SIEM-Ansätze zur Erhöhung der IT-Sicherheit auf Basis von IF-MAP

Prof. Dr. Kai-Oliver Detken[1] · Thomas Rossow[2] · Ralf Steuerwald[2]

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

[2]Hochschule Hannover, Ricklinger Stadtweg 120, D-30459 Hannover
thomas.rossow@hs-hannover.de, ralf.steuerwald@hs-hannover.de

Zusammenfassung

Die Bedrohung durch Cyberkriminalität in Deutschland wächst. Zu diesem Ergebnis kommt das Bundeskriminalamt (BKA) in seinem im September 2012 vorgestellten Lagebild Cybercrime. Zunehmend stehen auch deutsche Mittelstandunternehmen im Fokus von Angreifern, laut des Branchenverbandes BITKOM. Gerade in kleinen und mittelständischen Unternehmen (KMU) wird der zunehmenden Bedrohungslage immer noch nicht ausreichend Rechnung getragen. Dabei spielt der Trend zu stark zunehmender geschäftlicher Nutzung von Smartphones, Tablets und Netbooks eine wichtige Rolle. Es sind heute zwar Sicherheitssysteme wie Firewalls, Virenscanner, Spamfilter und VPN-Gateways häufig im Einsatz, arbeiten aber typischerweise isoliert voneinander. Viele Angriffe können jedoch nur durch die Kombination von Daten verschiedenster Systeme erkannt werden. Aber auch selbst wenn ein Angriff erkannt wird, erfolgen Gegenmaßnahmen oft zu spät und der Angreifer hat bereits den Betrieb wichtiger Systeme gestört oder sensible Informationen erlangt. Zudem findet eine kontinuierliche und proaktive Überwachung von IT-Systemen (Clients, Server, Netzwerkkomponenten, Firewall etc.) sowie der Vorgängen und Ereignissen im Netz meist nicht statt. Dies können aber sog. Security Information and Event Management (SIEM) Lösungen leisten, die in der Lage sind Meldungen und Warnungen einzelner Sicherheitskomponenten zusammenzuführen und auszuwerten. Allerdings sind diese Systeme heute oftmals sehr komplex, kostspielig und durchaus nicht fehlerfrei. Dieser Beitrag stellt daher einen SIEM-Ansatz aus dem Forschungsprojekt SIMU vor, der auf der Metadatenspezifikation IF-MAP der Trusted Computing Group (TCG) basiert und eine Datenkorrelation effektiver und einfacher umsetzen soll.

1 Einleitung

Security Information and Event Management (SIEM) Systeme bieten durch das Sammeln von Informationen und Ereignissen verschiedene Ansätze, um Bedrohungen zu erkennen und zu verhindern. So kann es beispielsweise eine organisatorische Policy (Richtlinie) geben, die besagt, dass Viren, die von extern oder intern im Netzwerk versendet werden können, nicht das Server-Netz, die DMZ oder das Internet erreichen dürfen. Dafür hat das Unternehmen folgende technische Maßnahmen getroffen:

- Anti-Viren-Software auf den Endsystemen
- Automatisches Patch-Management

- Proxy-basierte Virus-Walls
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)

Nun tritt der Fall auf, dass ein Virus sich über einen Gastzugang ins Netzwerk gelangt. Dadurch, dass der Virus SSL-verschlüsselte Kommunikation verwendet, ist er durch die Proxy-Systeme und die Virus-Wall allerdings nicht zu entdecken. Mittels netzbasierter Anomalie-Erkennung kann der Virenbefall jedoch durch ein SIEM-System erkannt und der Gast halbautomatisiert (durch das Reagieren auf ein Ticket des verantwortlichen IT-Administrators) in ein Quarantänenetz verschoben werden. Das SIEM-System ist nun in der Lage den Erfolg dieser Maßnahme zu erkennen, indem durch die Funktion Key-Performance-Indikation die Komponenten der Infrastruktur herausgehoben werden können, die genutzt wurden, um den Virus zu erkennen und zu stoppen. Es ist daher eine Aussage über die Qualität der IT-Sicherheitsinfrastruktur möglich geworden.

Auf Basis dieses und weiterer Anwendungsszenarien wurden im SIMU-Projekt (www.simu-project.de) die Kernanforderungen an ein SIEM-System herausgearbeitet, welches sich für den Einsatz in unterschiedlichen Unternehmensgrößen eignet. Bisher sind SIEM-Systeme für den Einsatz im KMU-Umfeld allerdings nicht anwendbar. Dafür sind vor allem folgende Gründe zu nennen:

1. Hohe Kosten für Einrichtung und Wartung, da neue IT-Infrastrukturkomponenten (Kollektoren) installiert, konfiguriert und gewartet werden müssen.
2. Hohe Kosten für den Betrieb, da umfangreiches Expertenwissen für die Auswertung und richtige Interpretation der Meldungen und Ausgaben eines SIEM-Systems erforderlich ist.
3. Mangelnde Skalierbarkeit auf kleine und mittlere Netze.

Wesentliches Ziel des SIMU-Projektes ist die Entwicklung eines SIEM-artigen Systems zur signifikanten, mit geringem Aufwand erzielbaren Verbesserung der IT-Sicherheit und von Kontrollmöglichkeiten in Unternehmensnetzwerken. Funktional soll SIMU ähnlich zu SIEM-Systemen arbeiten und im Wesentlichen Vorgänge und Ereignisse im Firmennetzwerk überwachen. Wo es sinnvoll erscheint soll SIMU automatisiert, in Echtzeit und pro-aktiv Maßnahmen zur Verbesserung der IT-Sicherheit einleiten.

