# Dateiserver: Gruppe 5 + 10

# Agenda



- Projektorganisation
- Funktionales Grobkonzept
- Sicherheitskonzept
- Datensicherungskonzept
- Technische Systembeschreibung
- Ausblick
- Fazit

# Projektorganisation



- Gruppendefinition
- Entscheidungsfindung
- Kommunikation
- Dokumentation***
- Vorgehensmodell****
- Versionskontrolle**
- Konfigurationsmanagement***
- Qualitätssicherung***
- Testverfahren***

*** Anzahl der Folien

# Projektorganisation



Gruppe 10

*Wir!*

Wer?

Gruppendefinition!

Nord

Gruppe 5

Süd

# Projektorganisation



## Entscheidungsfindung?

*Demokratie ist, wenn zwei Wölfe und ein Schaf entscheiden, was es zu essen gibt.*[1]

[1] Aus Michael Moore „Capitalism“

# Projektorganisation



Doodle

*Skype*

Screen

Mumble

## Kommunikation

Jabber

Newsgroup

TeamViewer

E-Mail

# Projektorganisation



GitHub

*Wiki*

LibreOffice

Dokumentation

Markdown

DokuWiki

LaTex

# Dokumentation



Sie befinden sich hier: start » sued_file » **gruppenarbeit**
Zuletzt angesehen: • sued_file • vorgehensweise • start • **gruppenarbeit**

Sidebar:

Diskussion:

- Startseite

Gruppe Nord:

1. **Netzwerk Nord**
   a. Netzwerkplan
   b. Domäne und DNS
   c. Anleitung zum Einbinden der Clients ins VPN-Nord
   d. Mailverlauf
2. **Zertifikat Nord**
3. **Mailserver Nord**
4. **Fileserver Nord**
   a. Vorgehensweise und Entscheidungsfindung
   b. Organisation der Gruppenarbeit
      I. Meeting - Protokolle.
   c. Systembeschreibung
   d. Dokumentation
5. **Webserver Nord**
   a. Vorgehensweise und Entscheidungsfindung
   b. Organisation der Gruppenarbeit
   c. Systembeschreibung
   d. Dokumentation

Gruppe Süd:

1. **Netzwerk Süd**
2. **Zertifikat Süd**
3. **Mailserver Süd**
4. **Fileserver Süd**
   a. Vorgehensweise und Entscheidungsfindung
   b. **Organisation der Gruppenarbeit**
      I. Meeting - Protokolle.
   c. Beschreibung des installierten Systems
   d. Dokumentation
   e. Anhang

sued_file:gruppenarbeit

**Dies ist eine alte Version des Dokuments!**

## Umsetzung der Gruppenarbeit

Wir haben uns entschlossen ein gemeinsames Kanbanboard via Trello zu benutzen. Trello unterstützt nicht alle Praktiken aber bietet ein kostenloses und einfaches Setup für alle Teilnehmer. Um fehlende Features wie die **Begrenzung der angefangenen Arbeit** abzudecken haben wir Konventionen definiert die z.b. die Aufgabenanzahl pro Spalte begrenzen.

Folgende Spalten haben wir definiert:

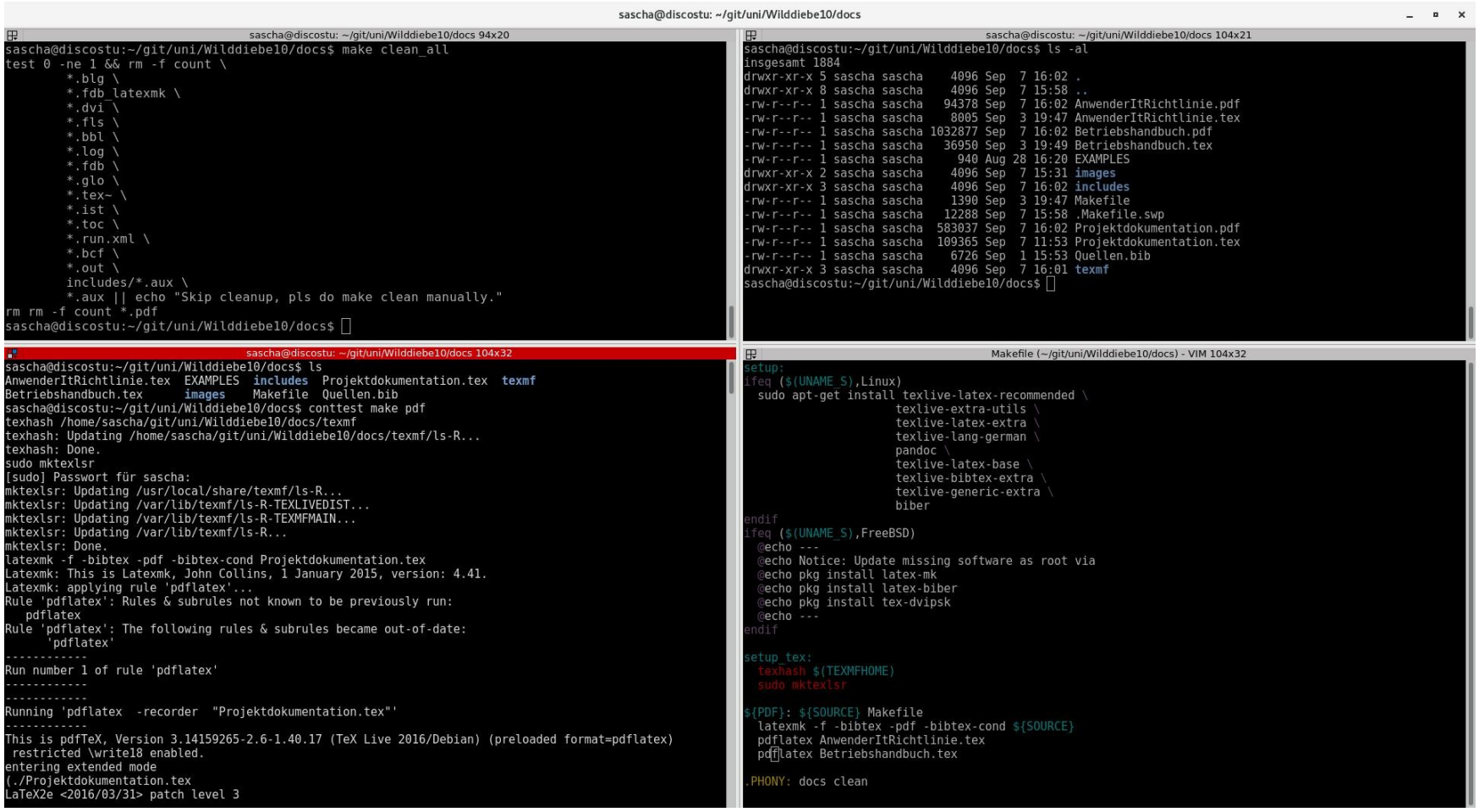
- *Backlog* - Aufgaben die auf Bearbeitung warten. Hier kann jeder zugreifen und sich eine Aufgabe nehmen. Um zu verhindern das Arbeit doppelt gemacht wird das übernehmen der Aufgabe durch hinzufügen der eigenen Person zur Aufgabe gekennzeichnet. Da die Zuordnung zu Personen erst in der nächsten Spalte passiert ist die **Taskanzahl nicht beschränkt**
- *In Progress*
  - *Research* - Aufgaben die in Bearbeitung sind und bei denen der Inhalt noch Evaluiert werden muss z.B. wenn noch nicht klar ist wie etwas konkret umgesetzt werden muss. Hier sollte die Anzahl, der Aufgaben pro Person, **zwei** nicht überschreiten.
  - *Working on* - Aufgaben die konkret in Bearbeitung sind. Hier sollte die Anzahl der Aufgaben pro Person **drei** nicht überschreiten.
  - *Blocked* - Die Aufgabe kann nicht weiter bearbeitet werden. Gründe hierfür können sein das Zuarbeit von anderen Personen fehlt oder technische Probleme eine weitere Bearbeitung verhindern. Die Anzahl der Aufgaben sollte pro Person **fünf Aufgaben** nicht überschreiten.
- *To Review* - Um sicherzustellen das alle Aufgaben gemäß DoD mit einem 4-Augen Prinzip bearbeitet werden werden Tasks die bereit zum Review sind hier gesammelt. Jeder kann sich hier Aufgaben nehmen und sich den Inhalt entweder vorstellen lassen oder selbständig anschauen und ggf. kommentieren oder ergänzen. Sollten Ergänzungen nötig sein muss der Task entsprechend wieder in einen Zustand der Bearbeitung verschoben werden. Die Aufgabenanzahl sollte pro Person **drei Aufgaben** nicht überschreiten.
- *Done* - Die Aufgabe ist gemäß DoD abgeschlossen. **Taskanzahl ist unbegrenzt**.
- *Ideas* - Aufgaben mit niedriger Priorität die optional umzusetzen sind. **Taskanzahl ist unbegrenzt**.

