IT Talk 06/2017

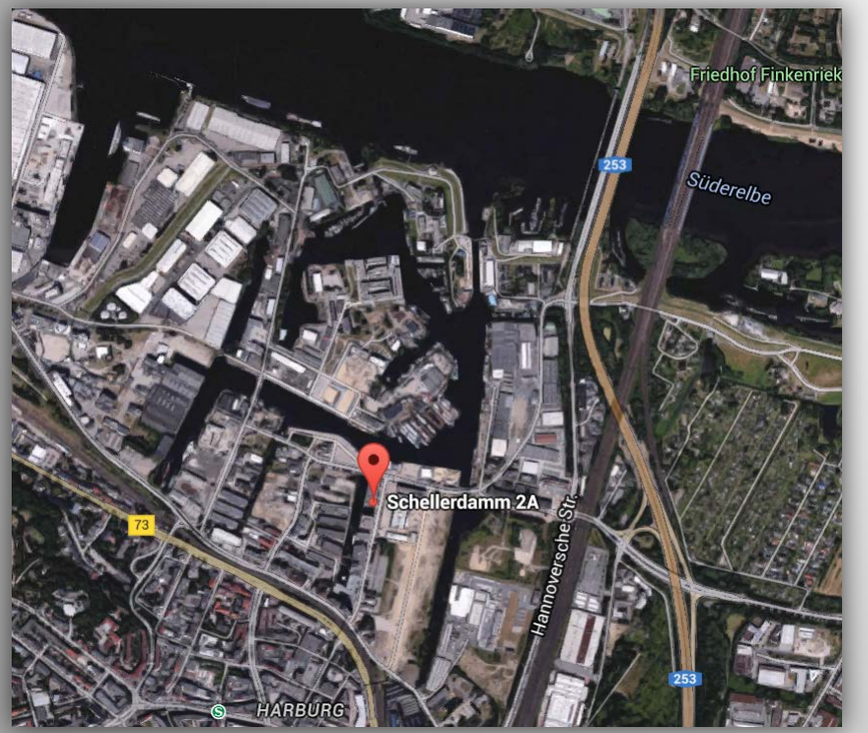
Security- & Threat Intelligence

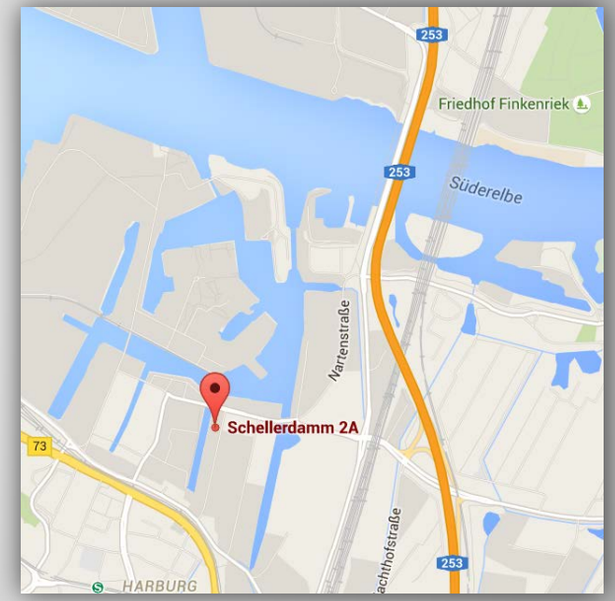
Mit Sicherheit sicher.

IT Talk 06/2017

tiri GmbH – Ihr Partner aus Hamburg

Im Herzen des Harburger Hafens





Schellerdamm 2a
D-21079 Hamburg

Security & Threat Intelligence

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

Security & Threat Intelligence

Informationssicherheit

- **Fakt ist….**

FRONTAL21 | 26.07.2016

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

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

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

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

Security & Threat Intelligence

Informationssicherheit

- **Fakt ist….**

bitkom

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.

Quelle: https://www.bitkom.org

Security & Threat Intelligence

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!**

Security & Threat Intelligence

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!)

Digitale Transformation

Security & Threat Intelligence

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.

