

Dateiserver: Gruppe 5 + 10

Agenda

2

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

Projektorganisation

3

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

Projektorganisation

4

Wir!

Gruppe 10

Wer?

Gruppendefinition!

Nord

Gruppe 5

Süd

Projektorganisation

5

Entscheidungsfindung?

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

¹ Aus Michael Moore „Capitalism“

Projektorganisation

6

Skype

Screen

Doodle

Mumble

Kommunikation

Newsgroup

Jabber

TeamViewer

E-Mail

Projektorganisation

7

Wiki

GitHub

LibreOffice

Dokumentation

DokuWiki

Markdown

LaTeX

Dokumentation

8

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

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 Evaluert 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

9

```
sascha@discostu: ~/git/uni/Wilddiebe10/docs
sascha@discostu:~/git/uni/Wilddiebe10/docs$ make clean_all
test 0 -ne 1 && rm -f count \
    *.blg \
    *.fdb latexmk \
    *.dvi \
    *.fls \
    *.bbl \
    *.log \
    *.fdb \
    *.glo \
    *.tex~ \
    *.ist \
    *.toc \
    *.run.xml \
    *.bcf \
    *.out \
    includes/*.aux \
    *.aux || echo "Skip cleanup, pls do make clean manually."
rm rm -f count *.pdf
sascha@discostu:~/git/uni/Wilddiebe10/docs$

sascha@discostu:~/git/uni/Wilddiebe10/docs 104x32
sascha@discostu:~/git/uni/Wilddiebe10/docs$ ls
AnwenderItRichtlinie.tex  EXAMPLES  includes  Projektdokumentation.tex  texmf
Betriebshandbuch.tex     images    Makefile  Quellen.bib
sascha@discostu:~/git/uni/Wilddiebe10/docs$ conttest make pdf
texhash /home/sascha/git/uni/Wilddiebe10/docs/texmf
texhash: Updating /home/sascha/git/uni/Wilddiebe10/docs/texmf/ls-R...
texhash: Done.
sudo mktexlsr
[sudo] Passwort für sascha:
mktexlsr: Updating /usr/local/share/texmf/ls-R...
mktexlsr: Updating /var/lib/texmf/ls-R-TEXLIVEDIST...
mktexlsr: Updating /var/lib/texmf/ls-R-TEXMFMAIN...
mktexlsr: Updating /var/lib/texmf/ls-R...
mktexlsr: Done.
latexmk -f -bibtex -pdf -bibtex-cond Projektdokumentation.tex
Latexmk: This is Latexmk, John Collins, 1 January 2015, version: 4.41.
Latexmk: applying rule 'pdflatex'...
Rule 'pdflatex': Rules & subrules not known to be previously run:
    pdflatex
Rule 'pdflatex': The following rules & subrules became out-of-date:
    'pdflatex'
-----
Run number 1 of rule 'pdflatex'
-----
Running 'pdflatex -recorder "Projektdokumentation.tex"'
-----
This is pdfTeX, Version 3.14159265-2.6-1.40.17 (TeX Live 2016/Debian) (preloaded format=pdflatex)
 restricted \write18 enabled.
entering extended mode
(./Projektdokumentation.tex
LaTeX2e <2016/03/31> patch level 3

sascha@discostu:~/git/uni/Wilddiebe10/docs 104x21
sascha@discostu:~/git/uni/Wilddiebe10/docs$ ls -al
insgesamt 1884
drwxr-xr-x 5 sascha sascha 4096 Sep  7 16:02 .
drwxr-xr-x 8 sascha sascha 4096 Sep  7 15:58 ..
-rw-r--r-- 1 sascha sascha 94378 Sep  7 16:02 AnwenderItRichtlinie.pdf
-rw-r--r-- 1 sascha sascha 8005 Sep  3 19:47 AnwenderItRichtlinie.tex
-rw-r--r-- 1 sascha sascha 1032877 Sep  7 16:02 Betriebshandbuch.pdf
-rw-r--r-- 1 sascha sascha 36950 Sep  3 19:49 Betriebshandbuch.tex
-rw-r--r-- 1 sascha sascha 940 Aug 28 16:20 EXAMPLES
drwxr-xr-x 2 sascha sascha 4096 Sep  7 15:31 images
drwxr-xr-x 3 sascha sascha 4096 Sep  7 16:02 includes
-rw-r--r-- 1 sascha sascha 1390 Sep  3 19:47 Makefile
-rw-r--r-- 1 sascha sascha 12288 Sep  7 15:58 .Makefile.swp
-rw-r--r-- 1 sascha sascha 583037 Sep  7 16:02 Projektdokumentation.pdf
-rw-r--r-- 1 sascha sascha 109365 Sep  7 11:53 Projektdokumentation.tex
-rw-r--r-- 1 sascha sascha 6726 Sep  1 15:53 Quellen.bib
drwxr-xr-x 3 sascha sascha 4096 Sep  7 16:01 texmf
sascha@discostu:~/git/uni/Wilddiebe10/docs$

Makefile (~/git/uni/Wilddiebe10/docs) - VIM 104x32
setup:
ifeq ($(UNAME_S),Linux)
    sudo apt-get install texlive-latex-recommended \
        texlive-extra-utils \
        texlive-latex-extra \
        texlive-lang-german \
        pandoc \
        texlive-latex-base \
        texlive-bibtex-extra \
        texlive-generic-extra \
        biber
endif
ifeq ($(UNAME_S),FreeBSD)
    @echo ---
    @echo Notice: Update missing software as root via
    @echo pkg install latex-mk
    @echo pkg install latex-biber
    @echo pkg install tex-dvipack
    @echo ---
endif

setup tex:
    texhash $(TEXMFHOME)
    sudo mktexlsr

${PDF}: ${SOURCE} Makefile
    latexmk -f -bibtex -pdf -bibtex-cond ${SOURCE}
    pdflatex AnwenderItRichtlinie.tex
    pdflatex Betriebshandbuch.tex

.PHONY: docs clean
```

