Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

3. VOICE ENTSCHEIDERFORUM

→ Managing Digital Security

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Teil 1

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. Hintergrund
2. Funktionsweise und Vergleich zu Alternativen
3. Vorteile von spotuation
4. Zukunft von spotuation
5. Einsatz der Technologie

Hintergrund „Cyber-Sicherheit“

„Kooperation von Staat, Wirtschaft, Gesellschaft.“

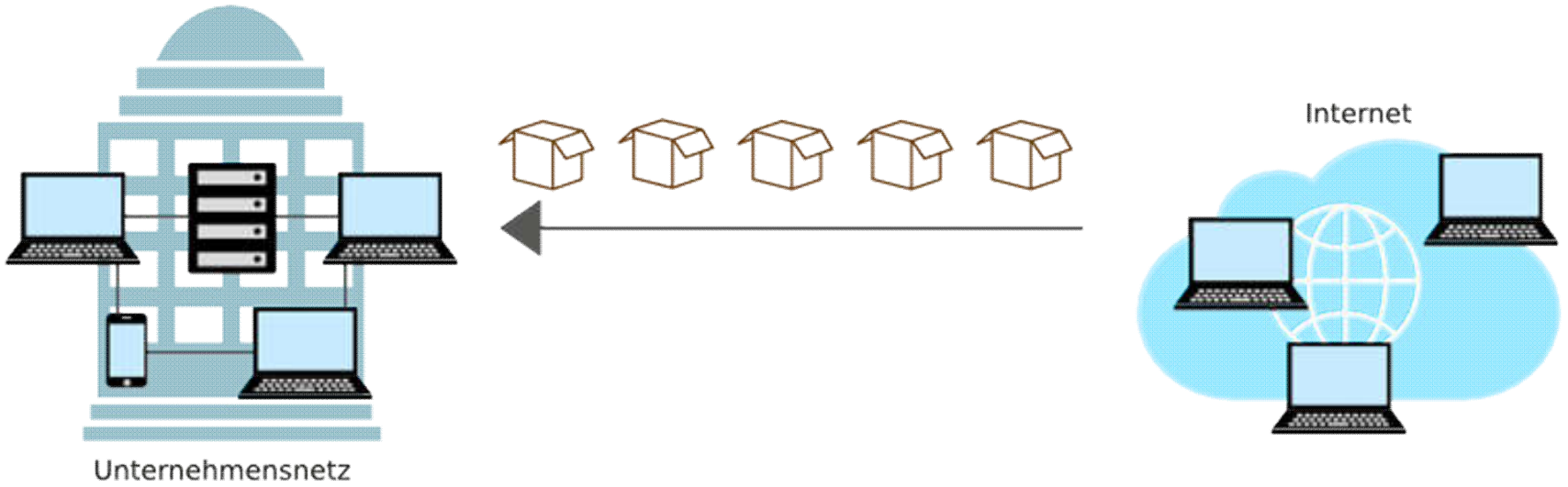
„Meldepflicht von Sicherheitsvorfällen von Unternehmen für große Statistik für die Frühwarnung“

Bundesamt für Sicherheit in der Informationstechnik

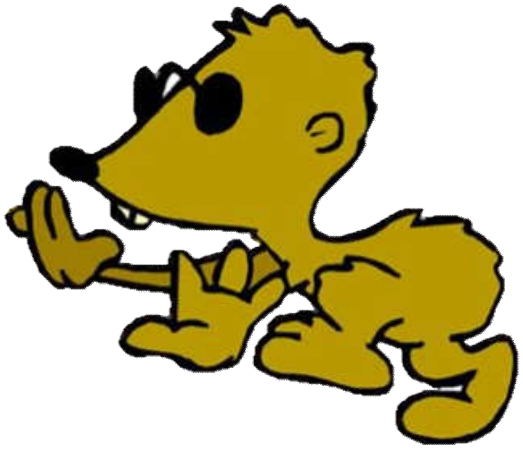
Position:

- 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

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

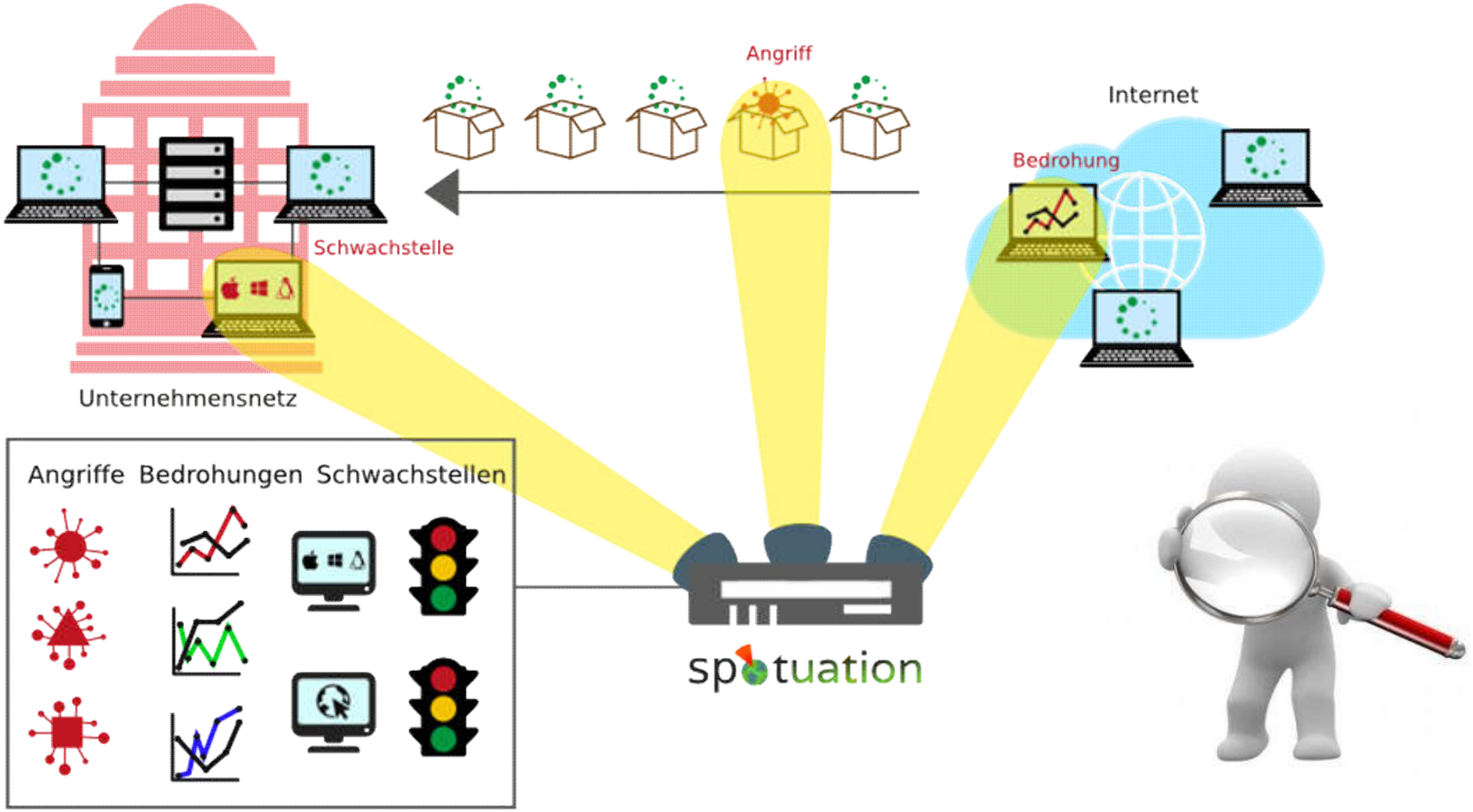


- Wer greift auf das Netzwerk zu?
- Wie sieht das Netzwerk aus?
- Welche Gefahren gibt es?
- Welche Schwachstellen sind vorhanden?



