässen die niedrig priorisierten Ereignisse zurückzuhalten um damit

Datenvolumen zu sparen. Im geschilderten Beispiel sind 86,33% der Log-Daten den beiden niedrigsten Prioritätskategorien zugeordnet und könnten verzögert gesendet werden, wenn es nötig ist.

4.2.2 Zählen häufig auftretender Zeilen

Das in Abschnitt 3.2.4 beschriebene Prinzip zur Datenreduktion durch Reduzierung häufig auftretender Zeilen auf ihre Anzahl soll im Folgenden praktisch überprüft werden. Dazu werden die zwei gleichen Referenztage wie im vorherigen Abschnitt verwendet. Ziel ist es einige Prozesse auf die Anzahl ihrer Events zu reduzieren um weitere Bandbreite und Speicherplatz zu sparen.

Zur Feststellung welche Prozesse bei einer Reduzierung die größte Datenersparnis bringen ist in Abbildung 11 dargestellt welche Prozesse die meisten Log-Zeilen produzieren.

Top 10 values	#	%
RILJ	10,202	12.641%
dalvikvm	9,743	12.073%
use-Rlog/RLOG-RIL(s)	8,331	10.323%
DCT	7,791	9.654%
PHONE	3,737	4.63%
am_create_service	3,253	4.031%
am_destroy_service	3,223	3.994%
GsmSST	3,031	3.756%
DC-1	2,838	3.516%
ActivityManager	2,374	2.942%

Abbildung 11: Verteilung der Log-Zeilen auf die Prozesse

Die größte Anzahl an Log-Zeilen produziert der Prozess RILJ. Diese Zeilen enthalten Meldungen, die von der Java-Abstraktionsebene des "Radio Interface Layer" (siehe [Pro]) von Android stammen. Diese Meldungen enthalten, wie später noch gezeigt wird, wichtige Informationen für die Erkennung eines Diallers in den Log-Daten (siehe Abschnitt 4.3.1).

Die folgenden vier Prozesse, die eine Menge von 36,68% der betrachteten Log-Daten ausmachen, enthalten jedoch für die weiteren Versuche keine Relevanz. Für den praktischen Einsatz ist eine kontinuierliche Auditierung der Zusammenfassung von Log-Daten durch Zählen unausweichlich.

Zur Durchführung der Versuche wurde ein Perl-Programm erstellt. Die durch die Prozesse generierten Ereignisse werden innerhalb eines gegebenen Zeitraumes gezählt und am

Ende des Zeitraumes je eine Log-Zeile pro Prozess mit der Anzahl ausgegeben. Diese erhalten eine willkürliche Priorität mit dem Wert 20 die nicht von Android verwendet wird. Dadurch lassen sich die Log-Zeilen leicht auffinden.

In Tabelle 14 ist gezeigt, wie sich der jeweilige Zählzeitraum auf die Anzahl der Log-Zeilen und damit auf Speicher und Bandbreite auswirkt. Die Anzahl der Log-Zeilen vor der Zusammenfassung beträgt 80093 Zeilen.

Zählzeitraum in Minuten	Zeilenanzahl	Ersparnis
90	50713	36,68 %
60	50765	36,62 %
45	50817	36,55 %
30	50925	36,42 %
15	51189	36,09 %
10	51417	35,80 %
5	52085	34,97 %

Tabelle 14: Verhältnis Zählzeitraum zu Log-Zeilenanzahl

In Abbildung 12 wird sichtbar, in welchem Zeitraum die Steigerung der Ersparnis am größten ist. Da die Genauigkeit bei Auswertungen besser ist wenn der Zählzeitraum möglichst klein gewählt ist, empfielht sich ein Zählzeitraum von 30 Minuten. Wird der Zeitraum größer gewählt, ist die Steigerung der Zeilenersparnis nur noch minimal. Von 30 zu 90 Minuten steigt sie nur um 0,26%. Wird der Zeitraum kleiner, gewählt sinkt die Ersparnis. Von 30 zu 15 Minuten sinkt sie um 0,33%, danach sinkt sie noch schneller.

