DECOIT

D•A•CH Security 2011

Konsolidierung von Metadaten

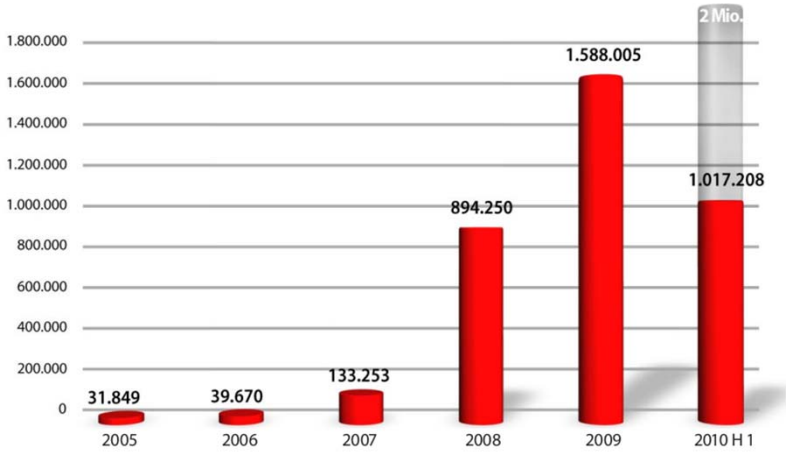
zur Erhöhung der Unternehmenssicherheit

Prof. Dr.-Ing. Kai-Oliver Detken
Geschäftsführer
DECOIT GmbH
URL: http://www.decoit.de
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

Anstieg von Malware

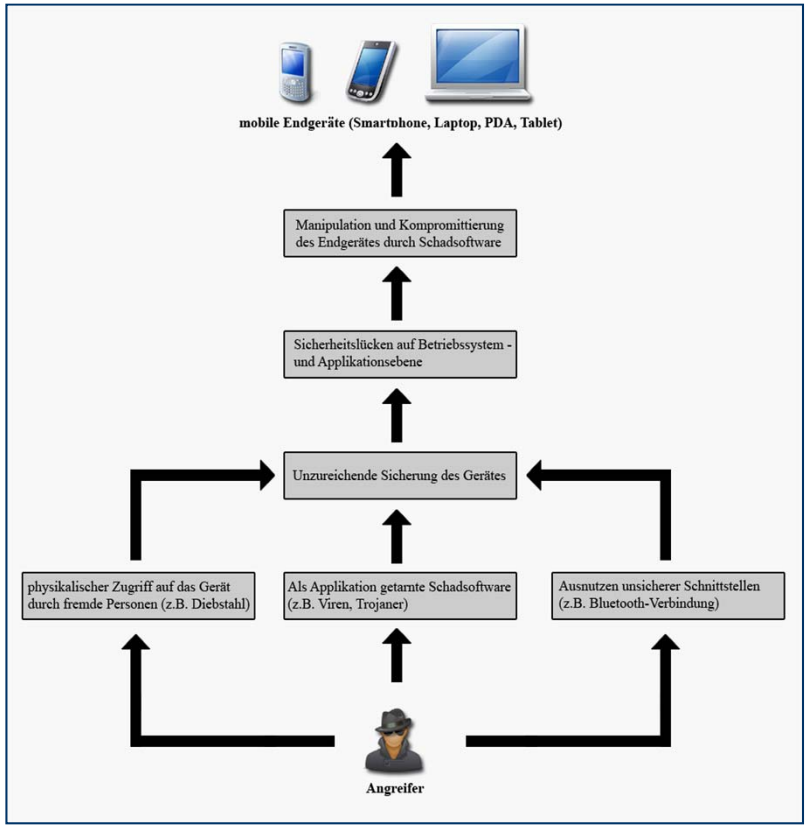
- Laut den Prognosen von Sicherheitsexperten wird es in den kommenden Jahren zu einem sprunghaften Anstieg von Schadsoftware (Malware) kommen
- Dabei rücken vor allem Smartphones und andere mobile Endgeräte (z.B. Tablet-PCs) zunehmend in den Fokus der Angreifer



