Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Ein Kommunikationslagebild
→ für mehr IT-Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

Agenda

1. Politischer Hintergrund
2. Funktionsweise und Vergleich zu Alternativen
3. Vorteile von spotuation
4. Zukunft von spotuation
5. Einsatz der Technologie
6. Mögliche Zusammenarbeit
7. So können Sie teilnehmen!

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Politischer Hintergrund „Cyber-Sicherheit“

„Kooperation von Staat, Wirtschaft, Gesellschaft.“

„Meldepflicht von Sicherheitsvorfällen von Unternehmen für große Statistik für die Frühwarnung“

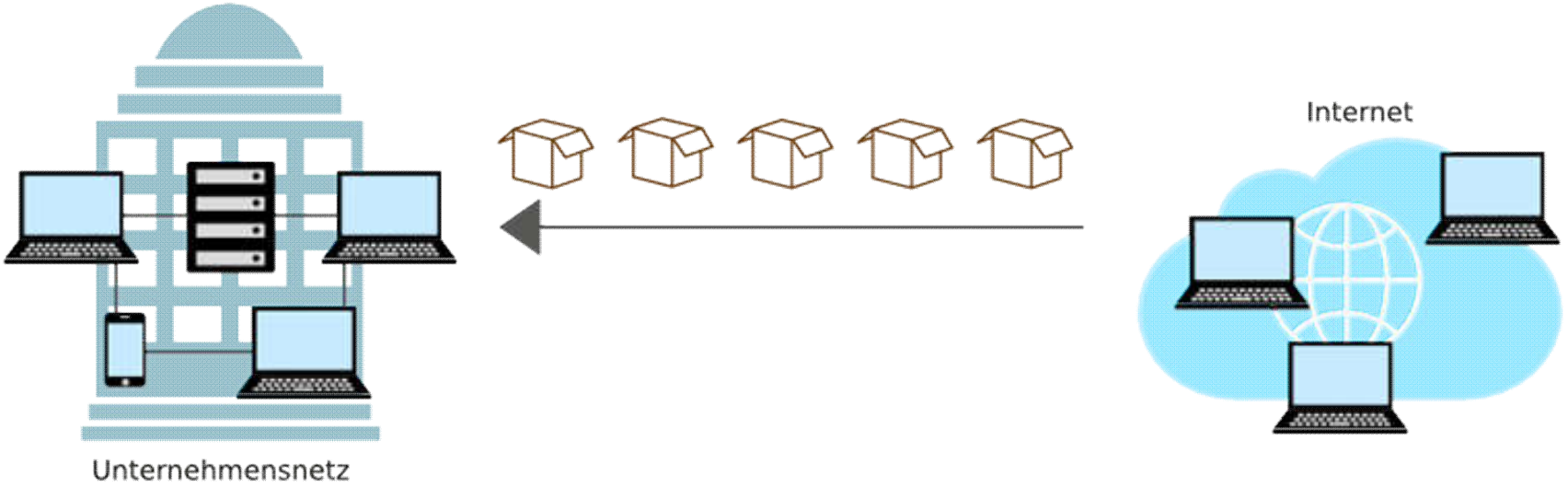
Bundesamt für Sicherheit in der Informationstechnik

Unsere Position:

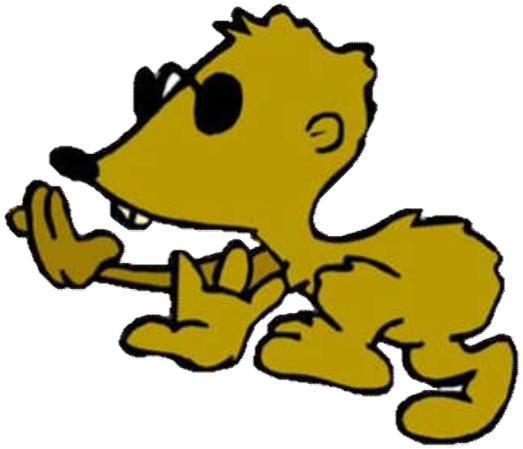
- Generierung eines Lagebildes der Unternehmenskommunikation zwischen Netzwerk(en) und dem Internet
- Vertrauenswürdige und datenschutzkonforme Kooperation
- Vergleich von Kommunikationslagebildern im Sinne der BSI-Initiative zur Früherkennung & zum gemeinsamen Lernen im Umgang mit Gefahren

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Ohne „spotuation“ (Kommunikationslagebild)
→ Was passiert in unserem Netzwerk?