Mit spotuation: Kommunikationslagebild

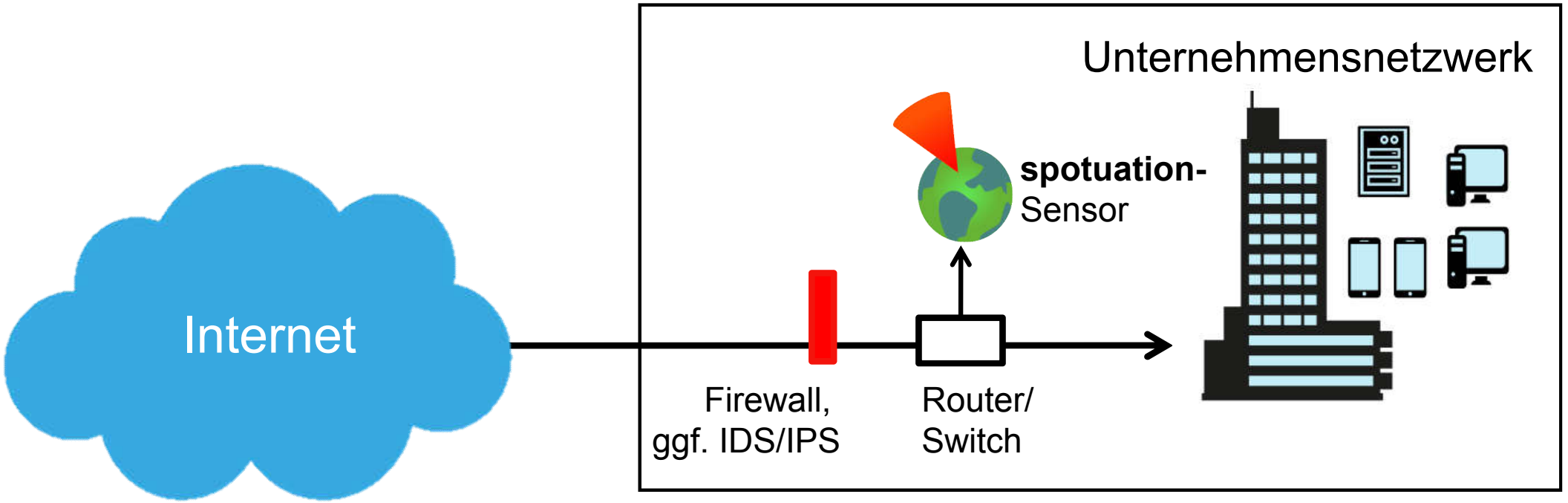
Angriffe, Bedrohungen und Schwachstellen im Überblick.



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

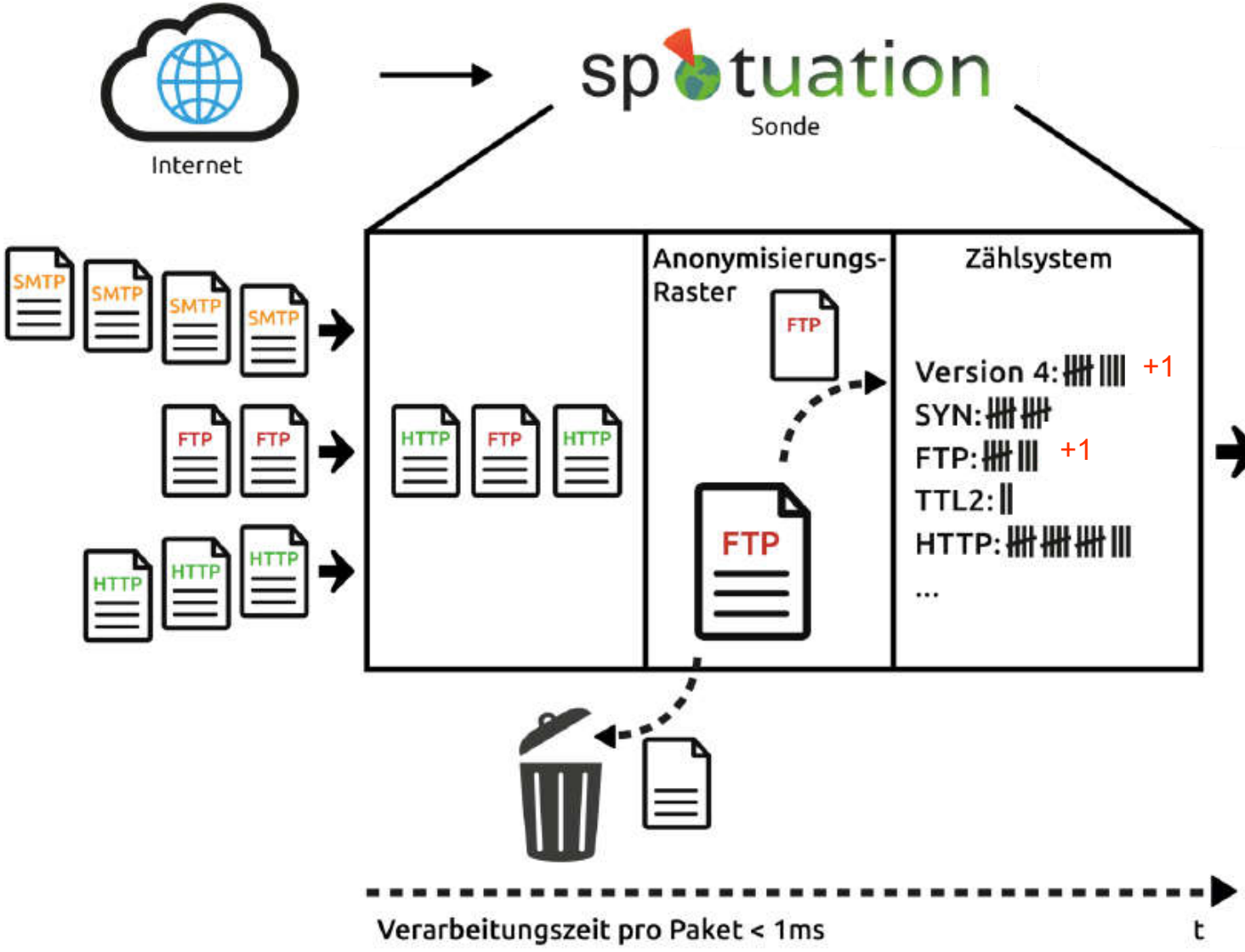
Einfacher Einsatz von spotuation

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



Beim Datenabgriff
→ Zählung von relevanten Merkmalen

Kommunikationsmerkmale enthalten umfassende Informationen:



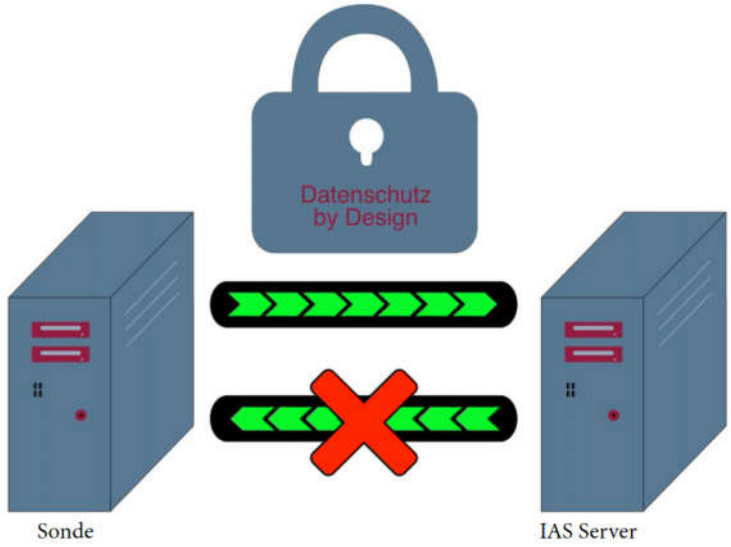
- **Angriffe**
- **Technologien**
- **Nutzung/Verteilung**

Nicht betrachtet:

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

Dadurch: Datenschutz „By Design“

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



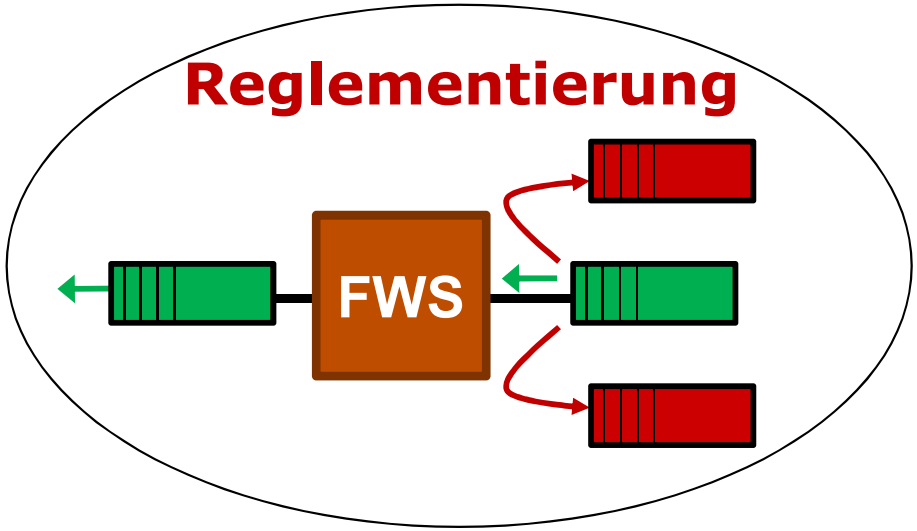
Abgrenzung gegenüber Firewall, IDS & IPS