GData Malware Report 2010

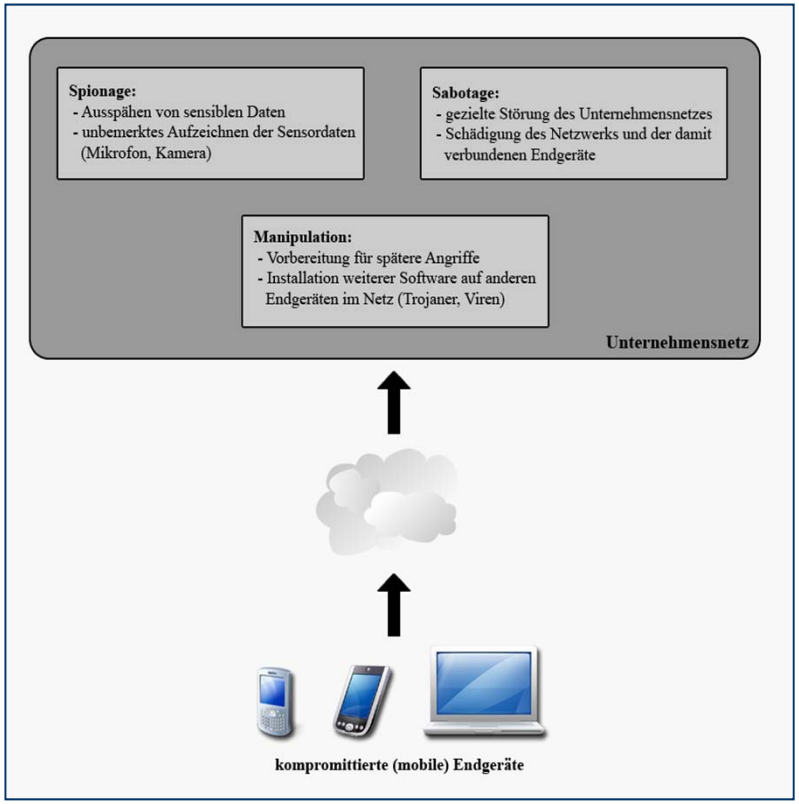
Kompromittieren mobiler Endgeräte

- Durch die Mobilität solcher Geräte erhöht sich auch gleichzeitig das Risiko des Verlustes oder des Zugriffs bzw. Diebstahls des Gerätes durch unbefugte Personen
- Unzureichende Sicherheitsvorkehrungen durch den eigentlichen Besitzer des Endgerätes (z.B. Einsatz von „schwachen" PIN-Codes) ermöglichen Daten auszuspähen oder sich mit Hilfe des Endgerätes selbst Zugang in das Netz des Unternehmens zu verschaffen
- Unbemerkten Manipulation des Gerätes (z.B. durch die Installation von Schadsoftware)



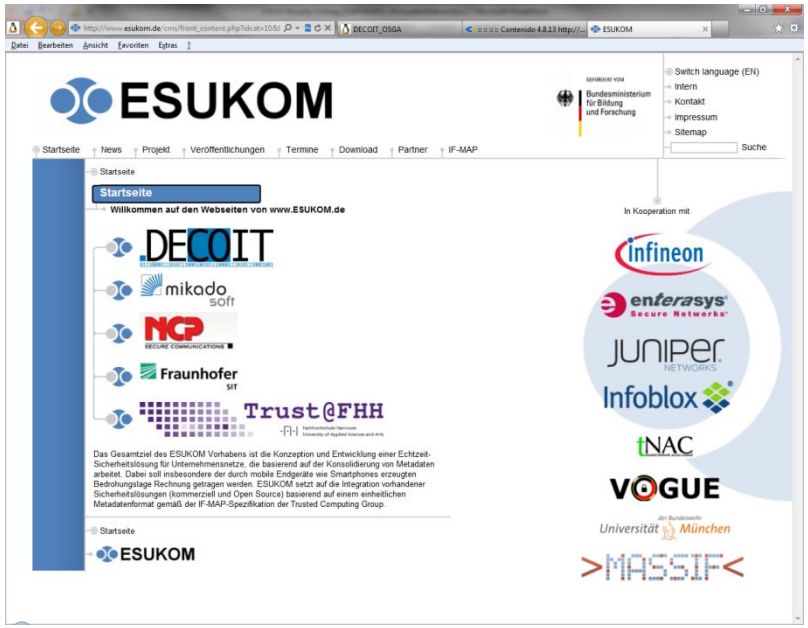
Gefahren beim Zugriff durch kompromittierte Endgeräte

- Ausspähen von sensiblen Daten (z.B. Nutzerdaten oder interne Unternehmensdaten)
- Zusätzliche Gefahren durch verschiedenen Sensoren und Schnittstellen heutiger mobiler Endgeräte
- Mobiles Endgerät kann als Überträger von Schadsoftware eingesetzt werden, um einen Angriff vorzubereiten
- Schädigung des Unternehmensnetzes oder der damit verbundenen Endgeräte