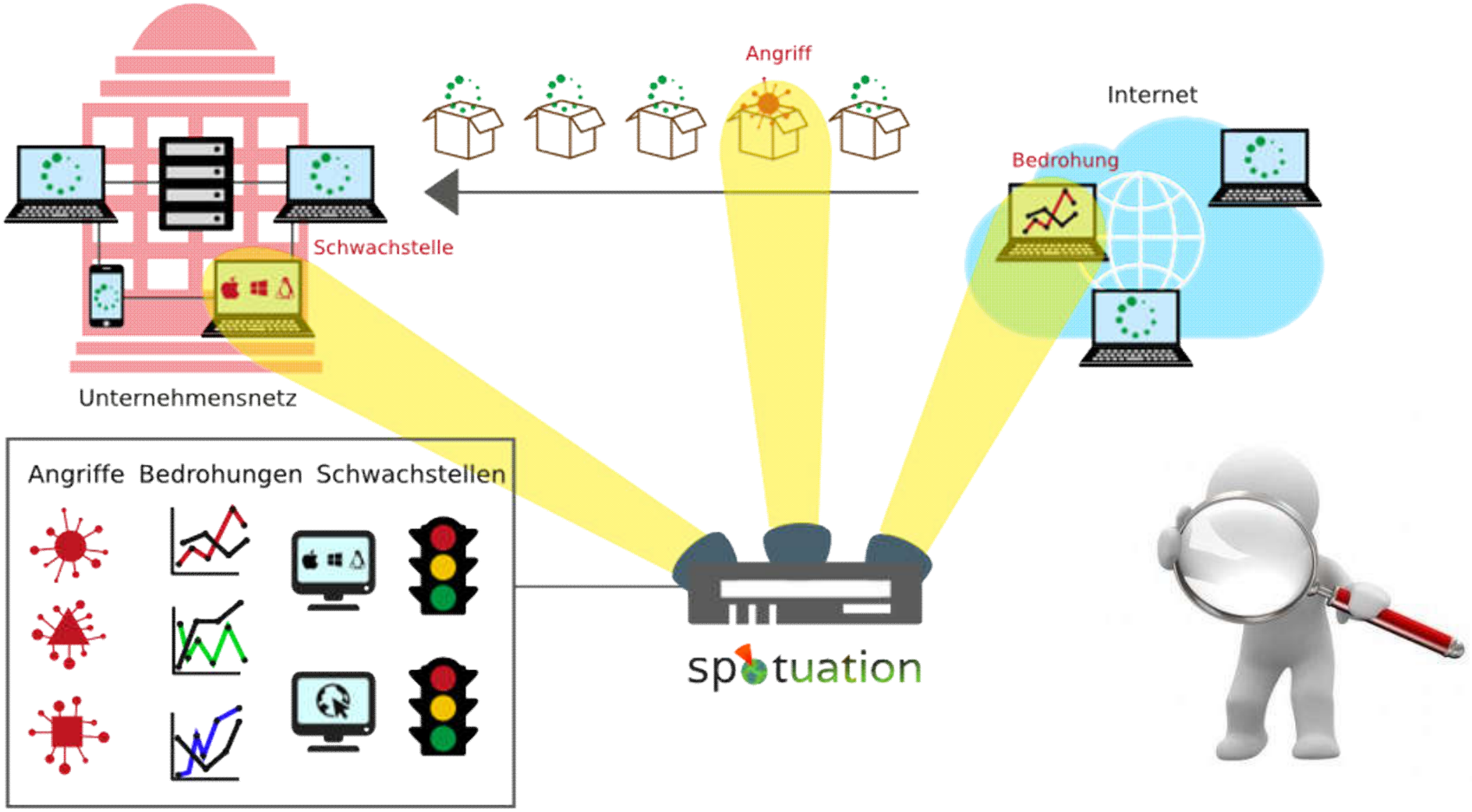
- Wer greift auf das Netzwerk zu?
- Wie sieht das Netzwerk aus?
- Welche Gefahren gibt es?
- Welche Schwachstellen sind vorhanden?



© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Mit spotuation: Kommunikationslagebild

Angriffe, Bedrohungen und Schwachstellen im Überblick.

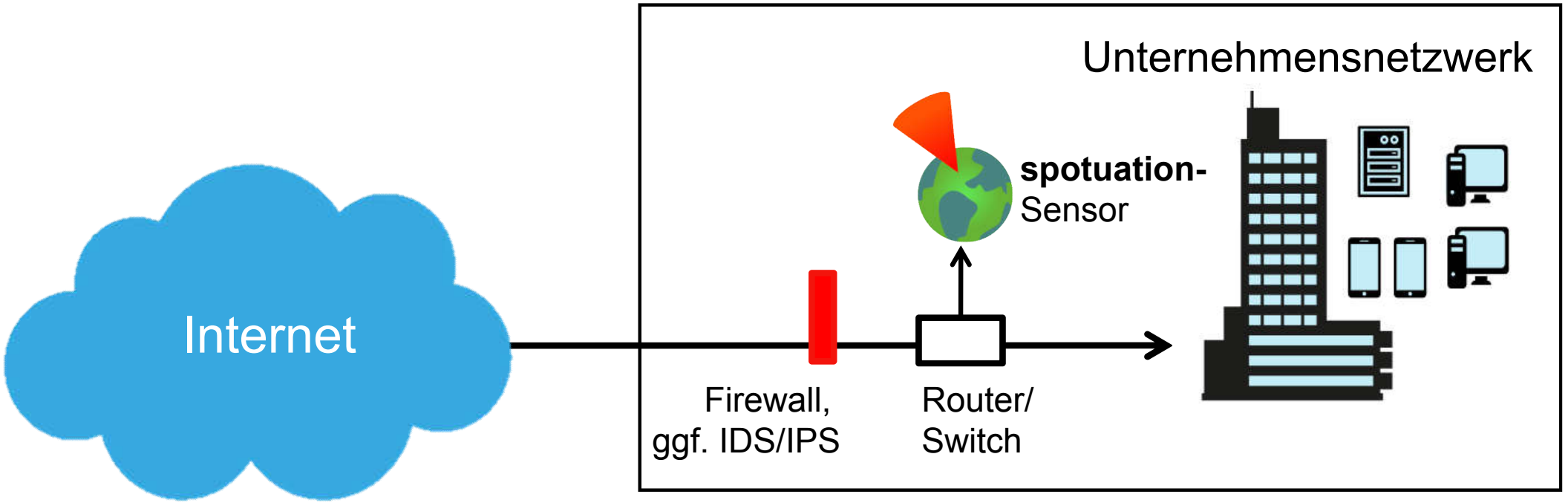


➢ **Das Kommunikationslagebild zeigt auch, was sicher ist!**

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Einfacher Einsatz von spotuation

