Anhang: Ein Fallbeispiel

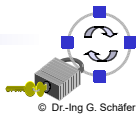
Das Internet-Analyse-System (IAS) als Komponente einer IT-Sicherheitsarchitektur

- Motivation
- Konzept
- Technik
- Auswertungsverfahren
- Beispiele
- Fazit und Ausblick

Die nachfolgenden Folien wurden zur Verfügung gestellt von:

Frank Waibel

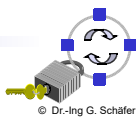
Bundesamt für Sicherheit in der Informationstechnik (BSI)
(präsentiert: 11. Deutscher IT-Sicherheitskongress, 12.05. - 14.05.2009, Bonn)



Motivation

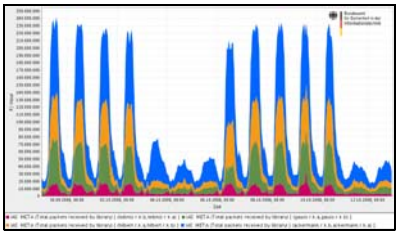
- Konzeption und Entwicklung des Internet-Analyse-Systems (IAS) als Beitrag zur IT-Krisenreaktion.
- Hintergrund: Nationaler Plan zum Schutz der Informationsinfrastrukturen (2005), UP Bund (2007)
- Aufbau eines nationalen IT-Frühwarnsystems im BSI:

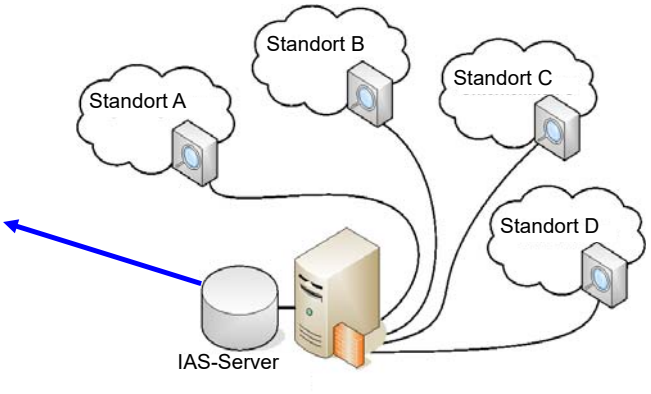
*”Aufgrund belastbarer Erkenntnisse über **drohende oder bereits eingetretene IT-Vorfälle**, die noch möglichst wenige betreffen, wird ein **nationales IT-Sicherheitslagebild** fortgeschrieben und bei ausreichender Relevanz eine **qualifizierte Warnung** an potenziell betroffene Bereiche verteilt, um dort zu erwartende **Schäden zu vermeiden oder zu verringern**.“*



Zielsetzung

- Zentrale Darstellung des Ist-Zustands des Internets
- Erfassung anonymisierter Daten / Datensparsamkeit
- Aufbau einer Datenbasis zur Profilgenerierung
- Zustandsüberwachung und Anomalieerkennung



