



IT Talk 06/2017

Security- & Threat Intelligence

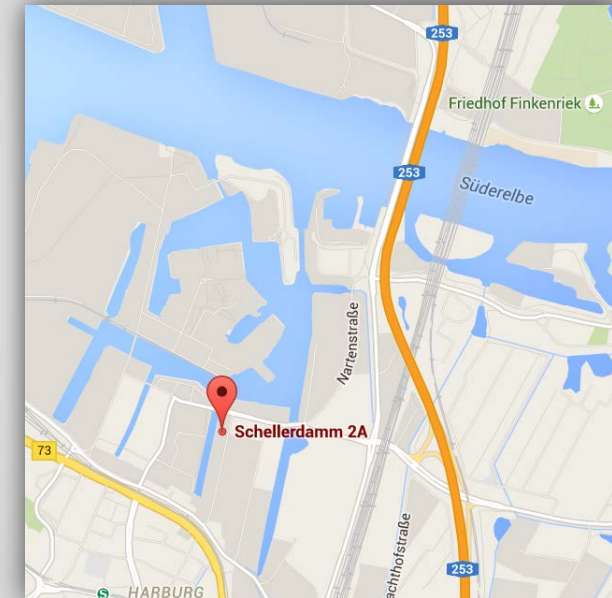
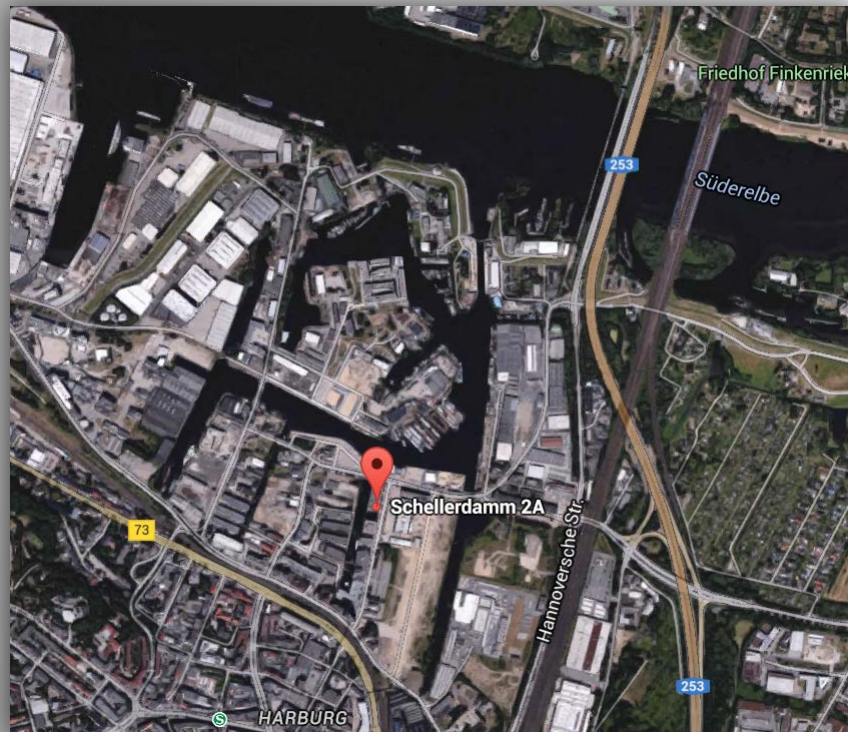
IT Talk 06/2017

Mit Sicherheit sicher.

tiri GmbH – Ihr Partner aus Hamburg



Im Herzen des Harburger Hafens



Schellerdamm 2a
D-21079 Hamburg



Informationssicherheit

- **Digitale Transformation – alles und jeder ist vernetzt!**



Q2-2016: **126 Millionen** Mobilfunkanschlüsse

584 Milliarden Emails pro Tag (ohne Spam)

Über 16 Millionen .de Domains registriert

DE-CIX Dez 2015: 5 TBit pro Sekunde Internet Traffic



Informationssicherheit

FRONTAL21 | 26.07.2016

▪ Fakt ist....

Experten sorgen sich um die Sicherheit der Datennetze von Bundeswehr und Bundesregierung. So wurde das IT-Netz der deutschen Streitkräfte im vergangenen Jahr 71 Millionen Mal von Hackern angegriffen.