ESUKOM-Projekt (www.esukom.de)

- Das ESUKOM-Projekt ist ein nationales BMBF-Projekt
- Es startete im Oktober 2010 und wird im September 2012 enden
- Folgende Partner sind in diesem Projekt involviert:
  - DECOIT GmbH (Konsortialführer)
  - Fraunhofer SIT (Darmstadt)
  - FH Hannover (Hannover)
  - NCP engineering GmbH (Nürnberg)
  - Mikado Soft GmbH (Berlin)
- Diverse Hersteller sind Kooperationspartner



Ziele des ESUKOM-Projektes

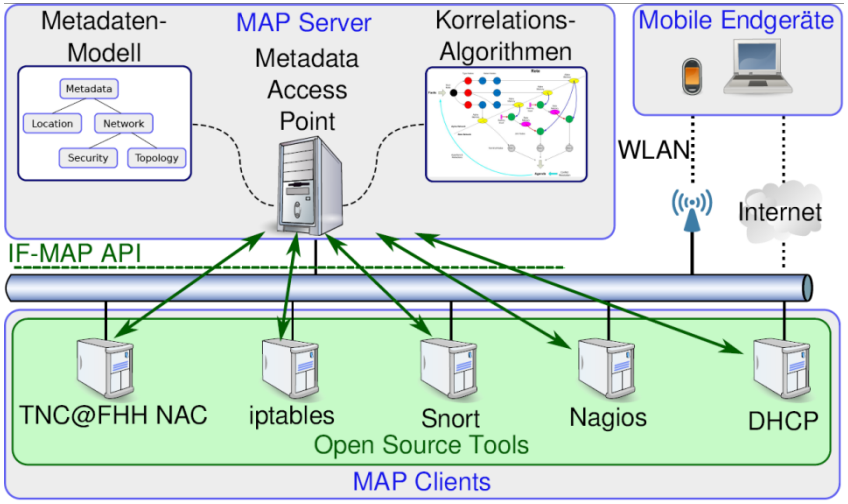
- Entwicklung von IF-MAP-Software-Komponenten zur Sammlung (IF-MAP-Client) und Veröffentlichung von Metadaten (IF-MAP-Server)
- Entwicklung eines fortgeschrittenen Metadaten-Modells
- Entwicklung von Konsolidierungs-Algorithmen
- Integration vorhandener Sicherheitstools
- Entwicklung logischer Komponenten:
  - MAP-Server
  - Metadatenmodell
  - Konsolidierungsalgorithmen zur Auswertung der Metadaten
  - Verschiedene IF-MAP-Clients, die mit dem MAP-Server miteinander kommunizieren können

Zentrale Komponente: IF-MAP (1)

- Die technologische Basis für das ESUKOM Projekt ist das IF-MAP (Interface for Metadata Access Point) Protokoll der TCG
- IF-MAP ist ein offenes, herstellerunabhängiges Client-Server Netzwerkprotokoll zum Austausch von beliebigen, in XML codierten Metadaten
- IF-MAP ist ein substantieller Bestandteil des Trusted Network Connect (TNC) Frameworks
- IF-MAP soll die Integration von vorhandenen, sicherheitsrelevanten Infrastrukturdiensten wie Firewalls, VPNs und IDS-Systemen ermöglichen
- Durch die Integration dieser Dienste erhält man eine ganzheitliche Sicht auf den aktuellen Status eines Netzwerkes, was Vorteile bei der Administration und der Erkennung von Bedrohungen verspricht

