GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Automatisches Erkennen mobiler Angriffe auf die IT-Infrastruktur

Prof. Dr. Kai-Oliver Detken,
DECOIT GmbH

ESUKOM

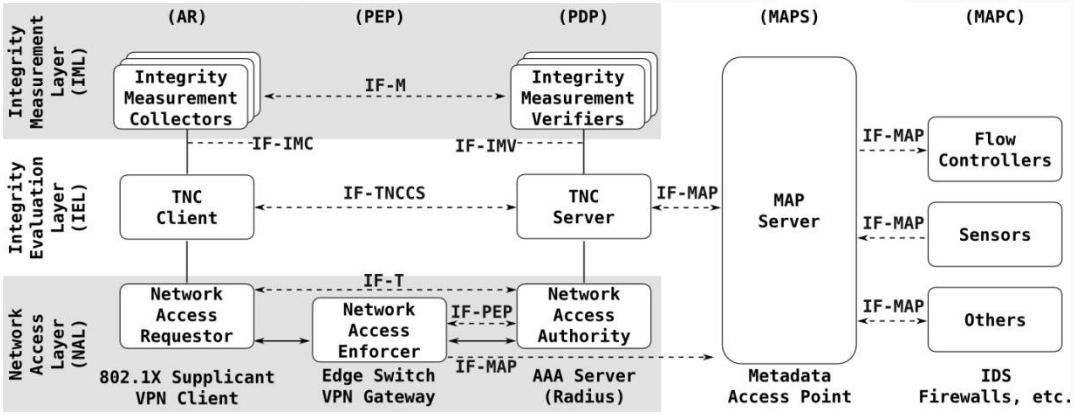
ESUKOM

Übersicht

- IF-MAP-Spezifikation
- ESUKOM-Projekt
  - Anomalie-Erkennung
  - Smartphone Awareness
  - Location-based Services
  - MalApp-Erkennung
  - Real-time Enforcement
- Detection Engine
- Fazit

IF-MAP-Spezifikation

- Die Trusted Computing Group (TCG) hat im Mai 2008 die erste Version der IF-MAP-Spezifikation veröffentlicht
- IF-MAP ist ein offenes, Hersteller-unabhängiges Protokoll zum Austausch von beliebigen Daten innerhalb eines Netzwerkes in Echtzeit
- IF-MAP ist ein integraler Bestandteil des Trusted Network Connect (TNC) Frameworks der TCG
- Das Format der Metadaten wird durch XML-Schemata beschrieben

