



Automatisiertes erkennen von „Grooming“ in (sozialen) Netzen

Markus Grüneberg

Public Sector Security Spezialist



Wo ist eine technische Zensur in der Demokratie durchsetzbar,

*....gehen wir aktiv oder proaktiv gegen
Missstände im Netz vor,*

..welche Maßnahmen sind im Netz heute realisierbar und wie wird darauf reagiert?

Akzeptierte Technologien – Hilfreiche Unterstützung...



www.norton.de/onlinefamily

**“Grooming” erkennen/vermeiden
vs.
Informationsaustausch realisieren**

Herausforderungen ...

- Soziale Netze
 - Jugendschutz vs. offene Netze - Akzeptanz
 - Nutzen unterschiedlichster Kommunikationswege
 - Bieten keine/kaum sicherheitstechnischen Schnittstellen
- Eltern
 - Regelmäßiges (Echtzeit) beaufsichtigen der Kinder
 - Interesse an der Erziehung
- Provider/Dienstleister
 - Wirtschaftliches Interesse
 - Bei Infrastrukturtechnologien – “Datenschutzfrage”

Annahmen ...

- Schutz wird von den Eltern (evtl. Politik) forciert
 - Interesse an der Thematik
 - Gemeinsame Einrichtung mit Kindern
 - Bereitschaft zum Aufwand / Installation
- Am Endgerät
 - Regelmäßiges (Echtzeit) beaufsichtigen der Kinder
 - Unterstützung durch Tools
- Provider/Dienstleister
 - Tatsächliche Nachfrage durch Endkunden
 - Einrichten einer “FSK” – Infrastruktur (Mobile/DSL)

Wesentliche Fragen zum Grooming ...

Wie findet eine solche Kommunikation statt?



In welcher Dynamik ändert sich die Kommunikation?




Wie kann man davor schützen?



Klassifizieren von Inhalten


DCM
Beschreibend



Definierte Daten

Variablen
Wörterbücher

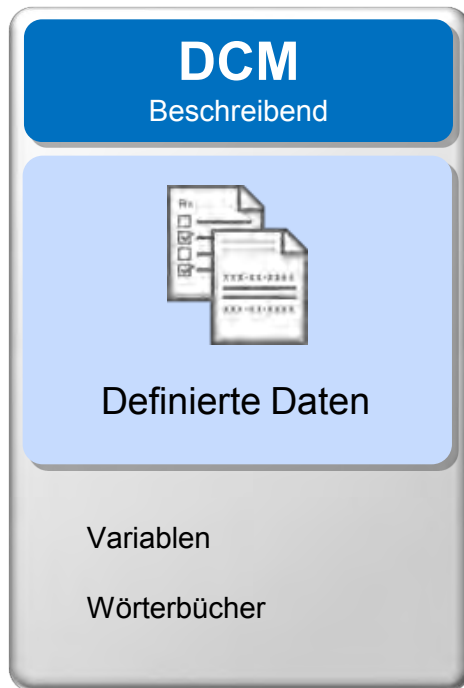
IDM
Indizierend



Unstrukturierte Daten
Geistiges Eigentum

Dynamische
Textinhalte

Klassifizieren von Informationen



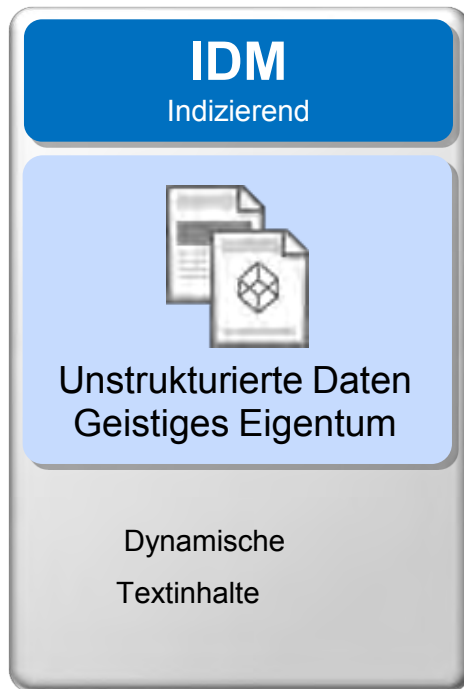
Vorteil:

Einfach zu definierende Wörter/Wortgruppen.
Zählt die Anzahl der „Incidents“

Nachteil:

Reagiert nicht auf „dynamisches“ Verhalten.
Funktioniert nicht in Echtzeit

Klassifizieren von Informationen



Vorteil:

Reagiert auf „dynamisches“ Verhalten.