Das SIMU-Projekt strebt daher die folgenden Merkmale als Projektziele an:

a. **Merkmal 1:** Leichte Integrierbarkeit in IT-Infrastrukturen von KMU. Durch die Verwendung von weit verbreiteten Standards bei Kommunikationsprotokollen und Datenformaten, die in typischen Netzkomponenten bereits implementiert sind, soll der Aufwand für Installation, Konfiguration und Wartung von zusätzlichen SIMU-Komponenten minimiert werden.

b. **Merkmal 2:** Einfache Nachvollziehbarkeit von relevanten Ereignissen und Vorgängen im Netz. Relevante Ereignisse und Vorgänge im Netz sollen leicht verständlich visualisiert werden. Dadurch wird Verständnis und Nachvollziehbarkeit von Vorgängen im Netz erleichtert und somit die IT-Sicherheit gestärkt.

c. **Merkmal 3:** Geringer Aufwand für Konfiguration, Betrieb und Wartung. Das SIMU-System soll mit standardisierten Vorkonfigurationen arbeiten und die Möglichkeit bieten aus der leicht verständlichen Visualisierung des Netzes teilautomatisch Richtlinien und Konfigurationen abzuleiten. Dadurch wird der Aufwand für Konfiguration, Betrieb und Wartung gegenüber klassischen SIEM-Systemen stark reduziert. Anpassungen an Regelsätzen sollen möglichst auch durch Netzwerk- oder Systemadministratoren ohne spezielle Ausbildung vorgenommen werden können.

d. **Merkmal 4:** Übertragbarkeit der Regelsätze auf unterschiedliche Szenarien. Eine umfassende Anpassung der Regelsätze für den Einsatz des SIEM-Systems in einer anderen Umgebung (z.B. einem anderen Unternehmen) ist in den meisten Fällen durch das Fehlen von Expertenwissen in kleinen Unternehmen schwierig oder nicht praktikabel. Deshalb muss beim Entwurf des Regelsystems auf eine möglichst gute Übertragbarkeit der Regeln Wert gelegt werden.

Die konkreten Ergebnisse des SIMU-Projekts sind prototypische Software-Komponenten, die integriert in die IT-Infrastruktur eines Firmennetzes die Funktionalität von SIMU realisieren. Die prototypischen Software-Komponenten können als Basis für die Entwicklung von kommerziellen und Open-Source-Produkten verwendet werden.

2 SIEM-Definition

Die Akronyme SEM, SIM und SIEM werden zum Teil synonym verwendet, obwohl es unterschiedliche Bedeutungen und Produktfähigkeiten zu beachten gilt. Der Bereich des Sicherheitsmanagements, der sich mit der Echtzeitüberwachung, Ergebniskorrelation und Event-Benachrichtigungen befasst, wird als Security Event Management (SEM) bezeichnet. Der zweite Bereich ermöglicht Langzeiterfassung, Analyse und Reporting von Log-Daten und ist als Security Information Management (SIM) bekannt. Beide Segmente können unterschiedlich kombiniert werden, um je nach Anforderungen und Leistungsfähigkeit ein SIEM-System zusammenzustellen.

Der Begriff „SIEM“ wurde letztendlich von Mark Nicolett und Amrit Williams von Gartner im Jahr 2005 geprägt, indem beide die SIEM-Produktfähigkeit als eine Sammlung, Analyse und Darstellung von Informationen aus Netzwerk- und Sicherheitsgeräten beschrieben, um Sicherheitslücken effektiver auf die Spur zu kommen und Identity-/Access-Management-Anwendungen für Unternehmensnetze zu ermöglichen. Dadurch würde man externe Bedrohungen eher oder überhaupt erst wahrnehmen. Der Schwerpunkt eines SIEM-Systems ist demnach die Überwachung und Verwaltung von Benutzerdiensten und -privilegien, Verzeichnisdiensten und Änderungen der Systemkonfiguration sowie die Bereitstellung zur Auditierung und Überprüfung der Vorfälle [WILL07]. Es geht damit einen Schritt weiter, als herkömmliche Monitoring-Systeme und bezieht explizit die IT-Sicherheit mit ein.

SIEM wird daher mittlerweile als eine sehr wichtige Komponente von Firmennetzen und IT-Infrastrukturen angesehen [NiKa12]. Diese kommen allerdings fast ausschließlich in großen Unternehmen zum Einsatz, da der Betrieb sehr komplex und kostenintensiv ist. Aktuelle SIEM-Systeme sind zudem auch nur dann nützlich, wenn Experten in IT-Abteilungen die Sicherheitswarnungen und Ausgaben des SIEM-Systems sinnvoll selektieren und interpretieren können, um dann geeignete Gegenmaßnahmen ergreifen zu können.

Eine weitere Schwierigkeit liegt in proprietären Datenformaten für System-Ereignismeldungen (Events) und deren unterschiedlicher Aussagekraft. Die Paketmenge pro Minute hat für sich genommen beispielsweise eine relativ geringe Aussagekraft, eine Virenwarnmeldung eines umfassenden Virenschutzsystems mit wiederum tausenden von hinterlegten Mustern hingegen eher eine hohe.