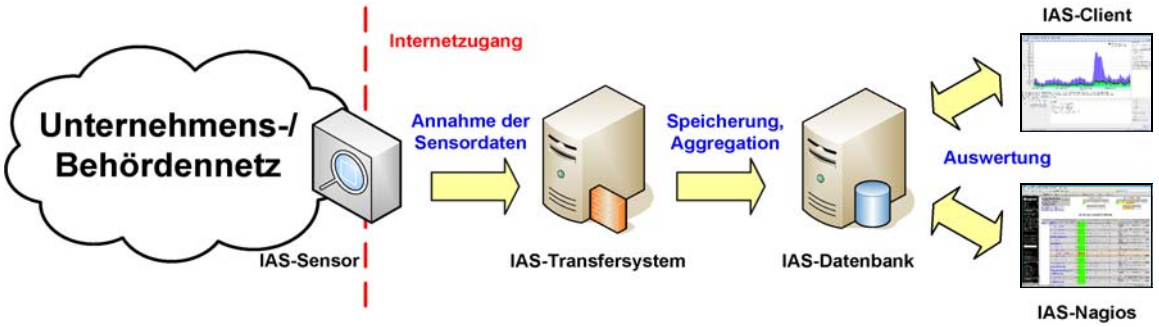


Entwicklungspartner: Institut für Internetsicherheit

Zeitraum: 2005-2008

Konzept des IAS

- Verteiltes System aus Sonden und Auswertungsstationen
- Platzierung der IAS-Sonden in Unternehmens-/Behördennetzen
- Passive Verkehrsanalyse und Erhebung von Zählerständen
- Periodische Übertragung an zentrales Annahmesystem
- Speicherung in Datenbank zur weiteren Analyse



Abgrenzung zu anderen Systemen

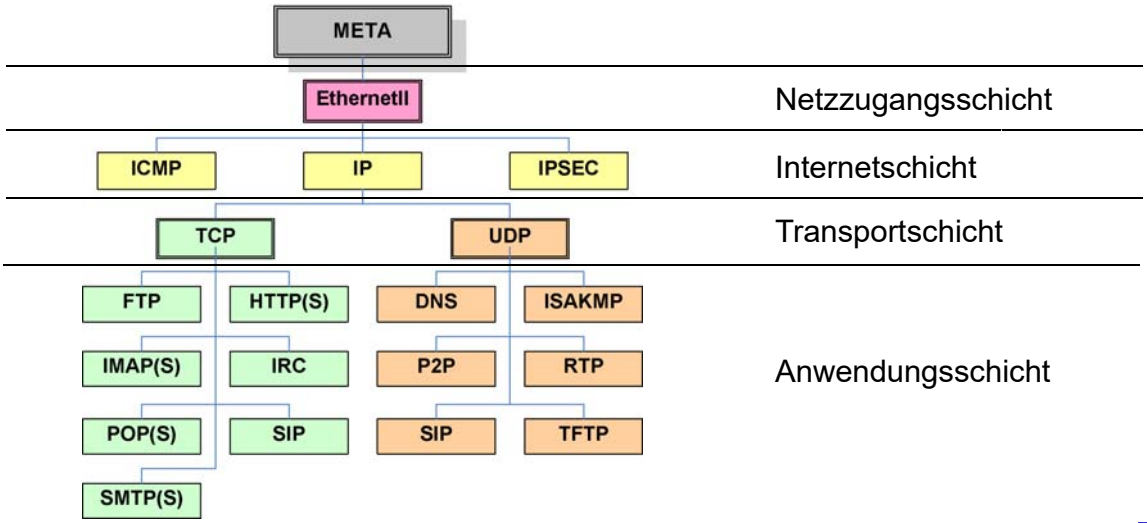
- Die Sensorik des IAS
  - erfasst keine IP-Adressen,
  - setzt keine TCP-Flows zusammen,
  - verwirft nach Abarbeitung eines Paketes seinen Kontext,
  - prüft nicht auf Signaturen,
  - arbeitet passiv, d.h. sie verändert den Datenstrom nicht,
  - wird nicht geroutet, d.h. keine eigene IP-Adresse, kein Ziel.

Datenschutz

- Damit grenzt sich die Sensorik ab von
  - reinen Paketsniffern oder NetFlow,
  - Firewalls, Application-Level-Gateways,
  - IDS / IPS, Honeypots.