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

- **Firewall**:

  Reglementierung

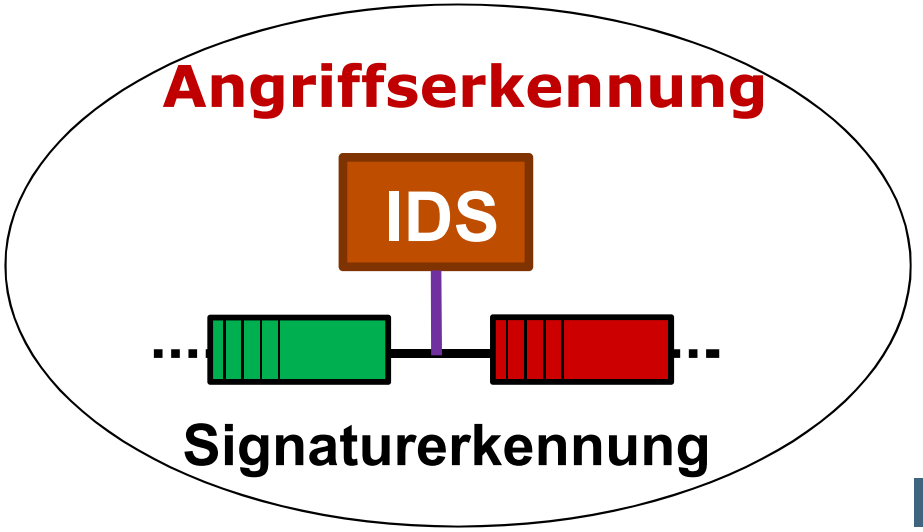
  „Was darf nicht rein?“



- **IDS/IPS**:

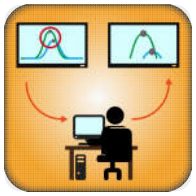
  Angriffserkennung durch Signaturen

  „Was darf rein?“

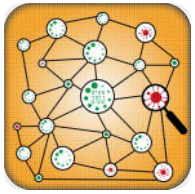


spotuation besteht aus fünf Anwendungen

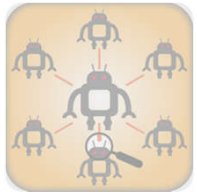
Echtzeit-Monitoring der wichtigsten Kommunikationsparameter



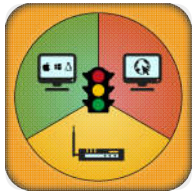
Expertensystem zur detaillierten Analyse



Angriffserkennung



Reporting: Schnelle Übersicht inkl. Bewertungen



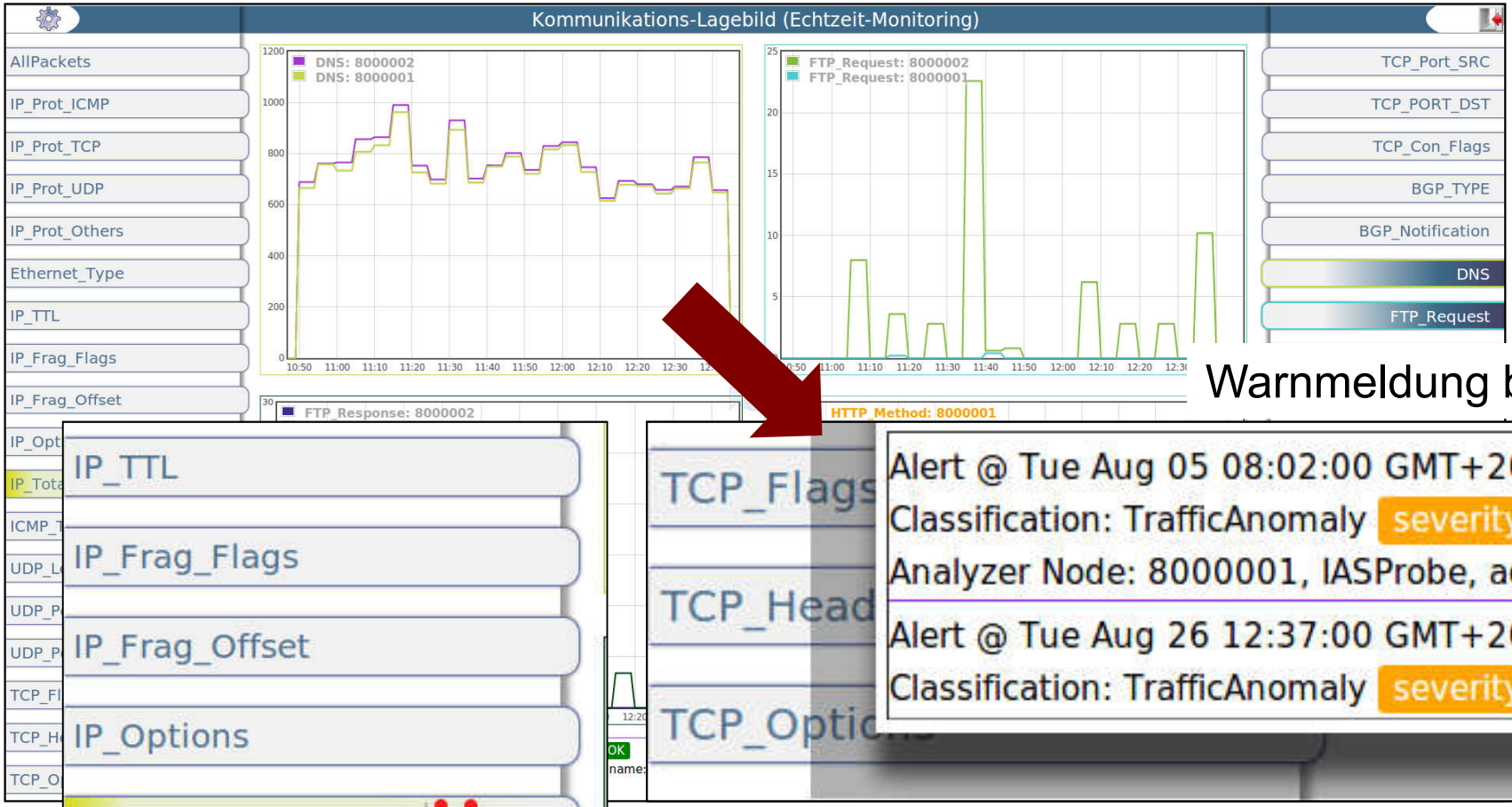
Reputationssystem: Erkennung und Bewertung verwendeten Technologien im Netzwerk

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

Echtzeit-Monitoring stellt den aktuellen “Gesundheitszustand” dar

Die wichtigsten sicherheitsrelevanten Merkmale auf einen Blick.