Um sicherheitsrelevante Events unterschiedlicher Güte in einem SIEM zusammenzuführen, erbringen sogenannte Kollektoren folgende Leistungen:

- **Extraktion:** Events sind in Rohform meist Einträge in Log-Dateien oder über das Netz versendete Systemmeldungen. Diese Informationen müssen aus den jeweils verwendeten Systemen oder Transportprotokollen extrahiert werden, um sie einem SIEM-System zugänglich machen zu können.
- **Homogenisierung/Mapping:** Events werden von unterschiedlichen Diensten erzeugt und aus unterschiedlichen Systemen extrahiert. Um eine Weiterverarbeitung in einem SIEM-System zu gewährleisten, müssen die relevanten Inhalte der einzelnen Events miteinander in Bezug gebracht werden können. Dafür sorgt ein entsprechendes „Umsortieren“ individueller Datenfelder in speziellen Eventformaten in ein standardisiertes, dem SIEM-System verständliches, Eventformat (z.B. IDMEF nach RFC-4765).
- **Aggregation:** Große Mengen gleichartiger Events über einen kurzen Zeitraum würden ein zentrales SIEM-System belasten ohne einen signifikanten Mehrwert zu erzeugen. Kollektoren aggregieren daher große Mengen gleichartiger Events über einen kurzen Zeitraum (sog. Bursts) zu einem einzigen Event mit höherer Aussagekraft (z.B. Event-Typ, Inhalt und Menge der ursprünglichen Meldungen).

Die Auswertung von Events wird anhand von Regelsätzen durchgeführt. Die Relevanz der Ergebnisse der Regelauswertung ist aber abhängig von den Eigenschaften bzw. dem Aufbau des jeweiligen Unternehmens. Beispiele hierfür sind primäre und sekundäre Geschäftsprozesse, organisatorische Prozesse, die Bedrohungslage oder eingesetzte IT-Assets. Die Operationalisierung übergreifender Strategien aber auch bereits das Ableiten von Regelsätzen aus konkreten Sicherheitsrichtlinien stellt für Unternehmen eine Herausforderung dar. Maschinenlesbare Sicherheitsrichtlinien sind komplex und deren manuelle Erstellung erfordert spezifisches Expertenwissen, das nur in begrenztem Maße zur Verfügung steht und dessen Bereitstellung kostenintensiv ist. Ohne ein wirksames Set an Regelsätzen ist ein SIEM-System in seiner Wirkung stark eingeschränkt und erbringt nicht die Leistungen, die dessen Anschaffungs- und Betriebskosten rechtfertigen würden. Daher ist die Verbreitung solcher SIEM-Systeme immer noch als gering zu bezeichnen.

3 SIEM-Ansätze

Die Zielsetzung bei der Implementierung von IT-Sicherheit ist im Grunde genommen relativ einfach: das Unternehmen und seine Assets sollten nach Schutzbedarfsfeststellung geschützt und die Kosten dieser Schutzmaßnahmen abgeschätzt und in Relation zu der Reduktion der Eintrittswahrscheinlichkeit eines Schadenfalles gestellt werden. Es kann ein positiver Beitrag zum Unternehmensergebnis geschaffen werden, wenn die Optimierung des Risikomanagements ermöglicht wird, ohne dabei die Verfügbarkeit im Netzwerk zu reduzieren, sondern sie im Gegenteil zu erhöht. Die Umsetzung ist dabei allerdings nicht als trivial zu bezeichnen.

3.1 Ist-Zustand

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

Zudem konzentrieren sich traditionelle Sicherheitslösungen ausschließlich auf die Abbildung ihrer eigenen Leistungsmerkmale. Andere Bereiche innerhalb des Unternehmens (z.B. Serversysteme, Applikationen, Facility Management, Zugriffskontrolle, Inventarisierungsverwaltung) werden nicht mit einbezogen. Dabei beinhalten gerade die genannten Bereiche die eigentlichen Unternehmenswerte. Obwohl man diese Unternehmenswerte also schützen will, bezieht man sie bei der Betrachtung der IT-Sicherheit nicht mit ein.

3.2 Soll-Zustand

Es ist daher anzustreben, dass man die Unternehmenswerte vorab definiert, sie in die Sicherheitsstrategie einbezieht und beim Einsatz von IT-Sicherheitskomponenten einen ganzheitlichen Kontext verfolgt. Dieser bezieht auch die Benutzergruppen mit ein, die für die verschiedenen Unternehmensbereiche zuständig sind. So muss beispielsweise ein Problem für einen technisch Verantwortlichen anders dargestellt werden, als für einen kaufmännisch Verantwortlichen. Zudem dürfen unterschiedliche Arbeitsgruppen nur die jeweiligen Bereiche einsehen, die für sie bestimmt sind. Zwar müssen alle Informationen in die Bewertung der Gesamtsicherheitslage einbezogen werden, sensitive Informationen aus „Gruppe A“ dürfen jedoch nicht in „Gruppe B“ auftauchen.

Eine Unterteilung könnte dabei wie folgt aussehen:

- Gruppe A: Netzwerk
- Gruppe B: Sicherheitskomponenten (IDS, IPS, Firewall, VPN, AV-Systeme)
- Gruppe C: Facility Management (Gebäudesicherheit, Zutrittssicherheit)
- Gruppe D: Serversysteme

Das Beispiel einer Gefährdung (ein erster kleiner Use Case) könnte beispielsweise so aussehen, dass sich ein Benutzer am Unternehmensnetz über Network Access Control (NAC) authentifiziert und das NAC-System nach Überprüfung der Login-Daten ihm Zugang gewährt. Der Benutzer kann nun auf die Unternehmensdaten zugreifen und geht seiner normalen Arbeit nach. In der Mittagspause nutzt er seinen privaten USB-Stick, um sich private Bilder anzuschauen (obwohl die Unternehmensrichtlinie ihm das nicht gestattet). Leider enthält der USB-Stick einen Virus, der sich umgehend mit einem Server im Netzwerk verbindet. Da eine Anmeldung am NAC-System erfolgt ist, kann der Virus bereits freigeschaltete Applikations-Ports zur Kommunikation nutzen. Die Firewall-Systeme und Switches merken also erst einmal nichts Ungewöhnliches.