Analysemodule der Sondensoftware

- Erfassung von Zählerständen für Protokollmerkmale (Deskriptoren)
  - ➡ Headerinformationen nach Anonymisierungsraster
- Orientierung an TCP/IP-Referenzmodell:



Beispiel: Analyse eines DNS-Pakets (1)

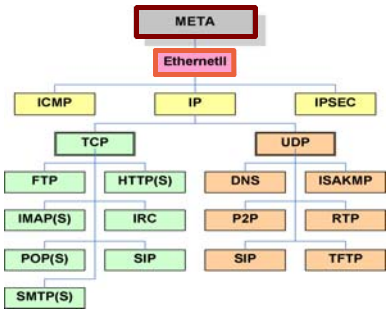
Netzwerkpaket

00 19 b9 e3 85 54 00 18 8b d6 c6 16 08 00 45 00 00
3b 86 a0 40 00 40 11 01 58 c0 a8 01 1c 53 ec 9d 09
d7 db 00 35 00 27 b2 f2 e4 bd 01 00 00 01 00 00 00
00 00 00 03 77 77 77 06 67 6f 6f 67 6c 65 02 64 65
00 00 01 00 01

descriptor	counter	description
1	1	META (Total packets received by library)
7	1	META (Total packets received by probe)
33	1	META (packet size 64-127 bytes)

...

Modul: META



Folgemodul: ETHERNET

Beispiel: Analyse eines DNS-Pakets (2)

Netzwerkpaket

00 19 b9 e3 85 54 00 18 8b d6 c6 16 08 00 45 00 00
3b 86 a0 40 00 40 11 01 58 c0 a8 01 1c 53 ec 9d 09
d7 db 00 35 00 27 b2 f2 e4 bd 01 00 00 01 00 00 00
00 00 00 03 77 77 77 06 67 6f 6f 67 6c 65 02 64 65
00 00 01 00 01

descriptor	counter	description
1	1	META (Total packets received by library)
7	1	META (Total packets received by probe)
33	1	META (packet size 64-127 bytes)
67586	1	EthernetII (type 0x0800 (ip))

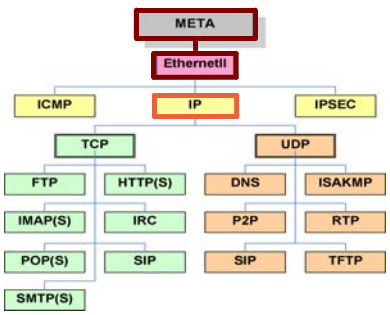
.....