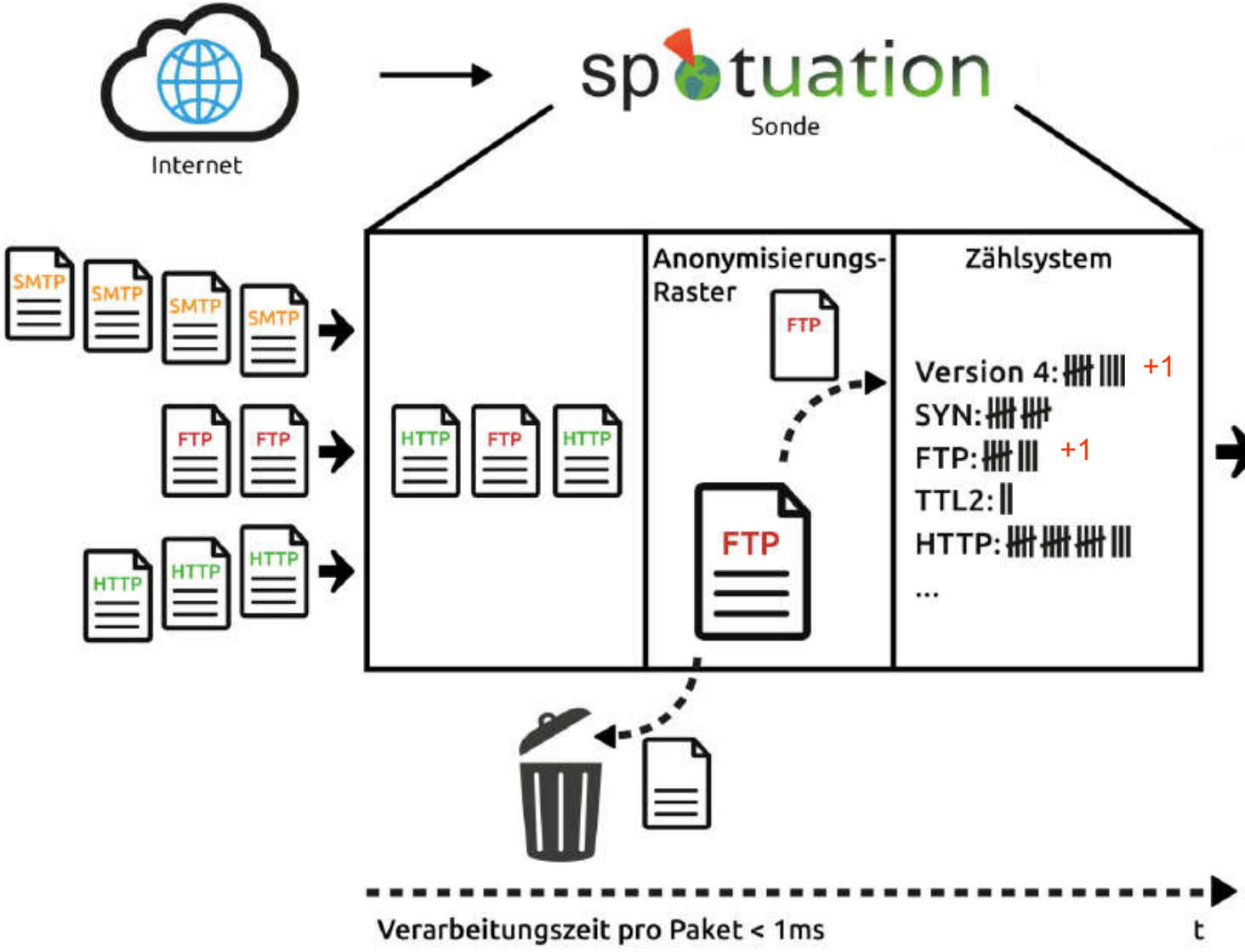
- Integration des spotuation-Sensors:
  - Mittels Tap am Router oder per Mirror-/SPAN-Port im Switch/Router
- Konfiguration und Auswertung bequem per Browser



© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Beim Datenabgriff
→ Zählung von relevanten Merkmalen

Kommunikationsmerkmale enthalten umfassende Informationen:



- **Angriffe**
- **Technologien**
- **Nutzung/Verteilung**

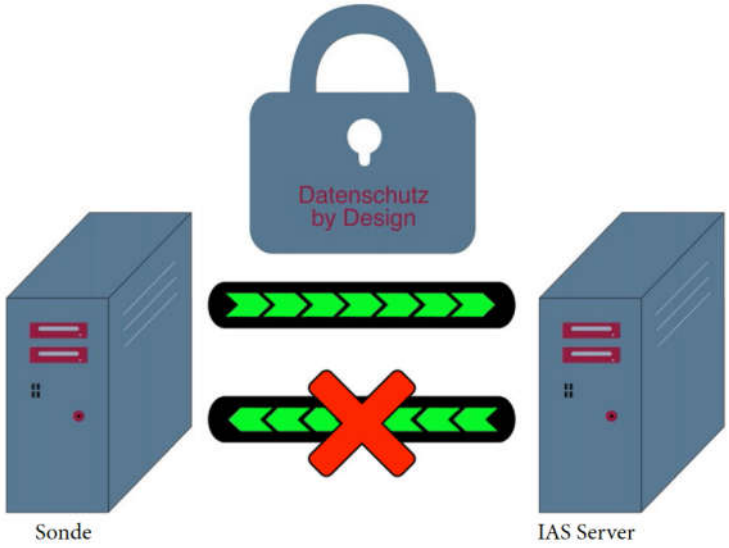
Nicht betrachtet:

- **IP-Adressen**
- **Inhalte wie E-Mails etc.**

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Dadurch: Datenschutz „By Design“

Entspricht vollständig den deutschen Datenschutzrichtlinien: es werden keine Inhalte analysiert, nur Bezeichnungen



Träger des Qualitätszeichens „IT Security made in Germany“ des IT-Sicherheitsverbands TeleTrusT e.V.

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

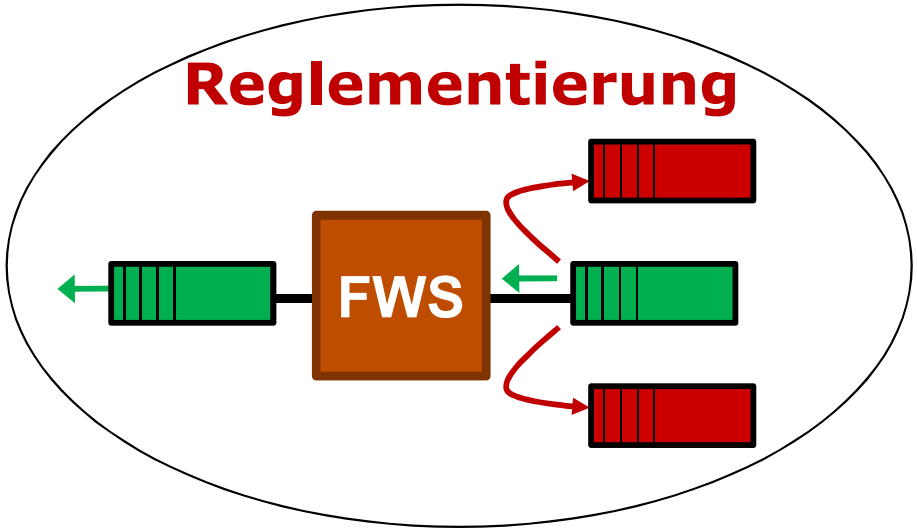
Abgrenzung gegenüber Firewall, IDS & IPS

Gängige Funktionsweise: Blockade nach dem Black-/White-Listing-Prinzip

- **Firewall**:

  Reglementierung

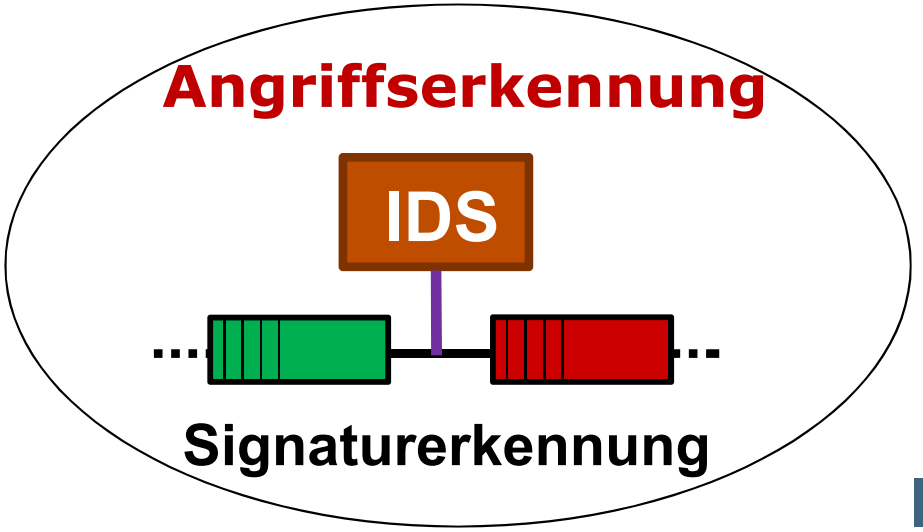
  „Was darf nicht rein?“



- **IDS/IPS**:

  Angriffserkennung durch Signaturen

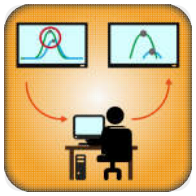
  „Was darf rein?“



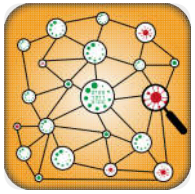
© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

spotuation besteht aus fünf Anwendungen

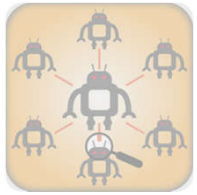
Echtzeit-Monitoring der wichtigsten Kommunikationsparameter



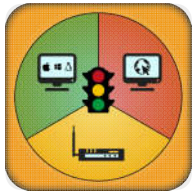
Expertensystem zur detaillierten Analyse



Angriffserkennung (in Zukunft auch Botnetze)



Reporting: Schnelle Übersicht inkl. Bewertungen



Reputationssystem: Erkennung und Bewertung Ihrer verwendeten Technologien im Netzwerk

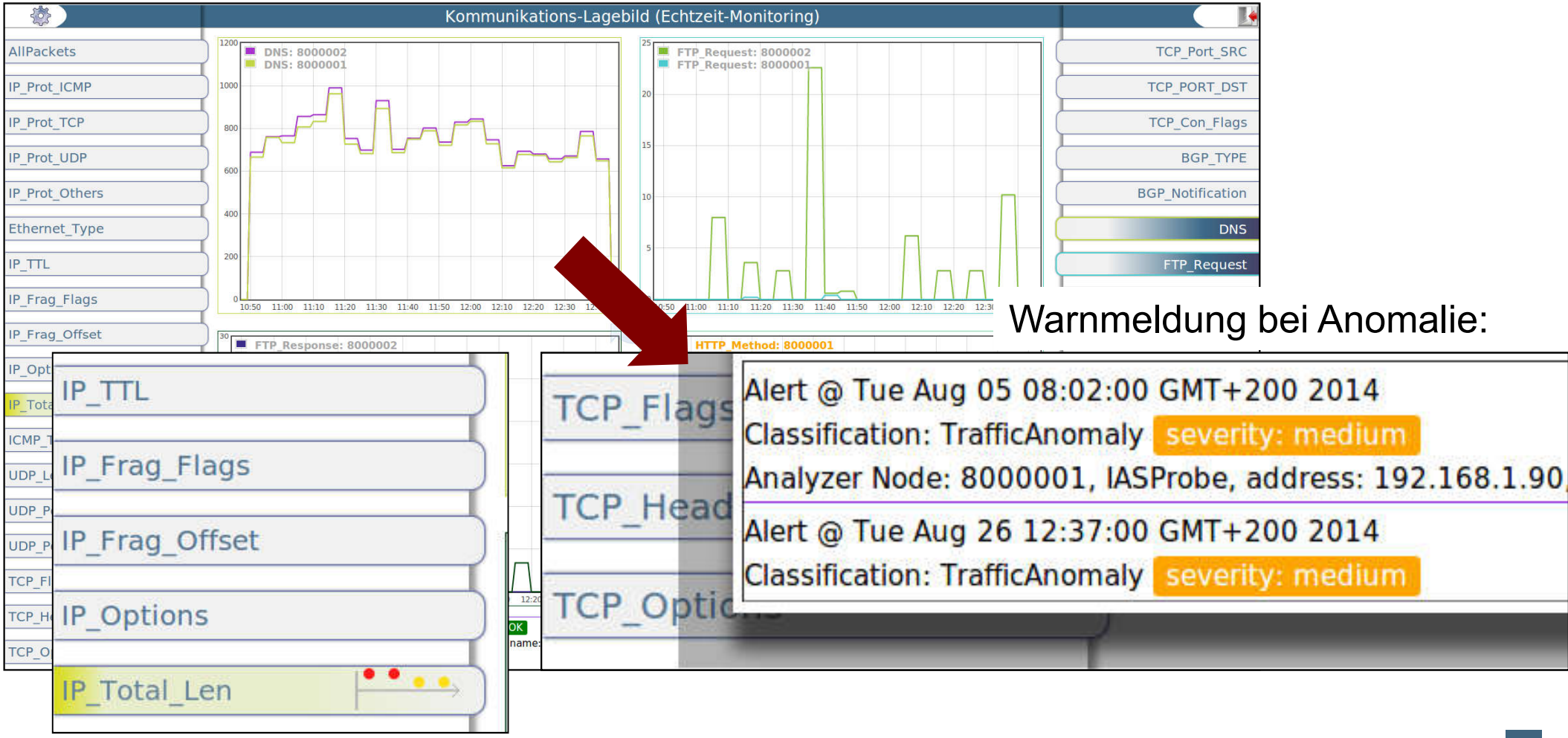
Zukunft: **Referenzsystem** - Vergleich von Lagebildern anderen Teilnehmer (Branchenvergleich)

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Echtzeit-Monitoring stellt den aktuellen “Gesundheitszustand” dar

Die wichtigsten sicherheitsrelevanten Merkmale auf einen Blick.