Dies ändert sich sobald ein SIEM im Einsatz ist. Dieses kann feststellen, dass der Mitarbeiter ungewöhnlich viele Datenpakete durch das Netzwerk schickt. Zudem kann das SIEM auf Port

80 ungewöhnlichen, mit seriellen, binären Daten gefüllten SOAP-Traffic entdecken, wo es normalerweise nur HTTP beobachtet. Auch die Tageszeit (die Mittagspause) ist ungewöhnlich für die hohe Aktivität. Das SIEM informiert daher die „Gruppe A“ und die „Gruppe D“. Das Management wird noch nicht informiert, da es noch unklar ist, ob wirklich eine Anomalie vorliegt.

Inzwischen ist der Virus weiter aktiv und versucht auf eine Datenbank zuzugreifen. Dabei entstehen viele Fehlauthentifizierungen, die ebenfalls vom SIEM registriert werden. Das SIEM ist nun in der Lage die beiden Events miteinander zu korrelieren und bewertet das korrelierte Ereignis höher als die Ursprungsereignisse. Neben „Gruppe A“ und „Gruppe D“, wird jetzt auch das Management informiert, da offenbar ein Angriff erfolgt.

Der Virus hat inzwischen Zugriff auf die Datenbank erhalten, wenn auch nur durch einen unautorisierten Gastzugang. Da nun Datenabwanderung aus einem internem System droht, fragt das SIEM bei der IT-Administration per E-Mail-Ticket nach, ob der Benutzer in Quarantäne gestellt werden darf. Die Quarantäne unterbindet vorerst nur den Datenbankzugriff. Sobald die IT-Administration das Ticket bestätigt hat, wird der Benutzer vom NAC-System in die Quarantänezone verschoben. Bei dem Versuch des Benutzers seine reguläre Arbeit wieder aufzunehmen wird er auf eine Webseite umgeleitet, die ihm mitteilt, dass er die Unternehmensrichtlinien verletzt hat und der Helpdesk bereits an dem Problem arbeitet.

Nachdem der Virus erkannt und eliminiert worden ist, wird der Benutzer wieder freigeschaltet. Anschließend wird der Vorfall im SIEM-System dokumentiert, damit spätere Auditoren den Vorfall nachvollziehen können.

3.3 SIEM-Technologie

Ein SIEM-System besteht aus diversen Modulen, die die folgenden Funktionen abbilden müssen:

a. **Event Correlation:** Logfiles werden aufgenommen, archiviert, normalisiert und korreliert, um eine Datenbasis zu schaffen, mit der Gefährdung erkannt werden können.

b. **Network Behaviour Anomaly Detection (NBAD):** Anomalien werden auf Netzwerkebene erkannt, Kommunikationsverhalten festgestellt und Abweichungen von der Normalität verfolgt bzw. bei Bedarf diese in die Korrelation der Problemstellung mit aufgenommen.

c. **Identity Mapping:** Sicherheitssysteme, die Anomalien oder Angriffe auf das Unternehmensnetz melden, beschreiben Angreifer bzw. Opfer stets mittels einer IP-Adresse. Das hilft aber nur bedingt weiter, weshalb die Identität der Person aufgelöst wird.

d. **Key Performance Indication:** Die IT-Sicherheit wird messbar gemacht, indem sicherheitsrelevante Informationen und Asset-Details zentral analysiert werden.

e. **Compliance Reporting:** Die IT-Compliance (u.a. Integrität, Risiko, Effektivität) des Unternehmens wird immer wieder hinterfragt und Ergebnisse miteinander verglichen.

f. **Application Programming Interface (API):** Anbindung vorhandener Sicherheitssysteme und Bereitstellung generischer Schnittstellen zur Integration unbekannter Geräte bzw. Systeme.

g. **Role Based Access Control:** Zentrale Sicht auf alle sicherheitsrelevanten Ereignisse innerhalb des Unternehmens, unter Berücksichtigung der Verantwortungsbereiche.

Diese Module machen die Intelligenz eines SIEM aus, die eine Risikoanalyse in Korrelation mit allen bekannten Events möglich macht. Über unterschiedliche Schnittstellen erhält das SIEM Informationen über Assets (z.B. Inventardaten), über Sicherheitslücken (Vulnerability und Patch Management) und kann auf die Dokumentation zugreifen. Zusätzliche Schnittstellen wird es zum Help-Desk oder Asset-Datenbanken geben. Auch das Zusammenspiel zum vorhandenen NAC-System muss über Schnittstellen ermöglicht werden. Abbildung 1 zeigt die wichtigsten Module eines SIEM und die Kommunikationsvariationen.