Modul: ETHERNET

00 19 b9 e3 85 54 00 18 8b d6 c6 16 08 00

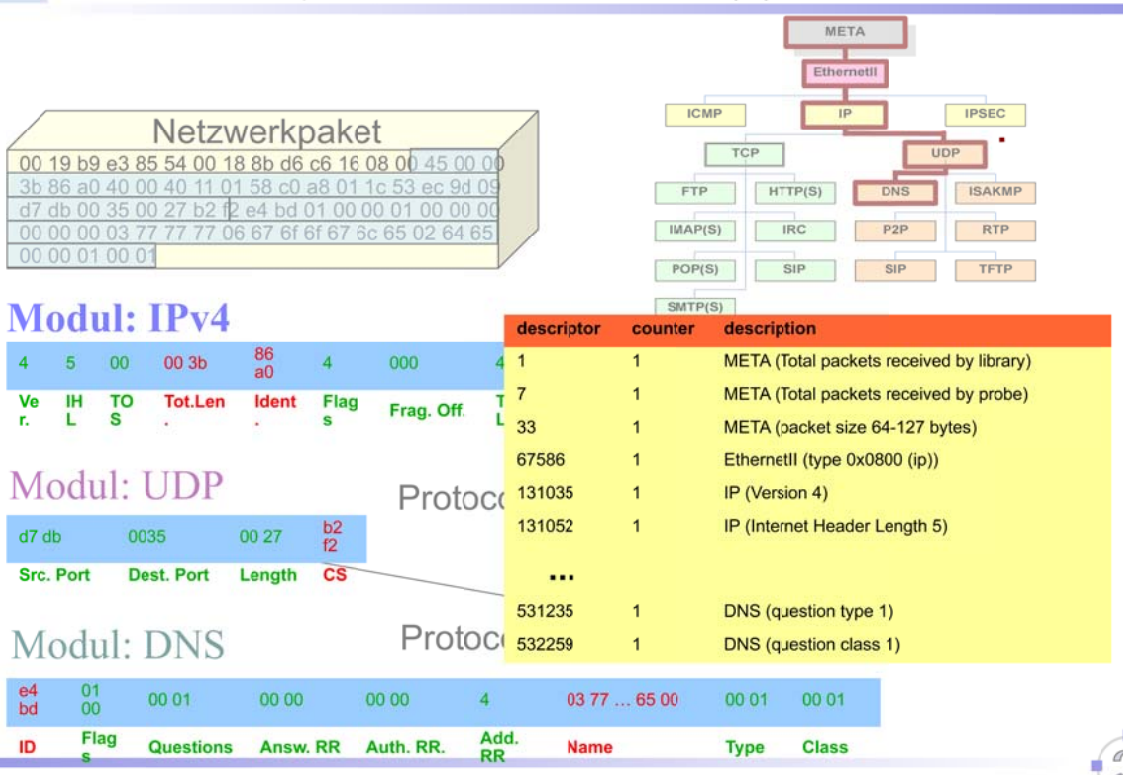
Dest. Addr. Src. Addr. Type

Type 0x800 = IPv4



Folgemodul: IP

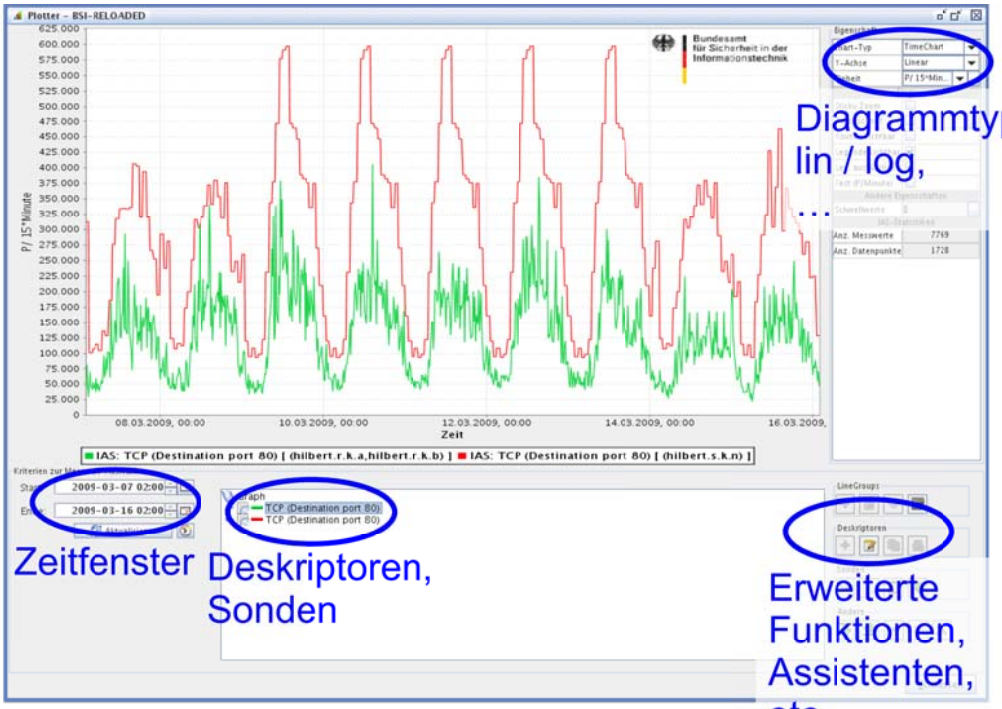
Beispiel: Analyse eines DNS-Pakets (3)



