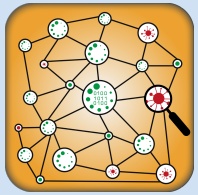
Internet-Analyse-System

Kommunikationslagebild für Unternehmen



Was ist das IAS?

Das Internet-Analyse-System (IAS) des Instituts für Internet-Sicherheit ist ein datenschutzfreundliches Analyse-Werkzeug für Unternehmensnetzwerke.

Mit Hilfe des IAS wird ein **Kommunikationslagebild** generiert, mit dessen Hilfe Informationen über die Nutzung von Technologien im Netzwerk erkannt, Zustände beobachtet und Probleme analysiert werden können.

Beispiel: Im Falle eines erkannten Angriffs kann das IAS hilfreiche und vielfältige Informationen liefern.

Hintergrund

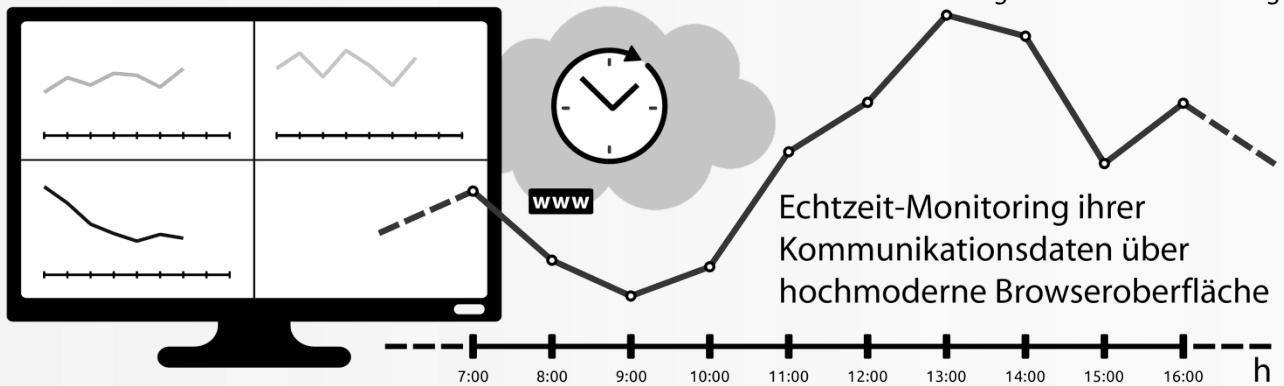
Unternehmen werden immer häufiger das Ziel von Cyber-Angriffen, bei denen immer größere Schäden entstehen. Dies hat erhebliche Beeinträchtigungen für den Unternehmenserfolg und deren Partner zur Folge.

Ziele

- **Übersicht & Bewertung** der Kommunikationslage von Unternehmen
- **Erkennung** von Angriffen & Bedrohungssituationen sowie vorhandenen Schwachstellen
- **Analyse & Auswertung** der erkannten Situationen
- **Vergleich** der Sicherheitslage zwischen Unternehmen (noch in der Entwicklung)

In der Angriffserkennung werden u.a. Anomalien gesucht und bei ihrer Entdeckung Warnmeldungen generiert. Die Ursachen können dann analysiert und interpretiert werden. Die exakte Kenntnis des aktuellen Zustands gewährleistet die Einschätzung von Bedrohungen. Mithilfe historischer Daten können signifikante Änderungen des Verkehrsaufkommens bewertet werden. Das Kommunikations-lagebild ist Basis für Maßnahmen zum Schutz und Erhalt der Funktionsfähigkeit des Netzwerkes.

Abbildung 1: Echtzeit-Monitoring



if(is) internet-sicherheit.

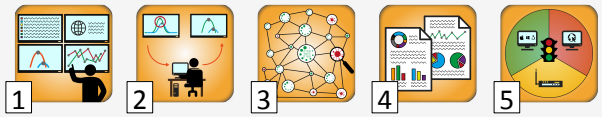
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
https://www.internet-sicherheit.de

Nutzen

Das IAS zeigt den Gesundheitszustand im Innern und Äußeren des Netzwerks. Es erlernt den Normalzustand der ein- und ausgehenden Kommunikation des Unternehmens. Auf dieser Basis können Abweichungen im Verlauf erkannt werden.

Dazu eröffnet das IAS einen Einblick in die verwendeten Technologien im eigenen Netzwerk wie Betriebssysteme, Browser, Verschlüsselungen, Versionsnummern, uvm. Damit können Schwachstellen im eigenen Netzwerk aufgedeckt werden. Auf diese Weise erlangen Sie Wissen über externe Bedrohungen und interne Schwachstellen und schaffen eine Basis zur Formulierung einer nachhaltigen **Sicherheitsstrategie**.

