DECOIT

CeBIT 2015

CeBIT cebit.com HANNOVER 16–20. MÄRZ 2015

IT-Sicherheit „Made in Germany“

Prof- Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
detken@decoit.de

Kurzvorstellung der DECOIT GmbH

- Gründung am 01.01.2001
- Seit 2003: Sitz im Technologiepark an der Universität Bremen
- Fokus: Herstellerneutrale, ganzheitliche Beratung von IT-Lösungen
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
  - Consulting: ganzheitliche sowie herstellerneutrale Beratung
  - Systemmanagement: Umsetzung und Support von Hersteller- oder Open-Source-Lösungen
  - Software-Entwicklung: Entwickeln von Individuallösungen mit hohem Innovationscharakter
  - Forschungsprojekte: innovative IT-Lösungen
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen

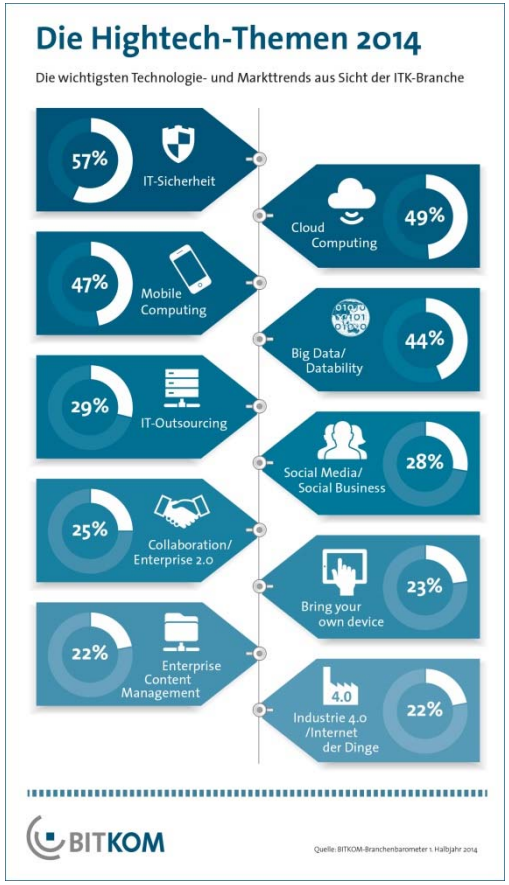
Entwicklung Thema IT-Sicherheit (1)

- Am Anfang stand die Verfügbarkeit und Vernetzung von IT-Services im Vordergrund
- Zur Absicherung wurden Access Control Lists (ACL) auf den Routern und Switches eingerichtet
- Statische Filter ließen sich allerdings nicht pflegen, weshalb diese später verbindungsabhängig (Stichwort: Stateful Inspection) in Firewalls umgesetzt wurden
- Application Ports wurden gesperrt, ohne den Datenverkehr zu analysieren
- Zur Anomalie-Erkennung wurden Intrusion Detection Systems (IDS) versucht einzuführen, ohne den administrativen Aufwand zu berücksichtigen
- Intrusion Prevention Systems (IPS) sollten hingegen Anomalien in der Entstehung verhindern und die Log-Flut eindämmen

Entwicklung Thema IT-Sicherheit (2)

- IPS-Lösungen erhöhten allerdings den Aufwand pro Port und Paket, was bei 10-Gbit/s-Netzen zu Performance-Engpässen führen konnte
- Zudem schafften Protokolle (z.B. SOAP), die über diverse Ports, Schichten und Verschlüsselung kommunizieren zusätzliche Herausforderungen
- Heute sind viele unterschiedliche Insellösungen im Einsatz (AV-, IDS-, IPS-, FW-, VPN-, NAC-Systeme etc.), die keine einheitliche Aussage über Anomalien im Netzwerk zulassen
- Zudem sind die verschiedenen Herstellerlösungen meistens nicht kompatibel zueinander!
- Zusätzlich wurde durch Sicherheitszwischenfälle das Vertrauen, besonders in amerikanische Sicherheitslösungen, gestört

IT-Sicherheit ist wichtigstes IT-Thema



- Aus Sicht der ITK-Branche ist das wichtigste Thema die IT-Sicherheit
- Bewusstsein für die Absicherung von IT-Systemen und den Datenschutz ist gestiegen
- Virenschutz und Firewalls reichen heute bei weitem nicht mehr aus
- BYOD und Smart-Grid-Vernetzung schaffen neue Sicherheitsanforderungen
- Die sichere Cloud-Nutzung ist ebenfalls nicht zu Ende diskutiert