Es be
völlig

rbb
H

G
u
P
Cy
Si

Berliner Zeitung ▶ Berlin ▶ Verkehr ▶ „WannaCry“: Hackerangriff legt S-Bahn-Automaten in Berlin lahm



„WannaCry“ Hackerangriff legt S-Bahn-Automaten in Berlin lahm

on
T-

🕒 17.05.17, 09:07 Uhr

Frankfurt, 10. Januar 2016



pwc

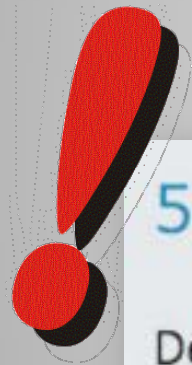
Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde

19.02.2016



Informationssicherheit

▪ Fakt ist....



51 Milliarden Euro Schaden pro Jahr

Der Digitalverband Bitkom hat in einer eigenen, umfangreichen Studie im Jahr 2015 den Schaden für die deutsche Wirtschaft durch digitale Wirtschaftsspionage, Sabotage und Datendiebstahl auf rund 51 Milliarden Euro pro Jahr geschätzt.

bitkom



Unternehmenskollaboration 4.0

- **Die Zusammenarbeit wird | muss sich ändern**
 - **Mensch-Maschinen Kommunikation** (Bsp. Smart-Factory)
 - **Always-On & Social Netzwerke** – weltweite Verbreitung von Informationen in Sekundenschnelle
 - **Zugriff** auf Unternehmensdaten **von überall** & zu jedem Zeitpunkt
- **Nutzung von „Hybriden Cloudlösungen“ unumgänglich!**
- **Alle Mitarbeiter rechtzeitig & praxisorientiert darauf vorbereiten!**



Datenschutz versus Technologie 4.0

- **Unterschätzen Sie nicht die datenschutzrechtlichen Aspekte!**
 - Mobile **Apps**, elektronische **Vertragsabschlüsse** ...
 - **Schutz von geistigem Eigentum** (Patent-, Gebrauchsmuster-, Design-, Marken- und Urheberrecht)
 - **Meldepflichten** bei Datenschutzverstößen (**Bußgelder** von bis zu **4% des Jahresumsatzes** möglich!)



TOP **5** Cloud Risiken

- 1. Datenverlust** - Daten können nicht nur durch Hackerattacken verlorengehen, sondern auch durch versehentliche Löschungen, Naturkatastrophen und ähnliches.
- 2. Unzureichendes Identitätsmanagement** - Hackerangriffe werden begünstigt durch ein fehlendes oder mangelhaftes skalierbares Authentifizierungssystem.
- 3. Unsichere Bedienoberflächen und APIs** - Schnittstellen sind besonders gefährdet, da sie zum einen die Verbindung zur Software von Drittanbietern herstellen und zum anderen meist übers Internet erreichbar sind.
- 4. Systemschwachstellen** - Sicherheitslücken sind ein altbekanntes Problem, in der Cloud werden ihre Auswirkungen potenziert.
- 5. Account Hijacking** - Der Diebstahl von Account-Daten birgt bei Cloud-Diensten zusätzliche Gefahren, Beispiel: privilegierte Zugriffe - kann drastische Ausmaße annehmen.



Threat Intelligence

Ein e... YOUR FILES HAVE BEEN MOVED TO A HIDDEN PARTITION AND CRYPTED
ESSENTIAL PROGRAMS IN YOUR COMPUTER HAVE BEEN LOCKED
AND YOUR COMPUTER WILL NOT FUNCTION PROPERLY.

— 0 —

ONCE YOUR BITCOIN PAYMENT IS RECEIVED YOUR COMPUTER AND
FILES WILL BE RETURNED TO NORMAL INSTANTLY.