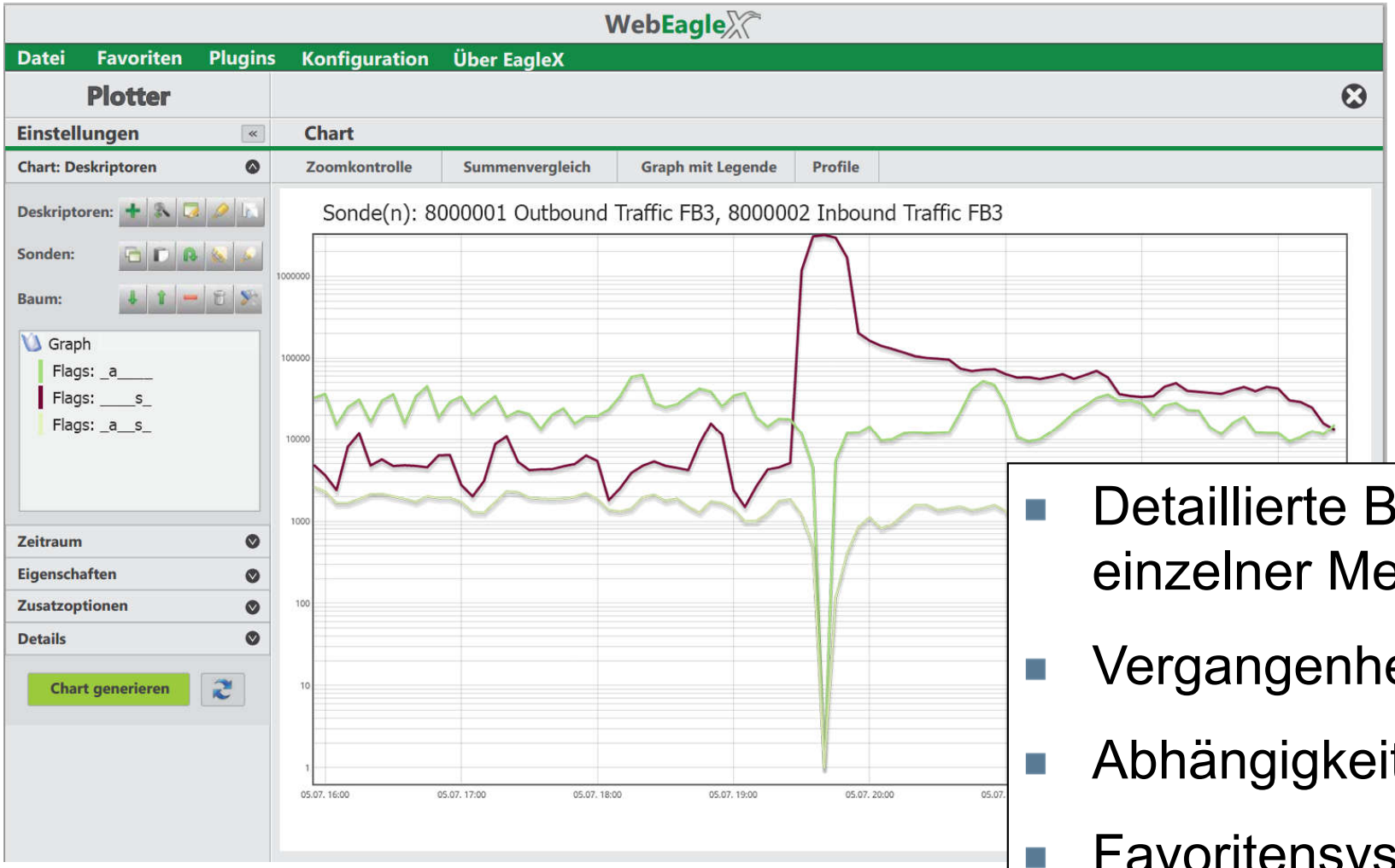
Live-Visualisierung auf Touch-Oberfläche:



Warnmeldung bei Anomalie:

Detaillierte Netzwerkanalyse mit dem Expertensystem

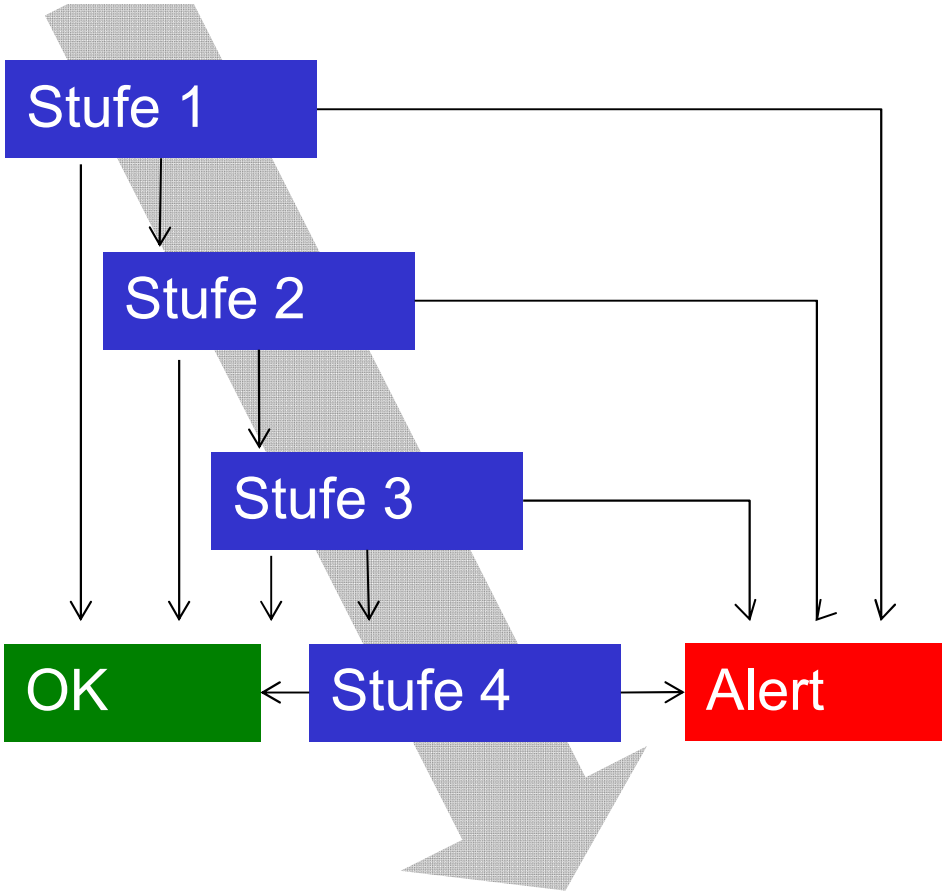
Details-on-demand-Ansicht in der Browser-Anwendung:



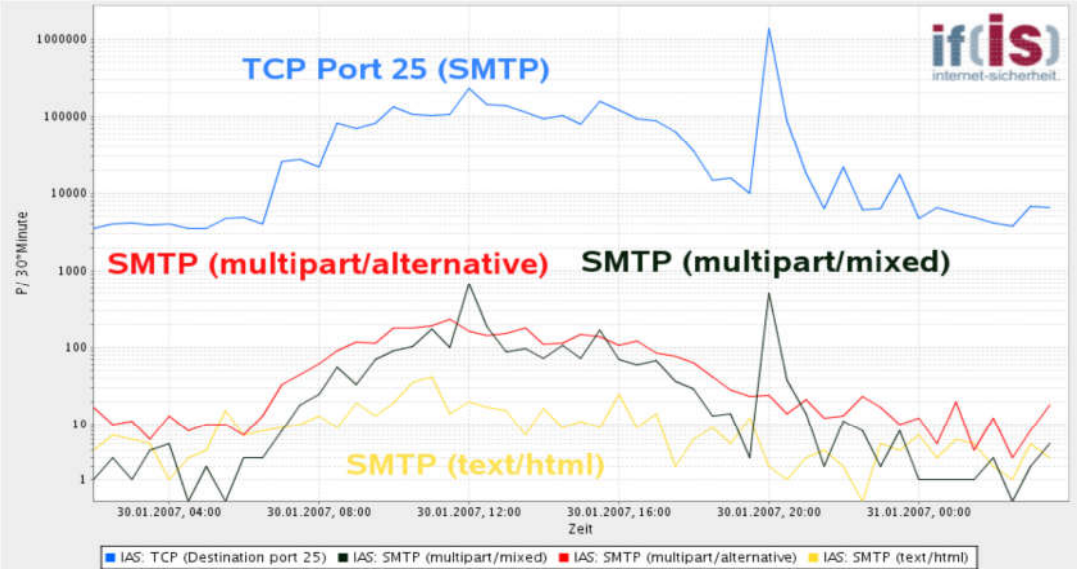
- Detaillierte Betrachtung einzelner Merkmale
- Vergangenheitswerte
- Abhängigkeiten
- Favoritensystem

Angriffserkennung durch ein mehrstufiges intelligentes System

Vorgang Angriffserkennung:

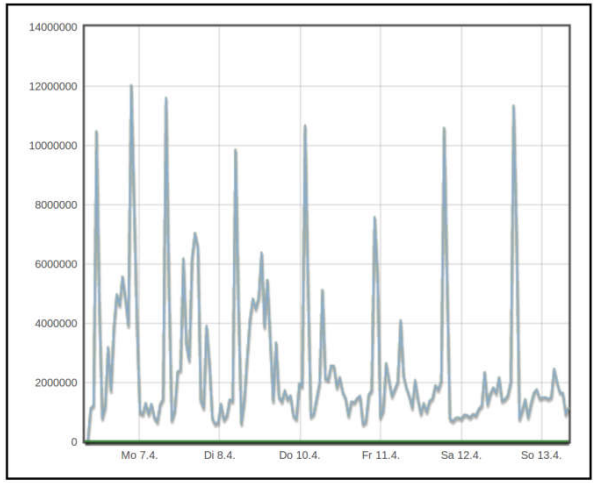


- Der Datenstrom mehrstufig analysiert
- Die Angriffserkennung erfolgt u.a. durch Anomaliedetektionen, womit auch neuartige Gefahren erkannt werden können
- Alarme werden zugestellt