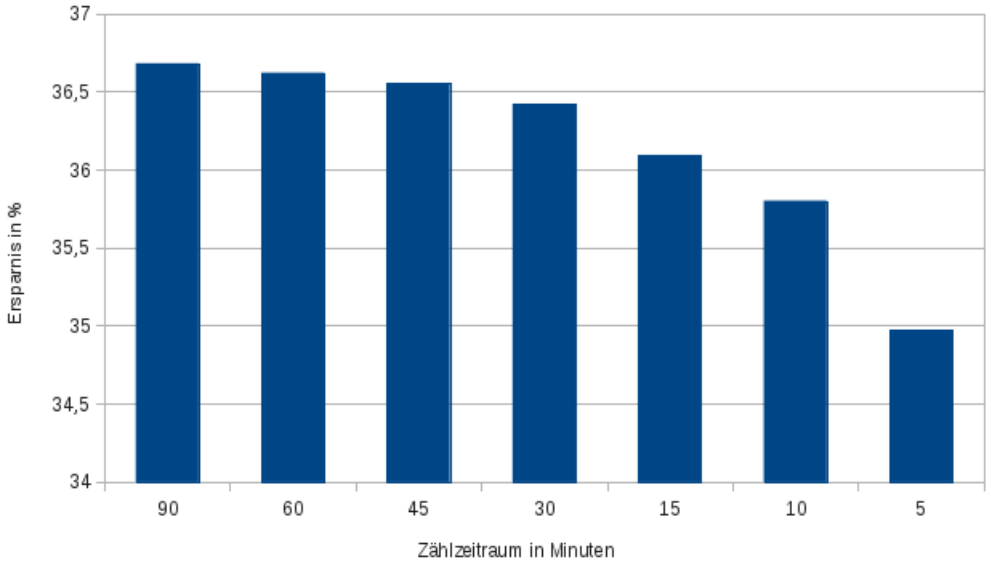

Abbildung 12: Ersparnis je Zeitraum

4.2.3 Einige einfache Operationen

Im folgenden werden drei typische Vorgänge mit einem mobilen Endgerät anhand der Log-Daten gezeigt. Das Senden einer SMS, ein Telefonanruf und das Erstellen einer Fotografie.

Das Senden einer SMS ist leicht in den Log-Daten festzustellen. Der bereits in Abschnitt 4.2.2 erwähnte Radio Interface Layer vermerkt den Vorgang im Log mit zwei Zeilen. Eine Zeile markiert den Vorgang "SMS zum Senden an den RIL gegeben", die andere enthält den Rückgabewert des RIL. In Abbildung 13 sind die Log-Daten, die beim Senden einer SMS entstehen, abgebildet.

```
<15>Aug 15 00:02:13 192.168.0.30 RILJ[651]: [30943]< SEND_SMS { mMessageRef = 2,
 mErrorCode = 0, mAckPdu = null}
<15>Aug 15 00:02:11 192.168.0.30 RILJ[651]: [30943]> SEND_SMS
```

Abbildung 13: Senden einer SMS

Ein Telefonanruf ist ebenfalls deutlich in den Log-Daten erkennbar. Anhand des Prozesses "PhoneUtils" können im Log die getätigten und empfangenen Anrufe nachvollzogen werden. Dies ist möglich, da der PhoneUtils-Prozess die Aktionen "placeCall", "answerCall" und "hangup" protokolliert.

Die Funktion “placeCall” wird immer aufgerufen, wenn eine Nummer angerufen wird und ist unabhängig von einer Antwort der Gegenstelle. Die Funktion “answerCall” wird nur bei einer vollständigen Verbindung ausgeführt, sie zeigt daher keine verpassten Anrufe. Die Funktion “hangup” wird beim Auflegen jeweils zwei Mal im Log geführt. Einmal mit der Nachricht welcher Anruf beendet wird und ein zweites Mal mit der Nachricht ob das Auflegen regulär durchgeführt wurde.

Einige Beispiele sind in Abbildung 14 zu sehen. Von unten nach oben gelesen sind drei Anrufe abgebildet. Ein von der Gegenstelle angenommener Anruf, ein eingehender Anruf und ein Anruf, der von der Gegenstelle nicht angenommen wurde. Die Telefonnummern in den Zeilen, die einen placeCall Aufruf enthalten, wurden bereits von Android mit X überschrieben.

```
<15>Aug 17 22:22:10 192.168.0.30 PhoneUtils[651]: - hangup(Call): regular hangup()...
<15>Aug 17 22:22:10 192.168.0.30 PhoneUtils[651]: hangup(): hanging up foreground call
<15>Aug 17 22:22:03 192.168.0.30 PhoneUtils[651]: placeCall()... number: xxxxxxxxxxxxxx,
    GW: null, emergency? false
<15>Aug 17 22:22:03 192.168.0.30 PhoneUtils[651]: checkAndCopyPhoneProviderExtras: some
    or all extras are missing.
<15>Aug 17 22:22:03 192.168.0.30 PhoneUtils[651]: checkAndCopyPhoneProviderExtras: some
    or all extras are missing.
<15>Aug 17 22:17:45 192.168.0.30 PhoneUtils[651]: - hangup(Call): regular hangup()...
<15>Aug 17 22:17:45 192.168.0.30 PhoneUtils[651]: hangup(): hanging up foreground call
<15>Aug 17 22:17:41 192.168.0.30 PhoneUtils[651]: answerCall(INCOMING)...
<15>Aug 17 22:12:26 192.168.0.30 PhoneUtils[651]: - hangup(Call): regular hangup()...
<15>Aug 17 22:12:26 192.168.0.30 PhoneUtils[651]: hangup(): hanging up foreground call
<15>Aug 17 22:12:11 192.168.0.30 PhoneUtils[651]: placeCall()... number: xxxxxxxxxxxx,
    GW: null, emergency? false
<15>Aug 17 22:12:11 192.168.0.30 PhoneUtils[651]: checkAndCopyPhoneProviderExtras: some
    or all extras are missing.
<15>Aug 17 22:12:11 192.168.0.30 PhoneUtils[651]: checkAndCopyPhoneProviderExtras: some
    or all extras are missing.
```