YOUR BITCOIN PAYMENT ADDRESS IS:

1G6tQeWrwp6TU1qunLjdNmLTPQu7PnsMYd

[COPY THE ADDRESS EXACTLY / CASE SENSITIVE]

[CONFIRM PAYMENT BELOW TO UNLOCK COMPUTER AND FILES]

IF YOU DO NOT HAVE BITCOINS VISIT WWW.LOCALBITCOINS.COM TO PURCHASE

IF YOU HAVE MADE THE BITCOIN PAYMENT CLICK BELOW TO UNLOCK YOUR COMPUTER AND FILES

I MADE PAYMENT
PLEASE VERIFY
AND UNLOCK MY COMPUTER

Your email

Comments

PAY
0.2
BTC

die digitale
als

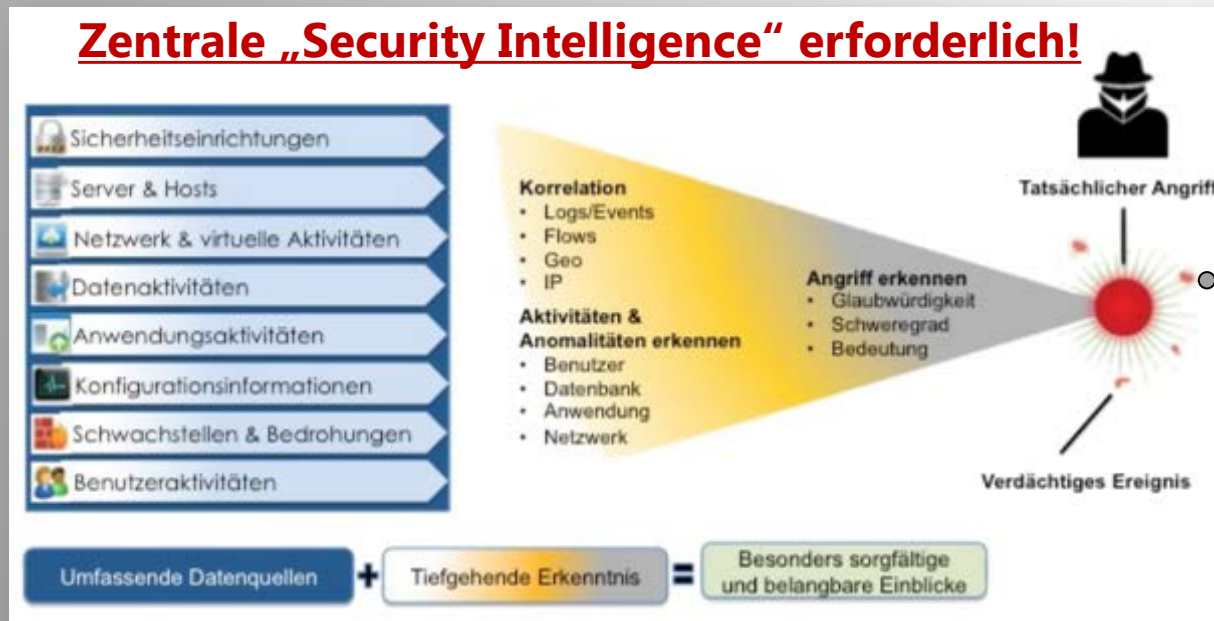
ssen
werden...

...a



Threat Intelligence

Security Monitoring im Jahr 2017...



Fakt ist...

*SIEM 4.0

- Transparenz jede Stunde auf IT-Infrastruktur
- Schwachstellen werden in Sekundenbruchteilen auf neue Schwachstellen überprüft
- Einschlägige Scan-Datenbanken durchforsten das komplette Internet in weniger als 6h
- Zentrale Logüberwachung noch immer ein Mysterium für viele IT's

*Security Information & Event Management



Fazit

Worauf ist bei der Transformation unbedingt zu achten?**1. Datenschutzerfordernungen von Beginn an klar definieren**

- Verträge, Bundesdatenschutzgesetz, spezielle Branchenrichtlinien ...

2. Einheitliche Sicherheitsvorgaben etablieren für

- Datenklassifizierung, Datenaustausch, Verschlüsselung & Authentifizierung ...

3. Transparenz der Datenhoheit in allen Projekten

- Big Data & Analytics sind wichtig, jedoch hohe Reputationsschäden bei Datenklau Vorfällen – klare Rahmenparameter für Ihre Partner

4. Sicherheitsbewusstsein im Unternehmen fordern & fördern

- Security Awareness Schulungen ...



