Netzwerküberwachung mit ELK

CryptoCon 2016

Alexander Böhm

22. Mai 2016

Am Anfang war . . .

1. Ein langsamer DSL-Anschluß
2. Die Frage:

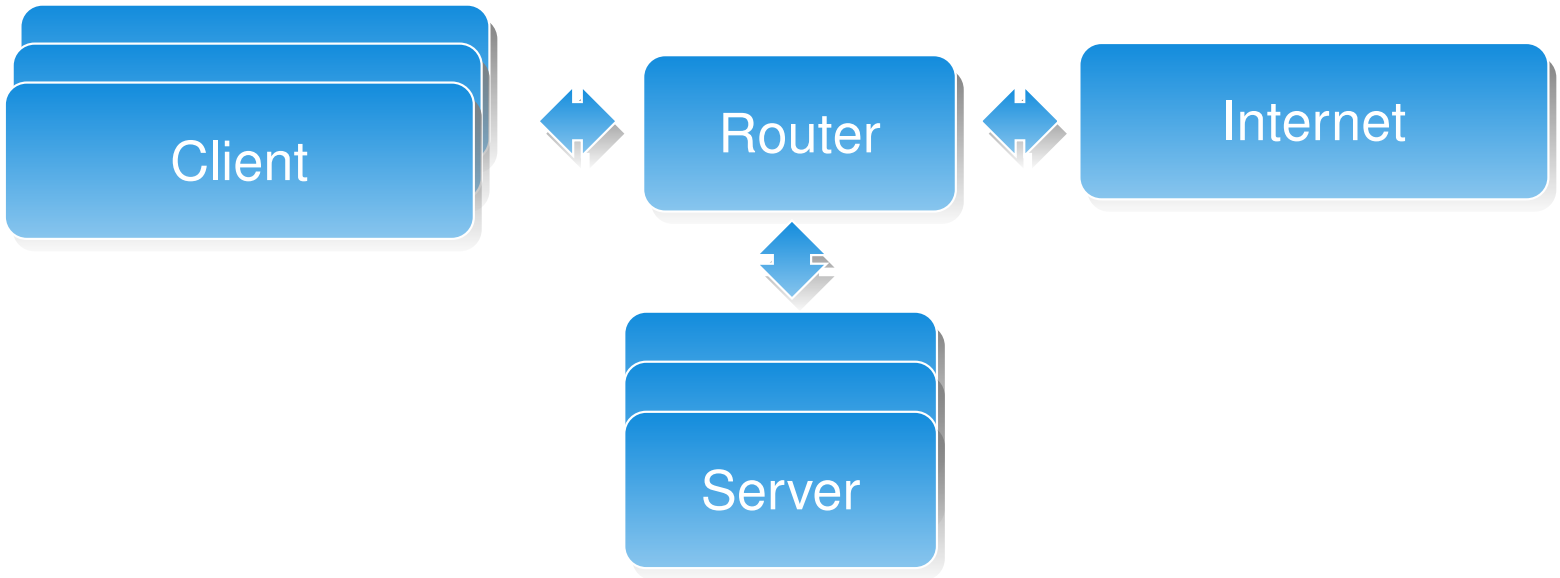
   Bin ich oder der Provider schuld?

Am Anfang war . . .

1. Ein langsamer DSL-Anschluß
2. Die Frage:

   Bin ich oder der Provider schuld?

Am Anfang war . . .



Die erste Antwort

- In der Regel lief alles
- Probleme in bst. Zeitfenstern

→ Regelmäßige Messungen

- Upload-/Downloadgeschwindigkeit
- Paketverlustraten
- . . .

- Befriedigende Antworten? . . . Nein

Die erste Antwort

- In der Regel lief alles
- Probleme in bst. Zeitfenstern

→ Regelmäßige Messungen

  - Upload-/Downloadgeschwindigkeit
  - Paketverlustraten
  - . . .

- Befriedigende Antworten? . . . Nein

Die erste Antwort

- In der Regel lief alles
- Probleme in bst. Zeitfenstern

→ Regelmäßige Messungen

  - Upload-/Downloadgeschwindigkeit
  - Paketverlustraten
  - . . .