Abbildung 14: Anrufablauf im Log

Die Verwendung der integrierten Kamera soll in einem dritten Fall in diesem Abschnitt gezeigt werden. Das Aktivieren der Kamera lässt sich sehr einfach durch das Starten der integrierten Fotografie-App erreichen. Dies löst sehr viele Ereignisse aus, die ins Log geschrieben werden. Der Auszug in Abbildung 15 wurde daher etwas gekürzt. Übersprungene Teile sind mit drei Punkten in eckigen Klammern gekennzeichnet.

Da die Fotografie-App gestartet wird ist die erste Meldung (ganz unten), die des ActivityManager über den Start der App. Die drei folgenden Einträge zeigen die Aktivierung der Kamera. Die Reihenfolge korreliert dabei mit der Hierarchiedarstellung aus [Docc]. Die letzte Ebene vor dem Kernelspace ist der CameraHAL (Hardware Abstraction Layer). “Der Hardware Abstraction Layer definiert das Standard-Interface, das der

Kamera Dienst verwendet und das implementiert sein muss, damit die Kamera korrekt funktioniert" (Übersetzt aus [Docc]).

Nach dem Aktivieren der Kamera wird geprüft ob der Speicherplatz für das Ablegen von Fotografien in das System eingebunden ist und die Vorschau wird aktiviert. Die beiden letzten Schritte zeigen das Beenden der Fotografie-App und das Deaktivieren der Kamera.

```
<14>Aug 17 22:46:23 192.168.0.30 CameraClient[127]: Destroying camera 0
<11>Aug 17 22:46:23 192.168.0.30 CameraHAL[127]: Adapter state switch PREVIE
    W_ACTIVE Invalid Op! event = 0xf
[...]
<15>Aug 17 22:46:10 192.168.0.30 PhotoView[25250]: compensation = 0, CameraR
    elativeFrame = Rect(0, 0 - 0, 0), mCameraRect = Rect(0, 0 - 0, 0)
<15>Aug 17 22:46:10 192.168.0.30 CameraStorage[25250]: External storage stat
    e=mounted
[...]
<14>Aug 17 22:46:09 192.168.0.30 CameraHAL[127]: camera_device open
<14>Aug 17 22:46:09 192.168.0.30 CameraClient[127]: Opening camera 0
<15>Aug 17 22:46:09 192.168.0.30 CameraHolder[25250]: open camera 0
[...]
<14>Aug 17 22:46:09 192.168.0.30 ActivityManager[373]: START u0 {act=android
    .intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x1020000
    0 cmp=com.google.android.gallery3d/com.android.camera.Camera bnds=[424,1
    040][552,1168]} from pid 675
```

Abbildung 15: Erstellen eines Fotos

4.3 Anwendung von Korrelationsszenarien

Ein grundlegendes Verständnis der Log-Daten eines Androidgerätes ist nun gegeben. Ziel dieser Arbeit ist es jedoch, die Verwendung der Log-Daten in einem SIEM-System näher zu analysieren. Wie einleitend zum praktischen Teil erwähnt, wird als SIEM-Lösung die Software Splunk eingesetzt. Splunk dient dabei nicht nur für den Empfang und die Darstellung der Log-Daten.

In Splunk wird die Erstellung von Alarmmeldungen auf vielfältige Weise unterstützt. Eine Übersicht gibt [Docd]. Insbesondere kann Splunk verschiedene Aktionen durchführen, die beim Auftreten eines Alarms ausgeführt werden. Darunter befinden sich einfache Aktionen, wie das Abbilden der Alarmmeldung im integrierten Alarm-Manager oder das Senden einer E-Mail. Es ist weiterhin möglich, eigene Scripte auszuführen (siehe [Doce]).

Dies ermöglicht es automatisch und völlig flexibel auf erkannte Bedrohungen zu reagieren. Damit ist es möglich die Schutzmaßnahmen aus der Risikobesprechung in Abschnitt 3.4 umzusetzen. Im Rahmen dieses Beispiels werden jedoch lediglich einfache Alarmmeldungen generiert.