Inhaltsverzeichnis

- Umsetzung der Gruppenarbeit
  - Statusmeetings (Standup-Meetings)
  - Reviews
  - Priorisierung
  - DoD
- Gemeinsames Repository
- Konfigurationsmanagement / Automatisierung
  - Ansible
    - Sicherheit
    - Qualitätssicherung

# Dokumentation





# Projektorganisation



Begrenze die Menge angefangener Arbeit

*Mache die Regeln für den Prozess explizit*

Kanban

Vorgehensmodell?

Trello

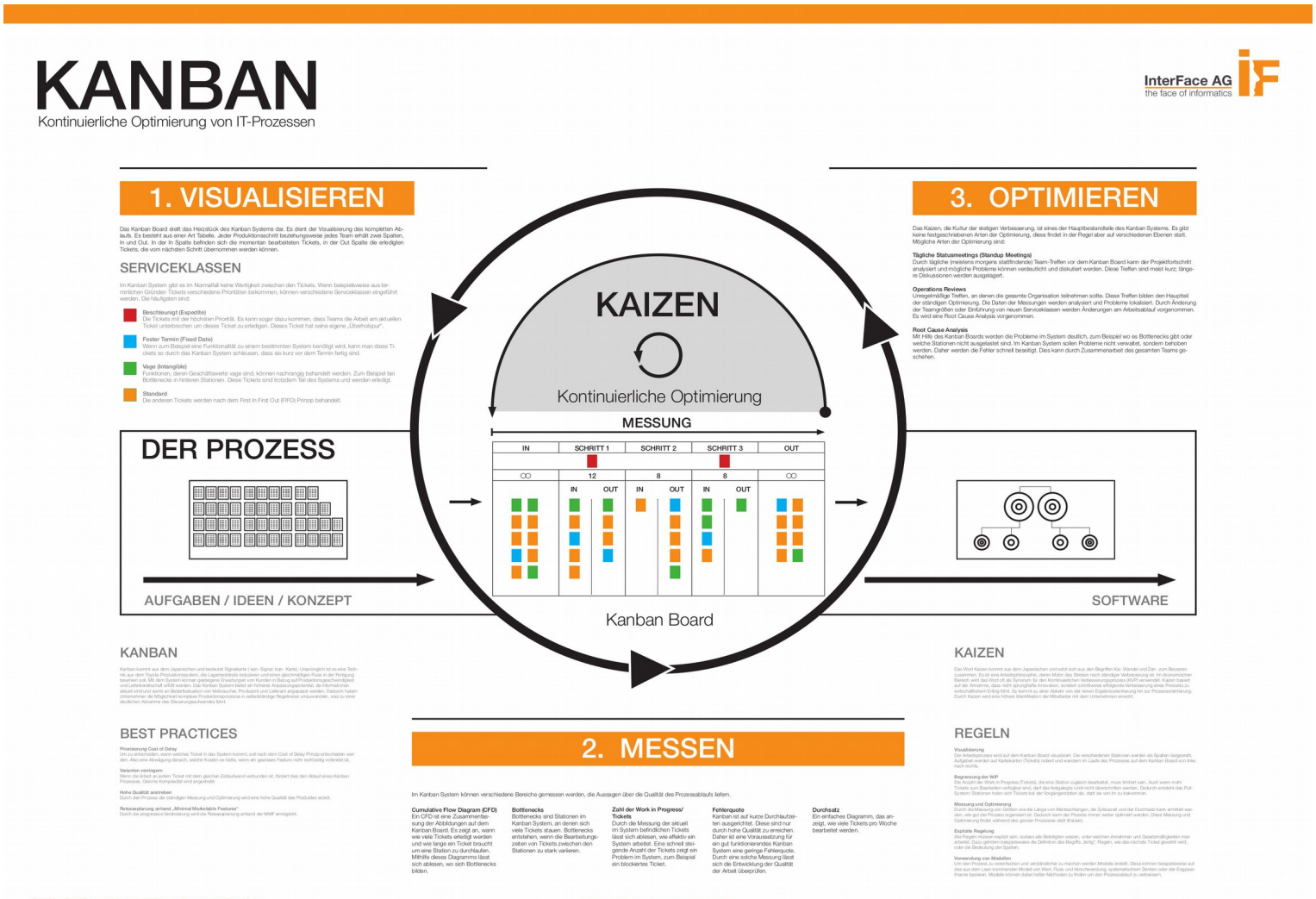
Reviews

Visualisiere den Fluss der Arbeit

Miss und steuere den Fluss

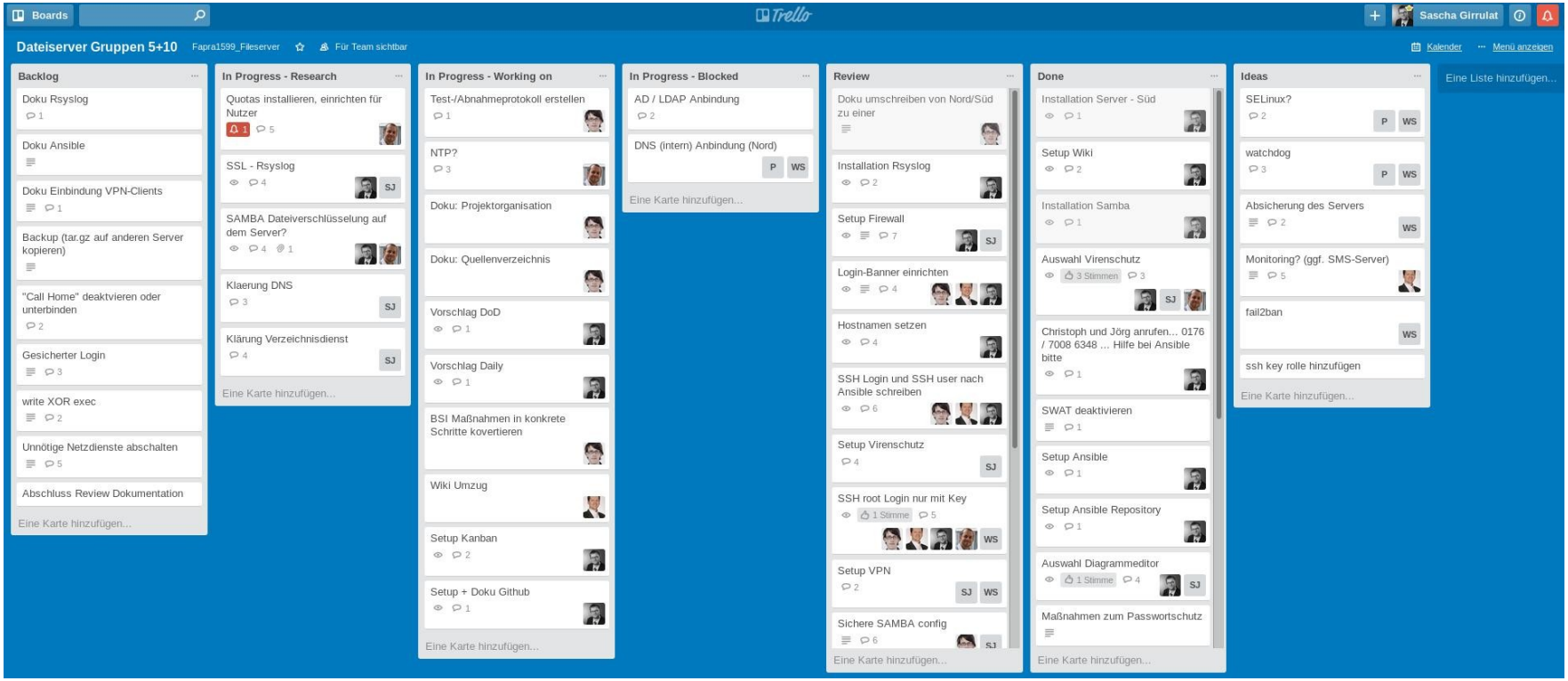
# Vorgehensmodell





# Vorgehensmodell





# Vorgehensmodell



Testen

Scrum

## DoD – Definiton of Done

*Mache die Regeln für den Prozess explizit*[1]

Dokumentation

4 Augen Prinzip

[1] David J Anderson. Kanban: Evolutionäres Change Management für IT-Organisationen. dpunkt. verlag, 2011

# Projektorganisation



Reviews

*Was?*

Git

## Versionskontrolle

Version Control: The Freedom to Delete[1]