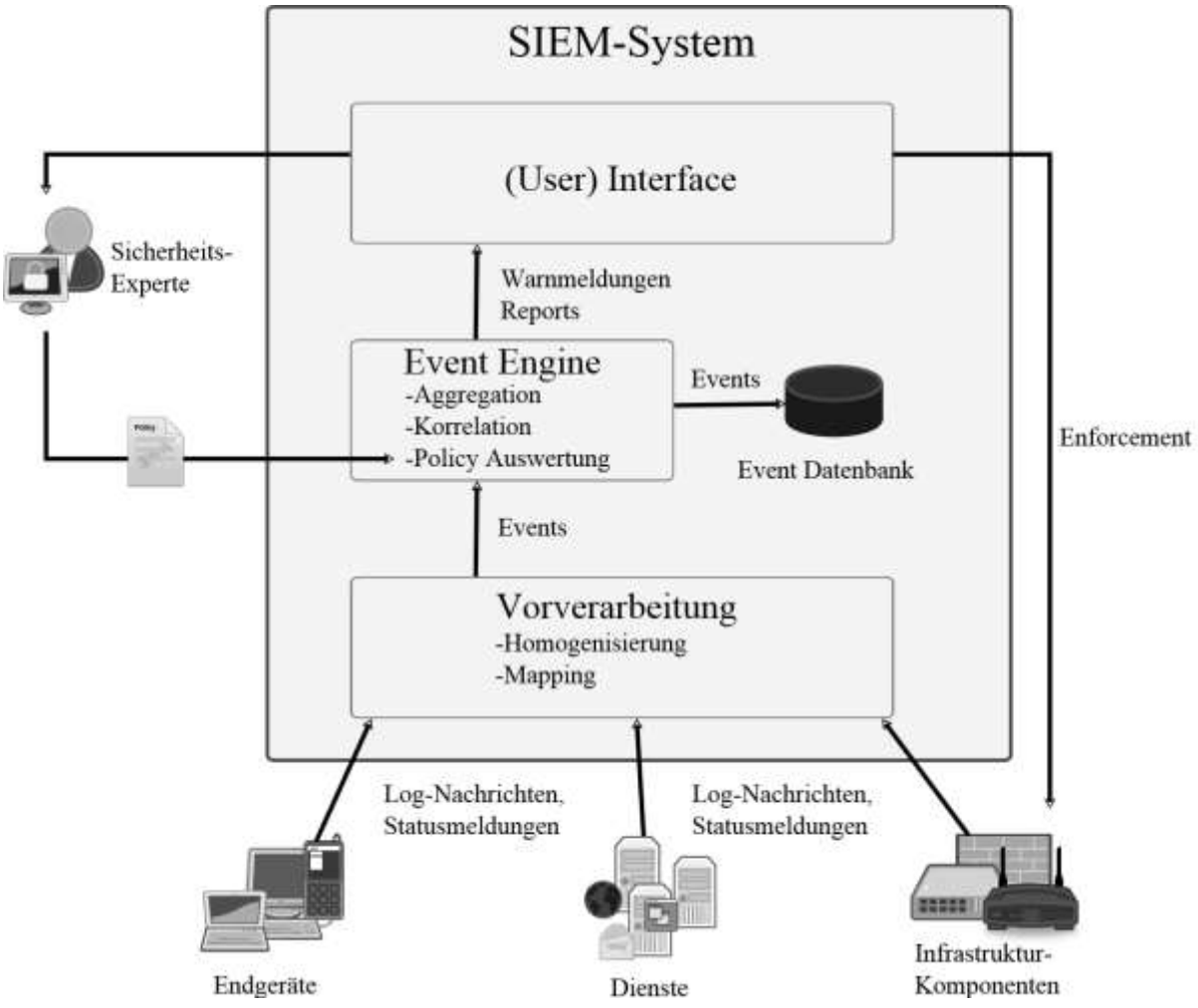

Abb. 1: SIEM-Systemaufbau und Kommunikationsschnittstellen

4 SIEM-Konzept

Die fachlichen Anforderungen für ein SIEM-System orientieren sich anhand des Haupt-Informationsflusses, d.h. vom Sammeln der Informationen über das Verarbeiten bis zur Reaktion oder Alarmmeldung. Die folgenden Anforderungen müssen daher erfüllt werden:

1. Sammeln von Daten der zentralen Dienste und Netzkomponenten.

2. Aggregation dieser Daten zu aussagekräftigen Ereignissen anhand einer flexibel definierbaren Policy.
3. Darstellungen der sicherheitsrelevanten Ereignisse in verschiedenen Detailstufen.
4. Auslösen von Alarmmeldungen oder ggf. aktiver Eingriff (Alerting/Enforcement).

Um angemessene Entscheidungen zu treffen, ist es wichtig, eine aktuelle und korrekte Wissensbasis über die Geräte, Benutzer und Eigenschaften des Netzwerkes zu besitzen. Zu diesen Informationen gehören:

- Daten über Geräte, die sich im Netz befinden, wie IP-Adresse, MAC-Adresse, DNS-Name, Betriebssystem, Verfügbarkeit des Gerätes (Ping), offene Ports, angebotene Dienste, Datendurchsatz und Systemzustand (installierte Software, Integritätszustand, CPU- und RAM-Auslastung etc.).
- Informationen über Benutzer, die an Systemen angemeldet sind, wie Benutzername, Benutzergruppen, Berechtigungen oder Zuordnung zu Geräten im Netzwerk.
- Detail-Informationen über den Zustand der zentralen Dienste im Netzwerk, beispielsweise Informationen über aktuell angemeldete Benutzer, Fehlermeldung und Status-Reports der Dienste.

Wenn die oben aufgeführten Metadaten zentralisiert und für berechtigte Komponenten zugreifbar sind, können viele Ansätze zur Erkennung und Behandlung von Bedrohungen miteinander kombiniert werden. So können Verletzungen von Unternehmensrichtlinien frühzeitig erkannt und ggf. Maßnahmen eingeleitet werden. Auch kann die SIMU-Engine (siehe SIMU-Architektur) durch das stetige Sammeln dieser Informationen den „Normalzustand“ erlernen und außergewöhnliche und nicht vorhergesehene Bedrohungen erkennen.