SIEM-Light mit dem ELK-Stack

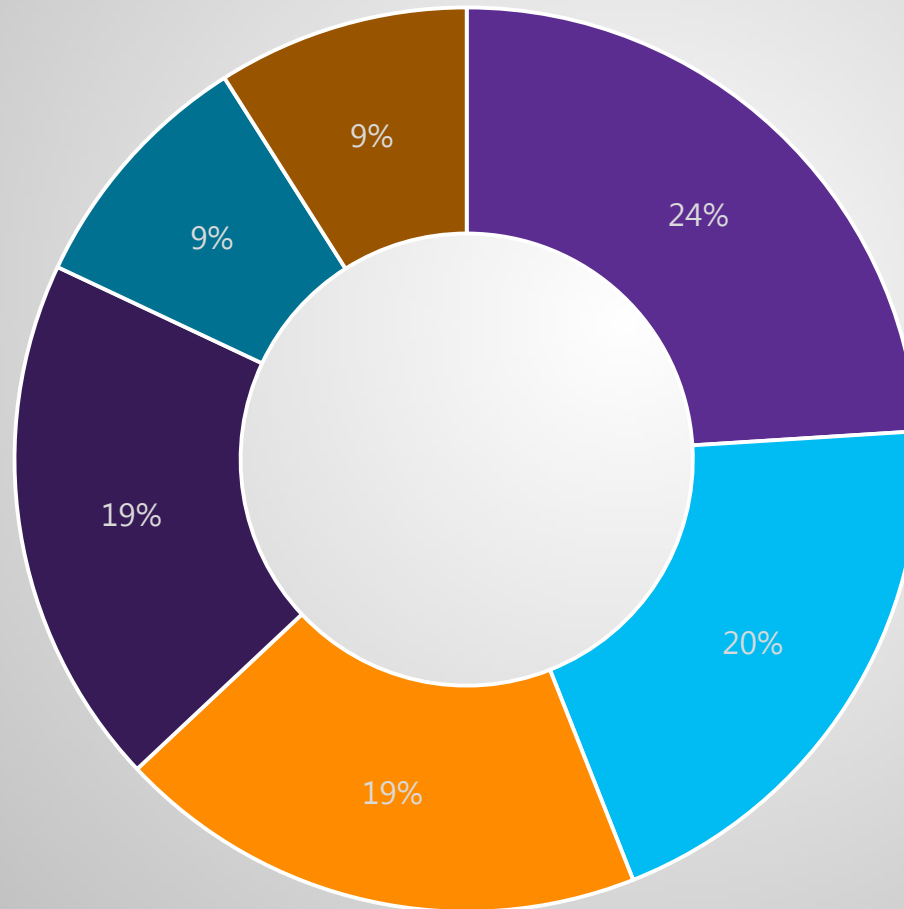
Juni 2017

Mit Sicherheit sicher.





Gefahren



- Web Application Angriff
- Andere
- Malware
- Applikationsspezifische Angriffe
- DoS / DDoS
- Reconnaissance



- Benötigt (SQL) Datenbank
 - Durch fehlendes Escapen wird Code ausgeführt
 - Ansehen von geschützten Daten
 - Löschen von Tabellen
- Cross-Site-Scripting
- Verändern einer Webpage durch Ausnutzen einer Schwachstelle
 - Böser Code wird ausgeführt



- Viren, Trojaner, Ransomware etc.
- Zum Stehlen von Informationen , Zerstören von Systemen etc.
- Zur Erpressung (Ransomware, Scareware etc.)
- Zum Einbinden in Botnet



Wana Decrypt0r 2.0

Oops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/15/2017 11:23:24
Time Left
02:23:53:40

Your files will be lost on
5/19/2017 11:23:24
Time Left
06:23:53:40

[About bitcoin](#)
[How to buy bitcoins?](#)

[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Angriffstypen

Applicationsspezifische Angriffe



EXPLOIT DATABASE Home Exploits Shellcode Papers Google Hacking Database Submit Search

Microsoft Windows Windows 7/2008 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)

EDB-ID: 42031	Author: sleepya	Published: 2017-05-17
CVE: CVE-2017-0144	Type: Remote	Platform: Win_x86-64
Aliases: EternalBlue	Advisory/Source: Link	Tags: N/A
E-DB Verified:	Exploit: Download / View Raw	Vulnerable App: N/A