GitHub

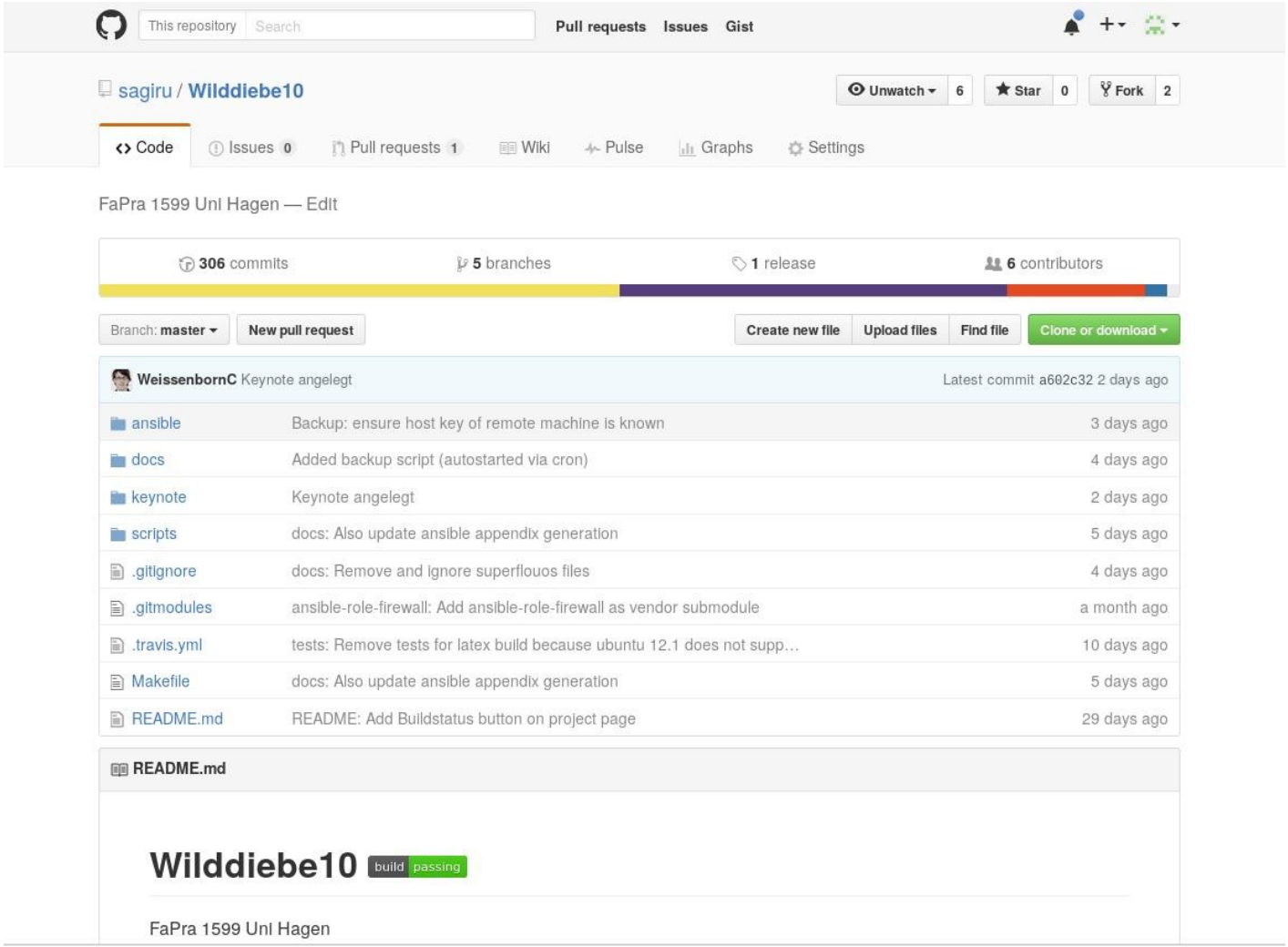
Eigenverantwortlich

Kollaboration

[1] Jez Humble und David Farley. Continuous delivery: reliable software releases through build, test, and deployment automation. Pearson Education, 2010.

# Versionskontrolle





# Projektorganisation



Puppet

Ansible

*Zuverlässig*

Versioniert

## Konfigurationsmanagement

The Power of Automated Deployment[1]

Chef

ssh

Reproduzierbar

Antipattern

[1] Jez Humble und David Farley. Continuous delivery: reliable software releases through build, test, and deployment automation. Pearson Education, 2010.

# Konfigurationsmanagement



```
234 The command "make syntax-checks" exited with 0.
235 $ make ci                                                                    69.38s
236 ansible-playbook -i tests/inventory tests/test.yml --connection=local --sudo
237
238 PLAY [file_server_sued] ********************************************************
239
240 TASK [setup] *******************************************************************
241 ok: [file-server-sued]
242
243 TASK [k1599_common : Ensure common packages are present] ***********************
244 ok: [file-server-sued] => (item=[u'sudo', u'python', u'openssl'])
245
246 TASK [k1599_common : Ensure unwanted packages are absent] **********************
247 changed: [file-server-sued] => (item=[u'rsh-client', u'rsh-server', u'rsh-redone-client', u'rsh-redone-server', u'xserver-xorg', u'mysql-server', u'mysql-server-5.7'])
248
249 TASK [k1599_common : Disable IPV6 by copying sysctl.conf] **********************
250 changed: [file-server-sued]
251
252 TASK [k1599_common : Ensure hostname is set as expected] ***********************
253 changed: [file-server-sued]
254
255 TASK [k1599_common : Ensure expected host entrys in /etc/hosts are present] ****
256 changed: [file-server-sued] => (item=file-server-sued)
257 changed: [file-server-sued] => (item=file-server-nord)
258
259 TASK [k1599_common : Ensure network hosts in /etc/hosts are present] ***********
260
261 TASK [k1599_ssh : Ensure package openssh-server] ********************************
262 ok: [file-server-sued]
263
264 TASK [k1599_ssh : Lege SSH-Konfigdatei auf Server an.] *************************
265 changed: [file-server-sued]
266
267 TASK [k1599_ssh : Lege Login-Banner mit Warnhinweis an.] ***********************
268 changed: [file-server-sued]
269
270 TASK [k1599_users : Ensure expected groups are created] ************************
271 changed: [file-server-sued] => (item=test-group-present)
272 changed: [file-server-sued] => (item=sshlogin)
273 changed: [file-server-sued] => (item=test-sued)
```

# Konfigurationsmanagement



- Verschlüsselung kritischer Daten

**Code 1: Auszug aus ansible/group_vars/file_server/public**

```
firstname: sascha
groups: sudo,file-sued,sshlogin,fapra1599,users
lastname: girrulat
name: sgirrulat
passwords:
  crypt: '{{ _vault_user_crypt_password["sgirrulat"] }}'
  plain: '{{ _vault_user_plain_password["sgirrulat"] }}'
```

**Code 2: Modifizierter Auszug aus ansible/group_vars/file_server/vault**

```
__vault_user_crypt_password:
  sgirrulat:        'xxxxxxx'

__vault_user_plain_password:
  sgirrulat:        'xxxxxxx'
```

# Projektorganisation



*Syntax*

Ansible
Best Practices

## Qualitätssicherung

If It Hurts, Do it More Frequently,
and Bring the Pain Forward[1]

Konventionen

Automatisiert

Testen

[1] Jez Humble und David Farley. Continuous delivery: reliable software releases through build, test, and deployment automation. Pearson Education, 2010.

# Qualitätssicherung



**Tabelle 17:** Beschreibung einiger von uns definierten Ansible Rollen A.2

| Bezeichnung | Beschreibung |
|---|---|
| k1599_anti_virus | ClamAV Virenscanner |
| k1599_common | Konfiguration allgemeiner Linux Server |
| k1599_file_server | Samba |
| k1599_openvpn_client | OpenVPN Client |
| k1599_rsyslog_client | RSyslog Client |
| k1599_rsyslog_server | RSyslog Server |
| k1599_ssh | OpenSSH |
| k1599_time_sync | NTP |
| k1599_users | Benutzerkonten und initiale Passwörter |
| k1599_quota | Quota (Speicherplatzbeschränkungen) |

# Qualitätssicherung



**Code 3: Auszug aus ansible/group_vars/file_server/public**

```
k1599_file_server_smbd_enabled: yes
```

**Code 4: Auszug aus ansible/roles/k1599_file_server/tasks/main.yml**

```
name: Ensure package samba is installed
package:
  name: samba

name: Create public dir
file:
  path: "{{ k1599_file_server_public_share_path }}"
  state: directory
  mode: '0777'

name: "Ensure service samba is started and enabled: {{
    k1599_file_server_smbd_enabled }}"
service:
  name: "{{ _smb_srv }}"
  state: started
  runlevel: '2 3 4 5'
  enabled: "{{ k1599_file_server_smbd_enabled }}"
```

# Qualitätssicherung



*Syntax*

travis-ci

Automatisch

## Testverfahren

ansible-spec

Always Run All Commit Tests Locally
before Commiting, or Get
your CI Server to Do it for You[1]

GitHub

schnelle Rückmeldung

Continuous Integration

[1] Jez Humble und David Farley. Continuous delivery: reliable software releases through build, test, and deployment automation. Pearson Education, 2010.