- Befriedigende Antworten? . . . Nein

Erkenntnis

- Grober Überblick möglich
- Wenige Client $\rightarrow$ Vielzahl an Protokollen/ Verbindungen

$\rightarrow$ Was läuft eigentlich im Netzwerk?

Erkenntnis

- Grober Überblick möglich
- Wenige Client $\rightarrow$ Vielzahl an Protokollen/ Verbindungen

$\rightarrow$ Was läuft eigentlich im Netzwerk?

Linux Tools

- Statistiken
  - *ifconfig*
  - SNMP
  - *netstat*

```
$ snmpwalk -v 2c -c public myrouter
. . .
iso.3.6.1.2.1.2.2.1.2.8 = STRING: "br0"
iso.3.6.1.2.1.2.2.1.2.10 = STRING: ppp_1_32_1"
. . .
iso.3.6.1.2.1.2.2.1.10.8 = Counter32: 1650532748
iso.3.6.1.2.1.2.2.1.10.10 = Counter32: 1075621140
. . .
iso.3.6.1.2.1.2.2.1.16.8 = Counter32: 1207938165
iso.3.6.1.2.1.2.2.1.16.10 = Counter32: 1636153067
. . .
```

Abbildung: SNMP-Anfrage: Empfangene und gesendete Bytes je Interface

Linux Tools

- Statistiken
  - *ifconfig*
  - *SNMP*
  - *netstat*
- Netzwerksniffer
  - libpcap
  - *Wireshark*
  - *iftop*

```
                 410KB          819KB          1.20MB         1.60MB    2.00MB
└──────────────────┴──────────────┴──────────────┴──────────────┴─────────┘
192.168.[redacted]:1197     <=> [redacted]:1197          3.22KB  2.81KB  2.33KB
10.[redacted]:35958         <=> 192.168.[redacted]:8201  2.45KB  1.42KB   824B
192.168.[redacted]:ssh      <=> 192.168.[redacted]:47652  202B   313B    331B
10.[redacted]:20979         <=> 192.168.[redacted]:http     0B   264B    66B
10.[redacted]               <=> 192.168.[redacted]          0B    50B    50B
10.[redacted]:44424         <=> 192.168.[redacted]:8201     0B    38B    10B
192.168.[redacted]:domain   <=> 192.168.[redacted]:47156    0B    37B     9B
192.168.[redacted]:domain   <=> 192.168.[redacted]:33437    0B    36B     9B
192.168.[redacted]:bootps   <=> 192.168.[redacted]:bootpc   0B    33B    25B
192.168.[redacted]:53830    <=> 192.168.[redacted]:9200     0B     0B  1.61KB
10.[redacted]:49048         <=> 192.168.[redacted]:8201     0B     0B   237B
10.[redacted]:13564         <=> 192.168.[redacted]:http     0B     0B    66B
192.168.[redacted]:bootps   <=> 192.168.[redacted]:bootpc   0B     0B    25B
192.168.[redacted]:netbios-dgm<=> 192.168.[redacted]:netbios-dgm 0B 0B    12B
192.168.[redacted]:domain   <=> 192.168.[redacted]:51798    0B     0B    11B
10.[redacted]:47108         <=> 192.168.[redacted]:8201     0B     0B    10B
10.[redacted]:11443         <=> 192.168.[redacted]:8201     0B     0B    10B
10.[redacted]:12482         <=> 192.168.[redacted]:8201     0B     0B    10B
192.168.[redacted]:domain   <=> 192.168.[redacted]:50953    0B     0B     9B
192.168.[redacted]:domain   <=> 192.168.[redacted]:58655    0B     0B     9B
192.168.[redacted]:domain   <=> 192.168.[redacted]:47545    0B     0B     9B
192.168.[redacted]:domain   <=> 192.168.[redacted]:55502    0B     0B     9B
192.168.[redacted]:domain   <=> 192.168.[redacted]:41989    0B     0B     9B

TX:             cum:   1.50MB   peak:   24.6rates:  2.95KB  2.65KB  3.35KB
RX:                    21.6MB           10.6KB     2.92KB  2.33KB  2.35KB
TOTAL:                 23.1MB           35.2KB     5.87KB  4.98KB  5.70KB
```