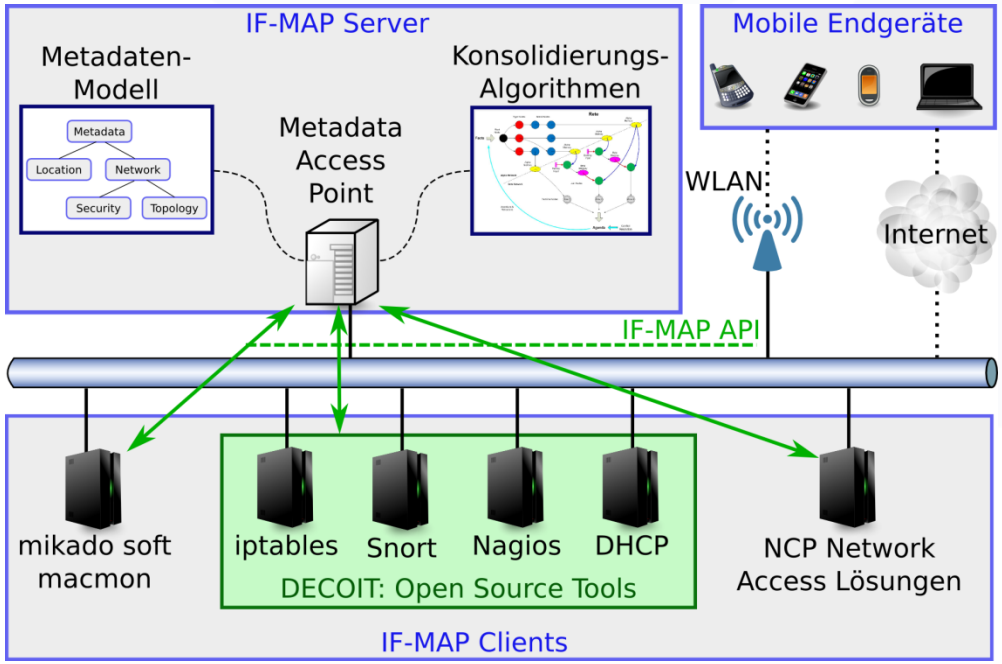


Das ESUKOM-Projekt

- Das Gesamtziel des ESUKOM Vorhabens war die Konzeption und Entwicklung einer Echtzeit-Sicherheitslösung für Unternehmensnetze, die basierend auf der Konsolidierung von Metadaten arbeitet
- Dabei standen insbesondere mobile Endgeräte (Smartphones) im Fokus
- ESUKOM setzte auf die Integration vorhandener Sicherheitslösungen (kommerziell und Open Source) basierend auf dem einheitlichen Metadatenformat IF-MAP der Trusted Computing Group (TCG)
- Dadurch ist eine gemeinsame Datenbasis möglich, die korrelierende Schlüsse auf die IT-Sicherheit zulässt
- Sicherheitsentscheidungen lassen sich nun auf Basis verschiedener Sicherheitskomponenten fällen

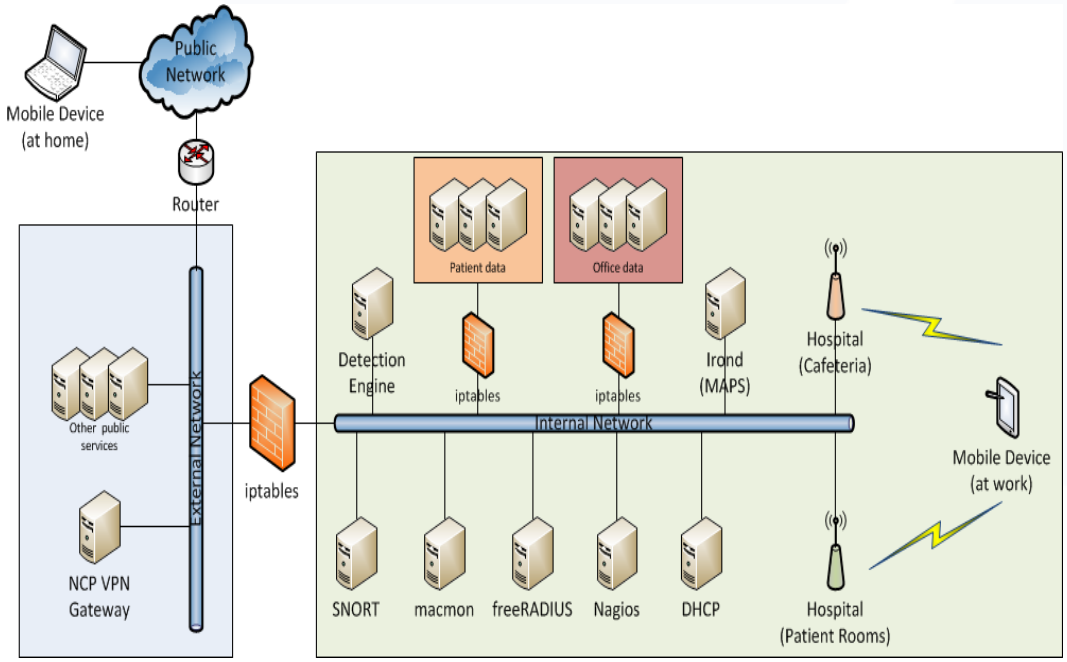
Das ESUKOM-Projekt (2)

- Projektlaufzeit: Okt. 2010 bis Sept. 2012
- Projektvolumen:
  - 177 PM
  - 1,5 Mio. Euro
- Projektpartner:
  - DECOIT GmbH (Konsortialführer)
  - FH Hannover
  - Fraunhofer SIT
  - NCP GmbH
  - mikado soft GmbH