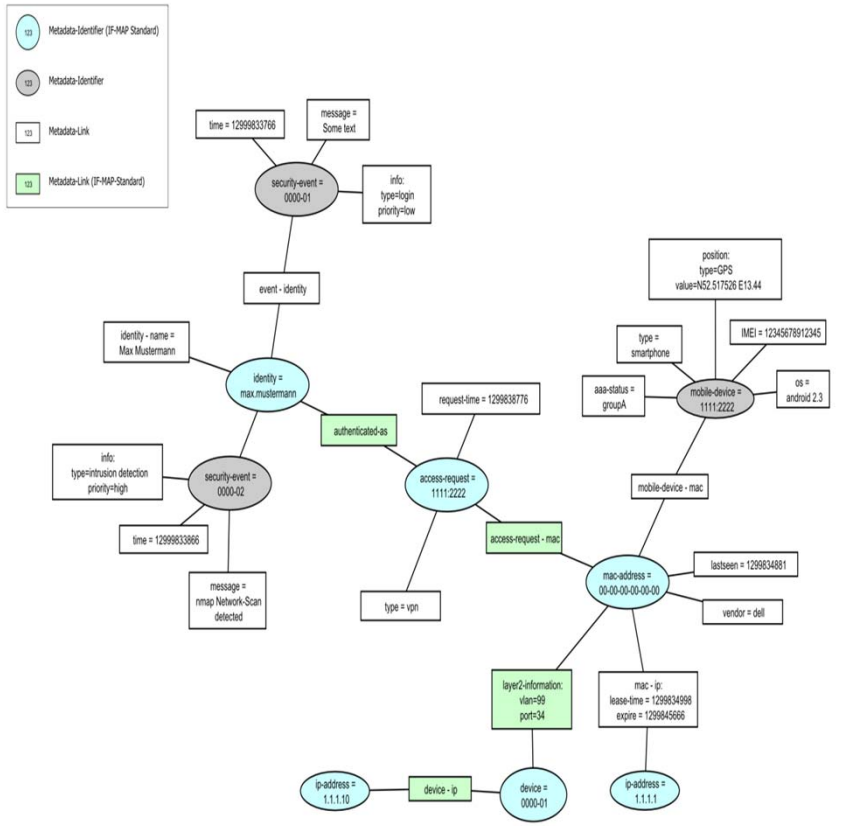
Zentrale Komponente: IF-MAP (2)

- MAP-Server:
  - Zustand des Netzes wird angezeigt
  - Zustand wird anhand des Metadatenformats beschrieben
  - Metadaten werden in Form von Graphen verwaltet
  - Durch Korrelation der vorhandenen Metadaten können sicherheitsrelevante Informationen abgeleitet werden
- MAP-Clients:
  - Publish-Operation veröffentlicht Metadaten
  - Search-Operation sucht nach bestimmten Metadaten
  - Subscribe-Operation informiert asynchron über relevante Änderungen der gespeicherten Metadaten im MAP-Server



Mehrwerte durch IF-MAP-Einsatz

- Mobiler Unternehmenszugang: Verbindungsdaten (MAC/IP-Adresse des Endgerätes, Zeitpunkt des Zugriffes, Nutzerrollen und Berechtigung etc.) werden an den MAP-Server übertragen und in den entsprechenden Meta-Daten-Graphen eingetragen
- Kompromittierte Endgeräte werden über den IF-MAP-Client erkannt und die Informationen an den IF-MAP-Server weitergeleitet
- Der IF-MAP-Server nimmt die entsprechenden Daten entgegen und fügt diese zum jeweiligen Metadaten-Graphen hinzu
- Der IF-MAP-Server benachrichtigt die MAP-Clients, die daraufhin weitere Maßnahmen einleiten können