Abbildung: Übersicht der Netzwerkverbindungen durch *iftop*

Linux Tools

- Zunächst praktisch
- Nur anwendbar auf einzelnen Rechnern
- Nur teilweise Echtzeit
- Unübersichlich
- Zusammenführung von Datenquellen

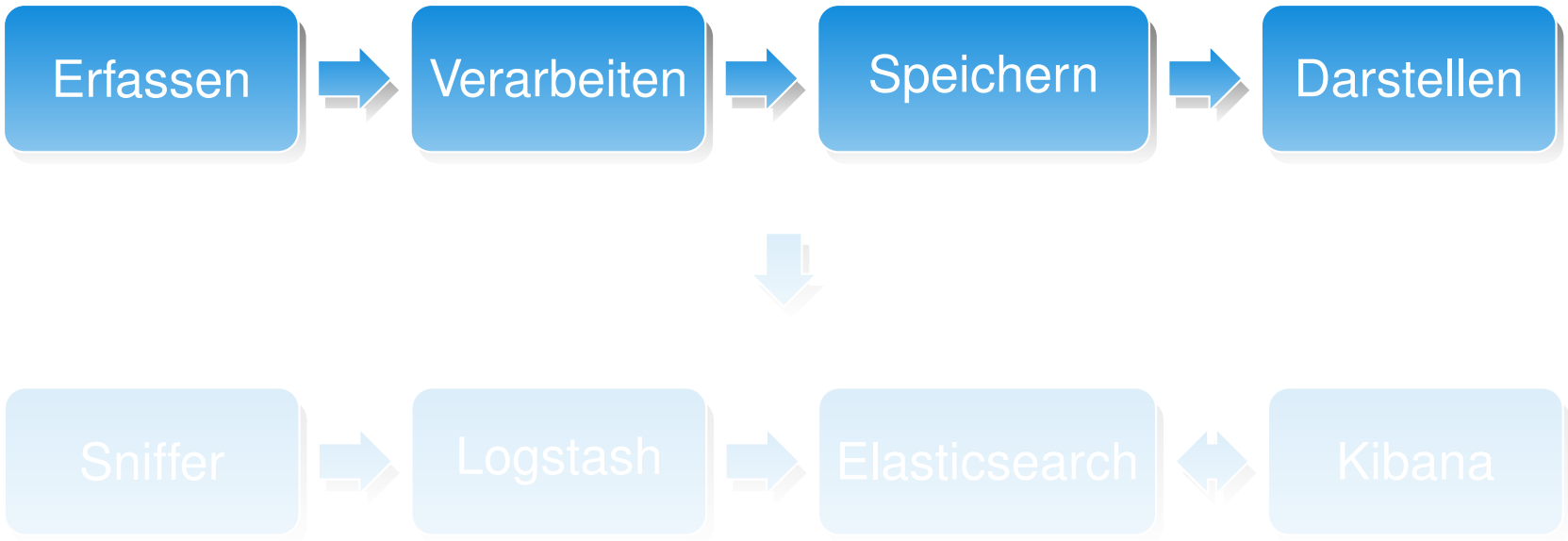
Nice to have

- (Nahezu) Echtzeit
- Verschiedene Selektoren und Ordnungen
- Diagramme

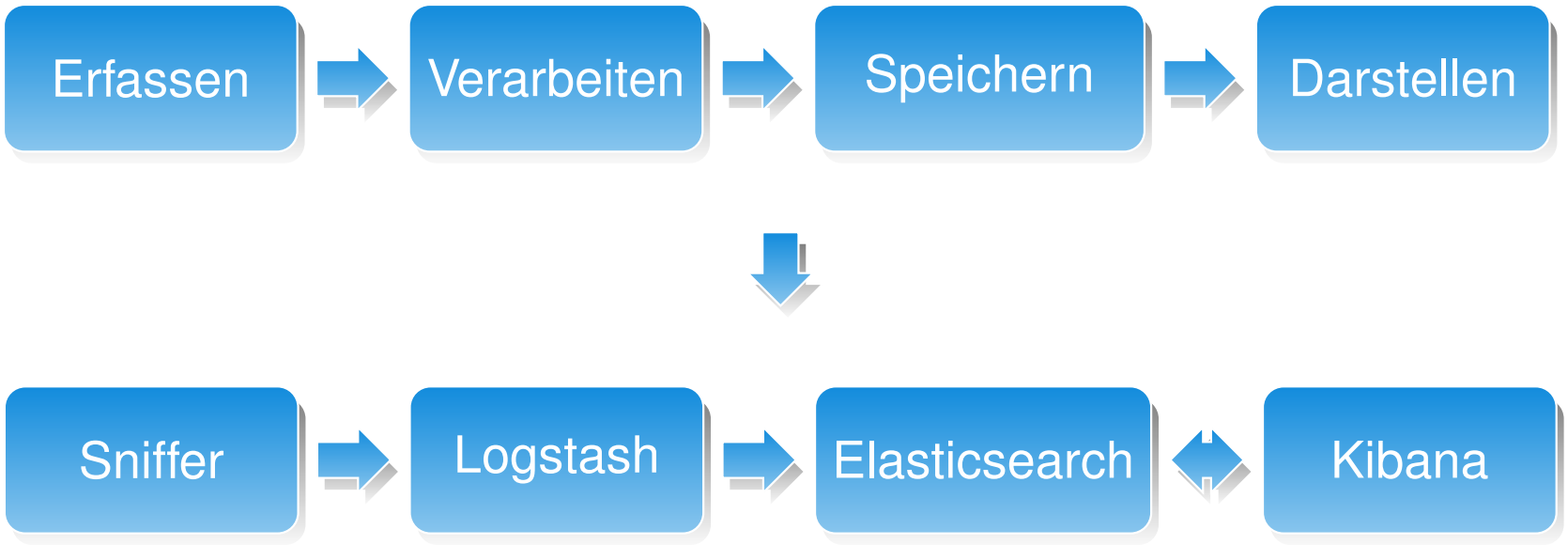
ELK-Stack

- Softwarestack für Big Data
- Dokumentorientierte-Datenbank Elasticsearch
- Datenaufbereitungswerkzeug Logstash
- Visualisierung mit Kibana

ELK-Stack


Erfassen
Verarbeiten
Speichern
Darstellen
Sniffer
Logstash
Elasticsearch
Kibana

ELK-Stack


Erfassen
Verarbeiten
Speichern
Darstellen
Sniffer
Logstash