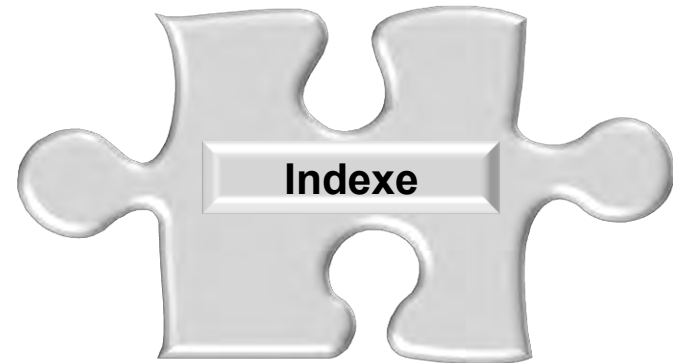
Klassifiziert in Echtzeit

Nachteil:

Muss ständig „gepflegt“ werden.

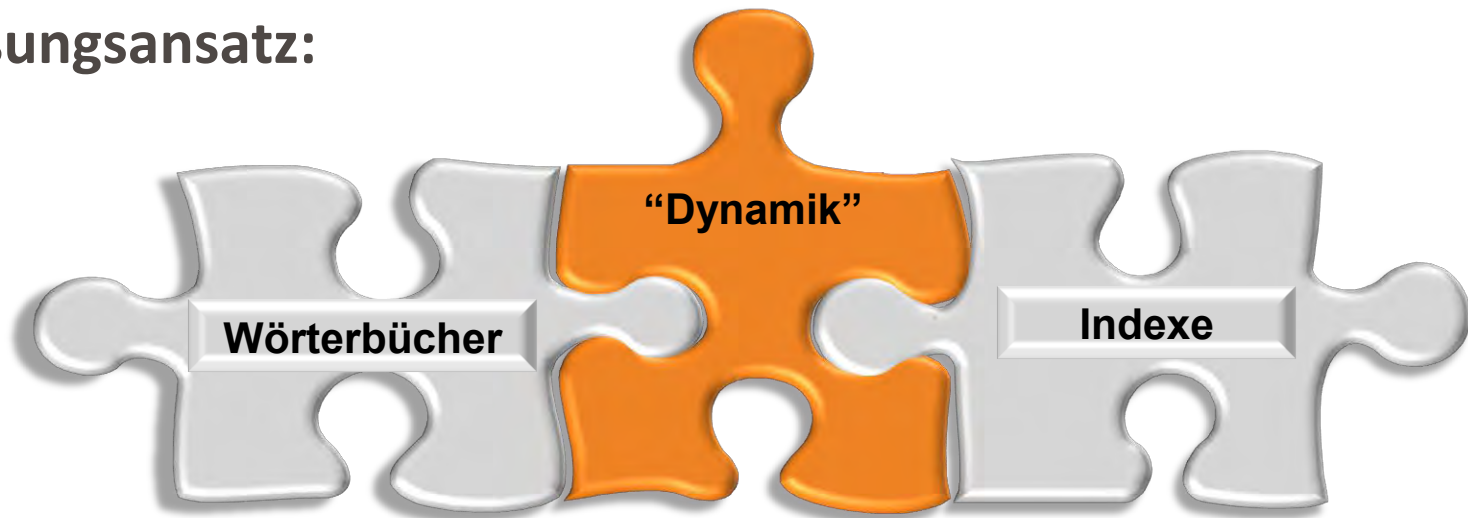
Automatische Pflege der “dynamischen” Kommunikation

Herausforderungen bei der Erkennung in “Echtzeit”:

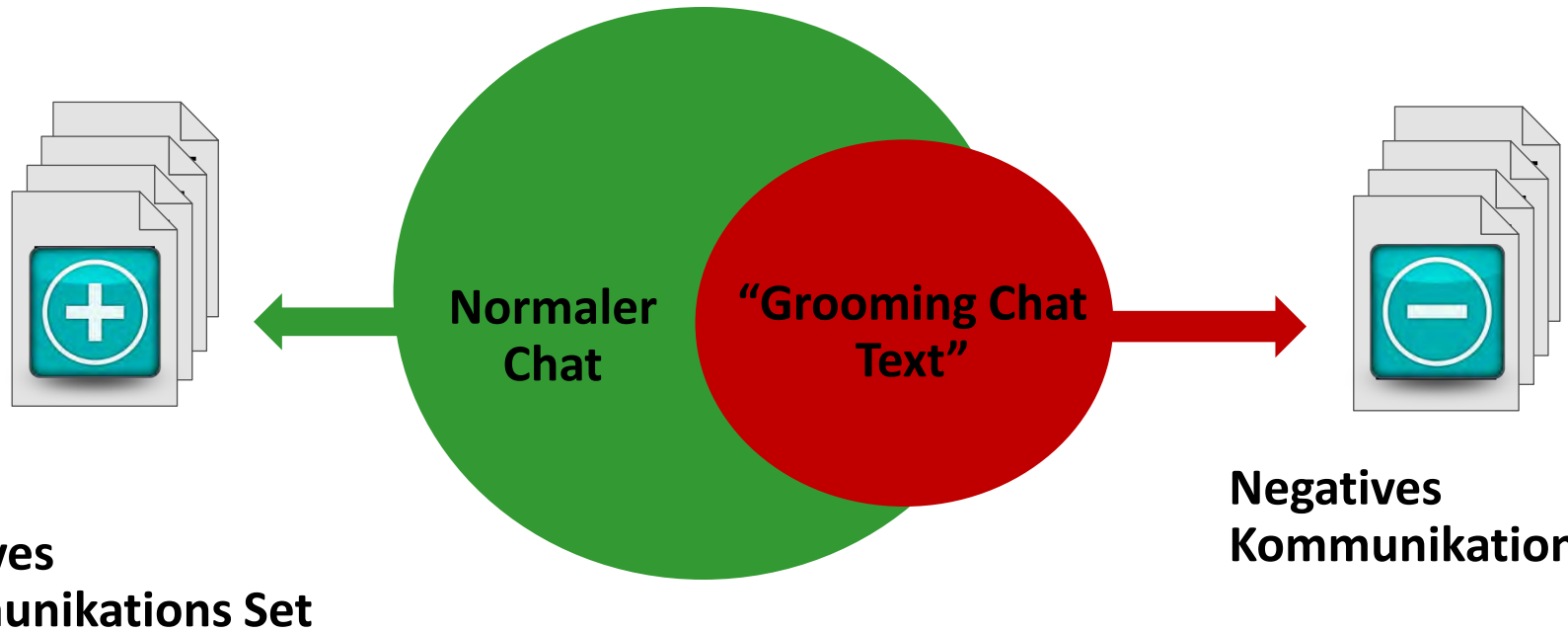


Automatische Pflege der “dynamischen” Kommunikation

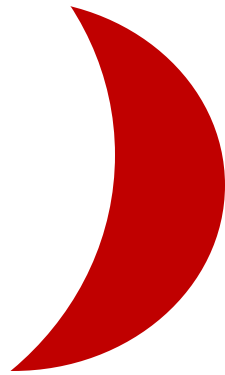
Lösungsansatz:



Automatische Pflege der “dynamischen” Kommunikation

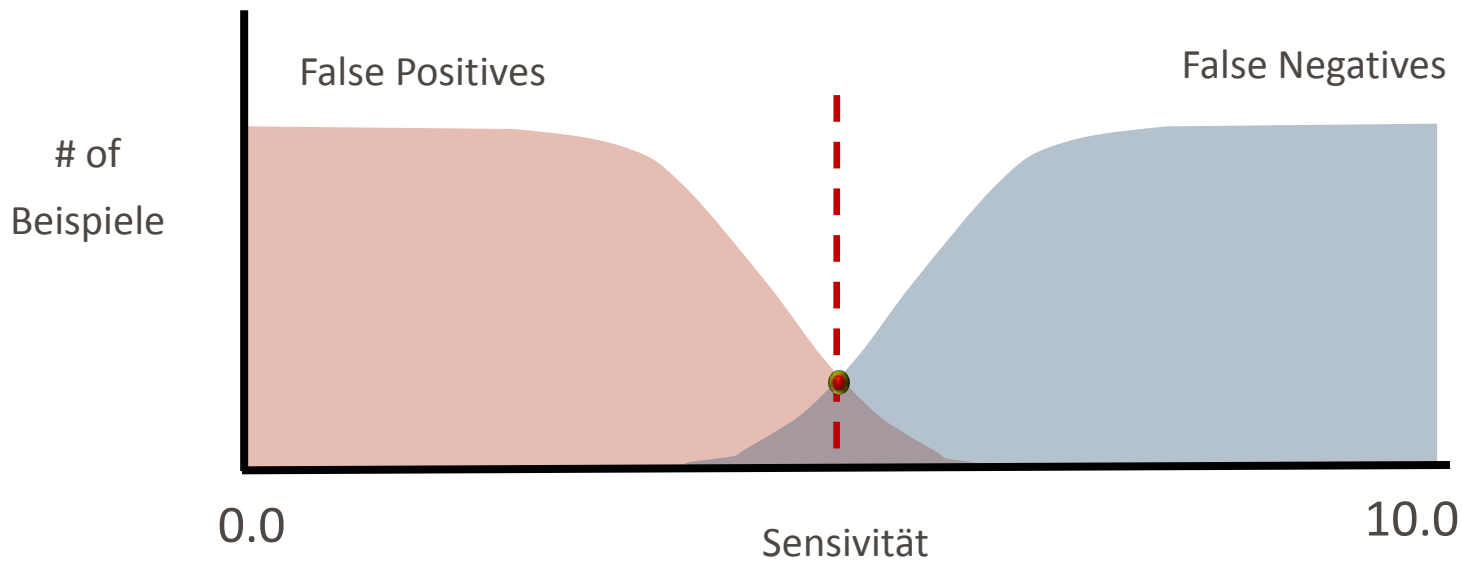


Automatische Pflege der “dynamischen” Kommunikation

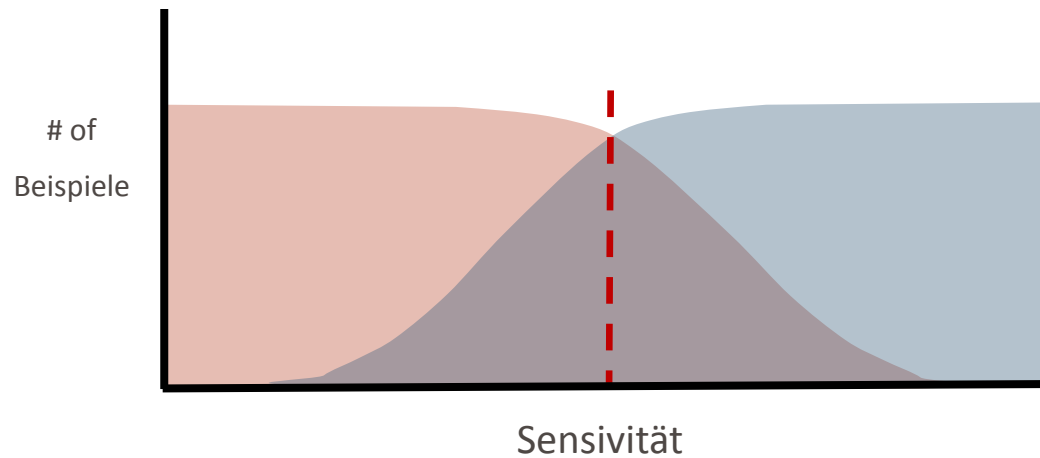
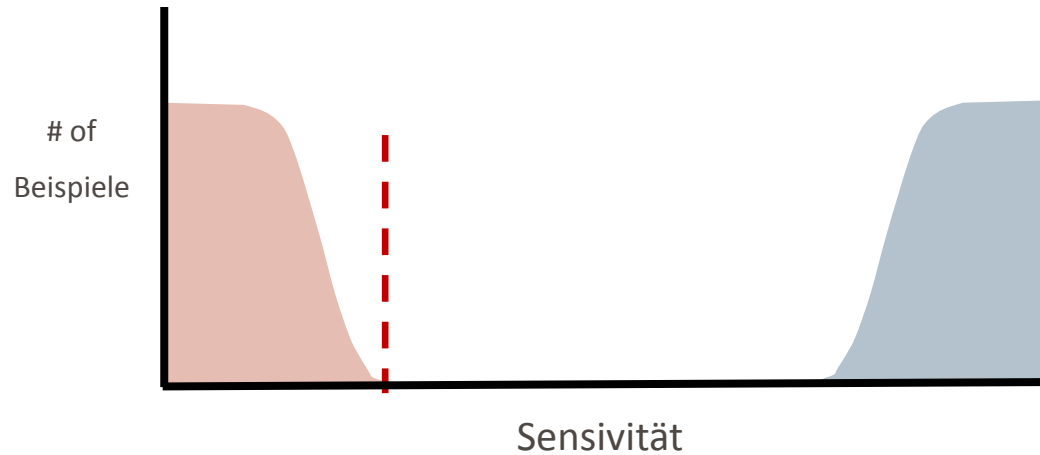