4.3.1 Erkennen eines Diallers

Nach der Beschreibung der ENISA in Abschnitt 2.4.8 verwendet ein Dialler Premium SMS Dienste oder Telefonnummern um dem Besitzer eines Smartphone Geld zu stehlen. In den Log-Daten werden Nummern, an die SMS gesendet oder die angerufen wurden, nicht geführt und können daher nicht überwacht werden.

Es ist jedoch möglich, die Häufigkeit mit der Anrufe getätigt oder SMS versendet werden auf Anomalien zu überwachen. Um dies mit Splunk zu ermöglichen, muss zuerst geklärt werden, wie eine Liste mit gesendeten SMS generiert werden kann. Für das Senden von SMS wurden in Abschnitt 4.2.3 bereits zwei charakteristische Log-Zeilen gezeigt.

Für eine Erkennung genügt eine Zeile. Da generell das Senden für die Erkennung eines Diallers interessanter ist als der Rückgabewert der Abstraktionsebene, werden für die Generierung einer Alarmmeldung Zeilen in der folgenden Form ausgewertet:

```
<15>Aug 15 00:02:11 192.168.0.30 RILJ[651]: [30943]> SEND_SMS
```

```
<15>Aug 12 15:57:42 192.168.0.30 RILJ[651]: [17724]> SEND_SMS
```

Klare Gemeinsamkeit dieser Zeilen ist der Prozessname “RILJ” und die Zeichenfolge “> SEND_SMS”. Nach diesen kann die Log-Datenbasis einfach durchsucht werden. In Splunk ermöglicht dies die folgende Suchanfrage:

```
source="Android" "RILJ'' ‘‘> SEND_SMS"
```

Mit dieser Abfrage kann bereits eine Liste aller gesendeten SMS erzeugt werden. Betrifft dies eine Vielzahl von Geräten soll die Anzahl der gesendeten SMS je Gerät in einem bestimmten Zeitraum ermittelt werden.

Die Festlegung des Zeitraumes erfolgt in Splunk über ein einfaches Menü, das sich rechts neben dem Suchfeld befindet. Die Anzahl der SMS je Gerät in diesem Zeitraum erfordert eine weitere Verarbeitung des Suchergebnisses. Mit Hilfe des Pipe-Symbols (ein senkrechter Strich “|”), kann das Ergebnis einer Abfrage an einen weiteren Befehl übergeben werden.

Damit lässt sich die Abfrage wie folgt erweitern, um eine Übersicht der gesendeten SMS je Gerät zu erstellen:

```
source="Android" "RILJ'' ‘‘> SEND_SMS" | stats count by host
```

Ein Ergebnis könnte etwa wie in Abbildung 16 aussehen.

	host ⇕	count ⇕
1	192.168.0.30	3
2	localhost	1

Abbildung 16: Gesendete SMS je Host

Ein Alarm, der bereits auf einzelnen SMS reagiert, ist nicht sinnvoll wenn die Abfrage zur Detektion eines Diallers verwendet werden soll. Die Abfrage kann jedoch noch weiter eingeschränkt werden. Mit dem "search" Befehl von Splunk ist es möglich eine Bedingung für die Anzahl zu definieren. Die Suche lautet dann wie folgt:

```
source="Android" "RILJ'' ‘‘> SEND_SMS" | stats count by host | search count
> X
```

Das "X" am Ende der Abfrage muss, je nach Einsatzgebiet des Smartphones und des gewählten Zeitraums durch einen Wert ersetzt werden, der eine ungewöhnliche Menge SMS repräsentiert. Das Ergebnis der Abfrage kann für eine automatische Alarmmeldung verwendet werden.

Zu Testzwecken wird der überwachte Zeitraum auf eine Stunde eingestellt und X auf 1 gesetzt. Den zugehörigen Dialog zur Erstellung des Alarms zeigt Abbildung 17. Die Angabe, dass die Alarmmeldung generiert wird sobald mehr als 0 Zeilen auftreten ist kein Fehler, da der Schwellwert für ungewöhnliches Verhalten bereits in der Abfrage durch X definiert wird.