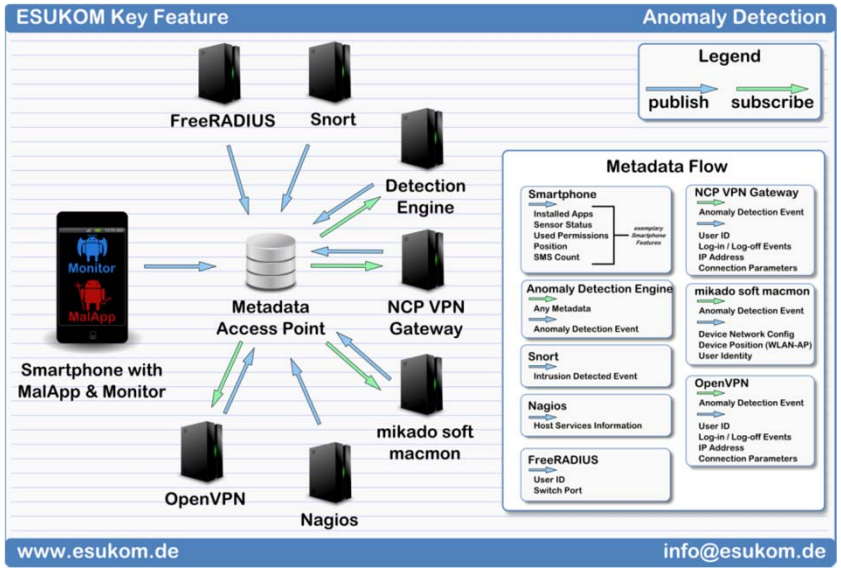


Ableitung von Kernanforderungen

- Anomalie-Erkennung: Normalverhalten und Grenzverhalten muss sich über das Sammeln möglichst viele Daten identifizieren lassen.
- Smartphone Awareness: Komponenten und Dienste innerhalb der IT-Infrastruktur eines Unternehmens sollen erkennen können, ob es sich bei angebundenen Geräten um ein Smartphone handelt sowie der Softwarezustand.
- Single-Sign-Off: Dem Anwender bleibt es somit erspart, verschiedenste Daten zur Authentifizierung, wie Kombinationen aus Benutzernamen und Passwörtern oder Zertifikaten, vorzuhalten
- Secure Evidence: Erzeugung eines möglichst gerichtsfesten Beweises über einen Vorgang.
- Identity Awareness: Fähigkeit von Netzwerkkomponenten, ihre Funktionsweise abhängig von der Identität des anfragenden Benutzers anzupassen. Das Ziel ist, die Konfiguration von Komponenten flexibler gestalten zu können.
- Location-based Services: Dienste und Anwendungen, die den aktuellen Aufenthaltsort des Benutzers für die Bereitstellung und Verarbeitung von Daten nutzen. Anhand des Aufenthaltsortes kann dann der Zugriff ausgeschlossen werden.
- Erkennen von MalApp-basierten Angriffen: MalApps sollen erkannt und so den Bedrohungen entgegen gewirkt werden können.
- Real-time Enforcement: Automatisierte Umsetzung von reaktiven Maßnahmen, die durch MAP kommuniziert und möglicherweise auch mit Hilfe von IF-MAP-Anwendungen ausgelöst werden können

Anomalie-Erkennung (1)

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

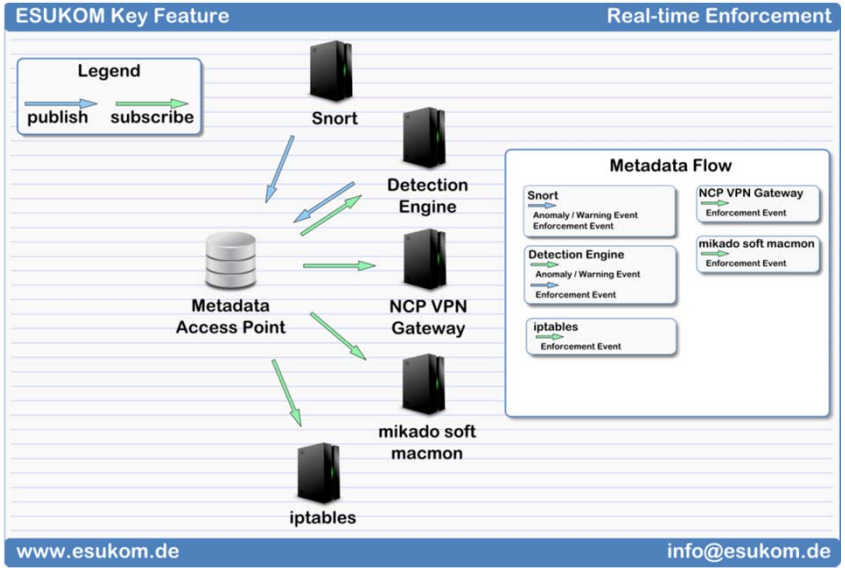


Anomalie-Erkennung (2)

- Die Anomalie-Erkennung könnte auf verschiedene Metadaten angewandt werden
- Dies sind einerseits die schon bekannten Network-Security Metadaten wie Access-Request, IP, MAC oder Location-Information
- Für die Anomalie-Erkennung kann es erforderlich sein, sowohl das Veröffentlichen als auch das Löschen der Metadaten zu persistieren
- Andernfalls wäre es z.B. nicht möglich, das Normalverhalten des Clients bzgl. der Anzahl der Logins zu bestimmen
- Folgende Daten können gesammelt werden:
  - Login-Count eines User Account (ID) oder eines Geräts (MAC)
  - Zeit des Logins im System
  - Anwesenheit erfasst z. B. durch ein Arbeitszeiterfassungssystem
  - Anzahl der MAC-Adressen, die mit einer User ID verbunden sind
  - Anzahl messbarer Aktionen im System

Real-time Enforcement (1)