**“Delta” der Inhalte
(Phrasen, Wörter,
Wortgruppen)**

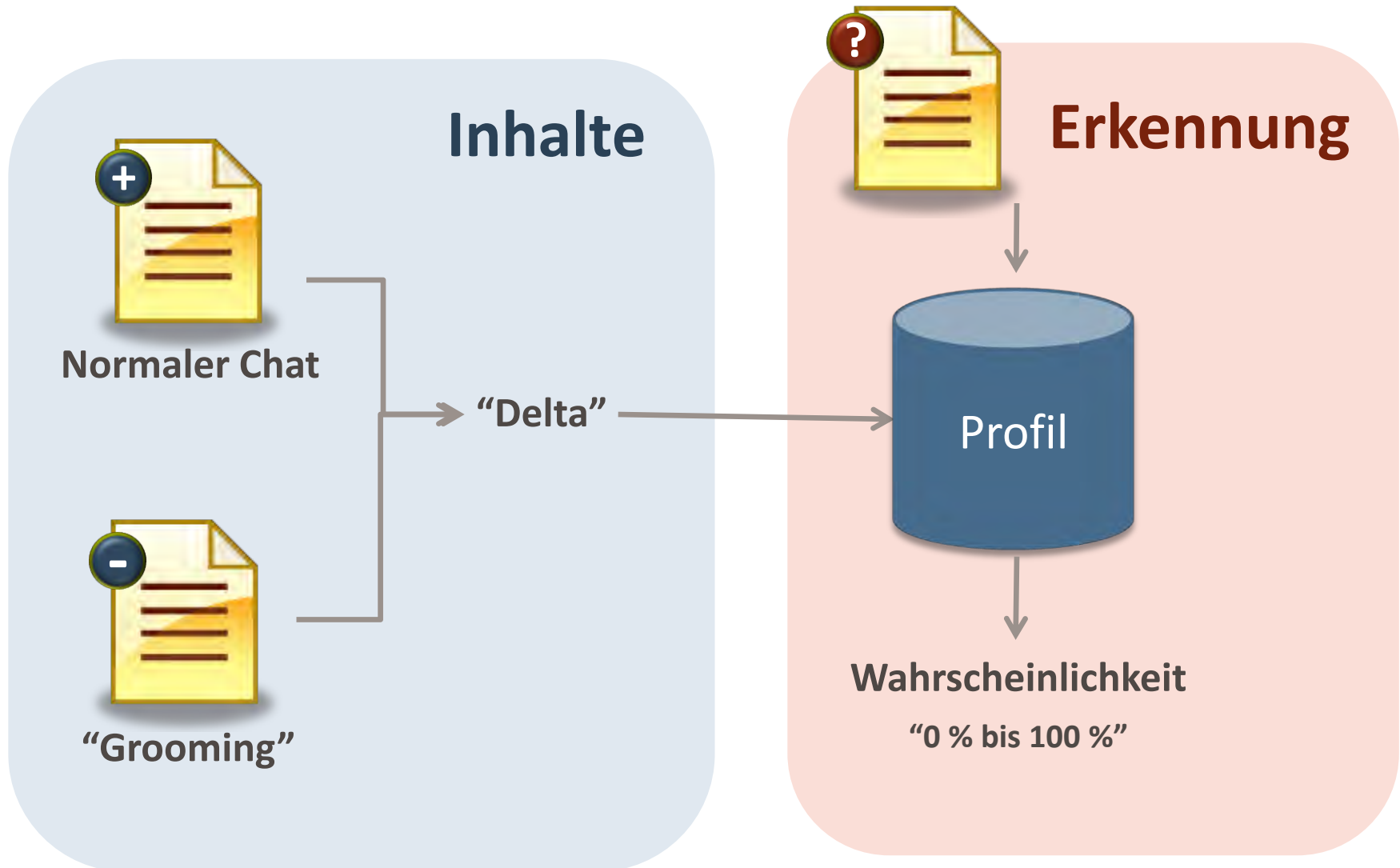
Automatische Pflege der “dynamischen” Kommunikation