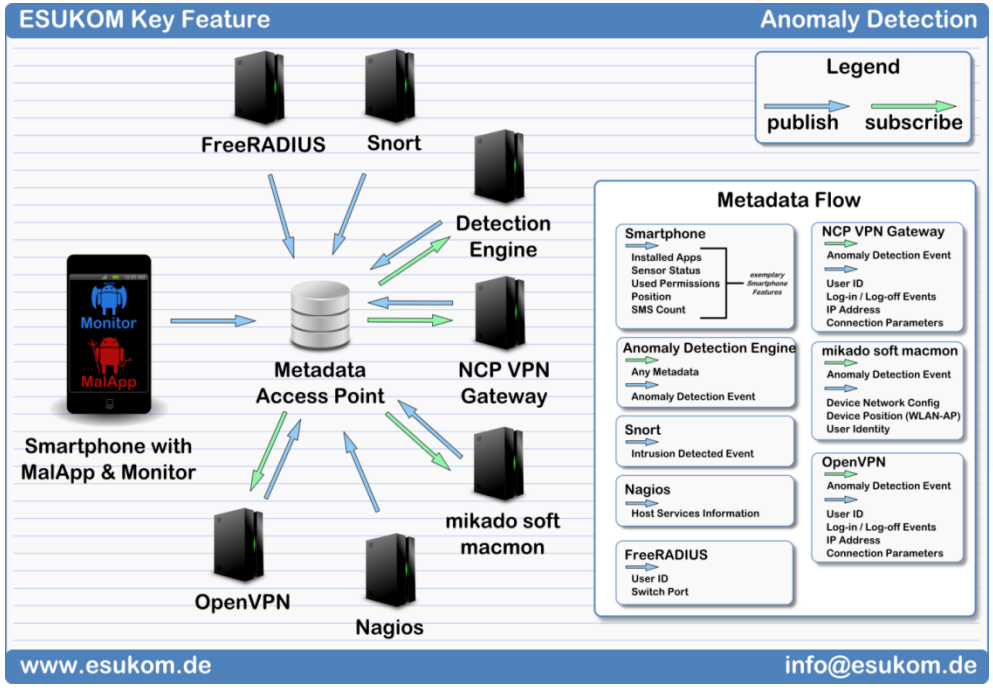
Generisches Anwendungsszenario

- IT-Umgebung in einem Krankenhaus wurde ausgewählt
- Das Szenario wurde aus sechs realen Kundenszenarien entwickelt
- Der gemeinsame Nenner aller Szenarien ist der mobile Mitarbeiter
- Ärzte nutzen in diesem Fall mobiles Equipment für Patientenakten
- Sicherheitsrichtlinien (Policys) wurden festgelegt
- Es kommen verschiedene IF-MAP-Clients zum Einsatz



Anomalie-Erkennung

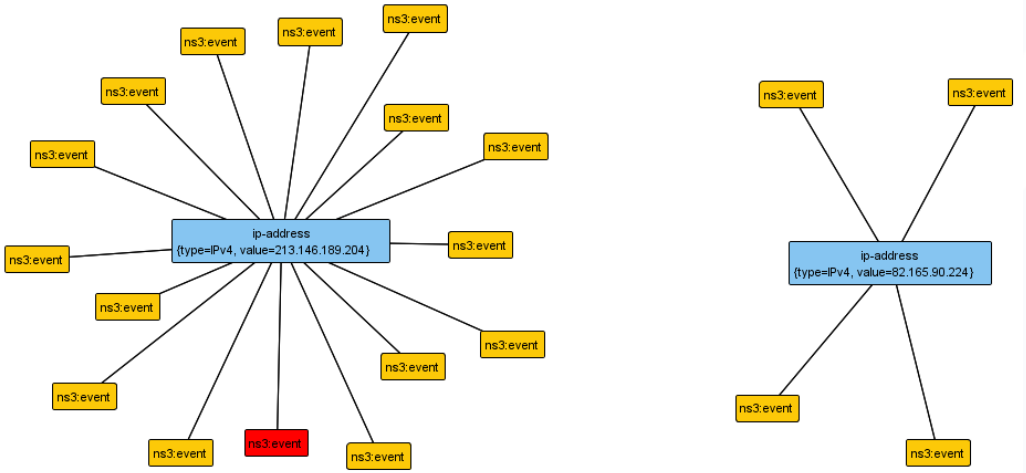
- Es werden möglichst viele Informationen gesammelt
- Normalverhalten und Grenzverhalten muss erkannt werden können
- Die Stärke von IF-MAP gegenüber einer IDS Anomalie-Erkennung liegt in der Diversität der Daten
- Anomalie-Erkennung kann auf verschiedene Metadaten angewandt werden
- Metadaten könnten sein: Login-Count, User Account, MAC-/IP-Adresse, Zeit im System