Security & Threat Intelligence

Threat Intelligence

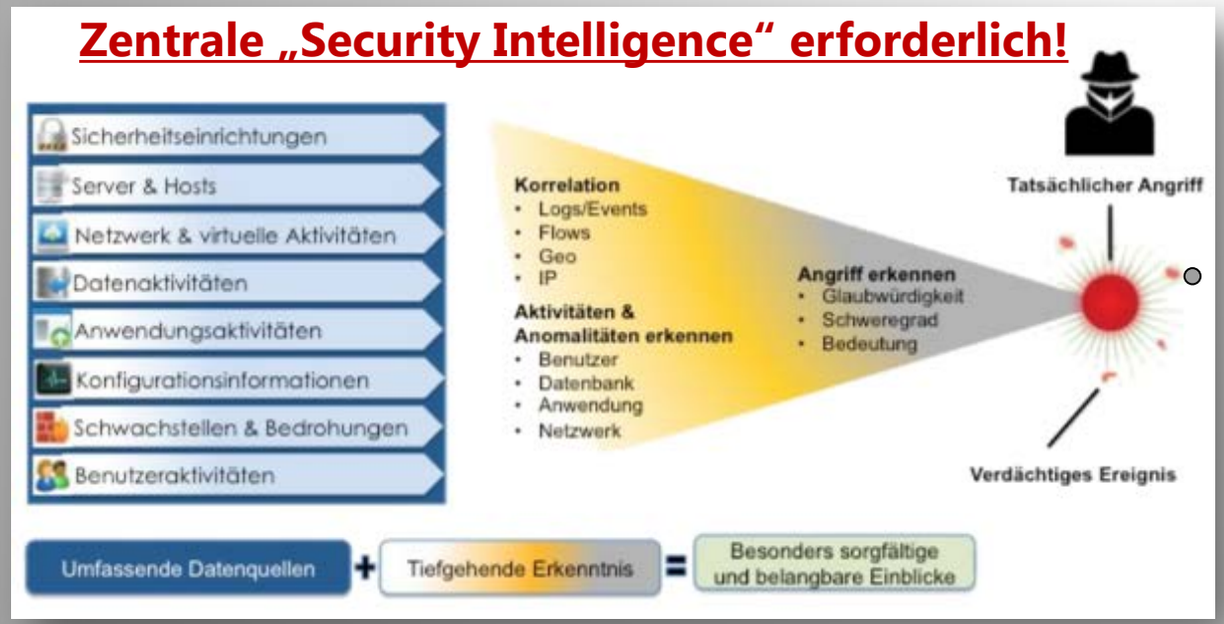
- **Ein e… die digitale …als**

…a… …ssen …erden…

Security & Threat Intelligence

Threat Intelligence

- **Security Monitoring im Jahr 2017…**



*Security Information & Event Management

Fakt ist…

*SIEM 4.0

- **…sans jede Stunde auf …kinfrastruktur**
- **…ionen werden in …chnelle 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**

Quelle: IBM

Digitale Transformation

Security & Threat Intelligence

Fazit

Worauf ist bei der Transformation unbedingt zu achten?

1. **Datenschutzanforderungen 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 …