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

Reporting: Nutzung und Verlauf Ihrer Kommunikation auf einen Blick

Browser-Nutzung:

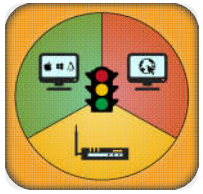
Browser	Anzahl Pakete	% Anteil
	9.338.428	**83,45**
MS Internet-Explorer 7	9.220.699	82,40
MS Internet-Explorer 8	85.103	0,76
MS Internet-Explorer 6	18.246	0,16
	1.282.904	**11,46**
Google Chrome 27	1.002.459	8,96
	539.530	**4,82**
Firefox 28	55.845	0,50
Firefox 4	52.528	0,47
Firefox 29	26.417	0,24
Firefox 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**



Reputationssystem zur Bewertung Ihrer Technologien im Netzwerk

if(is) internet-sicherheit.

Sicherheitsbezogene Bewertung der analysierten Systeme (im Report enthalten)

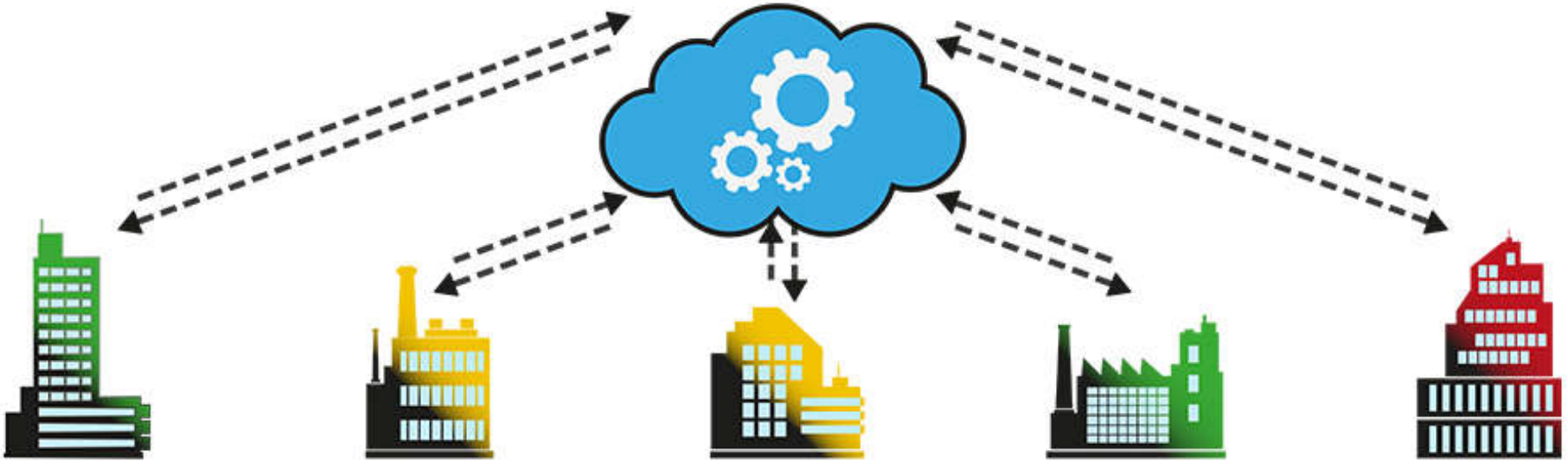
Betriebssystem	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Linux (64-32)	814.885.708	79,83	591.963	7,83	85,17
Windows (128-96)	134.621.513	13,19	83.996	1,11	12,09
Router (255 -160)	38.707.963	3,79	16.362	0,22	2,35
Rest	**32.622.223**	**3,20**	**2.675**	**0,04**	**0,38**
Gesamt	**1.020.837.407**	**100,00**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

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?

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**

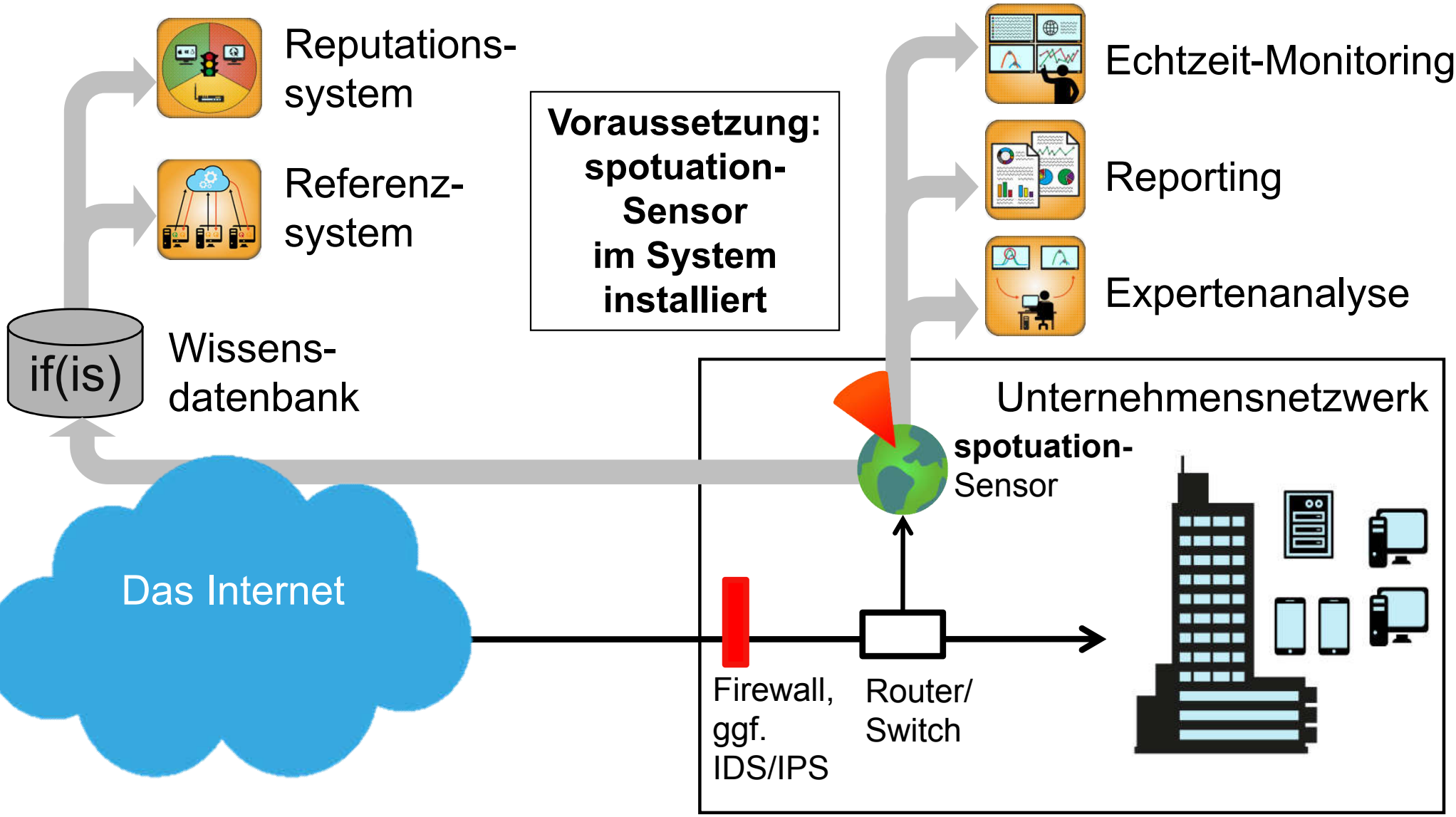
In Branche:

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

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

Aufbau von spotuation im Überblick

Aus eigener Infrastruktur oder über den Browser verwendbar!

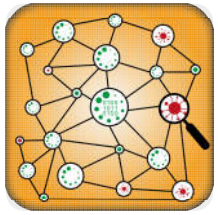


Benefits

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

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



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.

Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

securityNews

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/channel/UCEMkHjW9dHcWfek_En3xhjg
-
- **Cybärcast – Der IT-Sicherheit Podcast**
  https://podcast.internet-sicherheit.de/

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

Google+
https://plus.google.com/107690471983651262369/posts

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Teil 2

Cloud Security

→ Probleme und Ideen

12 Tücken der Cloud-Nutzung
→ Cloud Security Alliance

- Cloud Security Alliance (CSA) is a **not-for-profit organization with a mission** to

  "**promote** the use of **best practices** for **providing security assurance** within Cloud Computing, and to **provide education** on the uses of Cloud Computing to help secure all other forms of computing."

12 Tücken der Cloud-Nutzung
→ 1. Datenpannen

- Cloud-Umgebungen sind mit vielen der gleichen Bedrohungen konfrontiert wie herkömmliche Unternehmensnetze,

  aber aufgrund der **riesigen Datenmengen**, die auf Cloud-Servern gespeichert sind, **werden Provider zu einem attraktiven Ziel**.

12 Tücken der Cloud-Nutzung
→ 2. „Zugriff“

- Unzureichendes Identitäts-, Credential- und Zugriffsmanagement

- Datenverstöße und andere Angriffe resultieren häufig aus laxer Authentifizierung, **schwachen Passwörtern** und **schlechtem Schlüssel-** oder **Zertifikatsmanagement**.

12 Tücken der Cloud-Nutzung
→ 3. Unsichere Schnittstellen

- IT-Teams nutzen Schnittstellen und APIs,
  um Cloud-Services zu verwalten und mit ihnen zu interagieren,

  einschließlich solcher, die Cloud-Provisionierung, Management,
  Orchestrierung und Monitoring anbieten.

12 Tücken der Cloud-Nutzung
→ 4. Schwachstellen des Systems

- **Organisationen teilen** sich Speicher, Datenbanken und andere Ressourcen in unmittelbarer Nähe und schaffen so **neue Angriffsflächen**.

  Glücklicherweise können Angriffe auf System-Schwachstellen mit "Basis IT-Prozessen" abgemildert werden.

12 Tücken der Cloud-Nutzung
→ 5. Kontoübernahme

- **Phishing**, Betrug und **Software-Exploits** sind nach wie vor erfolgreich.

  Cloud-Dienste verleihen der Bedrohung eine neue Dimension, denn Angreifer können Aktivitäten ausnutzen, Transaktionen manipulieren und Daten ändern.

12 Tücken der Cloud-Nutzung
→ 6. Böswillige Eingeweihte

- Die **Insiderbedrohung** hat viele Gesichter:
  ein aktueller oder ehemaliger Mitarbeiter, ein Systemadministrator, ein Auftragnehmer oder ein Geschäftspartner

  Die Agenda bösartiger Aktionen reicht von Datendiebstahl bis hin zu Rache.

12 Tücken der Cloud-Nutzung
→ 7. APTs

- Die CSA bezeichnet fortgeschrittene persistente Bedrohungen (APTs) als "parasitäre" Angriffsformen.

  APT´s infiltrieren Systeme, um Fuß zu fassen, und **exfiltrieren** dann heimlich **Daten** und **geistiges Eigentum** über einen längeren Zeitraum hinweg.

12 Tücken der Cloud-Nutzung
→ 8. Datenverlust

- Berichte über **permanente Datenverluste** aufgrund von **Providerfehlern sind äußerst selten geworden**.

  Aber böswillige Hacker sind dafür bekannt, dass sie Cloud-Daten dauerhaft löschen, um Unternehmen und Cloud-Rechenzentren zu schädigen.

12 Tücken der Cloud-Nutzung
→ 9. Ungenügende Sorgfaltspflicht

- Organisationen, die die Cloud nutzen, ohne das Umfeld und die damit verbundenen **Risiken vollständig zu verstehen**, können mit einer Unzahl von kommerziellen, finanziellen, technischen, rechtlichen und Compliance-Risiken konfrontiert werden.

12 Tücken der Cloud-Nutzung
→ 10. Missbrauch u. schädliche Nutzung

- Cloud-Services können zur Unterstützung schädlichen Aktivitäten genutzt werden.

  Ein Beispiel ist die **Nutzung von Cloud-Computing-Ressourcen**, um einen Verschlüsselungsschlüssel zu knacken …
  … aber auch für DDoS, Spam, …

12 Tücken der Cloud-Nutzung
→ 11. Denial of Service

- DoS-Attacken gibt es schon seit Jahren.

  Sie haben aber mit Cloud-Computing wieder an Bedeutung gewonnen, weil sie oft die **Verfügbarkeit der Cloud-Dienste** beeinträchtigen.

12 Tücken der Cloud-Nutzung

→ 12. Geteilte Technologie-Schwachstellen

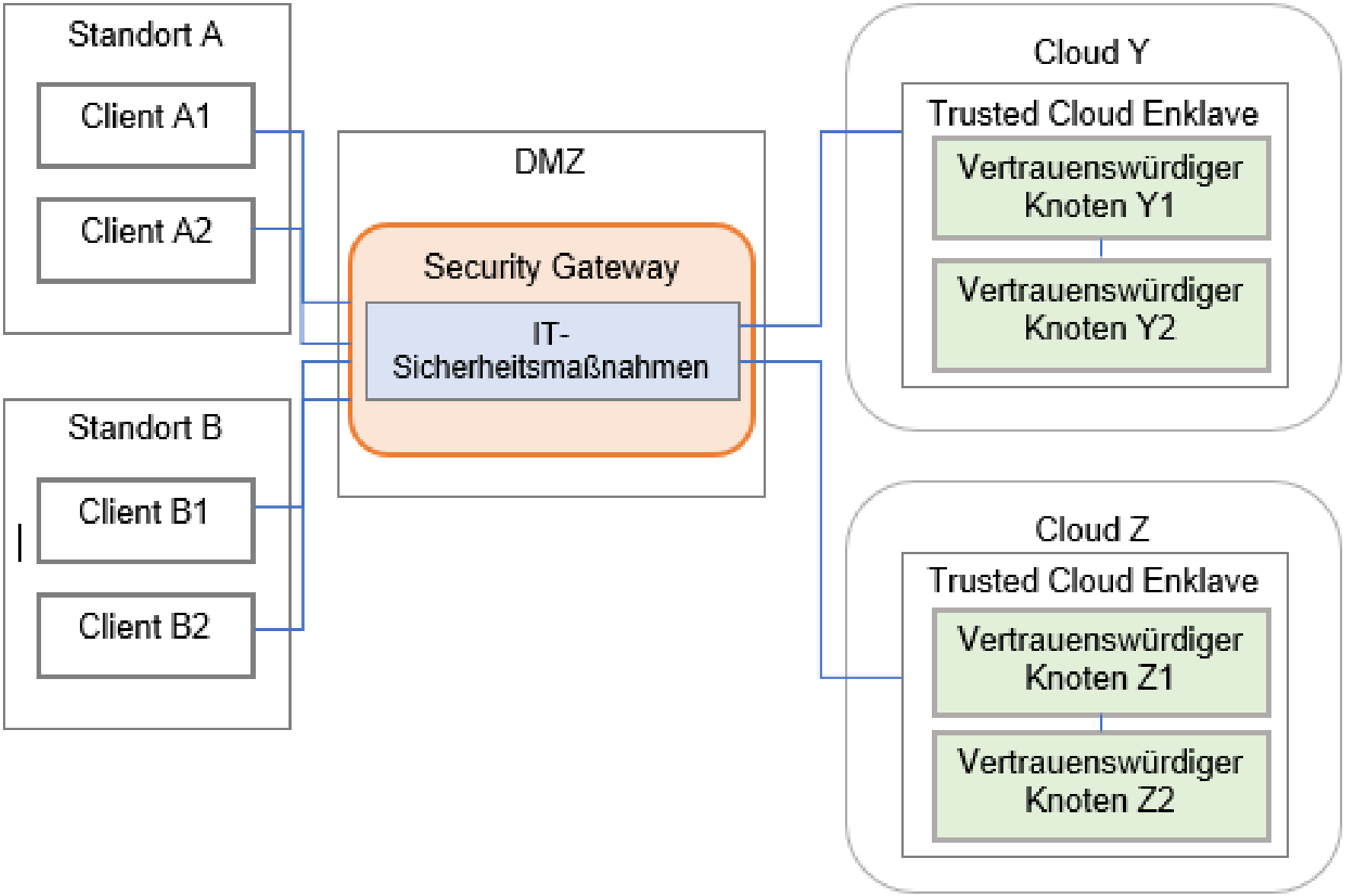
- **Schwachstellen** in **gemeinsam genutzter Technologie** stellen eine erhebliche Bedrohung für Cloud Computing dar.