Deutsche IT-Sicherheitslösungen

- Durch die Abhörskandale der NSA werden immer häufiger amerikanische Firmen in Frage gestellt
- Eingebaute „Backdoors“ ermöglichen NSA & Co. den einfachen Zugriff auf IT-Infrastruktur (Beispiel: Router)
- Gefragt sind daher immer mehr deutsche Lösungen!
- Die DECOIT GmbH arbeitet daher an eigenen Lösungen und kooperiert eng mit deutschen Herstellern

NCP SECURE COMMUNICATIONS

macmon nac intelligent einfach

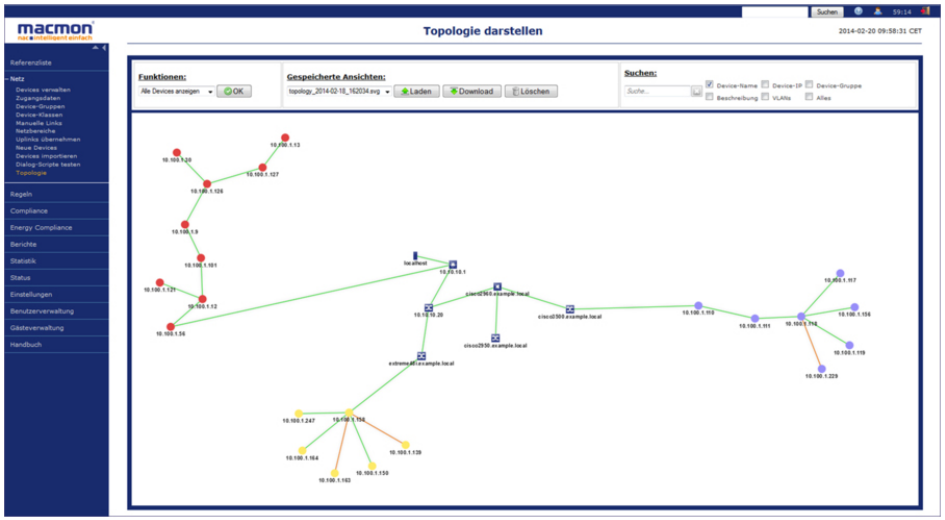
TELCO TECH NETWORK SECURITY ENGINEERED IN GERMANY

SECUREPOINT SECURITY SOLUTIONS

AVIRA

Beispiel macmon secure

- Sofortige Netzwerkübersicht
- Herstellerneutral durch SNMP-Anbindung
- Mehrstufige Zugriffskontrolle
- Mischbetrieb mit/ohne 802.1X
- Anbindung an führende Security-Produkte
- Intelligente Gäste-Verwaltung
- Steuerung des Netzwerkzugangs mobiler Geräte
- Analyse der IT Compliance



Beispiel NCP

- Die GovNet Box ist eine hochsichere VPN-Lösung für die Geheimhaltungsstufe VS-NfD (BSI-Zulassung)
- Sie kann als sichere Remote-Access-Lösung an beliebigen Windows-Endgeräten eingesetzt werden
- Sie enthält einen TPM-Chip der TCG, zur Überprüfung der Integrität
- Die Basis für die Entwicklung wurde in dem F&E-Projekt VOGUE gelegt, welches die DECOIT GmbH von 2009 bis 2011 koordinierte

Open Source Software (OSS)

- Neben deutschen Herstellern, gibt es auch verschiedene Open-Source-Projekte, die sich gegenüber proprietären Lösungen wie folgt auszeichnen:
  - Quellcode ist offengelegt und kann eingesehen werden
  - Bugs werden kommuniziert und umgehend beseitigt
  - Offene Schnittstellen und Formate werden verwendet
  - Weltweite Community pflegt den Software-Code
  - Keine Lizenzkosten
  - Keine Backdoors

DECOIT

Auswahl von Open-Source-Projekten

- Firewall- und VPN-Gateway pfsense, iptables
- VPN-Einwahl durch OpenVPN, FreeRADIUS
- Monitoring mit Icinga, Nagios, check_mk
- Netzwerk-/Rechner-Scan mit Nessus, Nmap, OpenVAS
- Identity Management mit UCS
- Anti-Viren-Lösung mit Comodo, ClamAV
- Anti-Spam-Lösung mit SpamAssassin
- Angriffserkennung durch Snort

pfSense OpenVPN UCS ICINGA freeRADIUS MK check SNORT SpamAssassin ClamAV Nessus Nmap COMODO OpenVAS

Consultancy & Internet Technologies

DECOIT

Beispiele Open Source

- Nmap: Werkzeug zum Scannen und Auswerten von Hosts in einem Computernetzwerk und fällt in die Kategorie der Portscanner.
- OpenVAS: Software-Framework aus verschiedenen Diensten und Werkzeugen und bildet eine Lösung für Schwachstellen-Scanning und Schwachstellen-Management.
- Snort: Network Intrusion Detection System (NIDS) und ein Network Intrusion Prevention System (NIPS). Es kann zum Protokollieren von IP-Paketen und zur Analyse von Datenverkehr in IP-Netzwerken in Echtzeit eingesetzt werden.