Das IAS im BSI

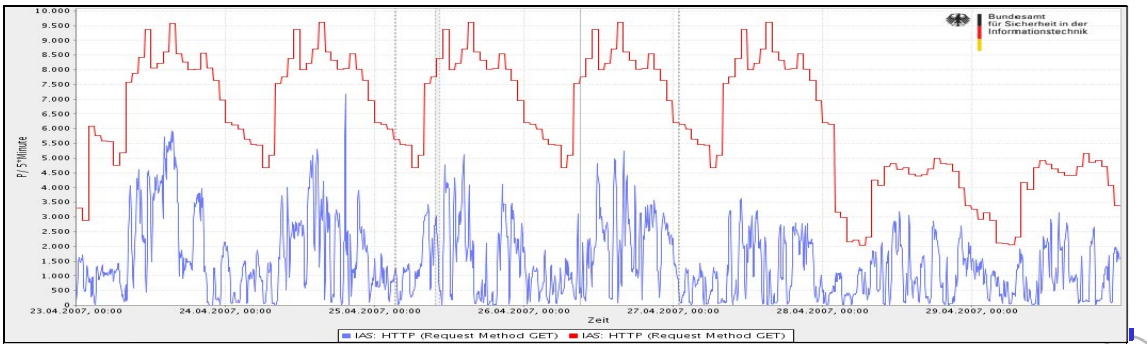
- 6 Sensoren, Fokus auf Regierungsnetzen
- Regelmäßige Auswertungen:
  - Tägliche Lagebeobachtung im Lagezentrum (IAS-Nagios)
  - Beitrag zur monatlichen BSI IT-Sicherheitslage / Quartalslageberichten
- Des Weiteren:
  - Einzelfallanalysen
  - Statistiken, Trends
  - Vorfallsbearbeitung
- Eigenständige Erweiterung und Pflege der Sondensoftware
- Optimierung der Auswertungsverfahren

IAS-Client zur manuellen Recherche



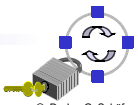
Anomalieerkennung

- Vorberechnung von Schwellenwerten (nach Tschebyscheff)
  - für ausgewählte Deskriptoren
  - basierend auf Messwerten der letzten Wochen
  - Unterscheidung von Tagestypen / stundengenau
- **Schwellenwert = Mittelwert + (Faktor * Standardabw.)**
- „pragmatischer“ Ansatz, erfahrungsbasiert.
- Liefert Indizien, ggf. für sicherheitskritischen Vorfall.



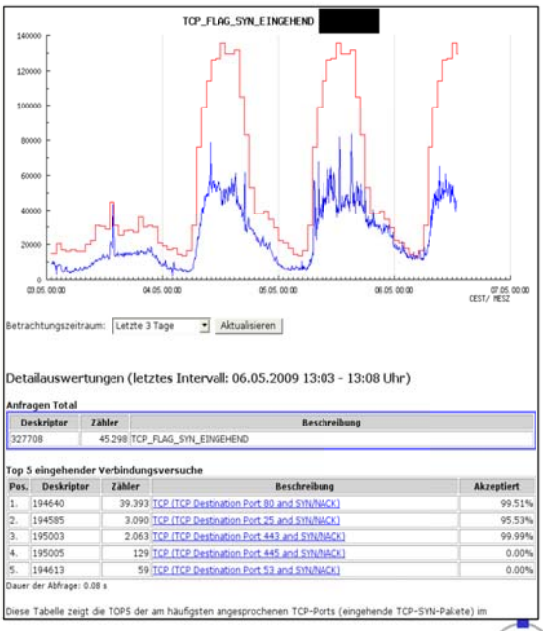
IAS-Lagebild mit Nagios

- Transparente Integration des IAS in Nagios (www.nagios.org)
- Abbildung von IAS-Entitäten auf Nagios-Elemente
  - (Sonden-)Standort → Host
  - Dienst-/Protokollmerkmal → Service
- Überwachung ausgewählter Dienste für einzelne Standorte
  - Fokus: Verfügbarkeit / Integrität
  - Merkmale: charakteristische Nutzungsprofile
  - z.B. auf Anwendungsebene: HTTP, SMTP, ...
- Bei Schwellenwertüberschreitung Benachrichtigung per E-Mail
- **Ziel: Automatische Erkennung von Anomalien als Hinweise auf (unerwünschte) Veränderungen**