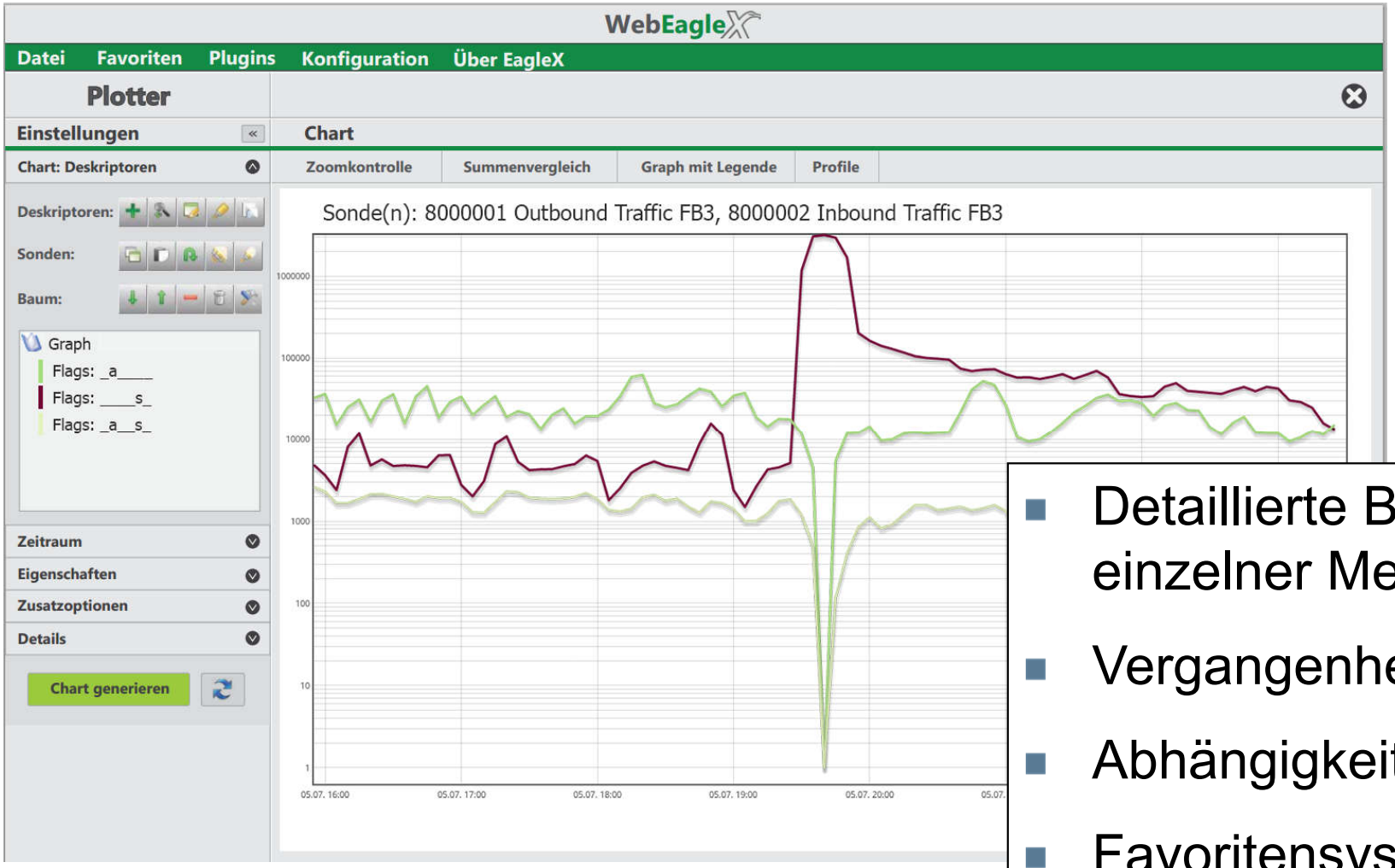
Live-Visualisierung auf Touch-Oberfläche:



© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Detaillierte Netzwerkanalyse mit dem Expertensystem

Details-on-demand-Ansicht in der Browser-Anwendung:

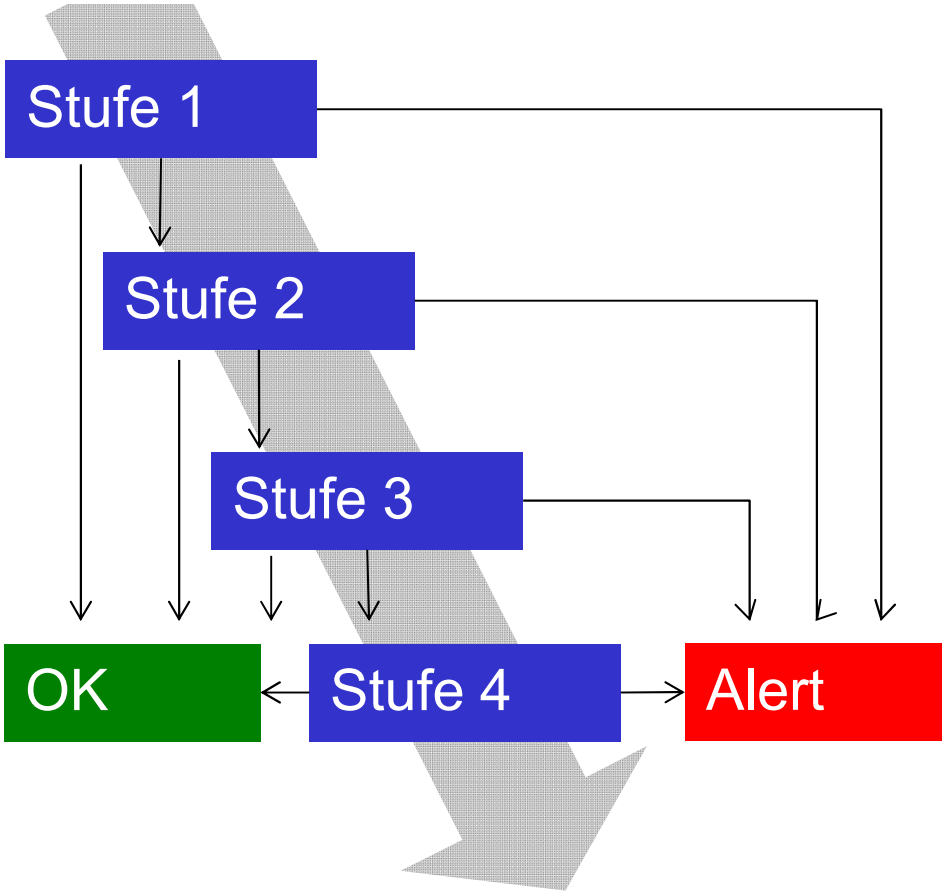


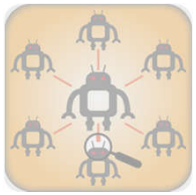
- Detaillierte Betrachtung einzelner Merkmale
- Vergangenheitswerte
- Abhängigkeiten
- Favoritensystem