Elasticsearch
Kibana

Umsetzung

- Sniffer?
- Open Source-Lösung?

“Aktiver” Ansatz

- Traffic capturing (bspw. *libpcap*)
- Protokoll Netflow
  - Switch/ Router
  - *fprobe*
  - *softflowd*
- *packetbeat*

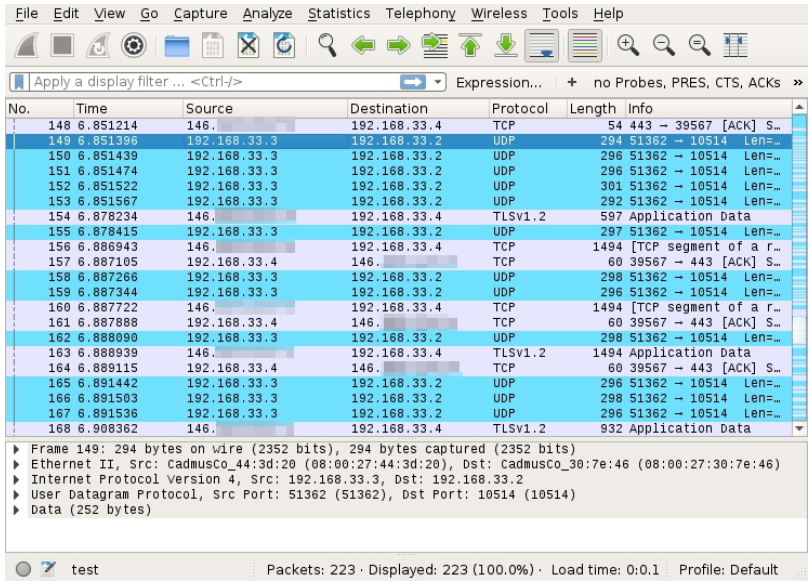


Abbildung: Visualiserung eines *pcap*-Dumps mittels *Wireshark*

“Passiver” Ansatz

- Paketfilter
  - Linux *iptables*
  - *BSD *pf*
- Nachricht für jedes Paket
- Weiterleitung Kernel-Log (bspw. syslog)

```
# iptables -A INPUT -j LOG
```



```
[ 1392.042460] IN=eth0 OUT=
MAC=08:00:27:1e:c6:7e:52:54:00:12:35:02:08:00
SRC=10.0.2.2 DST=10.0.2.15 LEN=40
TOS=0x00 PREC=0x00 TTL=64 ID=61706
PROTO=TCP SPT=54824 DPT=22
WINDOW=65535 RES=0x00 ACK URGP=0
```