Projektorganisation

10

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

11

KANBAN

Kontinuierliche Optimierung von IT-Prozessen

InterFace AG
the face of informatics

1. VISUALISIEREN

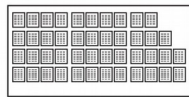
Das Kanban Board stellt das Herzstück des Kanban Systems dar. Es dient der Visualisierung des kompletten Ablaufs. Es besteht aus einer Art Tabelle, jeder Produktionsschritt beziehungsweise jedes Team erhält zwei Spalten, In und Out. In der In Spalte befinden sich die momentan bearbeiteten Tickets, in der Out Spalte die erledigten Tickets, die vom nächsten Schritt übernommen werden können.

SERVICEKLASSEN

Im Kanban System gibt es im Normalfall keine Worklog zwischen den Tickets. Wenn beispielsweise aus betrieblichen Gründen Tickets verschiedene Prioritäten bekommen, können verschiedene Serviceklassen eingeführt werden. Die Aufgaben sind:

- **Dringlichkeit (Expedite)**
Die Tickets mit der höchsten Priorität. Es kann sogar dazu kommen, dass Teams die Arbeit am aktuellen Ticket unterbrechen um dieses Ticket zu erledigen. Dieses Ticket hat seine eigene „Deadline“.
- **First In First Out (FIFO)**
Wenn zum Beispiel eine Funktionalität zu einem bestimmten System benötigt wird, kann man diese Tickets in die First In First Out Spalte schreiben, dass die kurz vor dem Team fertig sind.
- **Vorteil (Benefit)**
Funktionen, deren Geschäftswerte klar sind, können nachrangig behandelt werden. Zum Beispiel bei Bugfixes in kritischen Situationen. Diese Tickets sind trotzdem Teil des Systems und werden erledigt.
- **Standard**
Die anderen Tickets werden nach dem First In First Out (FIFO) Prinzip behandelt.