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffserkennung durch ein mehrstufiges intelligentes System

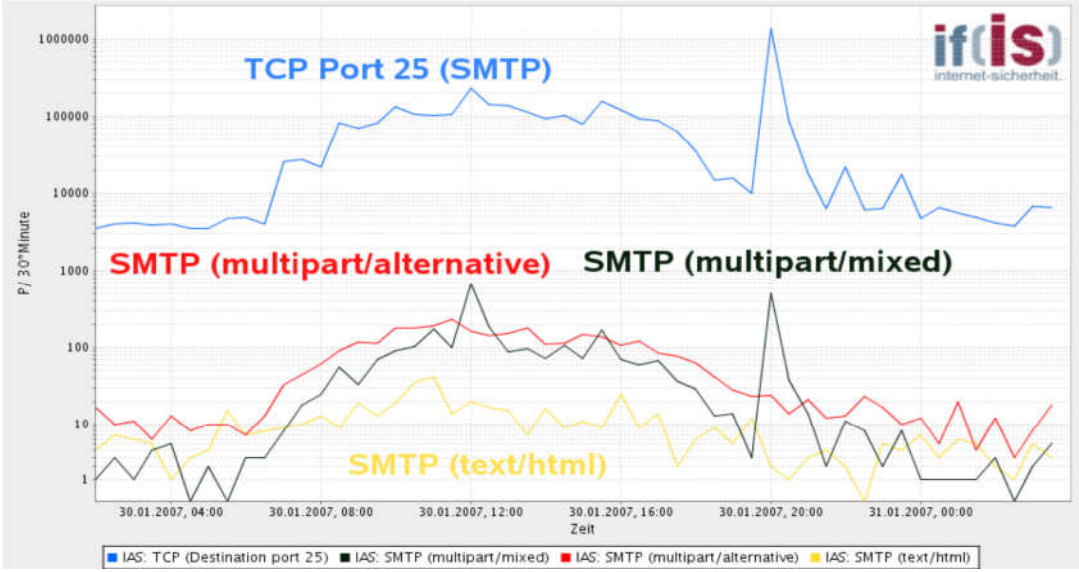
Vorgang Angriffserkennung:





Zukünftige weitere Stufe:
Botnetzerkennung

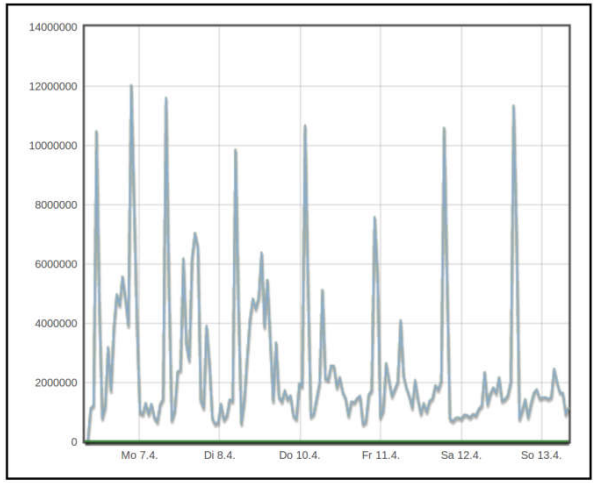
- Der Datenstrom mehrstufig analysiert
- Die Angriffserkennung erfolgt u.a. durch Anomaliedetektionen, womit auch neuartige Gefahren erkannt werden können
- Alarme werden zugestellt



© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Reporting:
Verteilung Ihrer Kommunikation

Traffic Wochenverlauf:



Traffic Art:

	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Src ≥ 1024 and Dst ≥ 1024 ("P2P")	47.129.445	5,67	15.769	0,21	2,36
Src < 1024 and Dst < 1024 ("B2B")	86.466	0,01	6	<0,01	<0,01
Src ≥ 1024 and Dst < 1024 ("P2B")	278.763.288	33,53	74.299	0,98	11,11
Src < 1024 and Dst ≥ 1024 ("B2P")	505.521.024	60,80	578.696	7,65	86,53
Gesamt	**831.500.223**	**100,00**	**668.769**	**8,85**	**100,00**

Ethernet-Übersicht:

	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Gesamt	**1.037.788.081**	**100,00**	**697.517,48**	**9,23**	**100,00**
davon VLAN	1.037.767.367	>99,99	697.514,90	9,23	>99,99
IPv4	1.037.762.016	>99,99	<0,01	<0,01	<0,01
IPv6	20.714	<0,01	2,58	<0,01	<0,01
davon nativ	0	0,00	0,00	0,00	0,00
davon 6*4	0	0,00	0,00	0,00	0,00
davon Teredo	20.714	<0,01	2,58	<0,01	<0,01
ARP	5.351	<0,01	<0,01	<0,01	<0,01
RARP	0	0,00	0,00	0,00	0,00

TOP Kommunikationsprotokolle:

Port		Pakete		Traffic	Bandbreite	
	Richtung	Anzahl	%	MB	Mbps	%
80 (HTTP)	DST	64.684.674	15,53	6.247	<0,01	1,87
	SRC	119.764.297	28,76	152.480	2,02	45,53
	Alle	**184.448.971**	**44,29**	**158.726**	**2,10**	**47,39**
22 (SSH)	DST	36.189.875	8,69	6.821	<0,01	2,04
	SRC	73.040.334	17,54	98.176	1,30	29,31
	Alle	**109.230.209**	**26,23**	**104.997**	**1,39**	**31,35**
443 (HTTPS)	DST	30.334.171	7,28	5.568	<0,01	1,66
	SRC	47.446.836	11,39	49.740	<0,01	14,85
	Alle	**77.781.007**	**18,68**	**55.308**	**<0,01**	**16,51**
	DST	13.320.318	3,20	1.285	<0,01	<0,01