Abbildung: Kernel Log-Nachricht durch *iptables* eines Netzwerkpakets

“Passiver” Ansatz

- Paketfilter
  - Linux *iptables*
  - *BSD *pf*
- Nachricht für jedes Paket
- Weiterleitung Kernel-Log (bspw. syslog)

```
# iptables -A INPUT -j LOG
```



```
[ 1392.042460] IN=eth0 OUT=
MAC=08:00:27:1e:c6:7e:52:54:00:12:35:02:08:00
SRC=10.0.2.2 DST=10.0.2.15 LEN=40
TOS=0x00 PREC=0x00 TTL=64 ID=61706
PROTO=TCP SPT=54824 DPT=22
WINDOW=65535 RES=0x00 ACK URGP=0
```

Abbildung: Kernel Log-Nachricht durch *iptables* eines Netzwerkpakets

“Passiver” Ansatz

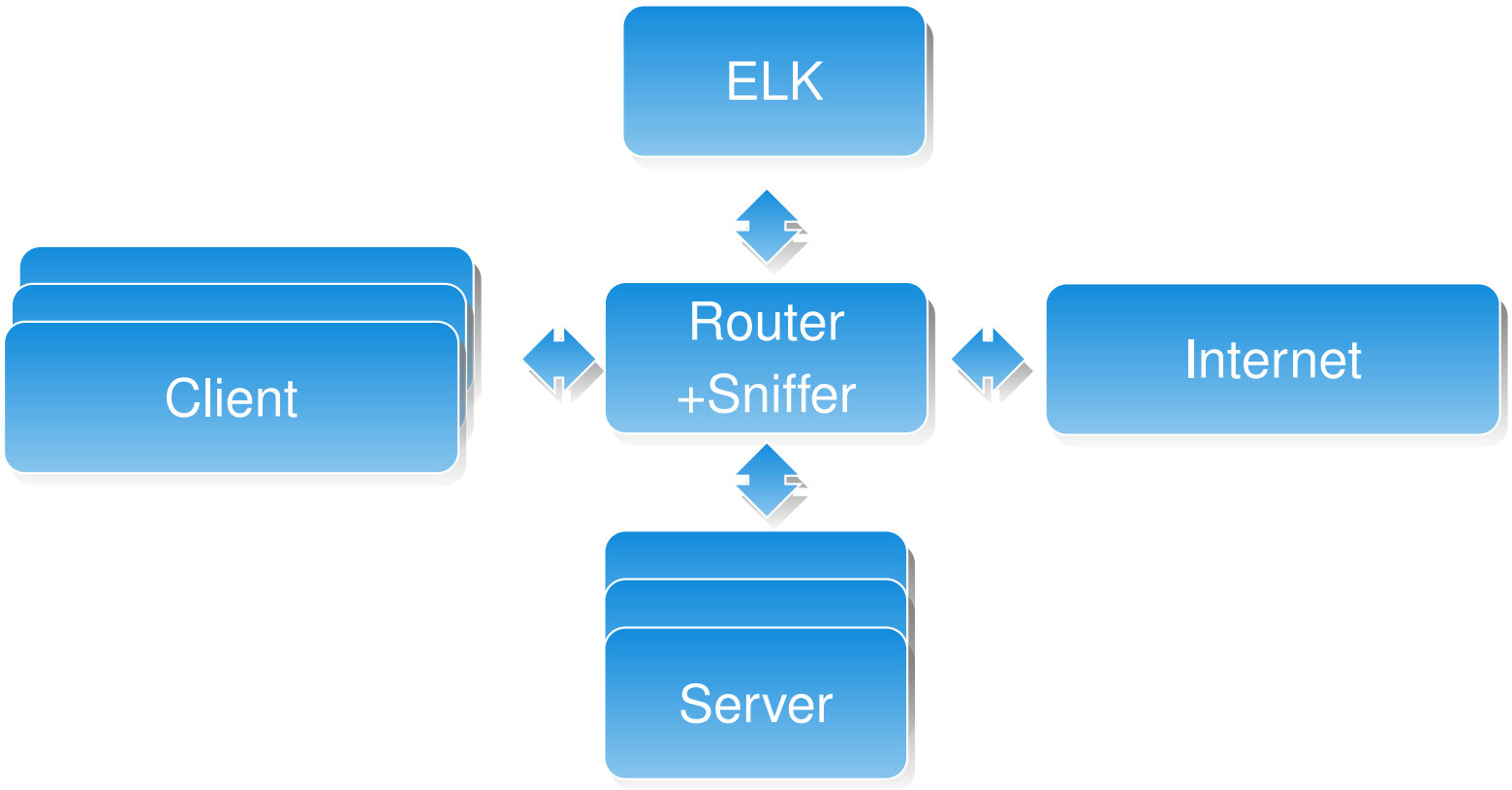
- Paketfilter
  - Linux *iptables*
  - *BSD *pf*
- Nachricht für jedes Paket
- Weiterleitung Kernel-Log (bspw. syslog)

```
# iptables -A INPUT -j LOG
```

```
[ 1392.042460] IN=eth0 OUT=
MAC=08:00:27:1e:c6:7e:52:54:00:12:35:02:08:00
SRC=10.0.2.2 DST=10.0.2.15 LEN=40
TOS=0x00 PREC=0x00 TTL=64 ID=61706
PROTO=TCP SPT=54824 DPT=22
WINDOW=65535 RES=0x00 ACK URGP=0
```