DER PROZESS

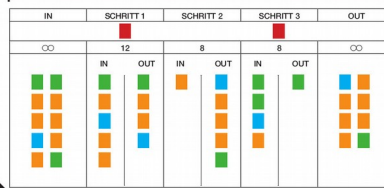


AUFGABEN / IDEEN / KONZEPT

KAIZEN

Kontinuierliche Optimierung

MESSUNG



Kanban Board

3. OPTIMIEREN

Das Kaizen, die Kultur der stetigen Verbesserung, ist eines der Hauptstandards des Kanban Systems. Es gibt keine festgeschriebenen Arten der Optimierung, diese findet in der Regel aber auf verschiedenen Ebenen statt. Mögliche Arten der Optimierung sind:

Tägliche Statusmeetings (Standup Meeting)

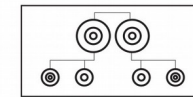
Durch tägliche Meetings morgens stattfindende Team-Treffen vor dem Kanban Board kann der Projektfortschritt analysiert und mögliche Probleme können verdundlicht und diskutiert werden. Diese Treffen sind meist kurz, längere Diskussionen werden ausgelagert.

Operations Reviews

Umfangreichere Treffen, in denen die gesamte Organisation teilnehmen sollte. Diese Treffen bilden den Hauptteil der ständigen Optimierung. Die Daten der Messungen werden analysiert und Probleme lokalisiert. Durch Änderung der Teamgrößen oder Einführung von neuen Serviceklassen werden Änderungen am Arbeitsablauf vorgenommen. Es wird eine Root Cause Analysis vorgenommen.

Root Cause Analysis

Mit Hilfe des Kanban Boards werden die Probleme im System deutlich, zum Beispiel wo es Bottlenecks gibt oder welche Stationen nicht ausgelastet sind. Im Kanban System sollen Probleme nicht verschoben, sondern behoben werden. Daher werden die Fehler schnell beseitigt. Das kann durch Zusammenstoß des gesamten Teams geschehen.



SOFTWARE

KANBAN

Kanban kommt aus dem japanischen und bedeutet Signalfarbe (Kan: Signal; Ban: Karte). Ursprünglich ist es eine Technik aus dem Textile Produktionsprozess, die Lagerbestände reduzieren und einen gleichmäßigen Fluss in der Fertigung bewerkstelligen soll. Bei der Kanban-Steuerung werden die Bewegungen von Kanban in Bezug auf Produktionsgeschwindigkeit und -kapazität analysiert. Die Kanban steuern, dass ein Produkt nicht überproduziert wird, sondern nur dann, wenn es benötigt wird und somit in der Produktion von Material, Produktion und Lagerung angepasst werden. Dadurch können Unternehmen die Möglichkeit komplexer Produktionsprozesse in selbstorganisierte Teams zu überführen, was zu einer deutlichen Abnahme des Steuerungsaufwandes führt.

BEST PRACTICES

Präzisierung Cost of Delay
In Kanban Systemen ist das Cost of Delay ein zentraler Bestandteil. Es ist die Kosten, die durch das Verschieben eines Tickets entstehen. Diese Kosten können in verschiedenen Formen auftreten, wie zum Beispiel in Form von Geld, Zeit oder anderen Ressourcen. Die Kosten können in verschiedenen Formen auftreten, wie zum Beispiel in Form von Geld, Zeit oder anderen Ressourcen.

Hohe Qualität anstreben
Wenn man die Qualität anstrebt, muss man auch die Qualität der Arbeit anstreben. Die Qualität der Arbeit ist ein wichtiger Bestandteil des Kanban Systems.

Regelmäßige Meetings
Durch die regelmäßigen Meetings und die Zusammenarbeit der Teams wird die Qualität der Arbeit verbessert.

Im Kanban System können verschiedene Bereiche gemessen werden, die Aussagen über die Qualität des Prozessablaufs liefern.

Cumulative Flow Diagram (CFD)
Ein CFD ist eine Zusammenfassung der Änderungen auf dem Kanban Board. Es zeigt an, wann wie viele Tickets erledigt werden und wie lange ein Ticket braucht, um eine Station zu durchlaufen. Mithilfe dieses Diagramms lässt sich erkennen, wo sich Bottlenecks bilden.

Bottlenecks
Bottlenecks sind Stellen im Kanban System, an denen sich viele Tickets stauen. Bottlenecks entstehen, wenn die Bearbeitungszeit von Tickets zwischen den Stationen zu stark variiert.