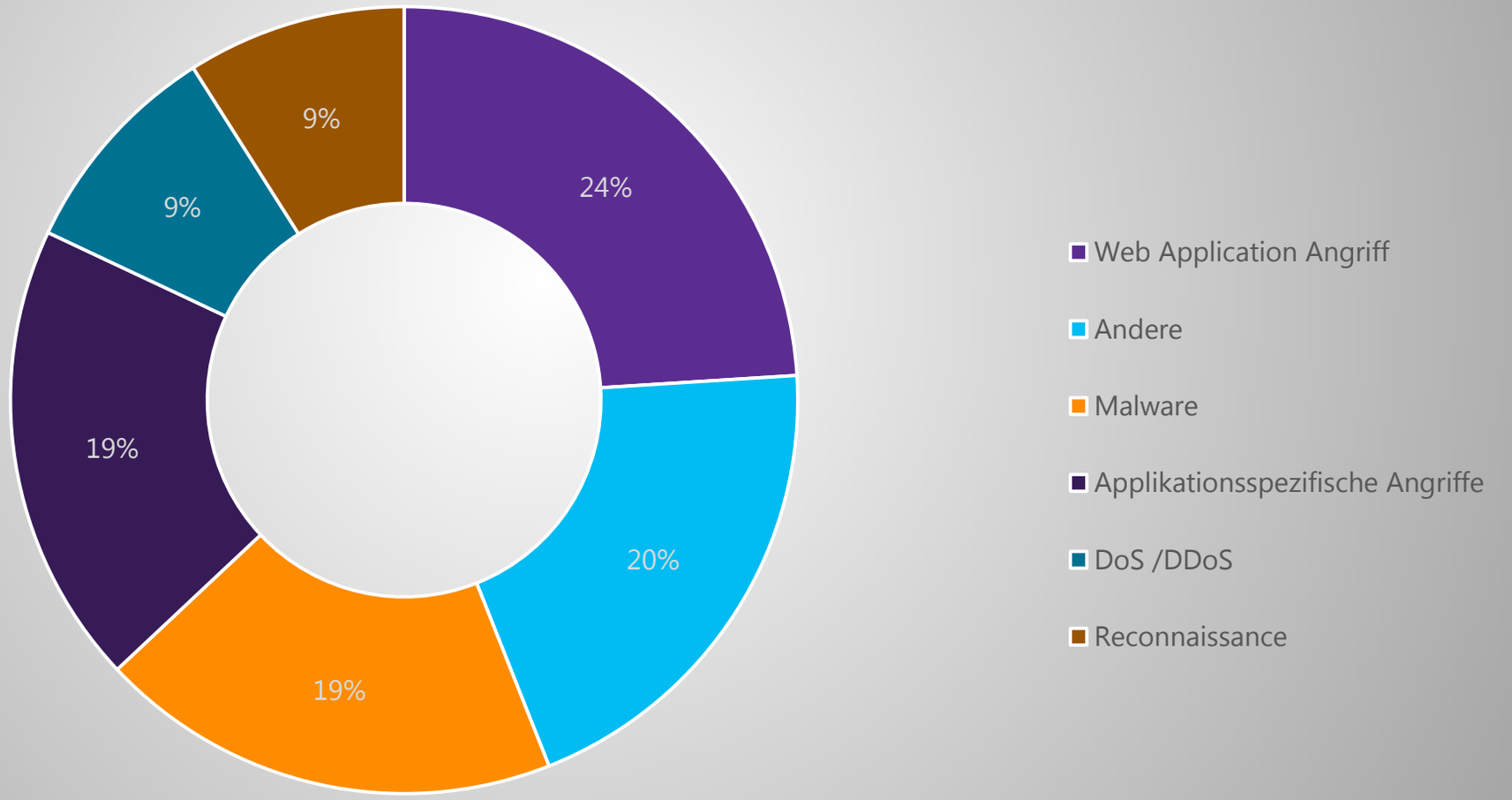
SIEM-Light mit dem ELK-Stack

Juni 2017

Mit Sicherheit sicher.

Gefahren

Logauswertung
Angriffstypen



Quelle : https://www.calyptix.com/top-threats/top-5-cyber-attack-types-in-2016-so-far/

Angriffstypen
Web Application Angriff

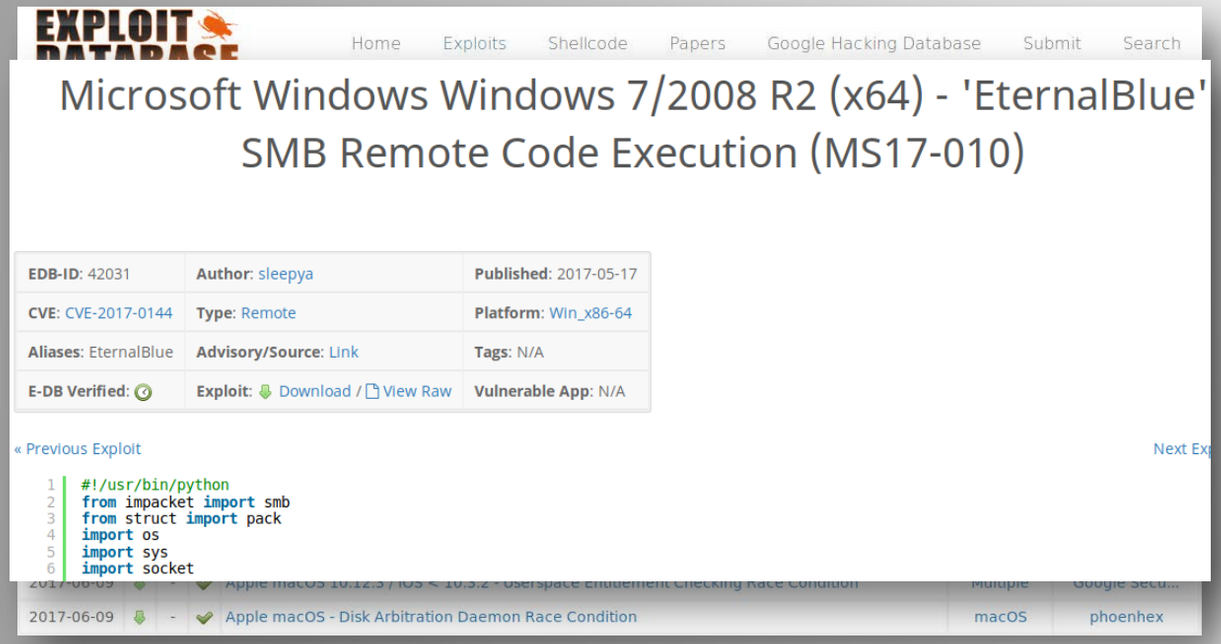
- Benötigt (SQL) Datenbank
  - Durch fehlendes Escapen wird Code ausgeführt
  - Ansehen von geschützten Daten
  - Löschen von Tabellen
- Cross-Site-Scripting
- Verändern einer Webpage durch Ausnutzen einer Schwachstelle
  - Böser Code wird ausgeführt