Automatische Pflege der “dynamischen” Kommunikation



Automatische Pflege der “dynamischen” Kommunikation



Automatisches Erkennen der "dynamischen" Kommunikation

Incident 00002435

Status: **New**
Severity: **High**

SMTP

Key Info | History | Notes | Correlations

Policy Matches

Policy	Matches
JPMC Test Policy [view policy]	66
Test JPMC (Vector Machine Learning)	66

Incident Details

Server: [vontu-monitor-one](#)
Date: 9/9/10 4:12 PM
Sender: [Unknown](#)
Recipient: [vontu.demo@gmail.com](#)
Subject: [Here's what I think you're looking for ...](#)
Attachments: [MSNMessageState.cpp](#)

Data Owner Name: [[change](#)]
Data Owner Email Address: [[change](#)]

Message Body

Attached: [Open Original Message](#)

Matches (matches found in 1 component)

MSNMessageState.cpp (66 Matches):

Similarity Score: 9.8 out of 10.

```
#include "stdafx.h" #include "MSNMessageState.h" #include "MSNPParser.h" #include "AutoArrayPtr.h" MSNMessageState::MSNMessageState(MSNMessageInputStream * rParserState, rDataLength_t rDataLength) { ... &rbIsPartialData, ChildProtocolInfo & rChildProtocolInfo) { UNREFERENCED_PARAMETER( rDataOffset); rChildProtocolInfo.m_ChildProtocolType.m_strProtocolType.clear(); // Reset the flag. rbIsPartialData = false; if (0 < rInputStreamReader.Available()) { //Adjust the size o...partial data is to be read. c_size_t iSizeOfDataToBeRead = dynamic_cast< MSNPParser &>( rStateParser).GetDataBlockSize() - m_iSizeOfPartialDataRead; /* AutoArrayPtr<<_byte_t> spachMessageData = AutoArrayPtr<<_byte_t>(new c_byte_t[ iSizeOfDataToBeRead]); */ String strMessageData; c_status_t lRet = rInputStreamReader. Read ( strMessageData, iSizeOfDataToBeRead); C_ RETURN_ERROR_IF_FAILED (lRet); ... C_ RETURN_ERROR_IF_FAILED ( lRet); m_strMessageData += strMessageData; m_iSizeOfPartialDataRead += strMessageData.length(); rDataLength = (long) strMessageData.length(); //Check if the data read is complete or partial if ( strMessageData.length() != iSizeOfDataToBeRead) { rbIsPartialData = true; rParserStateData = strMessageData; } else { rParserStateData = m_strMessageData; SkipEndOfPacketBytes ( rInputStreamReader); } } else rbIsPartialData = true; return C_ SUCCESS; } c_uint8_t MSNMessageState:: NextExpectedState () { return MSNPParser::keMSNEndOfParsing; ...
```

Attributes

No custom attributes defined

Ein Möglicher Ansatz

Möglichkeiten bei der Erkennung

Finden

2



- Starten der Erkennung um verdächtige Inhalte auf dem Endpunkt zu erfassen

Überwachen

3



- Kontrolle der Inhalte in Echtzeit
- Überwachen von Ereignissen (Fotoupload/Links)