  Cloud-Service-Provider teilen sich Infrastruktur, Plattformen und Anwendungen.

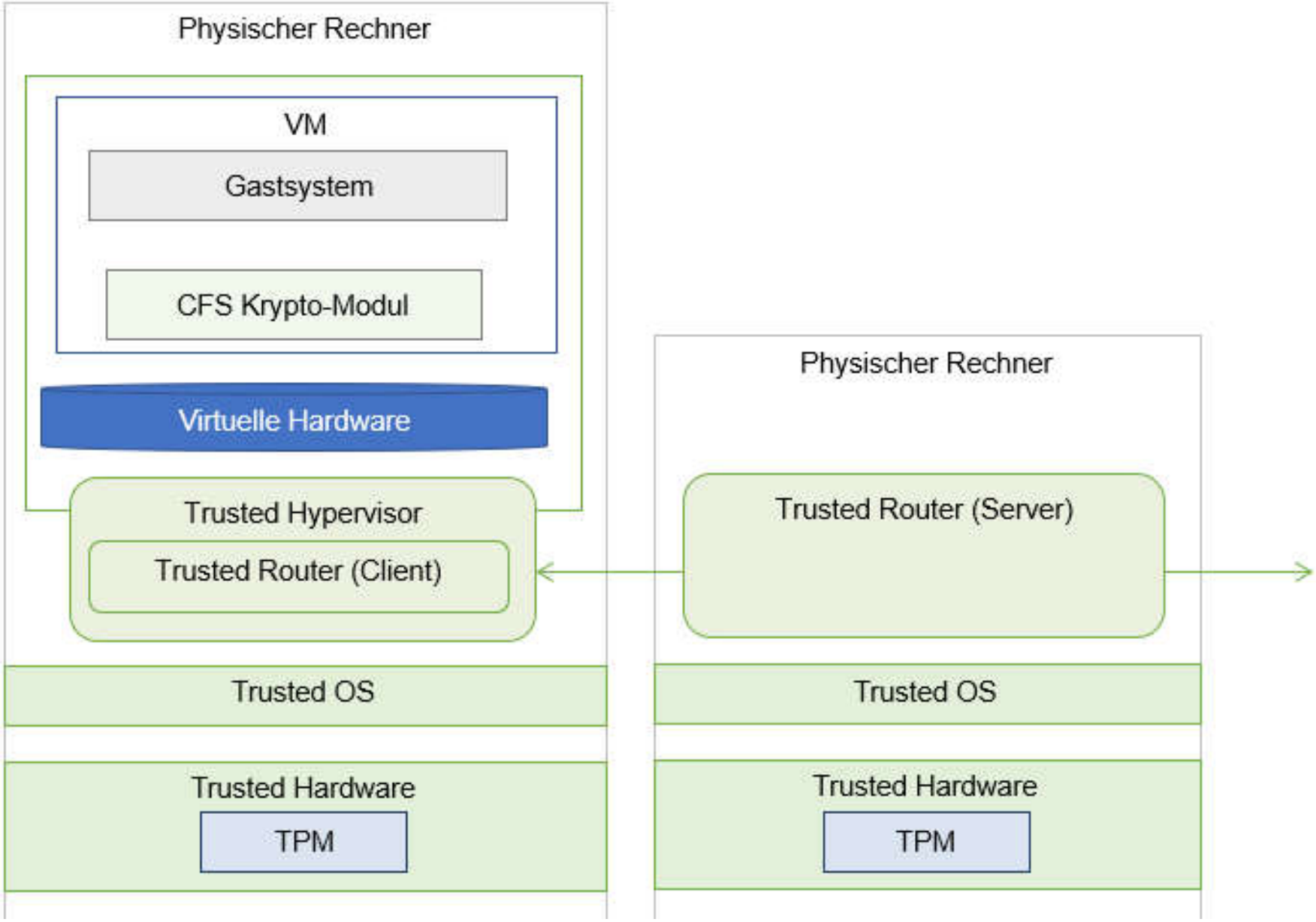
  Wenn eine Schwachstelle auf einer dieser Ebenen auftritt, betrifft sie alle.

Trusted Cloud Enklave (Idee)

→ Eine Lösung für das fehlende Vertrauen



Trusted Cloud Enklave (Umsetzung)
→ Vertrauenswürdige Komponenten (TPM)



Cloud Security

→ Probleme und Ideen

Cloud Security spielt eine wichtige Rolle!

Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/channel/UCEMkHjW9dHcWfek_En3xhjg

-
- **Cybärcast – Der IT-Sicherheit Podcast**
  https://podcast.internet-sicherheit.de/

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

Google+
https://plus.google.com/107690471983651262369/posts

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

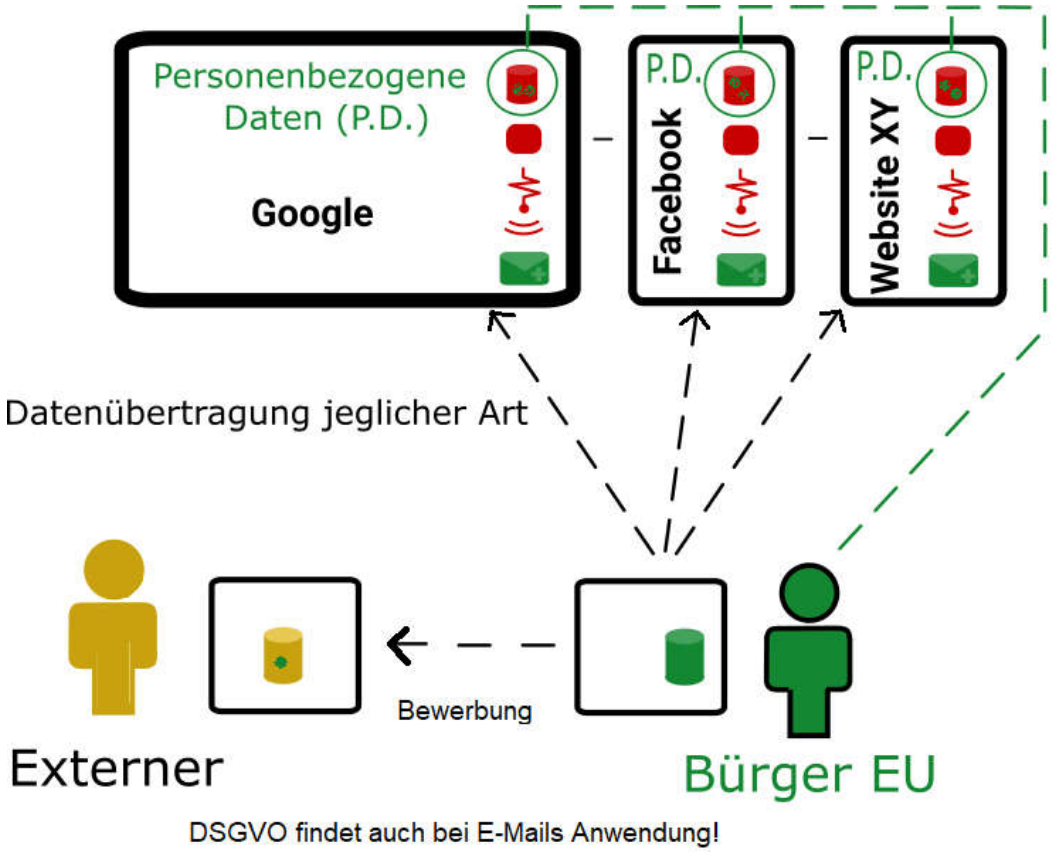
Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Teil 3

Überblick zur EU-Datenschutzgrundverordnung

Rechte der Bürger



DSGVO findet auch bei E-Mails Anwendung!