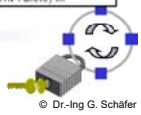


IAS-Lagebild mit Nagios (2)

- Direkte Auswertung via Weboberfläche möglich

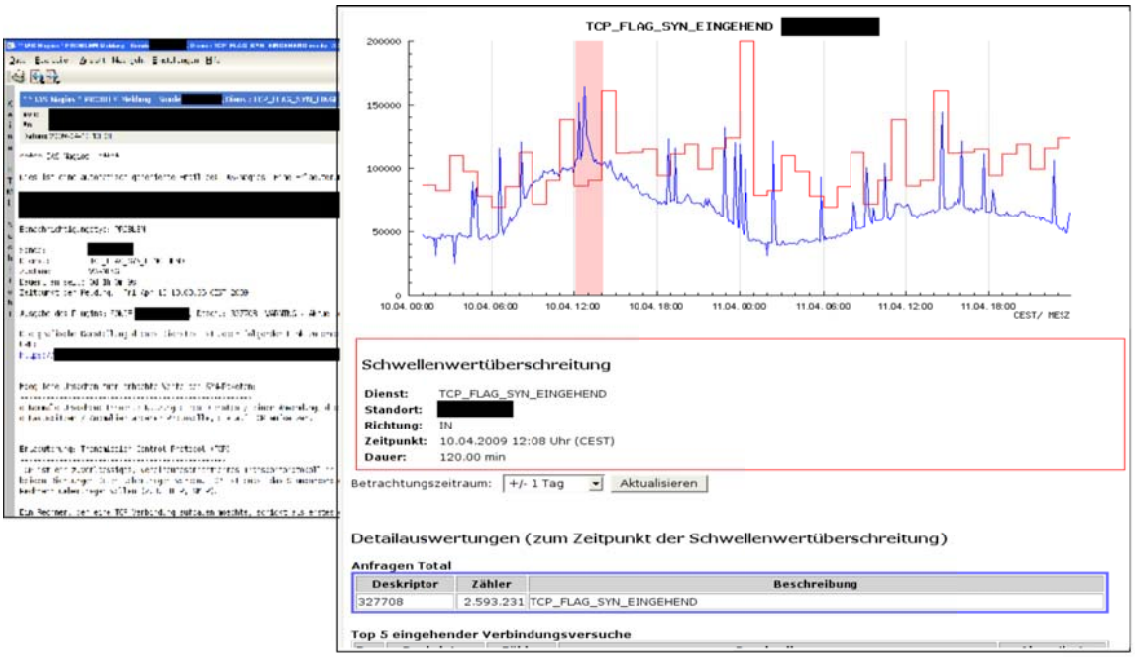


- Für jeden Dienst:
  - Grafische Darstellung
  - Detailauswertungen
  - Allgemeine Erläuterung
  - Interpretationshinweise
  - Zusatzinformationen