Schützen

4



- Normale Kommunikation zulassen
- Blockieren, oder Entfernen
- Benachrichtigen der Eltern

1



- Definieren der Inhalte für die Erkennung

Verwalten

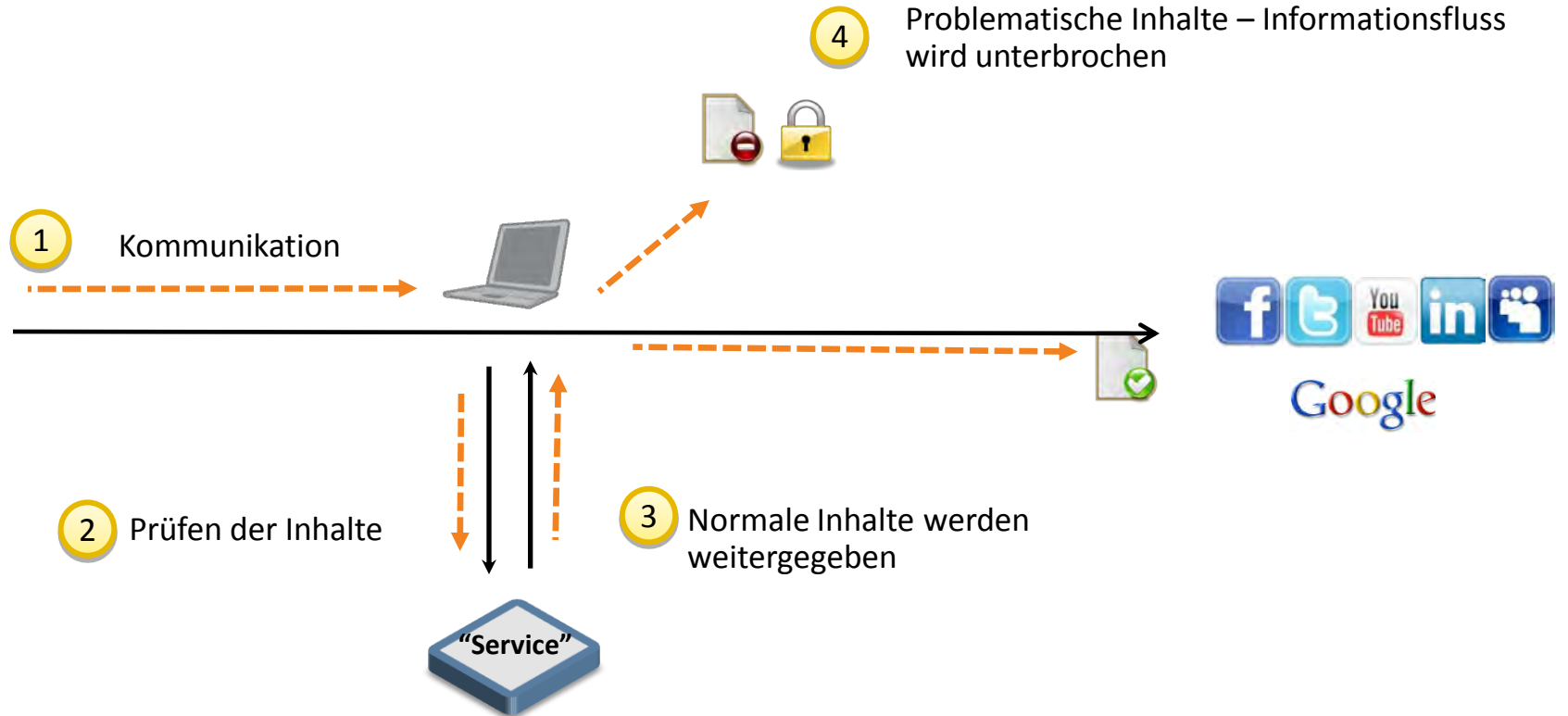
5



- Berichten bei Auffälligkeiten und Vorfällen

Überwache die Kommunikation

Eingehende und Ausgehende Kommunikation







Punkt.

Markus Grüneberg

Markus_Grueneberg@Symantec.com

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.