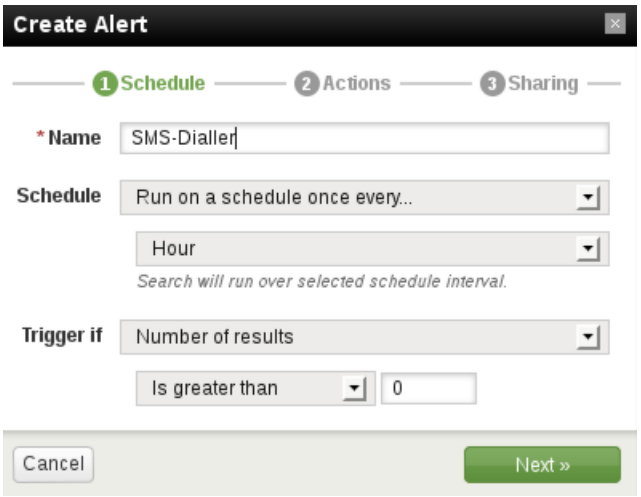

Abbildung 17: Erstellen eines Alarms für ungewöhnliche SMS-Häufung

Die Überwachung auf eine ungewöhnliche Häufung von Telefonanrufen erfolgt analog dazu. Die Abfrage auf die zu zählenden Log-Zeilen muss dazu wie folgt angepasst werden:

```
source="Android" "PhoneUtils" "placeCall()" | stats count by host |
search count > X
```

Ein Beispiel für eine generierte Alarmmeldung zeigt Abbildung 18.

Abbildung 18: Beispiel Dialler Alarmmeldung

Wird in der Ansicht auf "View results" geclickt, öffnet sich ein Abfragefenster mit den für diesen Alarm relevanten Ereignissen. Dies wird in Abbildung 19 dargestellt.

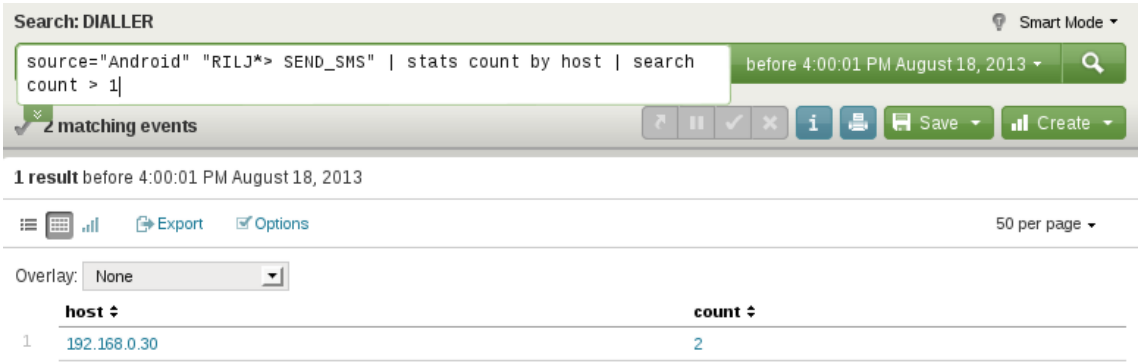

Abbildung 19: Ereignisse Dialler Alarmmeldung

4.3.2 Erkennen von Überwachung

Eine Überwachung des Benutzers durch eine Schadsoftware könnte zum Beispiel dadurch zu erkennen sein, dass die Kamera des Telefons aktiviert wird, während das Gerät nicht in Benutzung ist. Wie bereits in Abschnitt 4.2.3, in den Erklärungen zu einigen Basisoperationen gezeigt wird, wird die Kamera auf der hardwarenächsten Abstraktionsebene durch den Prozess "CameraHAL" gestartet.

Im Falle der Erkennung einer Überwachung ist dieses Ereignis jedoch noch nicht ausreichend. Wird die Kamera aktiviert kann dies aus dem einfachen Grund geschehen,

dass ein Foto aufgenommen werden soll. Anders als bei den SMS ist auch die Anzahl der Aktivierungen nur eingeschränkt aussagekräftig, da eine Überwachung nur ein einziges Aktivieren der Kamera erfordert, um über einen längeren Zeitraum Bildmaterial zu erfassen.

Ein Hinweis auf eine Überwachung entsteht jedoch wenn die Kamera aktiviert wird während das Android System gerade inaktiv ist. Dazu muss eine Abfrage erstellt werden, die auf ein Ereignis zwischen zwei anderen Ereignissen wartet. In Splunk ist dies mit Transaktionen möglich. Zu berücksichtigen ist, wie beim vorherigen Abschnitt über die Erkennung eines Diallers, dass die Transaktionen auf einen Host beschränkt sein müssen. Diese Gruppierung lässt sich bei Transaktionen durch Angabe des Feldnamens als Parameter erreichen.