4.1 SIMU-Architektur

Abbildung 2 zeigt die SIEM-Architektur des SIMU-Projektes, die das IF-MAP-Protokoll als zentrales Protokoll zum Austausch von Metadaten in den Mittelpunkt stellt. Neben den Open-Source-Tools, die schwerpunktmäßig integriert werden, sind die deutschen Herstellerlösungen NCP-VPN und macmon NAC ebenfalls Teil der Architektur.

Die SIMU-Architektur teilt sich in zwei Schichten, die durch das IF-MAP-Protokoll miteinander verbunden werden:

a. Die **SIMU-Kollektoren- und Flow-Controller-Schicht**, welche für Datensammlung und Enforcement verantwortlich ist (siehe Punkt 1 und Punkt 4 der Anforderungen).
b. Die **SIMU-Engine**, welche die den zentralen Wissens- und Datenspeicher, Komponenten zur Korrelation, Aggregation und Darstellung von Daten sowie Protokollschnittstellen enthält.

Die SIMU-Engine muss u.a. die Ergebnisse der Datenanalyse durch die SIMU-GUI entsprechend aufbereitet darstellen. Die grafische Oberfläche muss dafür mit der Detection Engine (intelligente Analyse der MAP-Server-Daten) und VisITMeta (grafische Darstellung des IF-MAP-Graphens) direkt kommunizieren sowie indirekt mit dem IO-Tool (Erhebung der Daten der IT-Infrastruktur). Sie muss Events eindeutig anzeigen und ensprechende

Mitteilungen an die IT-Administration schicken. Dieser SIMU-GUI kommt damit eine zentrale Bedeutung zu.

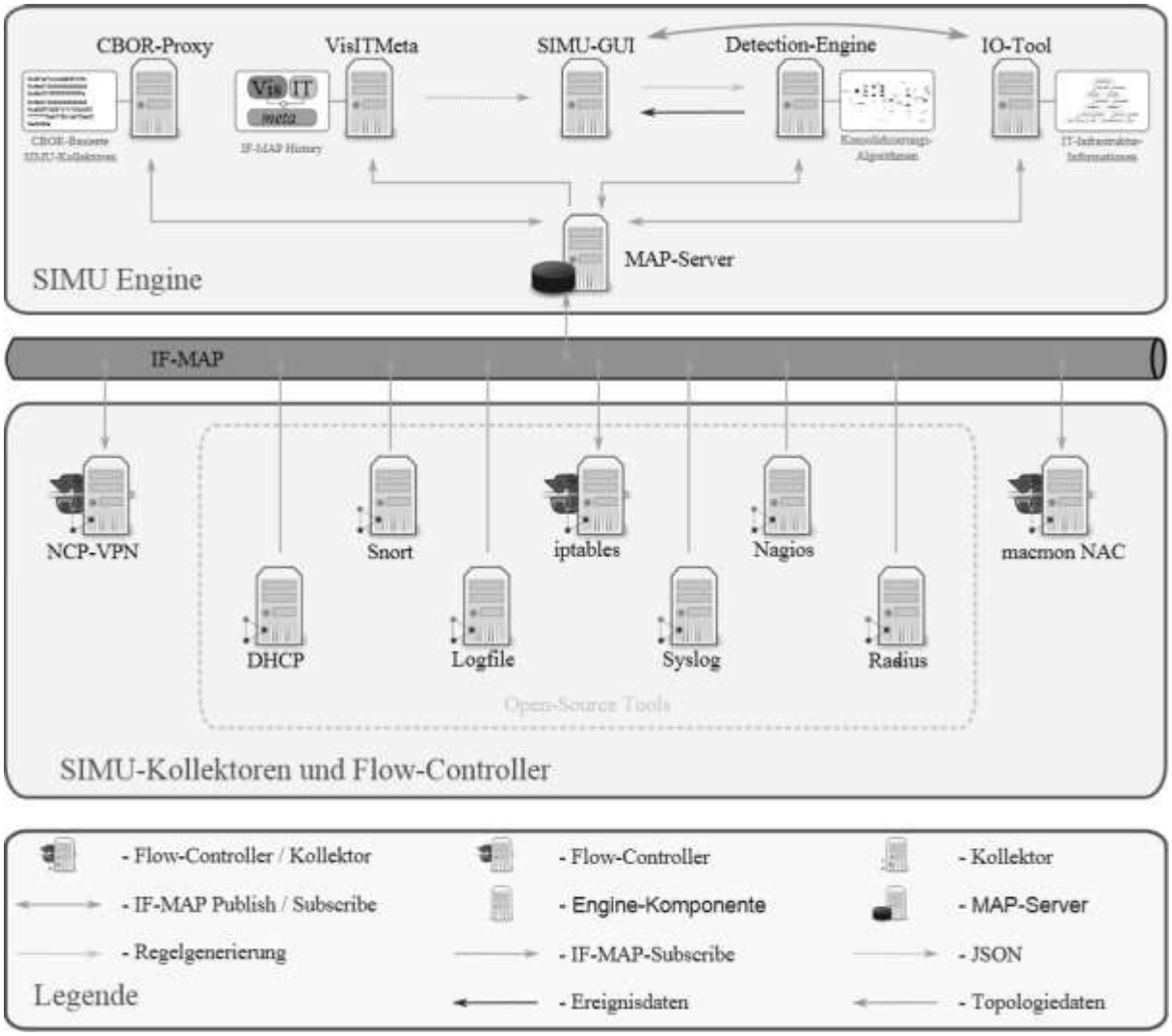

Abb. 2: SIEM-Architektur im SIMU-Projekt

4.2 IF-MAP

Für den Austausch von Informationen zwischen der SIMU-Engine und den Kollektoren und Flow-Controllern wird das IF-MAP-Protokoll der Trusted Computing Group (TCG) eingesetzt [TCG14]. IF-MAP ist ein offen spezifiziertes, herstellerunabhängiges Protokoll zum Austausch von Metadaten innerhalb eines Netzwerkes in Echtzeit. Es ist zudem ein integraler Bestandteil des Trusted Network Connect (TNC) Frameworks der TCG; kann jedoch auch (wie in SIMU) losgelöst von TNC verwendet werden.