Angriffstypen
Malware

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

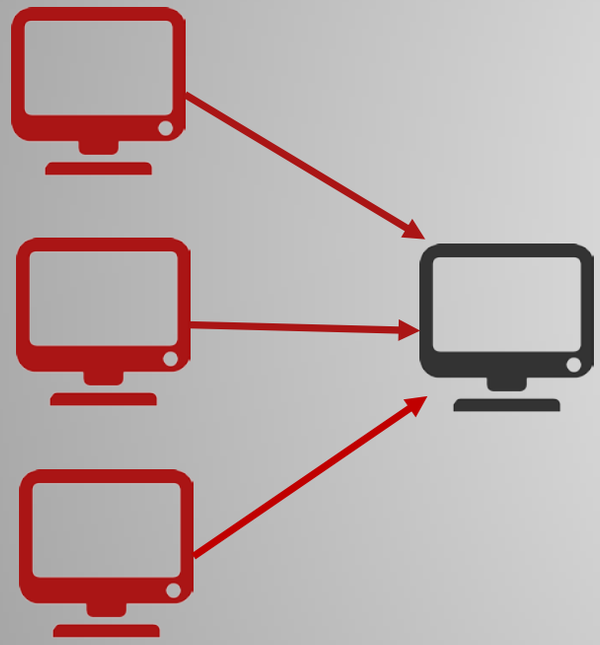
Angriffstypen
Malware

Angriffstypen
Applicationsspezifische Angriffe



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

Angriffstypen
DoS /DDoS



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

Angriffstypen
Reconnaissance

- 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.

Angriffstypen
Andere

- 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)

http://www.freepik.com

Logdatensammlung

Logdatensammlung
Warum?

- 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.