Eine Abfrage auf alle Ereignisse, die zwischen dem Deaktivieren und dem Aktivieren eines Android Smartphones liegen, kann wie folgt formuliert werden:

```
source="Android" | transaction host startswith="Going to sleep"
endswith="Waking up from sleep"
```

Die Nachrichten “Going to sleep” und “Waking up from sleep” sind Informationen des PowerManagerService und tauchen in dieser Form in den Log-Daten des Galaxy Nexus auf. Die erfassten Transaktionen können nun in einem nächsten Schritt weiter gefiltert werden, indem nach der Kameraaktivierung gesucht wird. Die Abfrage wird dazu mit einer Suche erweitert:

```
source="Android" | transaction endswith="Waking up from sleep"
startswith="Going to sleep" | search "CameraHAL" "camera_device open"
```

Dies führt auf dem Testsystem zu einem leeren Ergebnis. Die Abfrage soll jedoch getestet und ihre Funktionsfähigkeit demonstriert werden. Dazu wird erneut die Android Debug Bridge verwendet. Mit dieser können vom PC aus Prozesse auf dem Androidsystem gestartet werden. Mit dem folgenden Aufruf wird die Kamera aktiviert ohne das Gerät aus dem Ruhezustand zu wecken oder das Display zu entsperren:

```
./adb shell "am start -a android.media.action.IMAGE_CAPTURE"
```

Mit weiteren Befehlen könnte auch eine Aufnahme erstellt werden. Dies ist für diesen Versuch jedoch nicht nötig. Wird jetzt die gezeigt Abfrage in Splunk ausgeführt, wird das Ergebnis aus Abbildung 20 zurückgeliefert.

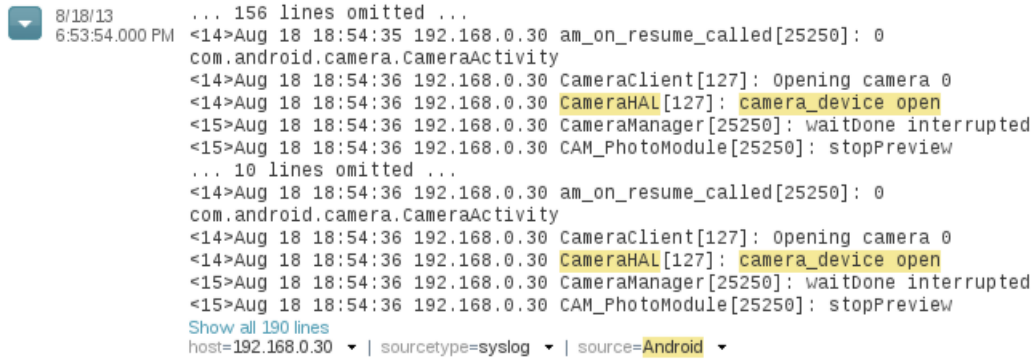

Abbildung 20: Kamera Aktivierung während Inaktivität

Auch aus dieser Abfrage kann eine Alarmmeldung generiert werden. Das Ergebnis zeigt Abbildung 21.

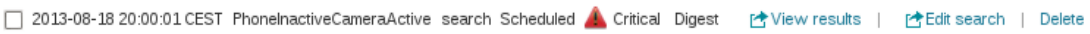

Abbildung 21: Alarmmeldung bei Kameraaktivierung

Dort führt ein Click auf “View results” ebenfalls zur Ansicht der Ergebnisse. Die Darstellung ist vergleichbar mit der in Abbildung 20.

5 Fazit

Zu Beginn dieser Arbeit wurden drei Fragen gestellt. Eine vierte Frage war diesen drei Fragen als Leitfrage vorangestellt. Die erste Frage war: “Wie kann eine sinnvolle Log-Datenverwaltung auf einem mobilen Endgerät umgesetzt werden?”. Hierzu wurden im Rahmen der Arbeit mehrere Ideen konzeptuell entwickelt und praktisch geprüft.

Diese machen es möglich Log-Daten sicher und effizient auf mobilen Endgeräten abzulegen und optimieren die Übertragung an ein zentrales SIEM-System. Im Rahmen der praktischen Prüfung konnte für das Betriebssystem Android festgestellt werden, dass die Logging-Mechanismen bereits ausgereift sind und gut funktionieren. Eine sinnvolle Log-Datenverwaltung ist in diesem Fall nicht nur möglich, sondern sollte auch einfach realisierbar sein.

Die zweite Frage war, ob und wie sich die Risiken für mobile Endgeräte mithilfe einer SIEM-Integration minimieren lassen. Die Risiken, die die ENISA als größte Bedrohungen für mobile Endgeräte identifizieret hat, wurden im Rahmen dieser Arbeit analysiert und Erkennungs- und Schutzmöglichkeiten im Rahmen des Konzeptes besprochen.

Im Rahmen der praktischen Überprüfung von zwei Beispielen verblüfften die Möglichkeiten, die Android hier bereits mit einfachen Bordmitteln bietet. Es ist sehr wahrscheinlich, dass auch für die anderen genannten oder neu entstehende Risiken mit den Möglichkeiten einer SIEM-Lösung Schutz- und Erkennungsmöglichkeiten entwickelt werden können.