DECOIT

Verwendung von Open Source

- Viele Hersteller setzen auf Open Source Software (OSS) in ihren eigenen Produkten
- Beispiele sind z.B. *iptables* in Firewall-Systemen oder *SpamAssassin* in Anti-Spam-Lösungen
- Dadurch ist selbst in „deutschen Lösungen“ kein 100%iger Herstellercode enthalten
- Aufgrund der Offenheit und Standardkonformität sowie der Lizenzkostenfreiheit können allerdings oftmals OSS-Lösungen gegenüber geschlossen Herstellerlösungen punkten

Forschungsprojekte „IT-Sicherheit“

- Um das Thema IT-Sicherheit herum wurden und werden von der DECOIT GmbH diverse F&E-Projekte durchgeführt:

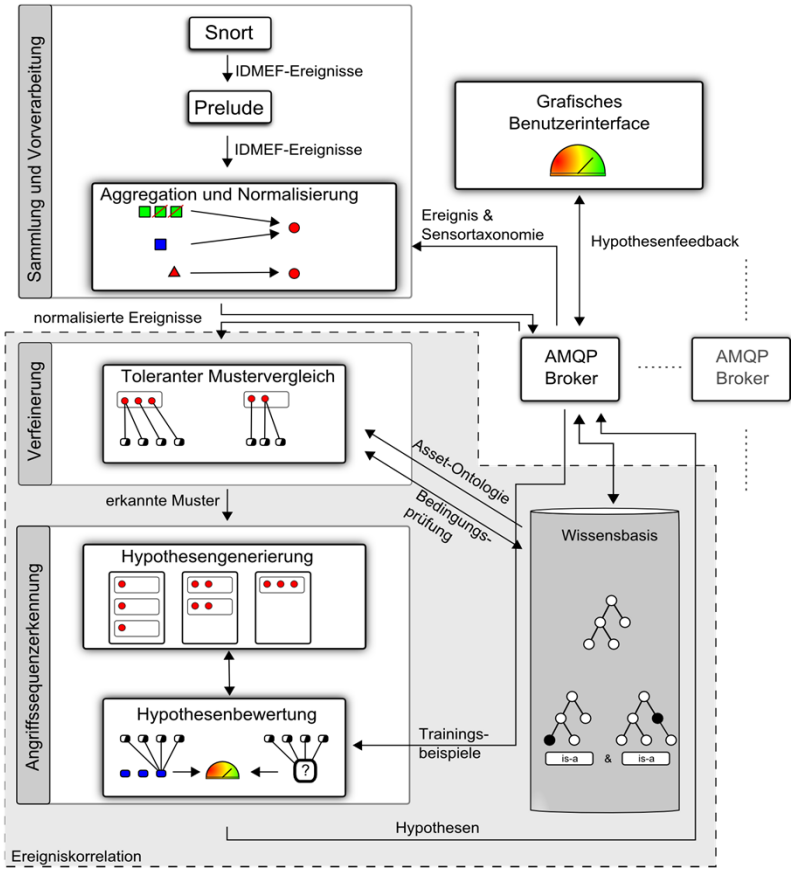
- Zusätzlich ist man in der Trusted Computing Group (TCG) aktiv, um die Themen TNC, NAC, IF-MAP, TPM etc. weiter voranzutreiben

www.imonitor-project.de

- Das iMonitor-Projekt vom BMWi startete im Juli 2013 und wird im Juni 2015 enden
- Partner des „Bremer Projektes“ sind:
  - DECOIT GmbH (Koordination, Entwicklung, Verwertung)
  - Universität Bremen, TZI (Entwicklung)
  - neusta GmbH (Entwicklung, Verwertung)
- Es soll eine neue Form der Ereigniskorrelation umgesetzt werden, die automatisiert neue Angriffsvarianten erkennt
- Korrelationsregeln sollen dabei nicht mehr nur manuell gepflegt werden müssen

www.imonitor-project.de

- Ziele von iMonitor
  - Integration von Sensorik
  - Entwicklung optimierter und skalierbarer KI-Verfahren
  - Datenschutzgerechten Austausch von Wissen über Sicherheitsvorfälle
  - Kombination mit anderen SIEM-Systemen
  - Verbesserung der Erläuterungen von Diagnosen von gemeldeten Vorfällen