Logdatensammlung
Bevor geloggt wird …

- 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 …

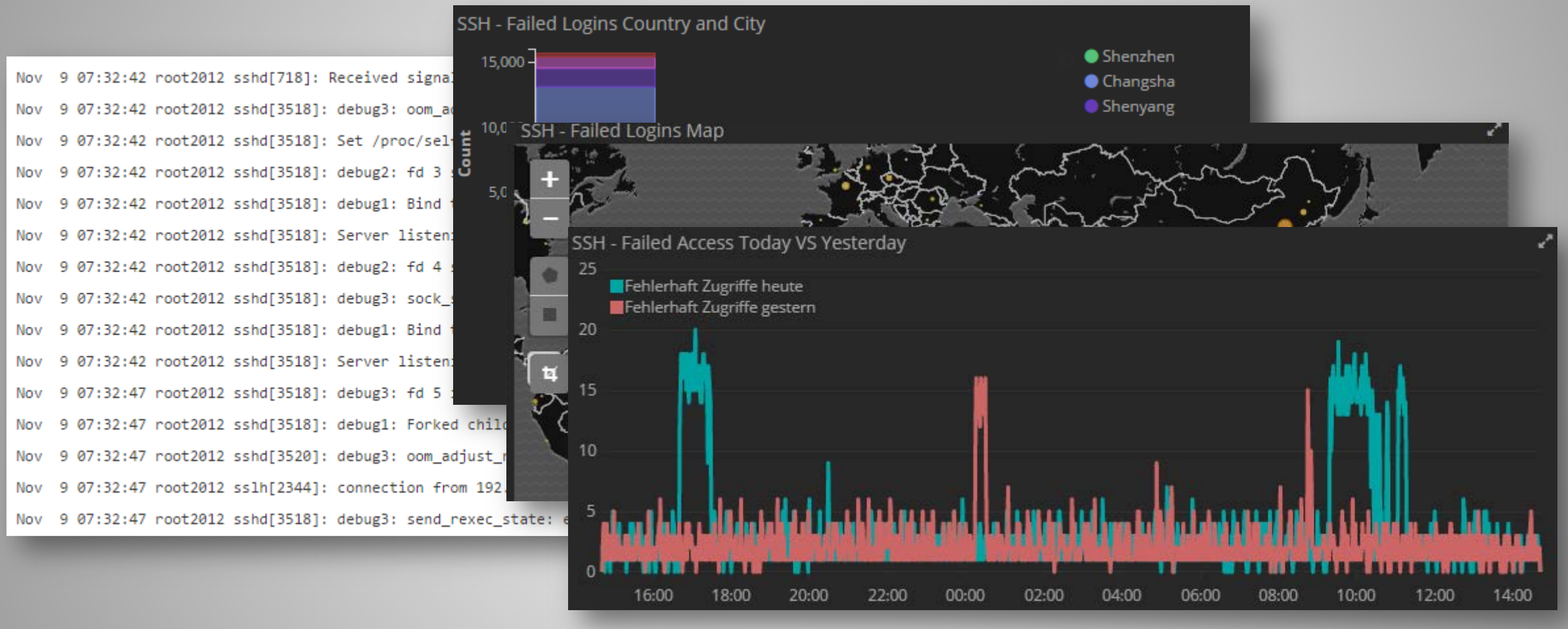
```
LogFormat "%{Host}i %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" \"%h\"" slog
CustomLog "/var/log/apache2/sogo.log" slog
```

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

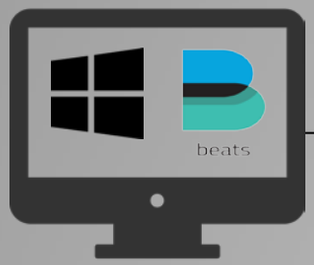
```
%{HOSTNAME:vhost} %{IPORHOST:proxyip} [%{HTTPDATE:timestamp}\] %{WORD:verb} %{NOTSPACE:request}
```

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

Wichtige Informationen herausfiltern

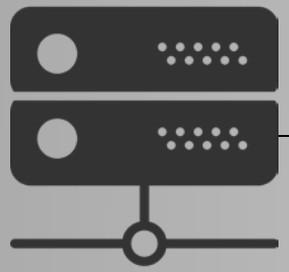


Aufbau



Windows Systeme

Syslog-basierte Systeme



Firewalls etc.

Rsyslog-Server

Logstash

Elasticsearch

Kibana

Logdatensammlung
Rsyslog

- 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

Logdatensammlung
Beats

- 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

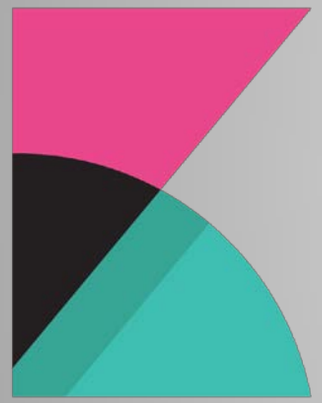
Logdatensammlung
Logstash

- 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

Logdatensammlung
Elasticsearch

- 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.

Logdatensammlung
Kibana



- 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


tiri GmbH
ありがとうございます
Salamat Po
متشكرم
Grazie
ευχαριστώ
Kiitos
谢谢
Merci!
ขอบคุณครับ
شكراً
Hvala
благодаря
Teşekkürler
شكريه
Dziękuję
Wir freuen uns auf Sie!
Terima Kasih
நன்றி
Mulţumesc
Tack
спасибо
Cám ơn
감사합니다
Dank u Wel
Tak
Ďakujem
Thank you!
Gracias
多謝晒
дякую
תודה
Děkuji
Obrigado
Köszönöm