Funktionsbausteine



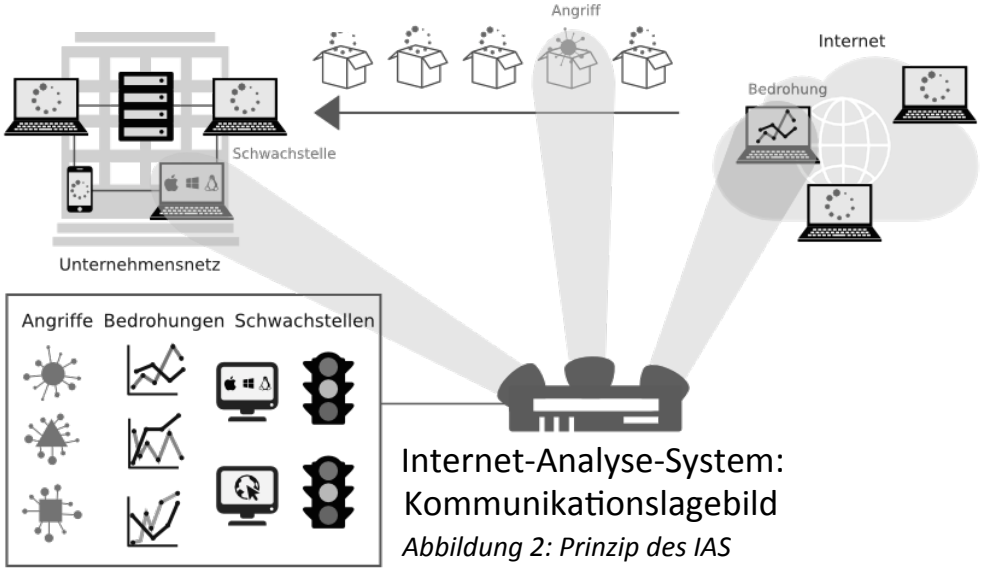
1. Das Kommunikationslagebild kann live im **Echtzeit-Monitoring** verfolgt werden.

2. Im **Expertensystem** können tiefergehende Analysen auch auf Basis der Vergangenheitsdaten vorgenommen werden.

3. Die **Angriffserkennung** analysiert den Traffic in mehreren Schritten auf Angriffe und Anomalien und sendet Warnungen aus.

4. Über definierte Zeiträume fasst ein **Reporting-System** relevante Informationen kompakt zusammen und stellt diese elektronisch zu.

5. Das **Reputationssystem** bewertet Technologien im Netzwerk in Bezug auf ihre Sicherheit.



Internet-Analyse-System: Kommunikationslagebild

Abbildung 2: Prinzip des IAS

Referenzsystem (in der Entwicklung)

Das Lagebild zu kennen ist gut – zu wissen wie man im Vergleich in seiner Branche dasteht ist wünschenswert. Es hilft, seine Sicherheit zielgerichtet durch das Aufdecken von Schwächen zu verbessern. Zu diesem Zweck werden die Daten von Teilnehmern **anonym** gesammelt, analysiert und vergleichbar gemacht.

Dafür suchen wir Partner!

Teilnahme in nur drei Schritten

1. Gemeinsame Planung & Beschaffung der Hardware
2. Installation der IAS-Sonde & Zugang zum System
3. Nutzung des Systems

(über **Kontakt** oder **www.spotuation.de**)

Was wird benötigt?

Das IAS verwendet zur Datenaufnahme einen eigenen **Sensor**. Dies ist ein Rechnersystem, das über seine Netzwerkkarte einen passiven Abgriff auf die Kommunikationsdaten eines Netzwerkes durchführt.

Die benötigte **Hardware** des Sensors für einen Durchsatz von 100 Mbit/s:

- Quad-Core-Rechner (Linux), 8GB
- RAID1 & 2 Netzwerkkarten

Funktionsweise

Der Sensor wird zum Beispiel am Mirror-Port des Routers installiert (siehe Abbildung 3). Dort analysiert er Informationen aus dem breiten Kommunikationsdatenstrom mit. Dabei reduziert der Sensor die Netzwerkdaten auf ein Minimum, um eine effiziente Analyse des Datenverkehrs zu ermöglichen.

Es bleiben alle wesentlichen Informationen erhalten, die Aufschluss über den Zustand und die Nutzung des Netzwerks liefern.

Datenabgriff

Die Rohdatenerfassung gliedert sich in drei Teile (siehe Abbildung 4). Links befindet sich schematisch das Internet. Es sind Pakete von drei unterschiedlichen Anwendungssitzungen dargestellt, im Beispiel SMTP-, FTP- sowie HTTP-Pakete. Die Pakete aus dem Internet werden in zufälliger Reihenfolge nacheinander von der Sonde ausgewertet (s. Abb. 4, Box 1).