Hilfreich waren dabei auch die vielfältigen Möglichkeiten mit der SIEM-Software Splunk Abfragen auszuführen, um so die Datenbasis zu analysieren.

Die dritte Frage war: “Ist eine SIEM-Integration praktische umsetzbar?”. Nach den Tests mit Android kann diese Frage klar beantwortet werden. Eine SIEM-Integration ist nicht nur umsetzbar, sondern im Falle des Betriebssystems Android naheliegend. Für erste Tests ist hier lediglich eine App notwendig. Durch die bereits ausgereiften Möglichkeiten auf die Log-Daten zuzugreifen, sollte auch eine eigene SIEM-Software, die dann noch weitere Möglichkeiten bieten kann, problemlos umsetzbar sein.

Zum Abschluss sei auch noch die Leitfrage dieser Arbeit beantwortet. Ja, es ist sinnvoll mobile Endgeräte in eine SIEM-Software einzubinden. Durch die Möglichkeiten, die von den mobilen Endgeräten gewonnenen Daten mit denen des Gesamtsystems zu korrelieren, entstehen weitere Möglichkeiten Bedrohungen zu erkennen und die Ergebnisse der praktischen Konzeptprüfung könnten dadurch übertroffen werden.

6 Ausblick

An die Erkenntnisse dieser Arbeit kann auf vielfältige Weise angeknüpft werden. Insbesondere wurde das Konzept durch die praktische Überprüfung auf seine grundsätzliche Realisierbarkeit geprüft. In einem größeren Kontext, beispielsweise durch den Einsatz vieler Endgeräte in einem Unternehmen, können noch viele Versuche durchgeführt und Analysen sowie Verbesserungen des in dieser Arbeit geschilderten Konzeptes vorgenommen werden.

Eine weitere Motivation für weiterführende Forschung ist die Plattformvielfalt, die bei mobilen Endgeräten herrscht. Das Konzept wurde generell ohne Fokus auf eine bestimmte Plattform erstellt. Eine praktische Prüfung, wie sie im Rahmen dieser Arbeit für Android vorgenommen wurde, ist jedoch auch für andere mobile Plattformen, zum Beispiel iOS, möglich. Eine Insellösung für eine einzelne mobile Plattform bietet für Unternehmen kaum Anreize, da die Vielfalt mobiler Endgeräte groß ist.

Auch das Thema MDM kann noch näher analysiert werden als dies in dieser Arbeit geschehen ist. Insbesondere ist zu klären ob es möglich ist, durch eine MDM-Lösung die Erfassung der Log-Daten auf dem Gerät durchzuführen. Damit wäre es möglich, beide Ansätze zu vereinen und ein Unternehmen müsste nur eine Lösung unterstützen.

Die bereits genannte Vielfalt der mobilen Plattformen existiert letztlich nicht nur zwischen unterschiedlichen Betriebssystemen. Auch verschiedene Betriebssystemversionen und Softwarezusammenstellungen sorgen für - teilweise massive - Veränderungen in den Log-Daten. Ein plattformunabhängiges Konzept behält in dieser Schnelllebigkeit seine Gültigkeit. Die praktische Umsetzung bleibt ein andauernder Prozess, vergleichbar mit der Log-Analyse auf klassischen Arbeitsplatz- und Serversystemen.

Literatur

[BIT13] BITKOM: *Bring Your Own Device.* http://www.bitkom.org/60376.aspx?url=20130404_LF_BYOD_2013_v2.pdf&mode=0&b=Themen&bc=Themen%7cSicherheit+%26+Vertrauen%7cDatenschutz, 2013. [Online; Stand 11. August 2013].

[BSI06] *Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen.* Technischer Bericht, Bundesamt für Sicherheit in der Informationstechnik, 2006. [Online; Stand 17. März 2013].

[CS12] Anton Chuvakin und Kevin Schmidt: *Logging and Log Management the Authoritative Guide to Understand the Concepts Surrounding Logging and Log Management.* Syngress, Dezember 2012.

[Doca] Android Developer Documentation: *Android Debug Bridge.* http://developer.android.com/tools/help/adb.html. [Online; Stand 15. August 2013].

[Docb] Android Developer Documentation: *Reading and Writing Logs.* http://developer.android.com/tools/debugging/debugging-log.html. [Online; Stand 15. August 2013].

[Docc] Android Source Documentation: *Camera Version 1.* http://source.android.com/devices/camera.html. [Online; Stand 17. August 2013].

[Docd] Splunk Documentation: *About alerts.* http://docs.splunk.com/Documentation/Splunk/5.0.4/Alert/Aboutalerts. [Online; Stand 17. August 2013].

[Doce] Splunk Documentation: *Set up alert actions.* http://docs.splunk.com/Documentation/Splunk/5.0.4/Alert/Setupalertactions. [Online; Stand 17. August 2013].