IF-MAP definiert im Wesentlichen zwei Rollen:

1. Ein Server, der **Metadata Access Point (MAP)**, dient als zentrale Zugriffspunkt und Sammelstelle für beliebige Metadaten.

2. **MAP-Clients (MAPCs)** können über das IF-MAP-Protokoll auf den MAP-Server zugreifen, um Metadaten zu veröffentlichen, sie zu durchsuchen oder Abonnements auf Metadaten registrieren.

Welche Art von Metadaten mit IF-MAP transportiert und gesammelt werden, kann durch die Definition eines Metadatenschemas auf die jeweilige Anwendungsdomäne angepasst werden. Die TCG schlägt unter anderem ein Schema speziell für die Anwendung im Bereich der Netzwerksicherheit vor [TCG12b].

Die Rolle eines MAPC kann von verschiedenen Komponenten übernommen werden. Zum Beispiel kann ein Policy Decision Point (PDP) nach erfolgreicher Authentisierung eines Benutzers die Ergebnisse einer etwaigen Integritätsüberprüfung des verwendeten Endgerätes in Form von Metadaten im MAP-Server veröffentlichen. Diese Metadaten werden in der Regel den erfolgreichen Zugriff des Access Requestors (AR) auf das Netzwerk widerspiegeln.

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

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

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

Technologisch setzt IF-MAP auf eine Reihe von etablierten Standard-Technologien. Als Framework zur Übertragung der Metadaten kommt das SOAP-Protokoll in Kombination mit HTTP(S) zum Einsatz. Das Format der Metadaten ist durch XML-Schemata beschrieben. Auf diese Weise können etablierte Sicherheitssysteme, die um MAP-Client-Funktionen erweitert worden sind, beliebige Metadaten über den aktuellen Status des Netzwerkes austauschen [DSBW12]. Das SIMU-Projekt wird aber auch den Einsatz von CBOR (Concise Binary Object Representation) nach RFC-7049 prüfen, um eine schlankere Kommunikation zu ermöglichen.

4.3 SIMU-Kollektoren und Flow-Controller

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

- **DHCP-Kollektor:** Extrahiert Metadaten zu aktuellen IP-Leases des DHCP-Servers aus dem Lease-File von DHCP-Servern.

- **Radius-Kollektor:** Liefert Metadaten zu Benutzeranmeldungen sowie Metadaten zu den Benutzern selbst (Gruppen, Berechtigungen).
- **Syslog-Kollektor:** Stellt voraggregierte Metadaten zum Zustand von Hosts und Diensten (CPU-Last, Fehlgeschlagene Log-Ins) zur Verfügung.
- **Nagios-Kollektor:** Veröffentlicht aus Nagios extrahierte Metadaten zum Zustand von Hosts und Diensten (u.a. Netzwerkverfügbarkeit).
- **Snort-Kollektor:** Übersetzt Snort-Alarme in IF-MAP-Metadaten.
- **Logfile-Kollektor:** Generischer Kollektor zur Auswertung beliebiger Log-Dateien und Transformation in IF-MAP Metadaten.

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

Des Weiteren ist die Integration folgender Flow-Controller-Komponenten geplant, die zum Teil auch Kollektoren-Funktionalitäten besitzen:

- **Iptables-Flow-Controller:** Ermöglicht das automatische Anlegen von Firewall-Regeln für Hosts als Reaktion auf bestimmte Metadaten und veröffentlicht diese als Enforcement-Reports im MAP-Server.
- **macmon NAC:** Das NAC-System von macmon secure publiziert verschiedene Daten zu aktiven Endgeräten im Netzwerk. Hierzu gehören vor allem Autorisierungsinformationen zu bekannten Endgeräten, deren Standort im Netzwerk (physikalischer Port, WLAN-AP) und weitere Geräte-Charakteristika wie Betriebssysteminformationen und offene Ports.
- **NCP-VPN:** Die von NCP entwickelte VPN-Lösung kann eine Reihe relevanter Metadaten auf dem MAP-Server zur Verfügung stellen. Dies sind insbesondere Informationen über angemeldeter Benutzer sowie die IP-Adresse der Geräte, mit denen die Benutzer im VPN angemeldet sind, Datendurchsatz und Verbindungszeit der jeweiligen Benutzer. Es wird ein Enforcement auf VPN-Ebene ermöglicht.

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

4.4 SIMU-Engine

Der MAP-Server stellt den zentralen Austauschpunkt von Informationen dar. Alle Sensoren und Flow-Controller veröffentlichen gesammelte Informationen via IF-MAP im MAP-Server. Die zweite Kernkomponente neben dem MAP-Server ist die Detection-Engine. Diese verwendet die Informationen aus dem MAP-Server, um zum einen Abweichungen von definierten Zu-

ständen festzustellen (Pattern Matching) und zum anderen, um durch den Einsatz von Anomalie-Erkennungsalgorithmen Abweichungen vom Normalverhalten festzustellen. Dafür kann die Detection-Engine auf den gesamten Datenbestand des MAP-Servers zugreifen.