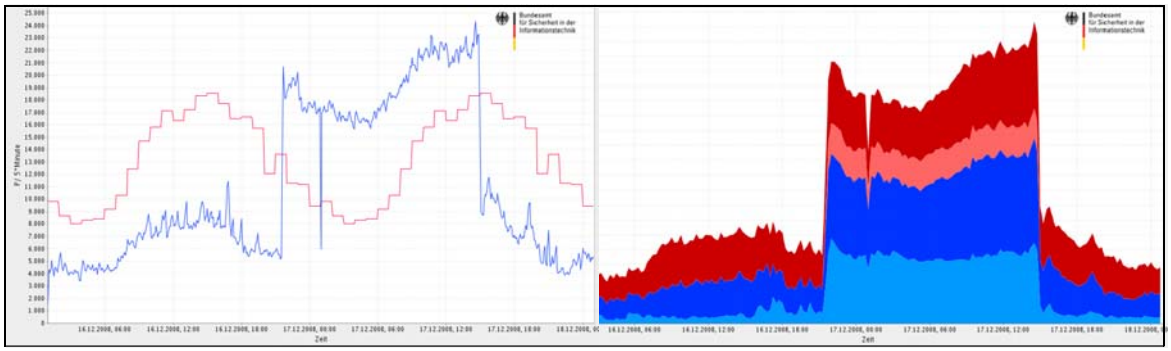


Warnung bei Anomalie

- E-Mail mit Link auf automatisch generierte Informationen:



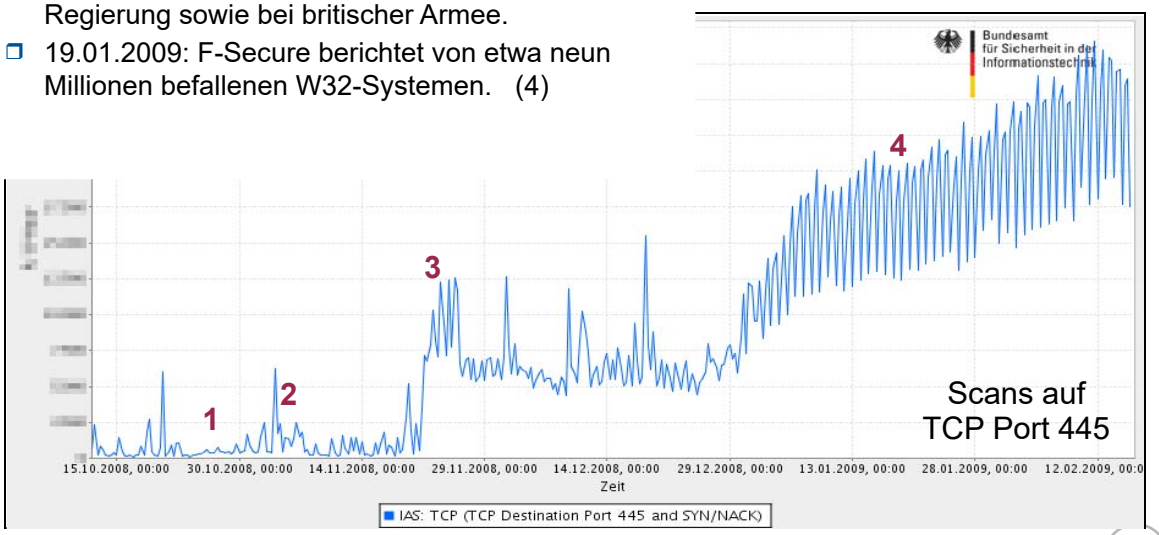
Beispiel: DNS Anomalie (12/2008)



- Im Dezember 2008: Anhaltende Spitze bei eingehenden DNS-Anfragen in mehreren Netzen
- IAS-Analyse zeigt, dass die Anfragen auf NS-Records zielen und teilweise abgewiesen werden
- Nachfrage bei Netzbetreibern und Partnern nach weiteren Informationen
  - Ergebnis: Anfragen zielen auf ".", und tragen als Absender zwei offensichtlich gespoofte osteuropäische IP-Adressen.
  - Vermutung: "reflected DDoS-attack"
  - Bestätigung: ISC SANS, 2009-01-18: *DNS queries for ".".*