Smartphone Awareness

- Erkennen von Angriffen auf Unternehmensnetze und die Einleitung entsprechender Gegenmaßnahmen
- Smartphone-Umsetzung anhand von Android wurde durchgeführt
- Ein IF-MAP-Client für Android wurde deshalb entwickelt
- Viele Informationen werden durch Android veröffentlicht

Grafische Darstellung über die irongui (1)

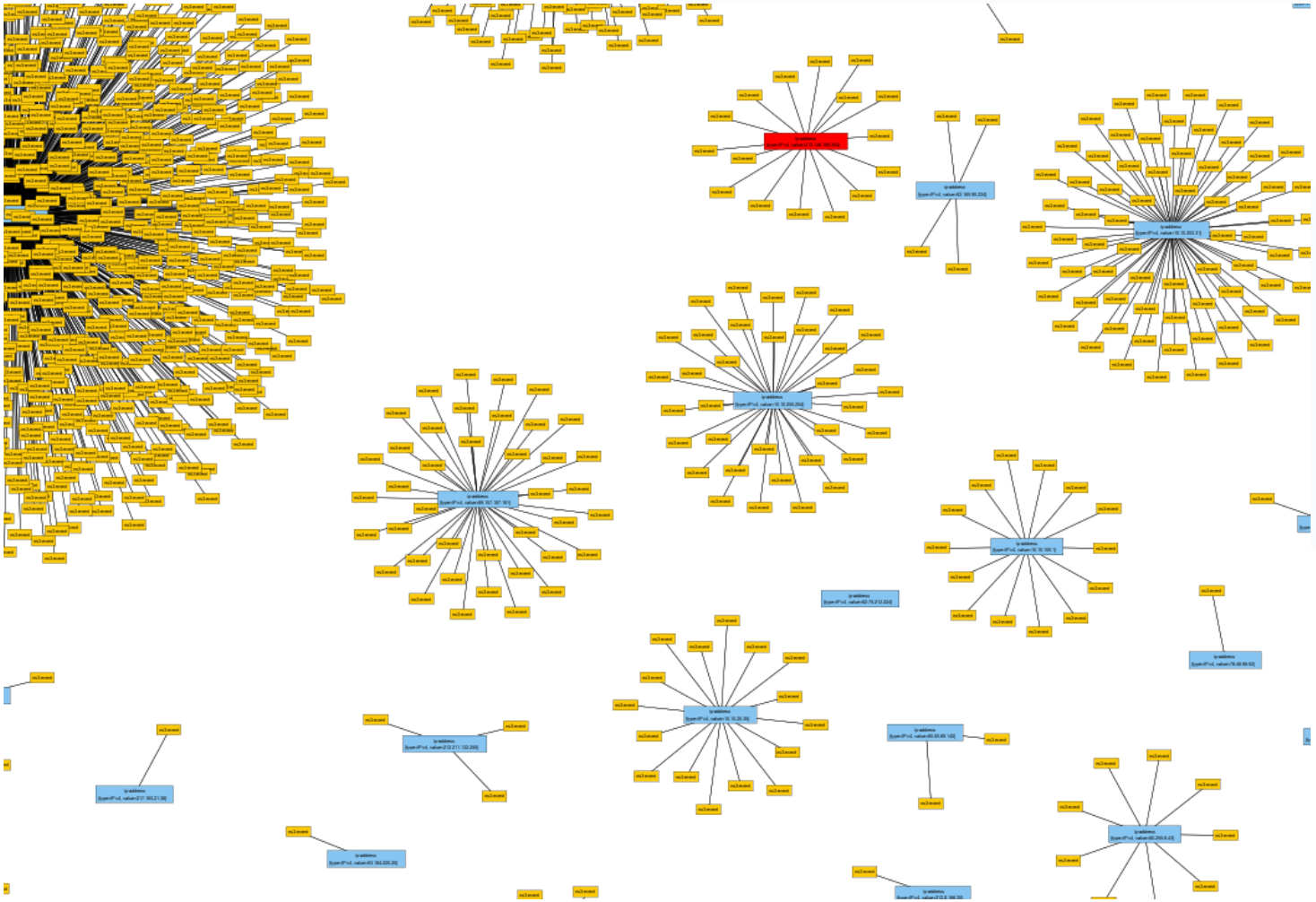


ns3:event {ifmap-timestamp=2011-04-07T16:56:21+02:00, ifmap-cardinality=multiValue, xmlns:soapenv=http://www.w3.org/2003/05/soap-envelope, ifmap-publisher-id=snort7821625671, xmlns:ns3=http://www.trustedcomputinggroup.org/2010/IFMAP-MI