Rechte der Bürger über ihre personenbezogenen Daten

- Auskunft über die personenbezogenen Daten (Art. 15 DSGVO)
- Löschung der Daten (Art. 17 DSGVO, Recht auf Vergessenwerden)
- Berichtigung der Daten (Art. 16 DSGVO)
- Einschränkung (Art. 18)
- Übertragbarkeit (Art. 20, automatische Übermittlung an Dritte)
- Widerspruch (Art. 21, z.B. gegen Werbung)

Grün: Daten die dem Bürger "gehören"

Gelb: Daten Dritter, die ggf. zu löschen sind

Rot: Daten Dritter, auf die kein direkter Zugriff möglich ist

Rechte der Bürger

Heiko Schöning – „Das neue EU-Datenschutzrecht", networker NRW e.V., 23.01.2018

Recht auf Auskunft

- Art. 15 DS-GVO regelt das „Auskunftsrecht der betroffenen Person“
- Folgende Informationen fallen darunter:
  - Zweck der Datenverarbeitung
  - Kategorien der Daten
  - Empfänger oder Kategorien von Empfängern
  - Dauer der Speicherung
  - Recht auf Berichtigung, Löschung und Widerspruch
  - Herkunft der Daten (falls diesen von fremden Quellen stammen)

Recht auf Löschung

„Recht auf Vergessen werden“

Daten müssen gelöscht werden, wenn:

- Die Speicherung der Daten **nicht mehr notwendig ist**
- Der Betroffene seine Einwilligung zur Datenverarbeitung **widerrufen** hat
- Die Daten **unrechtmäßig verarbeitet** werden
- Eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht

Ausnahmen sind u.a.:

- Datenspeicherung ist für **rechtliche Verpflichtungen** notwendig
- Archivzwecke oder wissenschaftliche / historische Forschungszwecke stehen entgegen
- **Rechtsansprüche**

Recht auf Berichtigung

Art. 16 DS-GVO regelt das Recht auf Berichtigung

Ohnehin besteht die **allgemeine Pflicht** des Verantwortlichen dafür zu sorgen, dass verarbeitete personenbezogene Daten sachlich richtig sind

Betroffene können zusätzlich die Vervollständigung seiner personenbezogenen Daten **ohne unangemessene Verzögerung** verlangen

Verantwortliche müssen entsprechende Möglichkeiten einfach zur Verfügung stellen

Recht auf Einschränkung

Art. 18 DS-GVO regelt Ansprüche der betroffenen Person gegenüber dem Verantwortlichen, die Verarbeitung ihrer personenbezogenen Daten „einzuschränken“

Anders als beim Recht auf Löschen muss der **Verantwortliche erst tätig werden**, wenn die betroffene Person ihre **Ansprüche konkret an ihn richtet**

Dabei wird nicht vorgeschrieben, wie dieser Anspruch geltend gemacht werden muss, somit ist grundsätzlich **jede Form möglich**

Folgende Szenarien sind dabei denkbar:

Bestreiten der Richtigkeit der personenbezogenen Daten

Unrechtmäßige Verarbeitung

Zweckfortfall beim Verantwortlichen

Recht auf Übertragbarkeit

Art. 20 DS-GVO regelt Recht auf Übertragbarkeit

Betroffene haben das Recht, ihre **Daten in einem gängigen Format** zu erhalten

Zusätzlich sind Betroffene befugt, die von ihm zur Verfügung gestellten Daten von einer automatisierten Anwendung auf eine andere Anwendung übertragen zu können

Grundidee war Daten zwischen sozialen Netzwerken zu übertragen

Stärkung der Kontrolle über die eigenen Daten, zum anderen Möglichkeit eines Anbieterwechsels

„Lock-in-Effekt“ soll vermeidet werden

Recht auf Widerspruch

Art. 21 DS-GVO setzt um, dass jeder betroffene Person das Recht zusteht, jederzeit gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen

Betroffene Personen müssen spätestens zum Zeitpunkt der ersten Kommunikation **ausdrücklich auf ihr Widerspruchsrecht hingewiesen** werden

Ausgenommen sind Daten, die zwingend schutzwürdig sind, z.B:

- Gründe des öffentlichen Interesses (Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, Finanzaufsichtsbehörden etc.)
- Schutz der öffentlichen Sicherheit

Fragebogen zur Umsetzung der DS-GVO des Bayerischen Landesamts für Datenschutzaufsicht

Struktur und Verantwortlichkeit im Unternehmen

Ist das Bewusstsein im Unternehmen vorhanden, dass die DS-GVO Chefsache ist, z.B. durch:

- Vorhandenseins einer Datenschutzleitlinie
- Beschreibung der Datenschutzleitlinie
- Regelung der Verantwortlichkeit
- Bewusstsein über Datenschutzrisiken
- Transparenz über Zielkonflikte
  (z.B. zwischen Marketing- und Rechtsabteilung)

Verfügt ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten?

- Wenn nein, warum nicht?
- Wenn ja, ist geklärt, wann er von wem einzubeziehen ist?
- Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?

Übersicht über Verarbeitungen

Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO?

- Wenn nein, warum nicht? Ist das dokumentiert?

Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design – Art. 25 DS-GVO)?

Einbindung Externer

Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden?

- Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter?
- Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?

Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?

- Wenn nein, warum nicht?

Haben Sie **insbesondere folgende Informationen** neu aufgenommen, sofern nicht bereits vorher enthalten:

- **Kontaktdaten** des Datenschutzbeauftragten
- **Rechtsgrundlage(n)** für die Verarbeitung personenbezogener Daten
- Falls Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen: die **berechtigten Interessen**
- Falls Sie Daten in Drittländer übermitteln: die von Ihnen zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (z.B. Standarddatenschutzklauseln)

Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

- **Dauer der Speicherung**; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer
- Bestehen der **Rechte betroffener Personen** auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität
- Sofern Verarbeitung auf Einwilligung beruht: das **Recht zum jederzeitigen Widerruf der Einwilligung**
- **Recht auf Beschwerde** bei der Aufsichtsbehörde
- Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
- Sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschließlich **Profiling** sowie – in diesem Fall – Informationen über die involvierte Logik sowie die Tragweite und die angestrebten **Auswirkungen der Verarbeitung für die betroffene Person**
- Sofern Sie die Daten nicht bei der betroffenen Person erhoben haben: **aus welcher Quelle die personenbezogenen Daten stammen** und ggf. ob sie aus öffentlich zugänglichen Quellen stammen

Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

Haben Sie Ihre Werbe-Einwilligungserklärungen für Kunden, Interessenten usw., an die Anforderungen von Art. 7 und 13 DS-GVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?

Haben Sie ein Verfahren eingerichtet um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO **zeitnah und vollständig erfüllen** zu können (Art. 12 Abs. 1 DS-GVO)?

Haben Sie **Verfahren eingerichtet um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen** zu können (Art. 20 DS-GVO)?

Verantwortlichkeit, Umgang mit Risiken

Gibt es für jede Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung nachweisen können, z.B. bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen (Art. 5 Abs. 2 DS-GVO)?

Haben Sie geprüft, ob die Einwilligungen, auf die Sie eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 und/oder 8 DS-GVO entsprechen?

Können Sie das **Vorliegen der Einwilligung nachweisen**?

Verantwortlichkeit, Umgang mit Risiken

Haben Sie einen Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art 24 Abs. 1 DS-GVO)?

Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DS-GVO angepasst?

Haben Sie insbesondere bestehende Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen durch eine risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten ersetzt?

Wurde ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen umgesetzt?

Verantwortlichkeit, Umgang mit Risiken

Wurden Schutzmaßnahmen wie Pseudonymisierung und der Einsatz von kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt?

Haben Sie sich auf die evtl. Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung vorbereitet?

Haben Sie eine geeignete Methode zur Bestimmung der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in Ihrem Unternehmen eingeführt?

Haben Sie eine geeignete Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung in Ihrem Unternehmen eingeführt? Haben Sie sich für einen Prozess der Datenschutz-Folgenabschätzung entschieden; haben Sie diesen schon einmal getestet?

Datenschutzverletzungen

Haben Sie gem. Art. 33 DS-GVO sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten **innerhalb von 72 Stunden an die Aufsichtsbehörde** möglich ist?

Haben Sie insbesondere sichergestellt, dass Datenschutzverletzungen in Ihrem Unternehmen erkannt werden können. Haben Sie dazu eine geeignete Methode zur Ermittlung eines Risikos bzw. eines hohen Risikos in Ihrem Unternehmen eingeführt?

Haben Sie einen Prozess aufgesetzt, wie mit **potentiellen Verletzungen intern umzugehen** ist?

Haben Sie festgelegt, **wer, wann und wie mit der Datenschutzaufsichtsbehörde** kommuniziert?

Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

securityNews

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/channel/UCEMkHjW9dHcWfek_En3xhjg
-
- **Cybärcast – Der IT-Sicherheit Podcast**
  https://podcast.internet-sicherheit.de/

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

Google+
https://plus.google.com/107690471983651262369/posts

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/