Durch die Anbindung des IO-Tool [BIRK12] wird der Datenbestand mit weiteren Asset-Informationen über die Netzwerkinfrastruktur angereichert, was eine Korrelation mit zusätzlichen Informationen ermöglicht. Das Normalverhalten des Systems wird durch eine Trainingsphase mit zuvor bereitgestellten Trainingsdaten berechnet. Für den wartungsarmen Betrieb ist es dabei zwingend notwendig, dass die verwendeten Anomalie-Erkennungsverfahren möglichst zuverlässig und selbstständig arbeiten. Dies gilt auch für die Trainingsphase solcher Erkennungsverfahren. Deshalb sind speziell sogenannte „nicht-überwachte“ (unsupervised) Verfahren (vgl. [CHAN09]) für die Anwendung in SIMU geeignet.

Beim Einsatz von „überwachten“ (supervised) oder „teilüberwachten“ (semi-supervised) Verfahren besteht der Nachteil, dass in der Trainingsphase jedes Datum vom Benutzer als Normalfall oder Anomalie gekennzeichnet werden muss. Dieses hat offensichtlich mehrere Nachteile: zum einen ist es extrem aufwändig eine große Anzahl von Trainingsdaten auf diese Weise manuell korrekt zu kennzeichnen, zum anderen ist das dafür nötige Expertenwissen beim jeweiligen Anwender nicht vorhanden. Darüber hinaus ist es sehr schwierig geeignete Trainingsdaten auszuwählen, die eine möglichst große Anzahl an Normalfällen und Anomalien abdecken.

Die VisITMeta-Komponente dient zur Langzeitarchivierung des IF-MAP-Graphen. Somit ist es möglich jeden beliebigen Zustand des Graphen zu einem späteren Zeitpunkt – z.B. zu Analysezwecken – zu rekonstruieren. Außerdem bietet VisITMeta sowohl Schnittstellen als auch Visualisierungskomponenten die in der SIMU-GUI verwendet werden können, um alle Aspekte des SIMU-Systems Zielgruppengerecht aufzubereiten und anzuzeigen.

5 Fazit

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

Das im SIMU-Projekt entwickelte SIEM-System soll speziell auf die Bedürfnisse von KMUs zugeschnitten sein. Dazu gehören unter anderem eine leichte Integrierbarkeit in eine bestehende Infrastruktur und der wartungsarme Betrieb des Systems. Durch den Einsatz von IF-MAP als Integrationsplattform ist es möglich herstellerübergreifend eine Vielzahl von Komponenten an das SIMU-System anzubinden, was Anpassungen bestehender Netzwerkinfrastrukturen auf ein Minimum reduziert und die verfügbare Datenbasis maximiert.

Die zentrale Verfügbarkeit von Infrastrukturdaten und dynamischen Ereignisdaten ermöglicht eine bessere und umfassendere Gesamtsicht auf den Zustand des Netzwerks. Gleichzeitig wird durch die Abbildung auf IF-MAP Metadaten eine erste Homogenisierungs-Stufe für Informationen aus unterschiedlichen Datenquellen und Formaten erreicht.

Durch den Einsatz von Anomalie-Erkennungs-Verfahren und Policy-basiertem „Pattern Matching“ kann diese Datenbasis genutzt werden, um Gefahren frühzeitig erkennen zu können. Das SIMU-System ermöglicht darüber hinaus eine automatisierte Reaktion in Form von Alarmen und Enforcement, beispielsweise auf Firewall- oder VPN-Ebene.

6 Danksagung

Das SIMU-Projekt (www.simu-project.de) ist ein gefördertes BMBF-Projekt mit einer Laufzeit von zwei Jahren, das im Oktober 2013 seine Arbeiten begonnen hat. An dem Projekt sind die Firmen DECOIT GmbH (Projektleitung), NCP Engineering GmbH, macmon secure gmbh sowie die deutschen Forschungseinrichtungen Fraunhofer SIT und Hochschule Hannover beteiligt. Daher gilt der Dank den Partnern des Projektes, die durch ihre Beiträge und Arbeiten diesen Bericht erst ermöglicht haben.

Literatur

[NiKa12] Mark Nicolett, Kelly M. Kavanagh: *Gartner Magic Quadrant for Security Information and Event Management Report*. Gartner-Report, 24 May, 2012

[WILL07] Amrit Williams Blog (Observations of a Digitally Enlightened Mind): *The future of SIEM - the market will begin to diverge*. January 2007

[TCG14] Trusted Computing Group: *TNC IF-MAP Binding for SOAP*. Specification Version 2.2, Revision 9, März 2014

[TCG12b] Trusted Computing Group: *TNC IF-MAP Metadata for Network Security*. Specification Version 1.1, Revision 8, Mai 2012

[DSBW12] Detken, Scheuermann, Bente, Westerkamp: *Automatisches Erkennen mobiler Angriffe auf die IT-Infrastruktur*. D.A.CH Security 2012: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Herausgeber: Peter Schartner und Jürgen Taeger, syssec Verlag, ISBN 978-3-00-039221-4, Konstanz 2012

[CHAN09] Varun Chandola, Arindam Banerjee, Vipin Kumar: *Anomaly detection: A survey*. ACM Computing Surveys, 41(3), 2009

[BIRK12] Birkholz, Sieverdingbeck, Sohr, Bormann: *IO: An interconnected asset ontology in support of risk management processes*. IEEE Seventh International Conference on Availability, Reliability and Security, Page 534-541, 2012