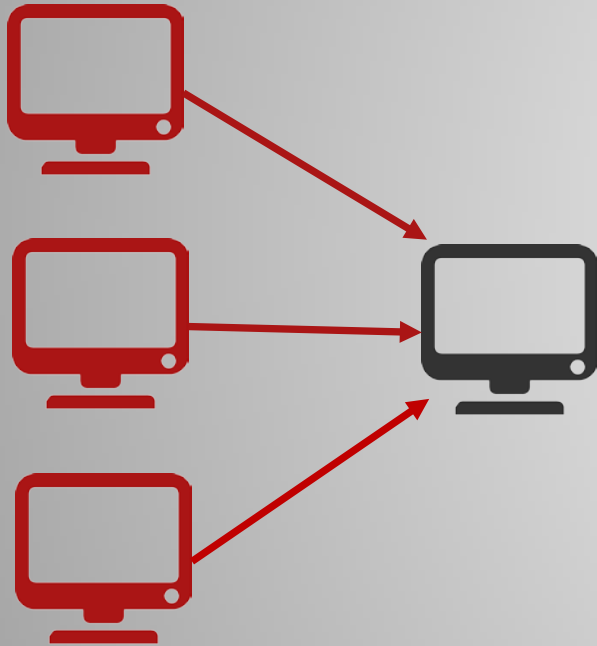
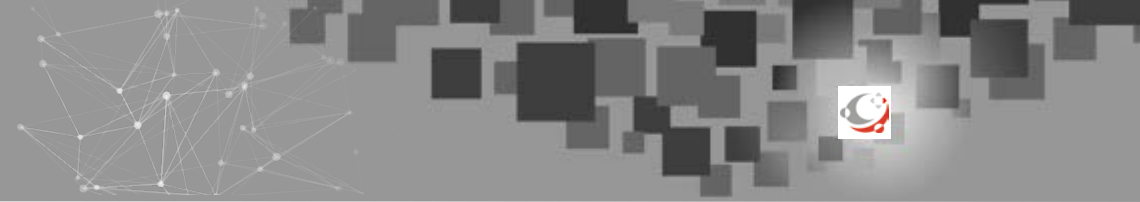
[« Previous Exploit](#) [Next Exploit](#)

```
1 #!/usr/bin/python
2 from impacket import smb
3 from struct import pack
4 import os
5 import sys
6 import socket
```

2017-06-09 Apple macOS 10.12.5 / iOS < 10.5.2 - Userspace Entitlement Checking Race Condition Multiple Google Secu...

2017-06-09 Apple macOS - Disk Arbitration Daemon Race Condition macOS phoenix

- Ausnutzen von Schwachstellen einer Anwendung
- Exploits können einfach online gefunden werden
- Ausführung beispielsweise mit Metasploit
- Beispiel: „Eternal Blue“



- Denial of Service
- Distributed Denial of Service
- Überlastung durch Datenansturm
- DDoS werden meist mit Botnetzen durchgeführt.



- Informationen über Ziel (Netzwerk beschaffen)
 - Was für Rechner sind im Netzwerk?
 - Welche Ports sind offen?
 - Welche Betriebssysteme sind installiert?
 - Netzwerkaufbau herausfinden
- Aktiv -> Direkt mit Zielsystem verbunden -> Aktive Scans
- Passiv -> Via Shodan, Netcraft, Google etc.



- Social Engineering
 - „Ich bin der IT-Experte. Ich muss mal an Ihren PC.“
 - Phishing
 - Dumpster Diving
- Physischer Diebstahl von Informationen
- Ausnutzen von Hardwareschwachstellen.
- Hacking über physischen Zugriff (Bsp. PoisonTap)



Logdatensammlung



- In vielen Fällen melden sich die Systeme. Es „hört“ nur keiner hin.
- Viele sicherheitsrelevante Logs gehen einfach unter.
 - Es sind zu viele Systeme.
 - Es wird zu viel geloggt.
 - Es wird zu wenig geloggt.
 - Die Logs werden nicht richtig gedeutet.
- Wenn frühzeitig die Zeichen bzw. Logs gedeutet werden, kann gehandelt werden.