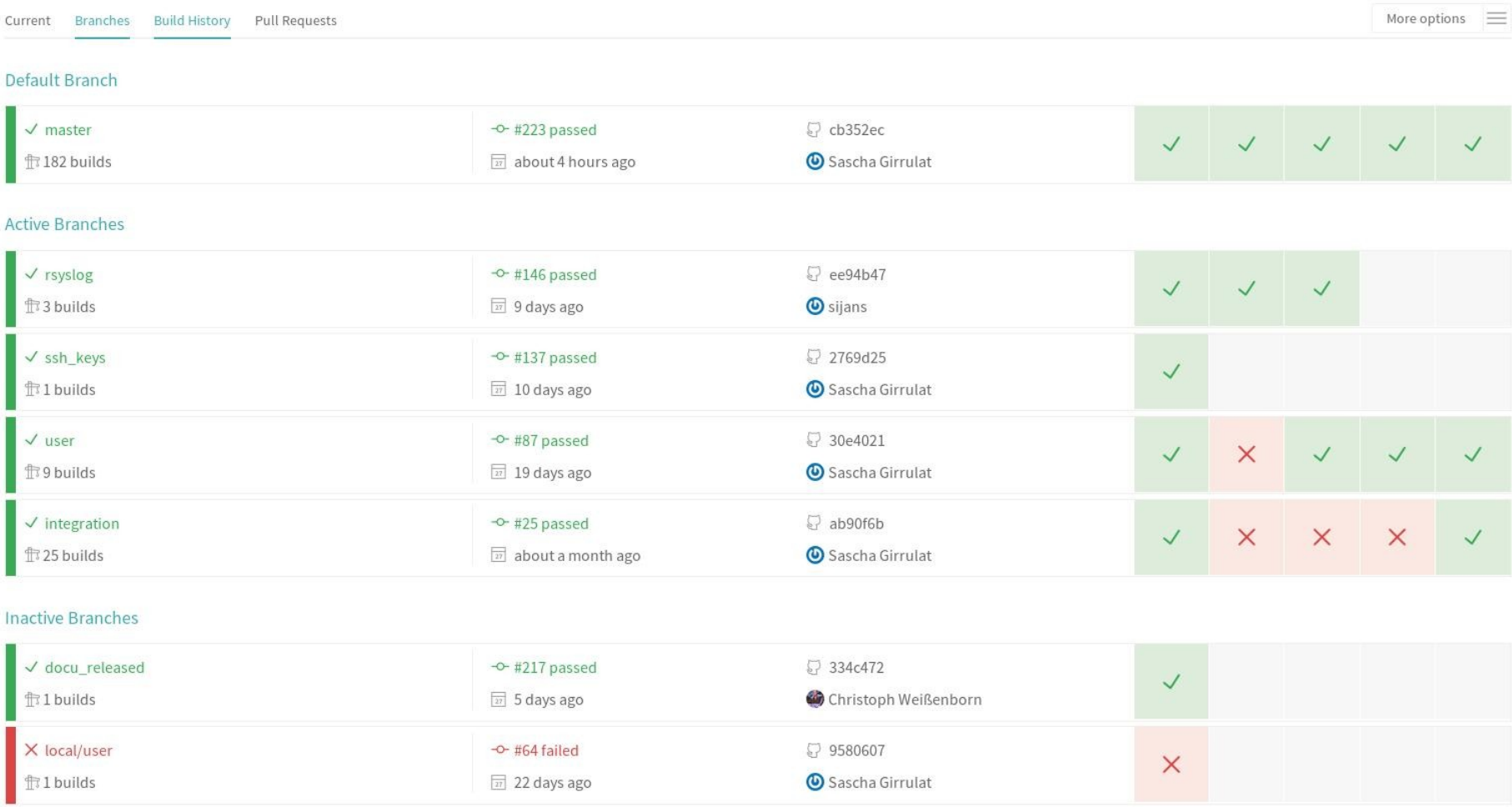
# Testverfahren



```
{
  "sudo": "required",
  "language": "python",
  "python": "2.7",
  "before_install": [
    "sudo apt-get update -qq",
    "sudo apt-get install -y curl make"
  ],
  "install": [
    "pip install ansible"
  ],
  "script": [
    "pushd ansible > /dev/null",
    "make syntax-checks",
    "make ci",
    "make ci | grep -q 'changed=0.*failed=0' && (echo 'Idempotence test: pass' && exit 0) || (echo 'Idempotence test: fail' && exit 1)\n",
    "popd > /dev/null",
    "sudo iptables -L -n | grep -q \"ACCEPT.*dpt:10514\" && (echo 'Port 10514 is open - pass' && exit 0) || (echo 'Port 10514 is not open - fail' && exit 1
    "sudo iptables -L -n | grep -q \"ACCEPT.*dpt:445\" && (echo 'Port 445 is open - pass' && exit 0) || (echo 'Port 445 is not open - fail' && exit 1)\n",
    "sudo iptables -L -n | grep -q \"ACCEPT.*dpt:22\" && (echo 'Port 22 is open - pass' && exit 0) || (echo 'Port 22 is not open - fail' && exit 1)\n",
    "getent passwd | grep -q 'test-user-present' && (echo 'User test-user-present is present - pass' && exit 0) || (echo 'User test-user-present is not pre
    "id test-user-present | grep 'users' | grep 'sudo' | grep -q 'sshlogin' && (echo 'User test-user-present is member of expected groups - pass' && exit 0
    "id test-user-present | grep -q -E \"gid=.*\\(test-sued\\)\" && (echo 'User test-user-present is member of the expected primary group - pass' && exit 0
    "ls -al /home/ | grep test-user-present | grep -E \"^drwx------.+\" && (echo 'Folder /home/test-user-present has mode 0700 - pass' && exit 0) || (echo
    "ls -al /home/ | grep test-sued | grep -E \"^drwxrwx---.+\" && (echo 'Folder /home/test-sued has mode 0770 - pass' && exit 0) || (echo 'Folder /home/te
    "getent group | grep -q 'test-group-present' && (echo 'User test-group-present is present - pass' && exit 0) || (echo 'User test-group-present is not p
    "sudo service ssh status && (echo 'Service ssh is running - pass' && exit 0) || (echo 'Service ssh is not running - fail' && exit 1)\n",
    "sudo service smbd status && (echo 'Service smbd is running - pass' && exit 0) || (echo 'Service smbd is not running - fail' && exit 1)\n",
    "grep -E -q '\\[test-sued\\]' /etc/samba/smb.conf && (echo 'Share /home/test-sued is present - pass' && exit 0) || (echo 'Share /home/test-sued is not
    "sudo service rsyslog status && (echo 'Service rsyslog is running - pass' && exit 0) || (echo 'Service rsyslog is not running - fail' && exit 1)\n",
    "sudo service nmbd status || (echo 'Service nmbd is not running - pass' && exit 1) && (echo 'Service nmbd is running - fail' && exit 0)\n",
    "sudo service openntpd status && (echo 'Service openntpd is running - pass' && exit 0) || (echo 'Service openntpd is not running - fail' && exit 1)\n",
    "sudo quotaon -up / ; if [ $? -eq 1 ]; then (echo 'Quotas are enabled - pass' && exit 0); else (echo 'Quotas are disabled - fail' && exit 1); fi\n",
    "sudo quotatool -d -u test-user-present / | awk '{ if ($4 == 102400 && $5 == 153600) exit 0; exit 1}' && sudo quotatool -d -u test-sued / | awk '{ if (
  ],
  "group": "stable",
  "dist": "precise",
  "os": "linux"
}
```