- Es handelt es sich um die automatisierte Umsetzung von reaktiven Maßnahmen, die durch den Metadata Access Point (MAP) kommuniziert und möglicherweise auch mit Hilfe von IF-MAP-Anwendungen ausgelöst werden können
- Es handelt es sich um eine alleinstehende Anwendung, bei der es darum geht, kritische Informationen zwischen IF-MAP Clients auszutauschen
- Zusätzlich werden automatisierte Reaktionen auf Analysen von anderen ESUKOM-Anwendungen ermöglicht
- Die größte Herausforderung ist das Verhindern von falschen Entscheidungen (sog. False Positives)
- Hierzu kann zum Beispiel eine strikte Policy bzgl. der Rechte zur Veröffentlichung solcher Informationen eingesetzt werden



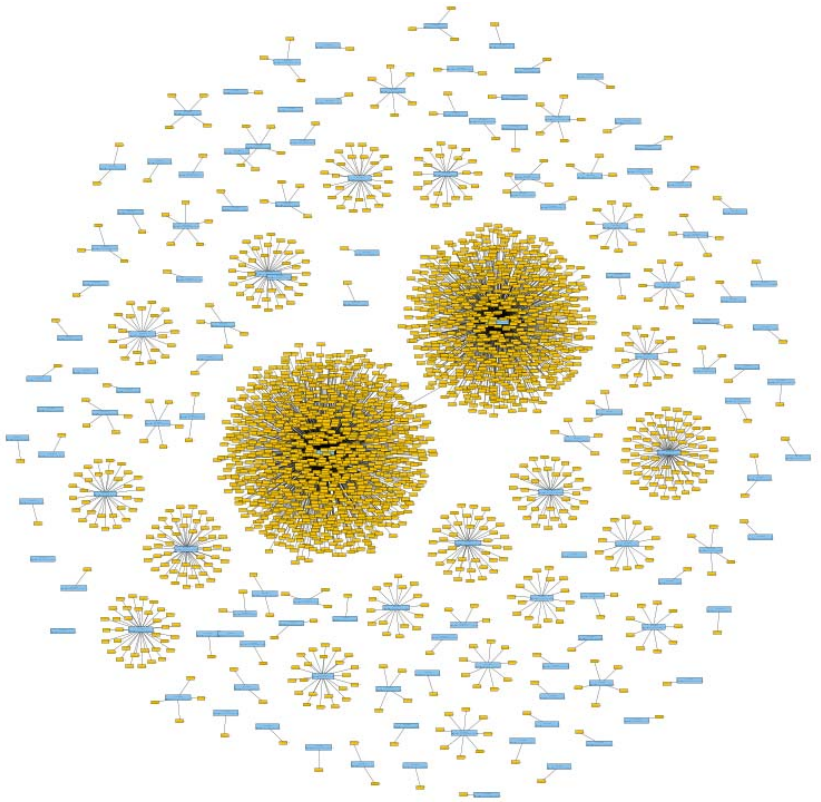
DECOIT

Real-time Enforcement (2)

- Die Reaktion eines Paketfilters auf erkannte Anomalien wäre ein Einsatzbeispiel
- Anomalien können durch ein IDS erzeugte Events sein, die auf eine Verletzung der Unternehmens-Policy hindeuten oder auch von der Anomalie-Erkennungs-Anwendung erzeugt werden
- Als Reaktion auf erkannte Anomalien wird es oft erforderlich sein, den Zugriff des verursachenden Endgerätes auf das Netzwerk zu limitieren
- Ein über IF-MAP an den MAP-Server angebundener Paketfilter kann sich über solche Events informieren lassen und seine Konfiguration entsprechend anpassen, zum Beispiel um den vom verursachenden Endgerät ausgehenden Traffic zu blockieren
- Dies ist insbesondere auch für verteilte Firewall-Umgebungen leicht umsetzbar

Zusammenfassung

- Zusammenfassung unterschiedlicher Metadaten würde die Sicherheit stark erhöhen
- Das ESUKOM-Projekt hat bereits diverse IF-MAP-Clients entwickelt und in ihren Prototypen integriert
- Ein IF-MAP-Server steht ebenfalls bereits zur Verfügung
- Visualisierung muss mit einer enormen Datenflut umgehen (siehe rechts)
- Diverse Hersteller aus der TCG sind an den ESUKOM-Arbeiten interessiert und kooperieren direkt mit dem Projekt
- Konsolidierungs-Algorithmen stellt mit die größte Herausforderung dar



DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
info@decoit.de

Consultancy & Internet Technologies