- Was will ich über die Systeme wissen?
- Welche Systeme sind relevant?
- Anpassen der Logs (Bsp. Apache CustomLog)
- Welche Logdaten sind dafür relevant?
 - Unwichtige Logs herausfiltern (durch Parsing, Verwendung von Log-Levels ...)
 - Wichtige Logs hervorheben (Bsp: Verwenden von Tags)

```
match => { "message" => "Failed password for %{USERNAME:username} from %{IP:src_ip} port %{BASE10NUM:port} ssh2" }  
add_tag => [ "ssh_failed_password" ]
```

Logdatensammlung Bevor geloggt wird ...



```
LogFormat "%{Host}i %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" \"%h\" " slog  
CustomLog "/var/log/apache2/sogo.log" slog
```



```
www.AdresseVerfremdet.de 5.8.156.43 - - [12/Jun/2017:09:55:25 +0200] "GET /somePage.de HTTP/1.1" ..."
```



```
{%{HOSTNAME:vhost} {%{IPORHOST:proxyip} [%{HTTPDATE:timestamp}\] {%{WORD:verb} {%{NOTSPACE:request}
```

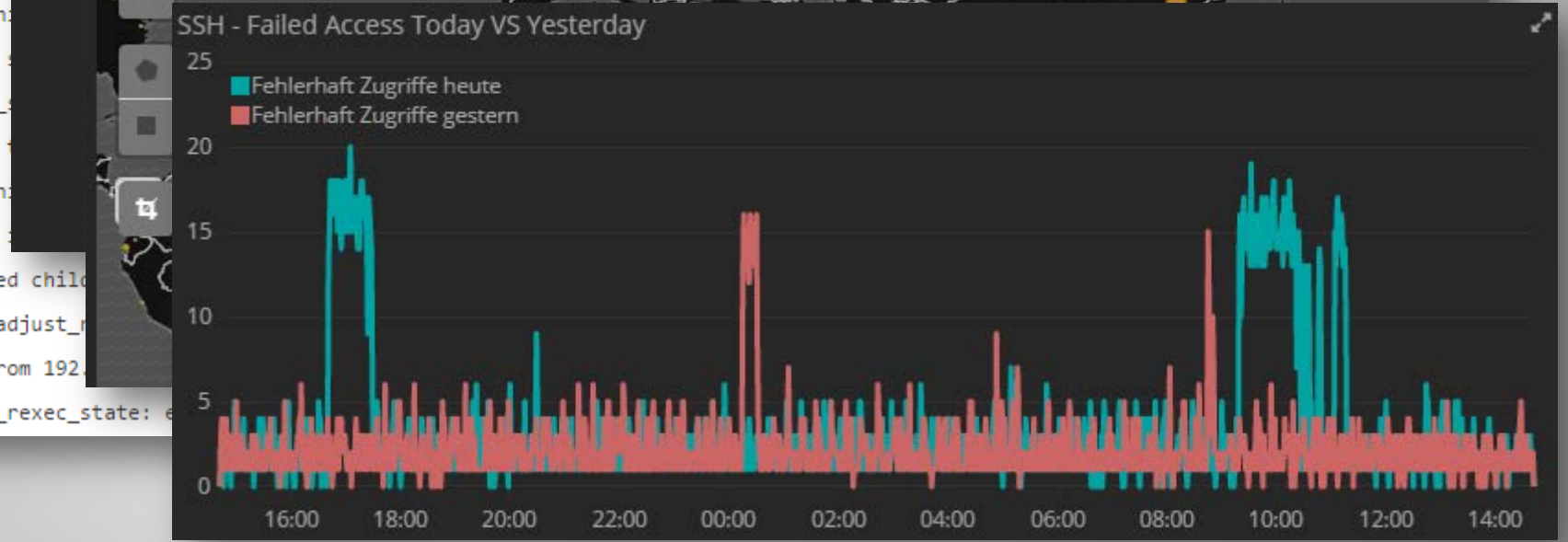
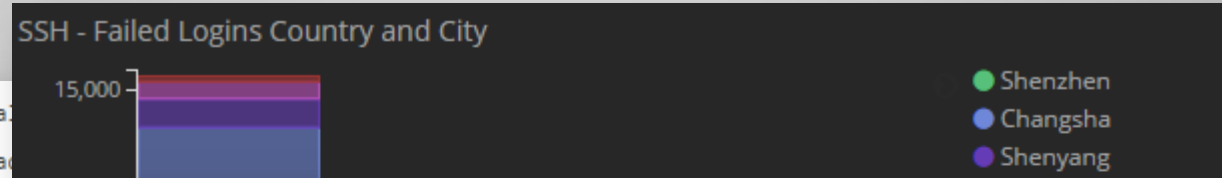


request	🔍 📄 *	/somePage.de
response	🔍 📄 *	301
timestamp	🔍 📄 *	12/Jun/2017:09:55:25 +0200
type	🔍 📄 *	syslog
verb	🔍 📄 *	GET
vhost	🔍 📄 *	www.AdresseVerfremdet.de