# Testverfahren





# Funkt. Grobkonzept



- Hardware
- Dateiservice

# Funkt. Grobkonzept



*Virtualisiert*

Ubuntu 16.04 LTS

„Hardware“

netcup

Hetzner

Debian Gnu/Linux 8.5

# Funkt. Grobkonzept



*http(s)*

OwnCloud

Dateiservice

WebDAV

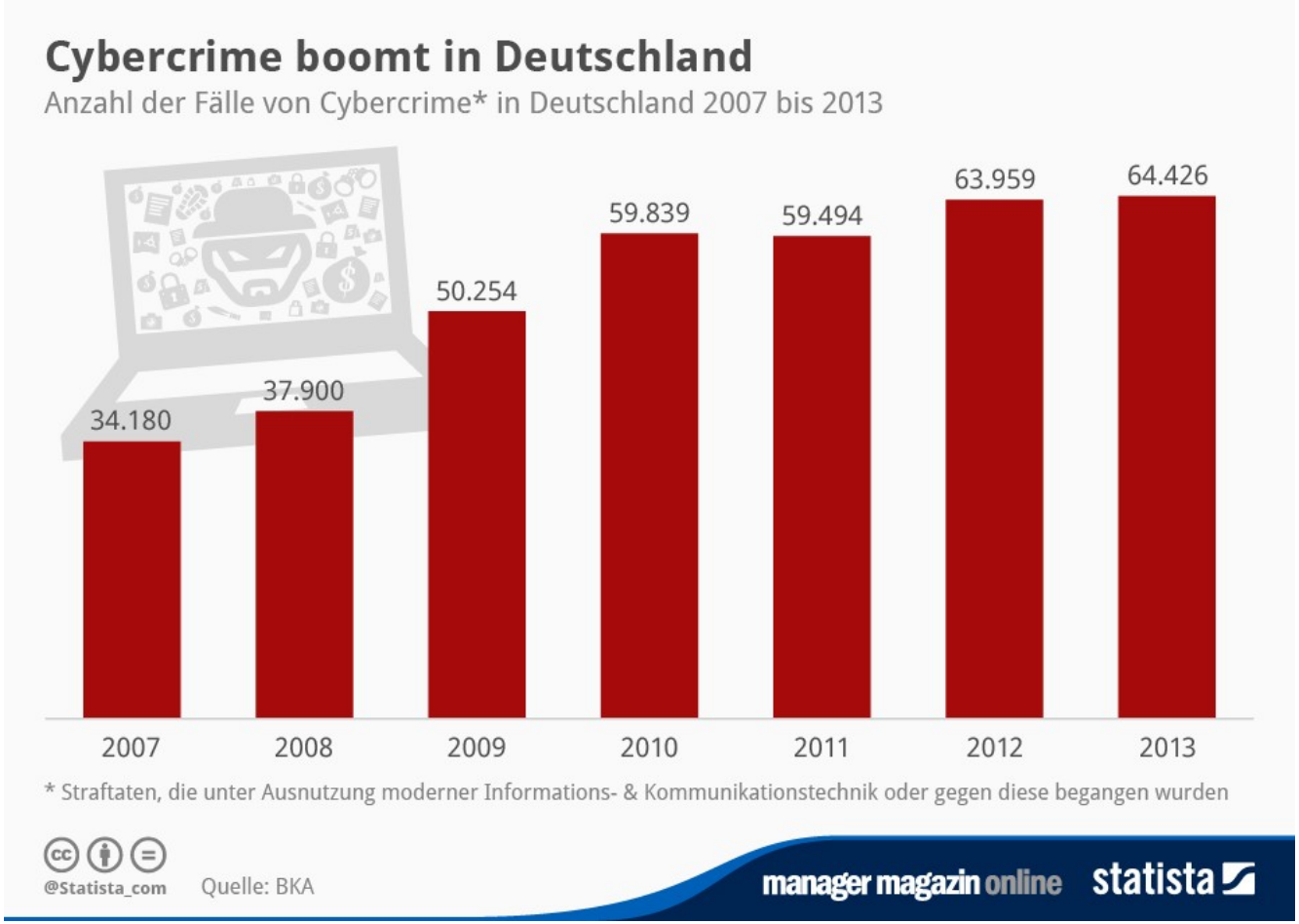
Samba

FTP

*smb3*

# Sicherheitskonzept





# Sicherheitskonzept



- IT-Sicherheitsstandard: BSI IT-Grundschutz
- ISO/IEC 27001
- Verteidigung in der Tiefe

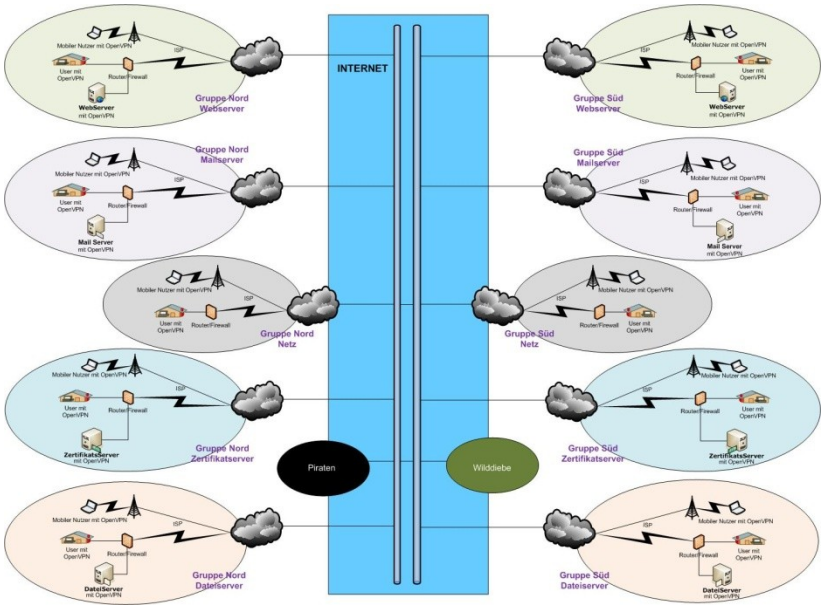
# BSI IT-Grundschutz



# BSI IT-Grundschutz

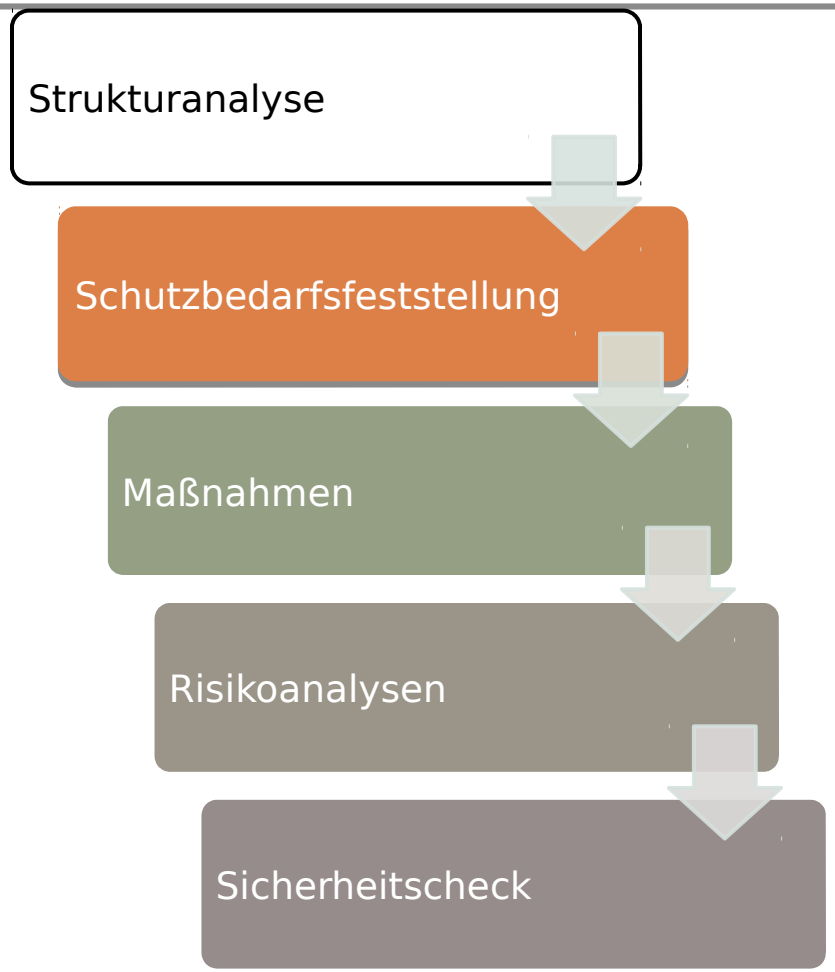


- Strukturanalyse
- Schutzbedarfsfeststellung
- Maßnahmen
- Risikoanalysen
- Sicherheitscheck