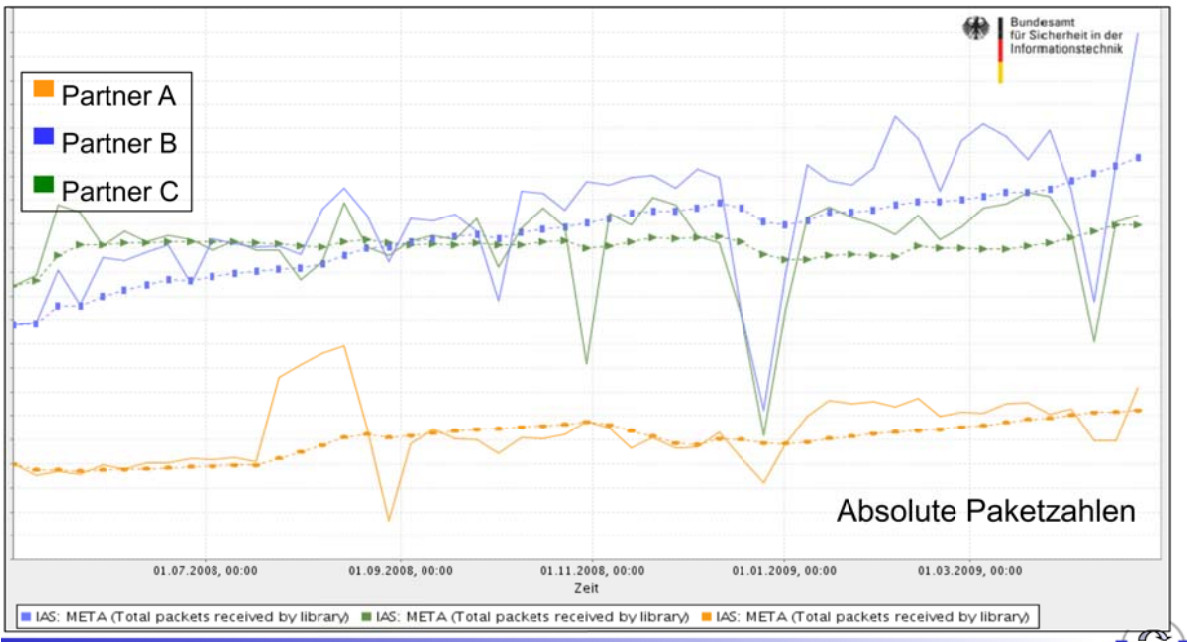
Beispiel: Conficker-Wurm

- 23.10.2008: Schwachstelle in Windows-RPC-Dienst, Exploit über Port 445/TCP möglich. → CERT-Bund Warnung (1)
- 03.11.2008: Wurm zu MS08-067 „in the wild“ gesichtet. (2)
- 27.11.2008: Microsoft beobachtet zunehmende Verbreitung. (3)
- Januar 2009: Wurm-Infektionen in Kärntner Regierung sowie bei britischer Armee.
- 19.01.2009: F-Secure berichtet von etwa neun Millionen befallenen W32-Systemen. (4)



Beispiel: Entwicklung Gesamtverkehr

Anstieg des beobachteten Verkehrs um bis zu 40%



Fazit und Ausblick

- Die IAS-Sensorik erhebt keine personenbeziehbaren Daten.
- Mit Anomalieerkennung und manueller Recherche lassen sich – trotz abstrakter Daten – viele Erkenntnisse gewinnen.
- Täglicher Einsatz des IAS im BSI-Lagezentrum und den Fachreferaten:
  - Lagebeobachtung
  - Vorfallsbearbeitung
  - Trendanalysen
- Kontinuierliche Weiterentwicklung der Auswertungen

➡ Das IAS leistet einen wichtigen Beitrag zur Netzsicherheit und ergänzt andere Quellen um wertvolle Zusatzinformationen

Mehr Informationen über das IAS erhältlich bei

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Frank Waibel
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5762
Fax: +49 (0)22899-10-9582-5762

frank.waibel@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de