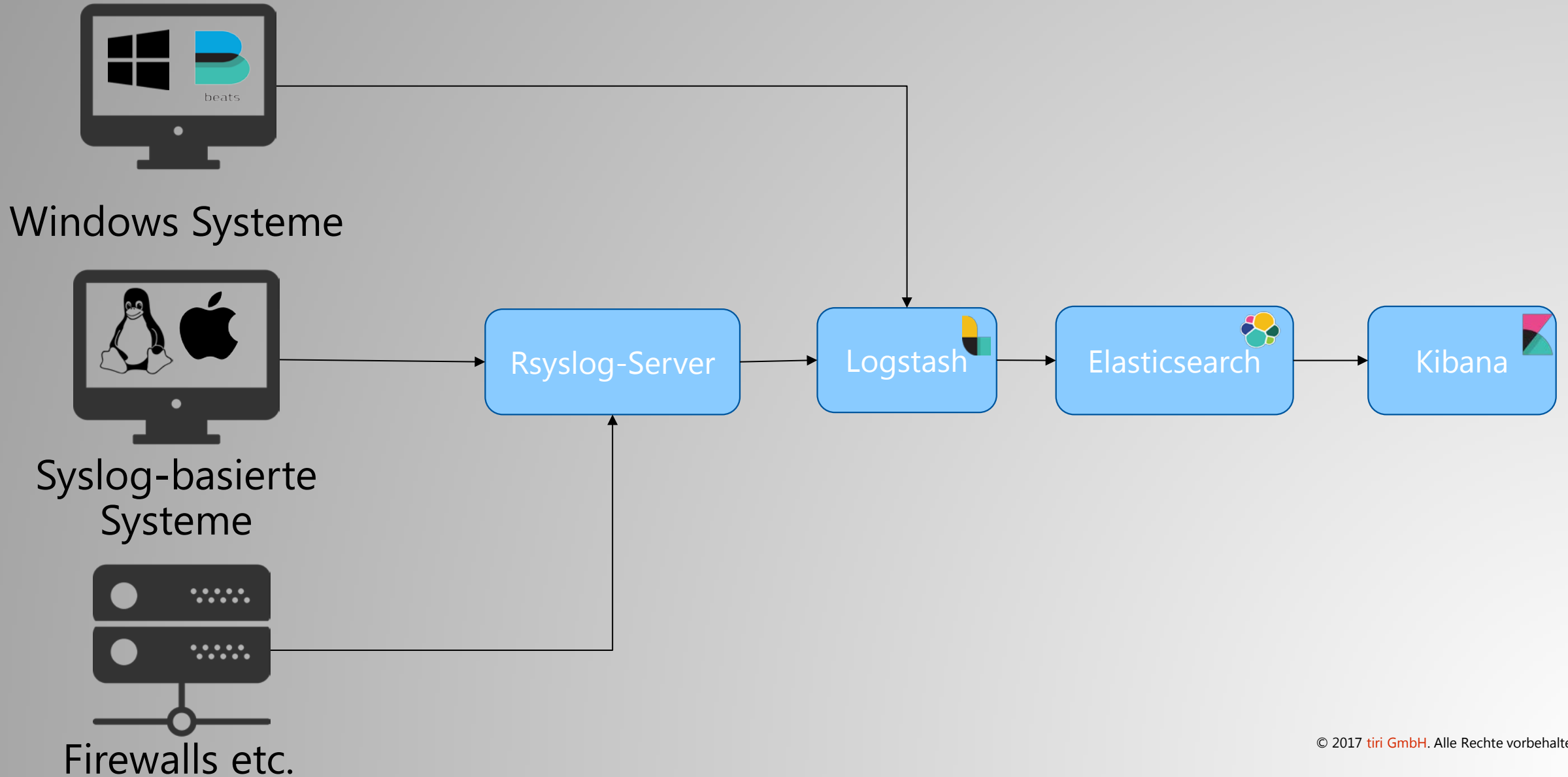
Wichtige Informationen herausfiltern



```
Nov 9 07:32:42 root2012 sshd[718]: Received signal
Nov 9 07:32:42 root2012 sshd[3518]: debug3: oom_adj
Nov 9 07:32:42 root2012 sshd[3518]: Set /proc/self
Nov 9 07:32:42 root2012 sshd[3518]: debug2: fd 3
Nov 9 07:32:42 root2012 sshd[3518]: debug1: Bind
Nov 9 07:32:42 root2012 sshd[3518]: Server listen
Nov 9 07:32:42 root2012 sshd[3518]: debug2: fd 4
Nov 9 07:32:42 root2012 sshd[3518]: debug3: sock_
Nov 9 07:32:42 root2012 sshd[3518]: debug1: Bind
Nov 9 07:32:42 root2012 sshd[3518]: Server listen
Nov 9 07:32:47 root2012 sshd[3518]: debug3: fd 5
Nov 9 07:32:47 root2012 sshd[3518]: debug1: Forked child
Nov 9 07:32:47 root2012 sshd[3520]: debug3: oom_adjus
Nov 9 07:32:47 root2012 sshh[2344]: connection from 192
Nov 9 07:32:47 root2012 sshd[3518]: debug3: send_rexec_state: e
```