# BSI IT-Grundschutz

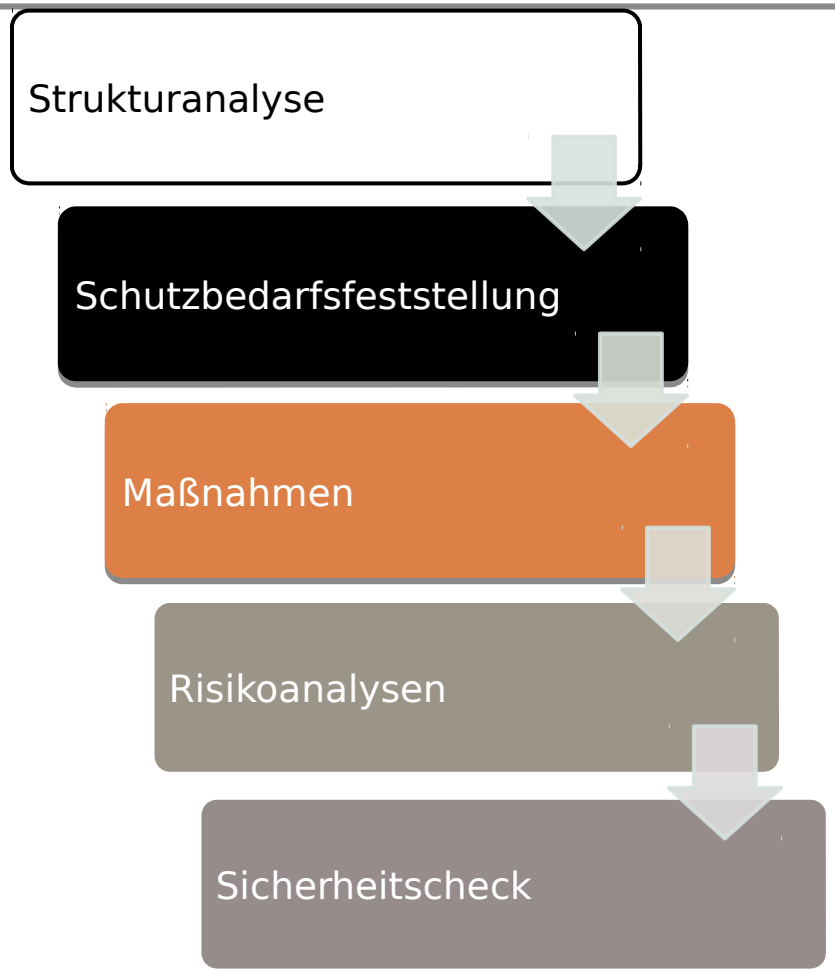





- Betrachtet
- Vertraulichkeit
- Integrität
- Verfügbarkeit

# BSI IT-Grundschutz

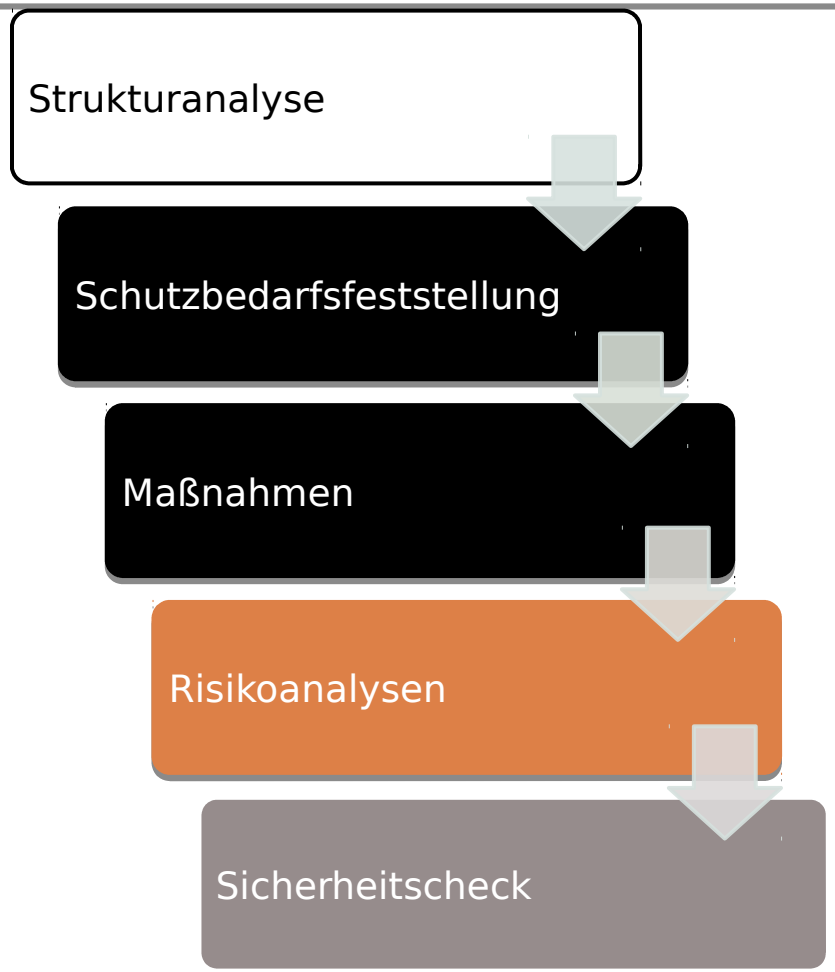





- 155 Maßnahmen
- 135 von uns zu verantworten
- 107 umgesetzt
- 3 Hardening verboten
- 1 geplant

# BSI IT-Grundschutz

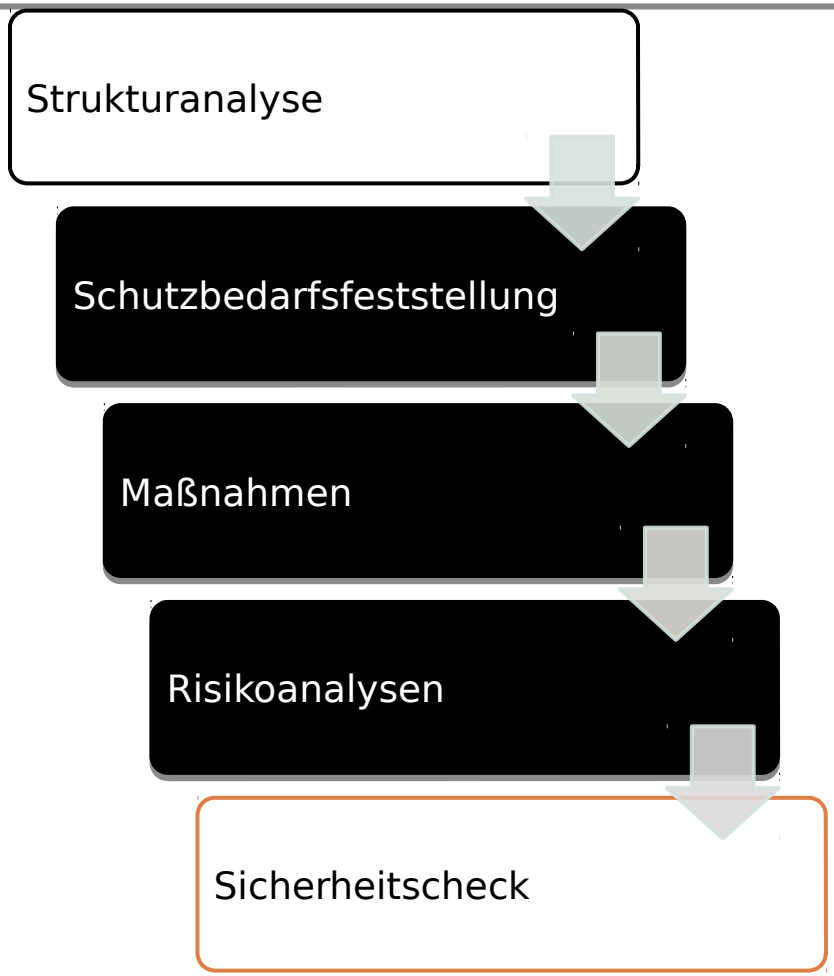





- Keine zentralen Management-Systeme
- Mumble-Server

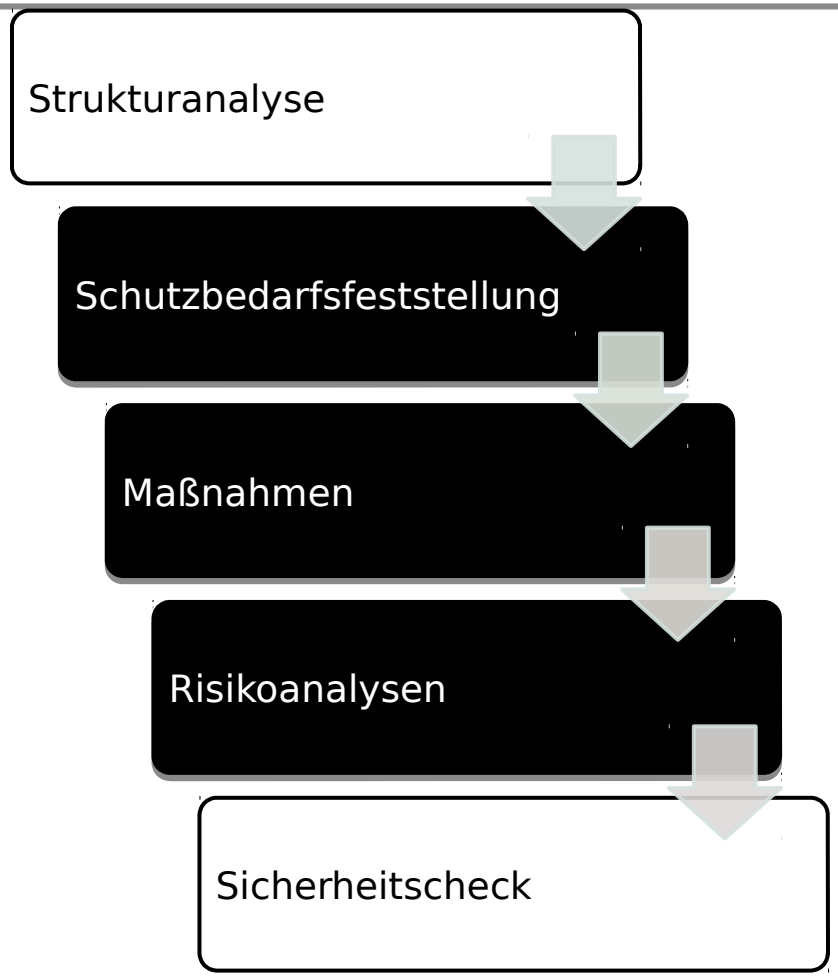
# BSI IT-Grundschutz





# BSI IT-Grundschutz






- Keine Hardware
- Kein Hardening
- Nur Dateiserver, nicht Umgebung

# Sicherheitskonzept - Ergebnisse



Tech. Maßnahmen

Betriebshandbuch


Richtlinie für Anwender

# Tech. Maßnahmen



- SAMBA-Konfiguration absichern
- iptables
- ClamAV+freshclam
- rsyslog
- Quota
- automatisiertes Backup
- NTP