Attributes	Value
significance	
value	critical
discoverer-id	
value	2
confidence	
value	100
name	
value	P2P Skype client login
type	
value	policy violation
magnitude	
value	45
discovered-time	
value	2011-01-17T14:12:25.000+01:00

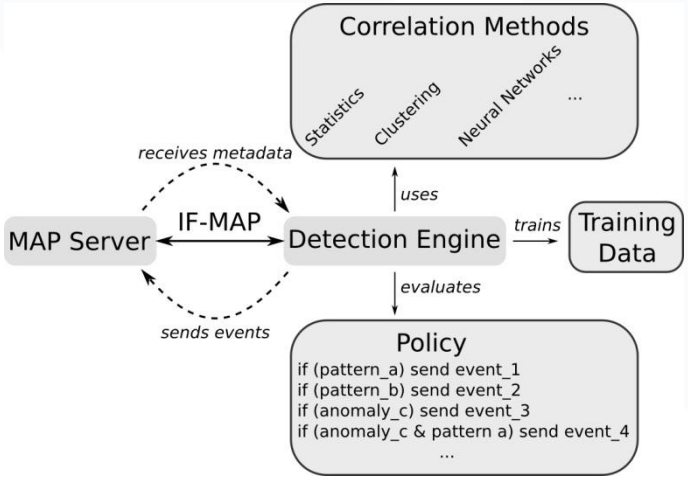
Last update: 07-04-2011 16:57:18

Grafische Darstellung über die irongui (2)



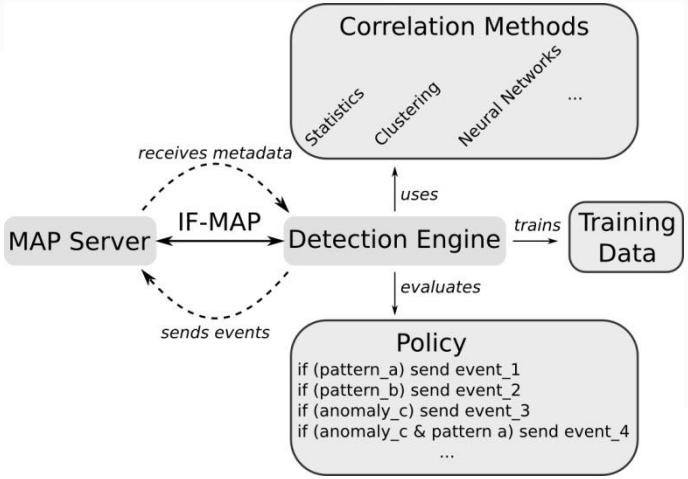
Detection Engine (1)

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



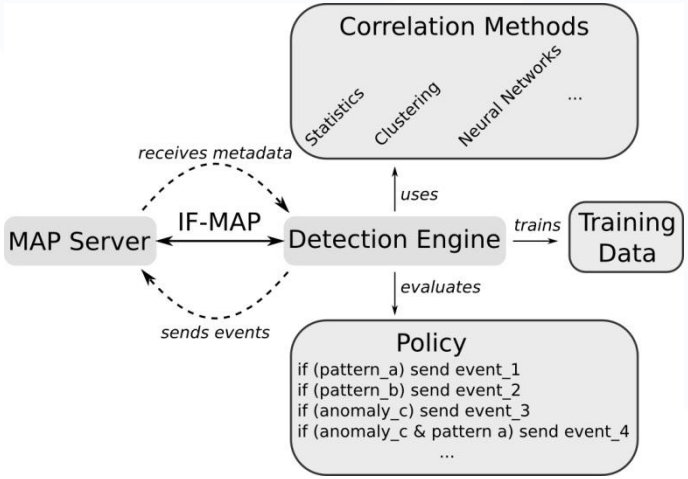
Detection Engine (2)