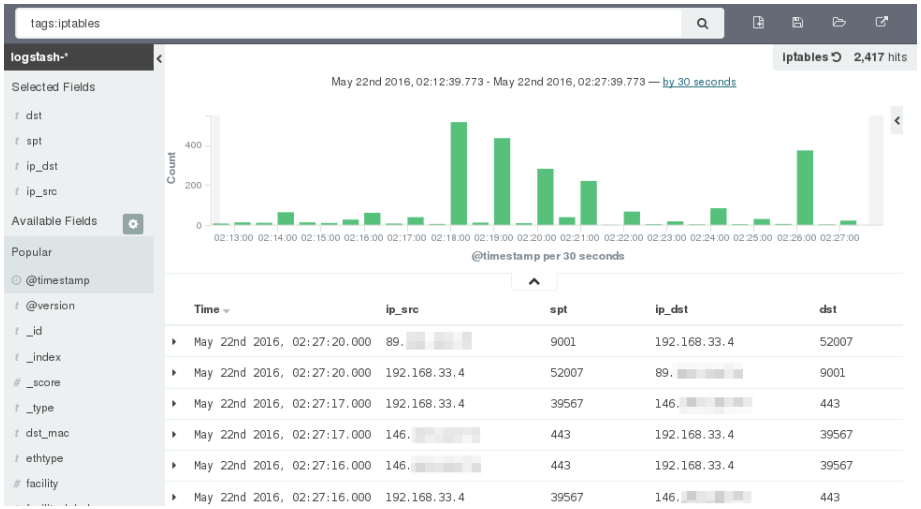
Abbildung: Kernel Log-Nachricht durch *iptables* eines Netzwerkpakets

Szenario



Demo

- Vagrant
- ELK-Node
- Router inkl. Sniffer
- Client-Node mit Tor



Weitere Möglichkeiten

- Metadatenanreicherung
  - Verbindung $\leftrightarrow$ User
  - IP-Adressen auflösen
  - GeoIP
- Deep Packet Inspection

Fazit

- Echtzeitüberwachung
- Kompletter Stack aus OSS-Komponenten
- Datenschutz?

- Folien und Software github.com/aboehm/CryptoCon2016

- Kontakt alxndr.boehm@gmail.com

  6FDE BFAC 1BBB F579 45DE 240E 5774 A845 5FDD D0B3

Links

- Elasticsearch
- Logstash
- Kibana
- Packetbeat
- softflowd mit Elasticsearch-Anbindung