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Reporting: Nutzung und Verlauf Ihrer Kommunikation auf einen Blick

Browser-Nutzung:

Browser	Anzahl Pakete	% Anteil
	9.338.428	**83,45**
MS Internet-Explorer 7	9.220.699	82,40
MS Internet-Explorer 8	85.103	0,76
MS Internet-Explorer 6	18.246	0,16
	1.282.904	**11,46**
Google Chrome 27	1.002.459	8,96
	539.530	**4,82**
Firefox 28	55.845	0,50
Firefox 4	52.528	0,47
Firefox 29	26.417	0,24
Firefox 3	13.014	0,12
Firefox 17	8.405	0,08
Firefox 30	7.921	0,07
	18.433	**0,16**
Thunderbird 24	14.732	0,13
	10.603	**0,09**
Opera 12	10.352	0,09
	134	**<0,01**
	104	**<0,01**
	4	**<0,01**

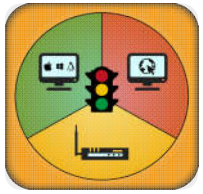
Betriebssystemverwendung:

Betriebssystem	Anzahl	%
Windows XP	3.624.220	24,69
Windows 2000	251.310	1,71
Windows 7	358.259	2,44
Linux 2.4	896.422	6,11
Linux 2.6	259.608	1,77
Mac OS	42.601	0,29
Cisco Router	0	0,00
Rest	**9.246.346**	**62,99**
Gesamt	**14.678.766**	**100,00**

- Betriebssystemnutzung
- Browser-Nutzung
- Verschlüsselungen
- Port-Scan-Versuche
- Bewertungen

Scan Versuche	
Anzahl	%
0	0,00
3.182.707	124,18
3.182.707	**123,96**
0	0
758.841	1.179,97
758.841	**1.179,97**
0	0,00
1.763.583	190,94
1.763.583	**190,94**
0	0
88.024	347,62
88.024	**347,62**
0	0,00
431.507	165,64
431.507	**165,60**
0	0
1.001	1.787,50
1.001	**1.787,50**
0	0,00
116.187	82,58
116.187	**82,56**
0	0,00
25.613	1.356,62
25.613	**1.353,04**
0	0
134	111,67
134	**111,67**
0	0
29.754	182,56
29.754	**182,56**
0	0,00
428.860	1.916,78
428.860	**1.327,74**

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen



Reputationssystem zur Bewertung Ihrer Technologien im Netzwerk

if(is) internet-sicherheit.

Sicherheitsbezogene Bewertung der analysierten Systeme (im Report enthalten)

Betriebssystem	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Linux (64-32)	814.885.708	79,83	591.963	7,83	85,17
Windows (128-96)	134.621.513	13,19	83.996	1,11	12,09
Router (255 -160)	38.707.963	3,79	16.362	0,22	2,35
Rest	**32.622.223**	**3,20**	**2.675**	**0,04**	**0,38**
Gesamt	**1.020.837.407**	**100,00**	**694.996**	**9,19**	**100,00**

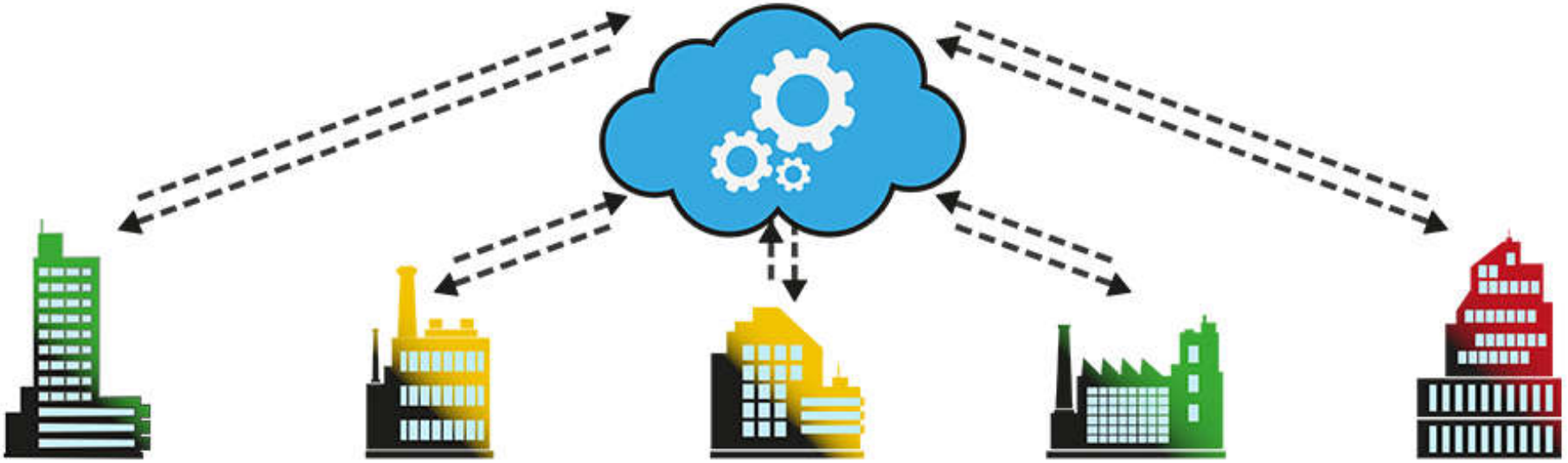
TLS - Version	Pakete	
	Anzahl	%
SSL Version SSL 2.0	0	0,00
SSL Version SSL 3.0	2.297	0,02
SSL Version TLS 1.0	9.735.781	88,34
SSL Version TLS 1.1	163	<0,01
SSL Version TLS 1.2	1.282.308	11,64
SSL Version Other	0	0,00
Gesamt	**11.020.549**	**100,00**

Bewertungs-Farbschema

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Zukunft: Referenzsystem zum Vergleich von Lagebildern

Anonymer Vergleich der eigenen Sicherheitslage:



- Vergleich je Branche / Region / Land
- Wie steht unsere Organisation da?
- Warum haben andere eine bessere Kommunikationslage?
- Was müssen wir für eine Verbesserung tun?