- Der ESUKOM-Ansatz verfolgt die Analyse des MAP-Graphen über eine sogenannte Detection Engine durchführen zu lassen
- Das Ziel war es, sowohl eine Muster- als auch eine Anomalie-Erkennung basierend auf den in Echtzeit gesammelten und vorliegenden Metadaten durchführen zu können
- Die Detection Engine ist als IF-MAP-Client realisiert worden
- Zur Mustererkennung reicht ein einfacher Vergleich, der in der Detection Engine Policy definierten Muster aus
- Wenn ein bestimmtes Angriffsmuster erkannt wird, wird direkt ein entsprechender Event veröffentlicht



Detection Engine (3)

- Die Erkennung von Anomalien ist dagegen komplexer
- Voraussetzung dafür ist, dass das Normalverhalten vorher entweder trainiert oder basierend auf Expertenwissen festgelegt worden ist
- Um Anomalien zu erkennen muss die Detection Engine eine Vielzahl von verschiedenen Verfahren aus dem Bereich der Statistik (Mittelwert, Median, Clustering) und des maschinellen Lernens (Neuronale Netze) unterstützen
- Sammeln von Trainingsdaten und KI-Schnittstelle zur Anbindung anderer Lösungen sind essentiell für die Anomalie-Erkennung
- Erste Erfahrungen konnten gemacht werden – u.a. werden die Policys relativ komplex



Fazit (1)

- Bisher konnten bisherige Ansätze nicht verschiedene Metadaten unterschiedlicher Messkomponenten integrieren
- Diese Ansätze waren in der Regel auf Messungen von nur einer Komponente beschränkt
- Eine Rückkopplung von Auswerte-Ergebnissen in Form von Events war ebenfalls bislang nicht möglich
- Das IF-MAP-Protokoll stellt eine ideale Basis für die Erfüllung der Anforderungen des ESUKOM-Projektes dar
- Die größte Herausforderung stellte die Detection Engine dar, da es eine offene Forschungsfrage ist, mit welchen Methoden welche Metadaten am geeignetsten auszuwerten sind, um bestimmte Anomalien erkennen zu können

Fazit (2)

- Die Detection Engine wurde daher so ausgelegt, dass diese Konfiguration flexibel über entsprechende Policys gesteuert werden kann
- Auch eine generische Schnittstelle zur Anbindung beliebiger Analyseverfahren (Correlation Methods) wurde geschaffen
- Es wurde auch eine Komponente entwickelt, die es erlaubt, über einen definierten Zeitraum die erforderlichen Trainingsdaten zu sammeln
- Diverse IF-MAP-Clients (Open Source, NCP, macmon) und ein IF-MAP-Server wurden entwickelt
- Das Projekt konnte seine Ziele dementsprechend alle erreichen

Vielen Dank!

…für ihre Aufmerksamkeit

ESUKOM

ESUKOM

Copyright 2010-2012

Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „01BY1050“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.

*Die in dieser Publikation enthaltenen Informationen stehen im Eigentum der folgenden Projektpartner des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes „**ESUKOM**“: DECOIT GmbH, Fachhochschule Hannover (FHH), Fraunhofer-Institut für Sichere Informationstechnologie (SIT), NCP engineering GmbH und der mikado soft GmbH. Für in diesem Dokument enthaltenen Information wird keine Garantie oder Gewährleistung dafür übernommen, dass die Informationen für einen bestimmten Zweck geeignet sind. Die genannten Projektpartner übernehmen keinerlei Haftung für Schäden jedweder Art, dies beinhaltet, ist jedoch nicht begrenzt auf direkte, indirekte, konkrete oder Folgeschäden, die aus dem Gebrauch dieser Materialien entstehen können und soweit dies nach anwendbarem Recht möglich ist.*