# Betriebshandbuch



- Change Management
- Incident Management
- Problem Management
- Service Management

# tlinie für Anwender



- Technische Anforderungen
- Richtiges Verhalten im Betrieb
- Reaktion bei Vorfällen

# Security Index



$$SI := \frac{siv(m_i)}{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

# Security Index



$$SI := \frac{\sum_{i=1}^{n} siv(m_i)}{}$$

# Security Index



$$SI := \frac{\sum_{i=1}^{n} siv(m_i) \times f(m_i)}{}$$

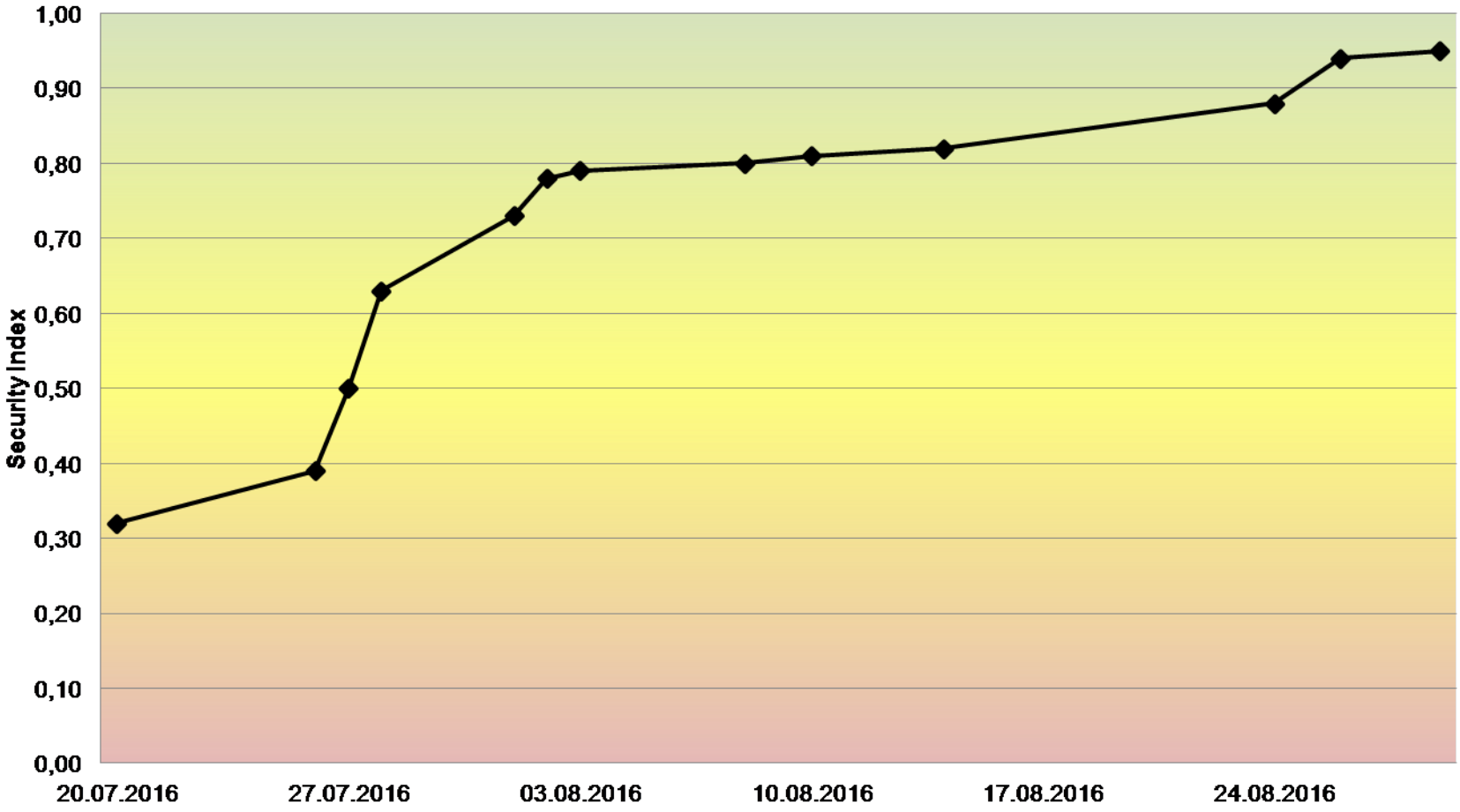
# Security Index



$$SI := \frac{\sum_{i=1}^{n} siv(m_i) \times f(m_i)}{\sum_{i=1}^{n} siv(m_i)}$$

# Security Index





# Datensicherungskonzept



- Sicherung & Wiederherstellung
- Vorgehensweise
- Sicherheitsaspekte

# Datensicherungskonzept



Sicherung & Wiederherstellung

# Datensicherungskonzept



- Zu sicherndes Volumen:

  50 Nutzer x 100 MB Quota => 5GB
- Änderungsvolumen: 20% → 1 GB täglich
- Verschlüsselte Backups
- Tägliches Vollbackup aller Nutzerdaten
- Kein Generationenprinzip

# Datensicherungskonzept



- System selbst wird nicht gesichert
- Stattdessen: Wiederherstellen des Zustands via Ansible
- Etwa 4 Stunden für Restore
- Problem: Risiko durch neue/veränderte Software => Prüfung der Systemsicherheit
- Sicherheit wichtiger als Vertraulichkeit

# Datensicherungskonzept



Vorgehensweise

# Datensicherungskonzept



- Backup-Skript auf beiden Servern:
  - /home/*, /share/public → backup.tar.gz
  - Verschlüsseln des Archivs mit GPG
  - Kopieren des verschlüsselten Archivs auf jeweils anderen Server via SCP
- Cron-Job 03:00 Uhr

# Datensicherungskonzept



Sicherheitsaspekte

# Datensicherungskonzept



- Backup-Skript enthält sensible Informationen

  → root:root 0700

- Ansible: Alle sensiblen Informationen im Vault
- Unverschlüsseltes Archiv wird nach dem Verschlüsseln wieder gelöscht

# Systembeschreibung



- OpenVPN & Namensauflösung
- Samba
- Virenscanner
- Firewall
- Benutzerverwaltung
- Secure Shell
- Logging
- Quota

# VPN & DNS



- Basis: Konfigurations-Templates der Netz-Gruppen
- Server-Zertifikate und Passwörter im Vault

  → werden nach /etc/openvpn/certs kopiert
- Systemd-Dienst

# VPN & DNS



- Abweichende Konfigurationen Nord ↔ Süd
  - Süd: +mtu, float, auth, verify-x509-name
  - Nord: +resolv-retry, remote-cert-tls

  → Merge der Konfigurationen/Verwendung von Ansible-Variablen

# VPN & DNS



- DNS:
  - Nord: DNS-Server bei Verbindungsaufbau übertragen
  - Anpassung der VPN-Konfiguration:

    script-security 2

    up /etc/openvpn/update-resolv-conf

    down /etc/openvpn/update-resolv-conf
  - Zusätzlich Einträge in /etc/hosts

# Samba



- Freie Implementierung des Server Message Block (SMB) Protokolls, auch als Common Internet File System (CIFS) bekannt
- Insbesondere gemeinsamer Zugriff auf Dateien in einem Netzwerk

# Samba



- Konfiguration via Ansible-Rolle `k1599_file_server`
- Pro Benutzer eine private Freigabe mit Passwort unter `$benutzername`
- Öffentliche Freigabe `public` für Zugriff ohne Authentifizierung
- Unterschiedliche Konfiguration für Nord und Süd Systeme via `smb.conf`

# Samba



- Zugriff ausschließlich aus den bekannten Netzbereichen von Nord und Süd
- Keine NTLM Authentifizierung
- Transportverschlüsselung optional
- Nur TCP auf Port 445 (kein NetBIOS) zugelassen