Anschießend werden alle aus Sicht des Datenschutzes bedenkliche Daten gelöscht

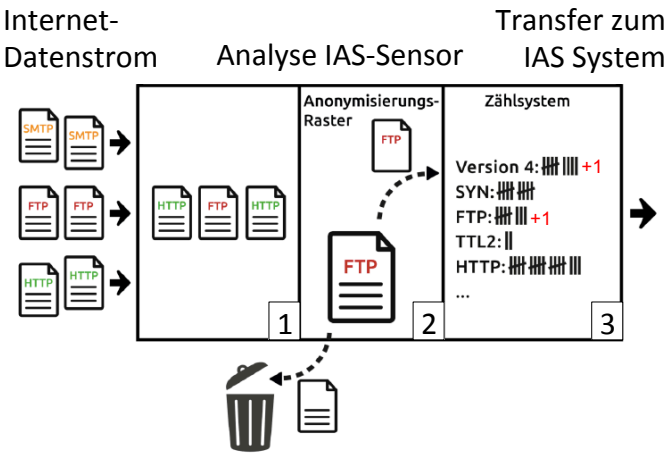


Abbildung 4: Darstellung Sensoranalyse

und unbedenkliche Header-Informationen der Pakete im Zählsystem gezählt (s. Abb. 4, Box 2).

Ähnlich wie bei einer Strichliste wird die Häufigkeit bestimmter Kommunikations-parameter, wie z.B. der Zielport eines TCP-Pakets, festgehalten (s. Abb. 4, Box 3).

Die vollständig anonymisierten Zählerstände (Rohdaten) werden von den Sensoren zu analytischen Zwecken gespeichert. Sie können entweder am eigenen System verarbeitet oder auch zu einem externen Analysesystem z.B. am if(is) übertragen werden.

Die gesammelten Rohdaten geben Aufschluss über die verwendeten Technologien im Netzwerk und geben ein repräsentatives Kommunikationslagebild über die Nutzung der analysierten Kommunikationsleitung ab.

Datenschutzrechtliche Bewertung

Das IAS verarbeitet lediglich die Rohdaten, die nach dem Löschvorgang des Sensors verbleiben. Diese enthalten Zählerstände als Ganzzahlen, die keine personenbezogenen Daten enthalten (nach § 3 Abs. 1 BDSG). Somit sind datenschutzrechtliche Regelungen nicht anwendbar, wodurch das IAS datenschutzkonform ist.

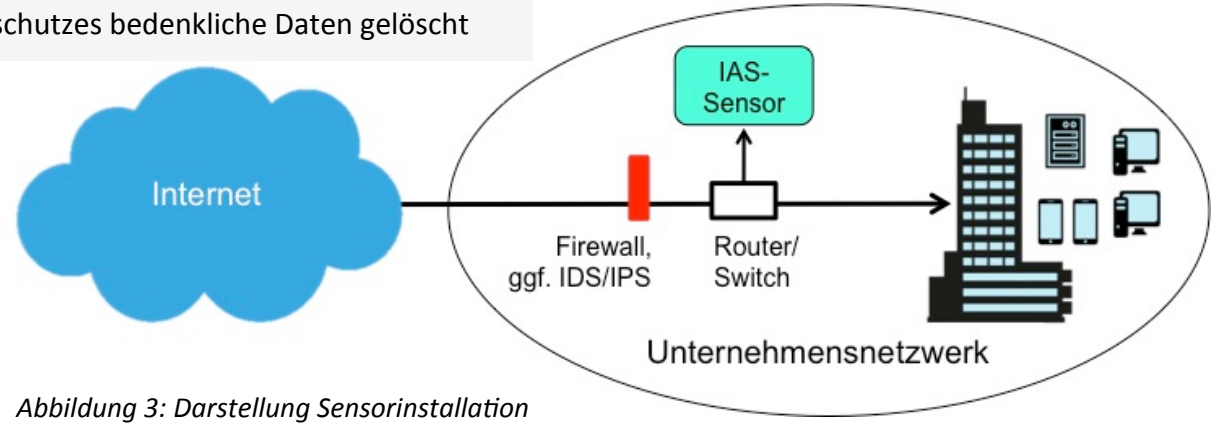


Abbildung 3: Darstellung Sensorinstallation

Kontakt

Diego Sanchez
Institut für Internet-Sicherheit - if(is)
Internet-Frühwarnsysteme (IFS)
Westfälische Hochschule Gelsenkirchen

Mail: sanchez@internet-sicherheit.de
Tel.: +49 (0)209 9596-876
Mobil: 0176 3202 5354