[Edi13] NXLOG Community Edition: *Reference Manual for v2.5.1089.* http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.pdf, 2013. [Online; Stand 13. August 2013].

[F2B11] *Fail2Ban: FAQ German.* http://www.fail2ban.org/wiki/index.php?title=FAQ_german&oldid=4362, 2011. [Online; Stand 13. Juli 2013].

[FN09] Chris Fry und Martin Nystrom: *Security Monitoring.* O'Reilly, Sebastopol CA, Februar 2009.

[Fri10] Stephen Fried: *Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World.* Auerbach Publications, Juni 2010.

[Ger09] R. Gerhards: *RFC 5424 - The Syslog Protocol.* Technischer Bericht, IETF, März 2009. IETF Proposed Standard.

[GK12] Benjamin Gray und Christian Kane: *Market Overview: Cloud-Hosted Mobile Device Management Solutions And Managed Services.* `www.tekserve.com/business/media/business/forrester-cloud-mdm-market-overview-2012.pdf`, Januar 2012. [Online; Stand 30. Januar 2013].

[HD10] Giles Hogben und Marnix Dekker: *Smartphones: Information security risks, opportunities and recommendations for users.* Technischer Bericht, ENISA - European Network and Information Security Agency, 2010. [Online; Stand 30. Januar 2013].

[Hyp10] Mikko Hypponen: *Warning On Possible Android Mobile Trojans.* `http://www.f-secure.com/weblog/archives/00001852.html`, Januar 2010. [Online; Stand 11. Juni 2013].

[Köl13] Tobias Költzsch: *Android läuft auf 80 Prozent der Smartphones.* `http://www.golem.de/news/mobile-betriebssysteme-android-laeuft-auf-80-prozent-der-smartphones-1308-100854.html`, August 2013. [Online; Stand 13. August 2013].

[MHH+10] David R. Miller, Shon Harris, Allen Harper, Stephen Vandyke und Chris Blask: *Security Information and Event Management (SIEM) Implementation.* Mcgraw-Hill Professional, November 2010.

[MMS09] F. Miao, Y. Ma und J. Salowey: *RFC 5425 - Transport Layer Security (TLS) Transport Mapping for Syslog.* Technischer Bericht, IETF, März 2009. IETF Standards Track der Network Working Group.

[MW04] Ulrike Meyer und Susanne Wetzel: *A Man-in-the-Middle Attack on UMTS.* `http://www.cs.stevens.edu/~swetzel/publications/mim.pdf`, 2004. [Online; Stand 25. Juni 2013].

[Okm09] A. Okmianski: *RFC 5426 - Transmission of Syslog Messages over UDP.* Technischer Bericht, IETF, März 2009. IETF Standards Track der Network Working Group.

[Pro] Android Open Source Project: *Radio Layer Interface*. http://www.kandroid.org/online-pdk/guide/telephony.html. [Online; Stand 17. August 2013].

[PW08] Johannes Plötner und Steffen Wendzel: *Linux: Das distributionsunabhängige Handbuch*. Galileo Computing, 2. Auflage, 2008.

[Ran05] Marcus Ranum: *System Logging and Log Analysis*. http://ranum.com/security/computer_security/archives/logging-notes.pdf, 1999-2005. [Online; Stand 2. April 2013].

[Sch10] Ben Schwan: *Smart oder Sicher?* http://www.heise.de/tr/artikel/Smart-oder-sicher-1140545.html, November 2010. [Online; Stand 30. Januar 2013].

[Sch12] Winn Schwartau: *The BYOD Mobile Security Spectrum: A Taxonomy*. http://www.mobileactivedefense.com/wp-content/uploads/2010/10/The-BYOD-Mobile-Security-Spectrum-July_1_2012FINAL.pdf, Januar 2012. [Online; Stand 1. Februar 2013].

[SPL+08] Aubrey-Derrick Schmidt, Frank Peters, Florian Lamour, Christian Scheel, Seyit Ahmet Çamtepe und Sahin Albayrak: *Monitoring Smartphones for Anomaly Detection*. http://www.luisolis.com/seminario2011/papers/Monitoring%20Smartphones%20for%20Anomaly%20Detection.pdf, November 2008. [Online; Stand 30. Januar 2013].

[Str07] Daehyun Strobel: *IMSI Catcher*. http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf, Juli 2007. [Online; Stand 25. Juni 2013].

[Sul13] Bob Sullivan: *A shock in the dark: Flashlight app tracks your location*. http://redtape.nbcnews.com/_news/2013/01/16/16530607-a-shock-in-the-dark-flashlight-app-tracks-your-location, Januar 2013. [Online; Stand 11. Juni 2013].