# Virenscanner



- Erkennung von mit Schadsoftware infizierten Dateien im Dateisystem
- Dazu werden Dateien auf charakteristische Daten (Signaturen) untersucht
- Wegen anhaltend hohen Aufkommens an neuer Schadsoftware ist die ständige Aktualisierung der Signaturbibliothek notwendig

# Virenscanner



- Einsatz der freien Software ClamAV
- Stündliche Aktualisierung der Signaturbibliothek durch das Zusatzpaket `freshclam`
- Befallene Dateien werden im Syslog vermerkt:

```
fileserver clamd[569]: ScanOnAccess:
/share/public/eicar.com: Eicar-Test-
Signature(44d88612fea8a8f36de82e1278abb02f:68)
FOUND
```

# Virenscanner



- Beschränkung auf Erkennung, da Zugriffsblockade technisch aufwendig (erfordert angepassten kernel) und erhöhte Systemlast bedingt
- Prüfung bei Zugriff auf Datei
- Trefferrate korreliert mit Preis bzw. Lizenzkosten des Virenscanners, da die zeitnahe Pflege der Signaturen und Software sehr aufwendig ist

# Firewall



- Es wurde über GitHub eine vorkonfigurierte Ansible-Role für die Firewall übernommen:

  https://github.com/geerlingguy/ansible-role-firewall

- Von uns erlaubte tcp_ports:

| | | | |
|---|---|---|---|
| 22 | SSH | all | Systemverwaltung |
| 445 | SMB | tun0 | Fileservice im VPN |
| 10514 | Rsyslog | tun0 | Fileservice im VPN |

# Benutzerverwaltung



- Kein Active-Directory im Netz verfügbar
- SMB – User sind deswegen Systemuser des Servers.

Beispiel Ansible-Config:

```
- firstname: tobias
  group: netz-nord
  groups: netz-nord,sshlogin,fapra1599,users
  lastname: winkelhorst
  name: twinkelhorst
  passwords:
    crypt: '{{ _vault_user_crypt_password["twinkelhorst"] }}'
    plain: '{{ _vault_user_plain_password["twinkelhorst"] }}'
```

# SSH



- Erreichbar über alle Interfaces (auch außerhalb des VPN)
- Kein root – Login
- Spezielle Gruppe sshlogin zur Abgrenzung zu anderen Systemusern

# Logging



tcp

*(sudo|do su)*

logrotate

SSL

## Rsyslog

k1599_rsyslog_client

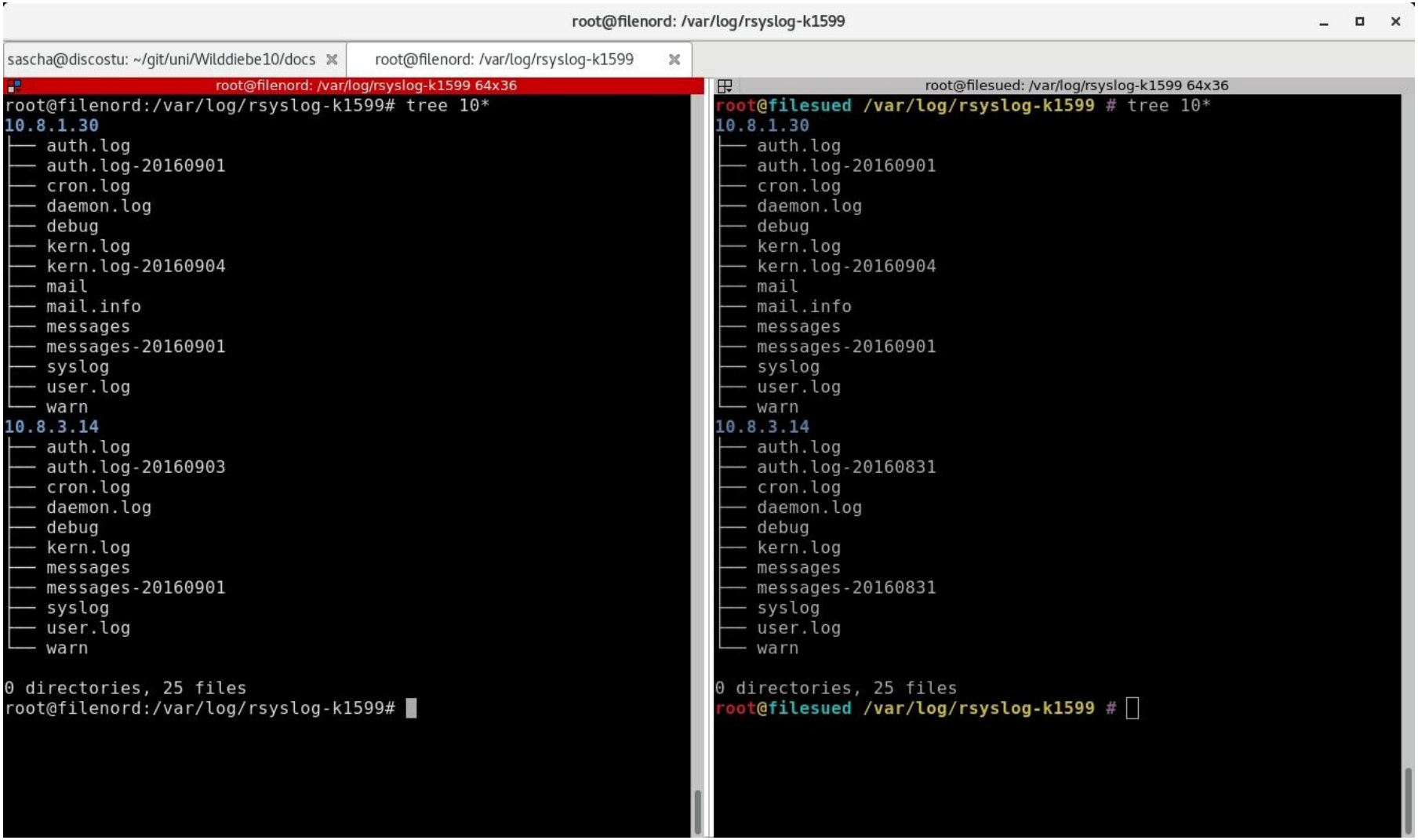
Nord

k1599_rsyslog_server

Süd

# Rsyslog - Server





# Rsyslog - Server



Code 26: Auszug aus _rsyslog_server/templates/etc/rsyslog.d/30_imtcp_remote_input.conf.j2

```
# Set certificates
global(
  defaultNetstreamDriver="gtls"
  defaultNetstreamDriverCAFile="/etc/rsyslog.d/certs/ca-chain.cert.
     pem"
  defaultNetstreamDriverCertFile="/etc/rsyslog.d/certs/cert.pem"
  defaultNetstreamDriverKeyFile="/etc/rsyslog.d/certs/privkey.pem"
)
```

Code 27: Whitelisting der CN

```
# Enable imtcp listener on port {{ k1599_rsyslog_port }}
module(
  load="imtcp"
  MaxSessions="{{ k1599_rsyslog_maxsessions|default(500) }}"
  StreamDriver.Mode="1" #Nur TLS zulassen
  StreamDriver.AuthMode="x509/name" # Pruefung des CN
  PermittedPeer=["FileNord","fileserver.mueller-backwaren.de"]
)

input(
  type="imtcp"
  port="{{ k1599_rsyslog_port }}"
  ruleset="imtcp_remote_input"
)
...
```

# Quota



- Ansible Rolle `k1599_quota`
- Option `usrquota` in `/etc/fstab`
- Quota Index initialisieren

  `quotacheck -vguma`
- Hard Limit 100 MB, Soft Limit 150 MB:

  `quotatool -b -q 102400 -l 153600 -u file-sued /`
- Quota aktivieren

  `quotaon -av`

# Kritische Selbstbetrachtung



- Keine Domäne durch Verzögerungen und unterschiedliche Realisierungsansichten
- Besser: Zentrale Komponenten früh gemeinsam besprechen, Abhängigkeiten klären

# Ausblick – Dateiserver



- Folgene Maßnahmen müssten für produktive Umgebungen umgesetzt werden

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| Einbindung Domäne | IT-Sichbeauftragter |
| Auth. Gegen AD | Vereinheitlichung der Betriebskonzepte |
| Monitoring | Zertifizierung |

# Fazit



- Einführung in aktuelle Thematik
- Selbstständigkeit
- Bereitstellung von Ressourcen (Server)
- Betreuung
- Aufgabenstellung:
  ENTWEDER Aufgabenstellung offen und Vorgehensweise fest; ODER A. Fest definiert und Vorgehensweise offen
- Ohne Lastenheft, Erfolgskriterien oder wenigstens einer „Vision“ ist erfolgreiche Zusammenarbeit nicht möglich!

# Feedback



- Von uns

- für uns