Aufbau









- Sammelt alle Logdaten auf Linuxsystemen
- Weiterleitung von Logdaten via TCP und UDP (auch mit TLS-Verschlüsselung)
- Aussortieren von Logdaten
- Zahlreiche Input- und Outputmodule (Logstash, Kafka, HDFS ...)
- Aussortieren von Logs



- Beats sind Agenten, welche Daten an Logstash oder Elasticsearch senden.



Beat	Aufgabe
 Filebeat	Datei-basierte Abholung
 Metricbeat	Systemmonitoring-Daten auslesen
 Winlogbeat	Auslesen von Windows Event-Logs
 Packetbeat	Auslesen von Netzwerkdaten



- Nimmt Daten von unterschiedlichen Quellen an.
- Bereitet diese so auf, dass eine spätere Suche einfach und performant ist.
 - Parsen mit Grok Patterns
 - Weitersenden als JSON
 - Einfügen der Location anhand eines GeoIP Lookup
- Versehen der Logdaten mit Tags



- Cluster aus mehreren Servern
- Logdaten werden verteilt auf allen Nodes gespeichert.
- Beherbergt die eigentliche Logdatensammlung
- Kann via Curl, Java, C#, Python etc. angesprochen werden.
- Kann via X-Pack um zahlreiche Funktionen erweitert werden.
 - Alerting, Machine Learning, Reporting etc.



- Weboberfläche zum Anzeigen und Auswerten der Logdaten
- Logdaten über Querrys durchsuchen
- Erstellen von zahlreichen Visualisierungen
- Dashboards für eine schnelle Übersicht erstellen
- Status des Elasticsearchclusters überwachen



Live Demo

Was können wir für Sie tun ?



Aufbau SIEM /SIEM
Light

Einrichtung von
Honeypots

Beratung zum Aufbau
einer zentralen
Logdatensammlung

Welche Logs
sollen
Ausgewertet
werden.

Welche
Systeme sind
relevant?

Entwurf einer
entsprechenden
Architektur



Hourglass icon (S.9) made by [Dave Gandy](#) from [flaticon](#)

Computer icon (S.4 ,S.5, S.8 S.16) made by [Roundicons](#) from [flaticon](#)

Documents icon (S.11) made by [Freepik](#) from [flaticon](#)

Spy icon (S.10) made by [Freepik](#) from [flaticon](#)

Server icon (S.11) made by [Madebyoliver](#) from [flaticon](#)

Tux icon (S.11) made by [Dave Gandy](#) from [flaticon](#)

Apple icon (S.11) made by [Dave Gandy](#) from [flaticon](#)

Elasticsearch, Kibana, Logstash and Beats icon (S. 16, S. 18 – 21) by [Elastic](#)

Windows icon made by [Icomoon](#) from [flaticon](#)



ありがとうございます

Salamat Po

متشكراً
謝謝

Grazie

ευχαριστώ

Merci!

Kiitos

ขอบคุณครับ

شكراً

Hvala

благодаря

Dziękuję

Teşekkürler

شكريه

Wir freuen uns auf Sie!

Terima Kasih

நன்றி

Mulțumesc

Tack

спасибо

Cám ơn

Dank u Wel

Ďakujem

Thank you!

감사합니다

Tak

Gracias

多謝晒

ДЯКУЮ

תודה

Obrigado

Děkuji

Köszönöm