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Referenzsystem: Praxisbeispiel

Eigenes Lagebild:

Z.B. hoher Anteil veraltete Betriebssysteme

Betriebssystem	Anzahl	%
Windows XP	3.624.220	24,69
Windows 2000	251.310	1,71
Windows 7	358.259	2,44
Linux 2.4	896.422	6,11
Linux 2.6	259.608	1,77
Mac OS	42.601	0,29
Cisco Router	0	0,00
Rest	**9.246.346**	**62,99**
Gesamt	**14.678.766**	**100,00**

In Branche:

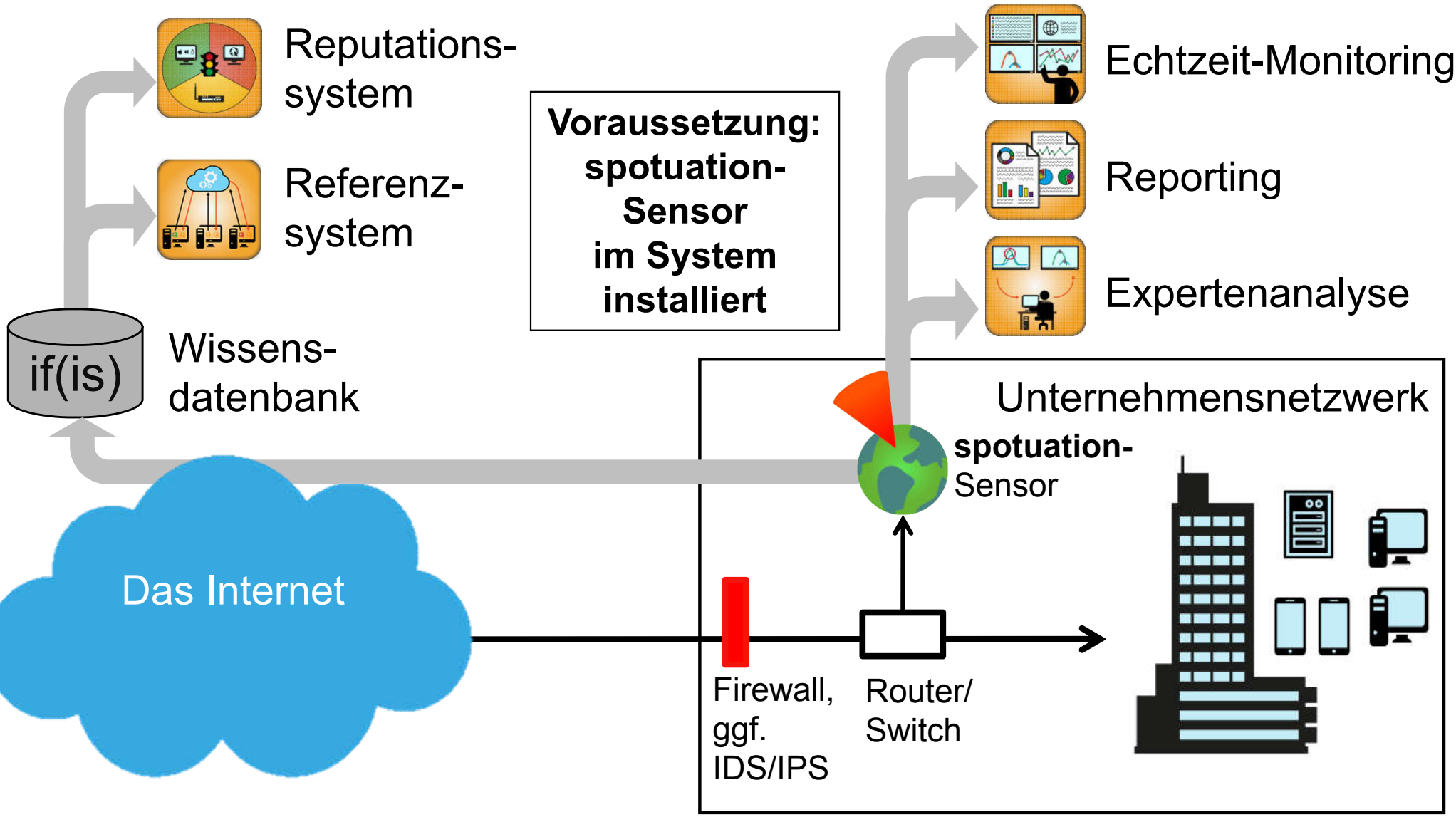
- Deutlich niedriger
- Handlungsbedarf zur Stärkung der eigenen Sicherheit!
- Investition in Aufrüstung

➢ Wissensaustausch zur **Frühwarnung**: Gemeinsam gegen Cyber-Angriffe!

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Aufbau von spotuation im Überblick

Aus eigener Infrastruktur oder über den Browser verwendbar!



© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

I. Eigener Sensor als Partner des if(is) und Nutzung der Technologie

Dazu mit drei Schritten zum Erfolg:

1. Gemeinsame Planung & Beschaffung der Hardware
2. Installation des spotuation-Sensors & Zugang zum System
3. Nutzung des Systems in der if(is)-Cloud

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Ihre Benefits

- Wöchentliche Reporte per E-Mail
- Sicherheitsaudit Ihrer Netzwerkumgebung sowie
- Expertenanalysen durch die IT-Sicherheitsexperten möglich (sicherheitsrelevante Info sind vorhanden)

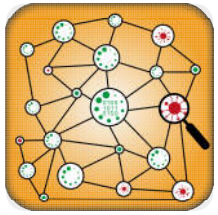
Unser Antrieb:

- Weiterentwicklung und Verbesserung der Technologie durch Ihr Feedback

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Die Key Facts

- Ganzheitliche Übersicht: Kommunikationslagebild
  → Was passiert im Netzwerk?
- Vollständig Datenschutzkonform
- Geringe Kosten, geringer Aufwand, großer Nutzen
- Einfache Browser-Bedienung und Cloud-Anwendung
- Basis für vielfältige Analysen und Erhöhung der Sicherheit
- Basis für neuen Managed Security Service
- Lernen im Unternehmensverbund



Weitere Infos: www.spotuation.de

© Dominique Petersen, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Ein Kommunikationslagebild
→ für mehr IT-Sicherheit

Gefahr erkannt, Gefahr gebannt.

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.