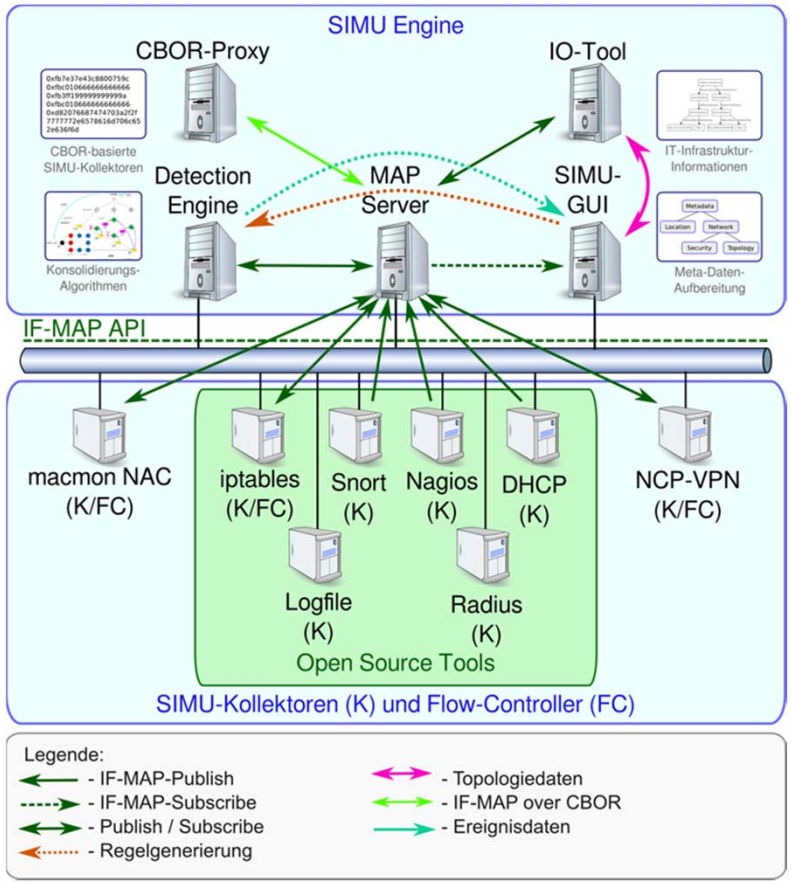


www.simu-project.de

- Das SIMU-Projekt vom BMBF startete im Oktober 2013 und wird im September 2015 enden
- Partner des Projektes sind:
  - DECOIT GmbH (Koordination, Entwicklung, Verwertung)
  - Hochschule Hannover (Entwicklung, Veröffentlichung)
  - Fraunhofer SIT, Darmstadt (Entwicklung, Veröffentlichung)
  - macmon secure gmbh (Entwicklung, Verwertung)
  - NCP GmbH (Entwicklung, Verwertung)
- Es soll eine leichte Integrierbarkeit in KMU-Infrastrukturen ermöglicht werden
- Die Nachvollziehbarkeit von relevanten Ereignissen und Vorgängen im Netz soll gegeben sein
- Geringer Aufwand für Konfiguration, Betrieb und Wartung

www.simu-project.de

- SIMU-Kollektoren und –Flow-Controller
  - IF-MAP-Clients
  - IF-MAP-Graph zur Analyse und intuitiven Regelerstellung
- SIMU-Engine
  - MAP-Server
  - Detection Engine
  - SIMU-GUI



Zusammenfassung

- Die Bundesregierung hat die Notwendigkeit erkannt, und wird auch in Zukunft Fördergelder im Bereich IT-Sicherheit im großen Umfang bereitstellen
- Dabei werden besonders „deutsche Lösungen“ favorisiert
- Die DECOIT GmbH ist als Open-Source-Spezialist besonders an offenen und herstellerneutralen Lösungen interessiert
- Nur durch offenen Quellcode können letztendlich Backdoors verhindert werden!
- Zielsetzung ist auch zukünftig durch Kooperationen mit deutschen Sicherheitsherstellern „deutsche Sicherheitslösungen“ mit zu entwickeln oder die Basis dafür zu legen

DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09