Zahl der Work in Progress Tickets
Durch die Messung der aktuell im System befindlichen Tickets lässt sich ablesen, wie viele ein System abarbeitet. Eine schnell ansteigende Anzahl der Tickets zeigt ein Problem im System, zum Beispiel ein blockiertes Ticket.

Fehlerrate
Kanban ist auf kurze Durchlaufzeiten ausgerichtet. Diese sind nur durch hohe Qualität zu erreichen. Daher ist eine Vollabdeckung für ein gut funktionierendes Kanban System eine geringe Fehlerrate. Durch eine solche Messung lässt sich die Entwicklung der Qualität der Arbeit überprüfen.

Durchsatz
Ein einfaches Diagramm, das anzeigt, wie viele Tickets pro Woche bearbeitet werden.

KAIZEN

Das Wort Kaizen kommt aus dem japanischen und bedeutet Verbesserung (Ka: Verbesserung; Zen: gut). Es ist eine Philosophie, die darauf abzielt, die Qualität der Arbeit zu verbessern. Die Kaizen-Philosophie ist eine kontinuierliche Verbesserung, die auf der Idee basiert, dass man die Qualität der Arbeit verbessern kann, indem man kleine Verbesserungen macht.

REGELN

Visualisierung
Das Kanban Board ist ein zentraler Bestandteil des Kanban Systems. Es dient der Visualisierung des Prozessablaufs und der Arbeit.

Begrenzung der WIP
Die WIP (Work in Progress) ist die Anzahl der Tickets, die in einem Schritt des Kanban Systems sind. Die WIP ist ein wichtiger Bestandteil des Kanban Systems.

Messung und Optimierung
Durch die Messung der Arbeit und die Optimierung des Kanban Systems wird die Qualität der Arbeit verbessert.

Explizite Regelung
Die Regeln des Kanban Systems sind explizit und werden von allen Teammitgliedern bekannt gemacht.

Vermeidung von Modulen
Die Module des Kanban Systems sind so gestaltet, dass sie die Arbeit erleichtern und die Qualität verbessern.

Vorgehensmodell

12

The screenshot displays a Trello board for 'Dateiserver Gruppen 5+10'. The board is organized into seven columns representing different stages of a project workflow:

- Backlog:** Contains tasks like 'Doku Rsyslog', 'Doku Ansible', 'Doku Einbindung VPN-Clients', 'Backup (tar.gz auf anderen Server kopieren)', 'Call Home deaktivieren oder unterbinden', 'Gesicherter Login', 'write XOR exec', 'Unnötige Netzdienste abschalten', and 'Abschluss Review Dokumentation'.
- In Progress - Research:** Includes 'Quotas installieren, einrichten für Nutzer', 'SSL - Rsyslog', 'SAMBAs Dateiverschlüsselung auf dem Server?', 'Klaerung DNS', and 'Klaerung Verzeichnisdienst'.
- In Progress - Working on:** Features 'Test-/Abnahmeprotokoll erstellen', 'NTP?', 'Doku: Projektorganisation', 'Doku: Quellenverzeichnis', 'Vorschlag DoD', 'Vorschlag Daily', 'BSI Maßnahmen in konkrete Schritte kovertieren', 'Wiki Umzug', 'Setup Kanban', and 'Setup + Doku Github'.
- In Progress - Blocked:** Lists 'AD / LDAP Anbindung' and 'DNS (intern) Anbindung (Nord)'.
- Review:** Includes 'Doku umschreiben von Nord/Süd zu einer', 'Installation Rsyslog', 'Setup Firewall', 'Login-Banner einrichten', 'Hostnamen setzen', 'SSH Login und SSH user nach Ansible schreiben', 'Setup Virenschutz', 'SSH root Login nur mit Key', 'Setup VPN', and 'Sichere SAMBA config'.
- Done:** Shows completed tasks such as 'Installation Server - Süd', 'Setup Wiki', 'Installation Samba', 'Auswahl Virenschutz', 'Christoph und Jörg anrufen... 0176 / 7008 6348 ... Hilfe bei Ansible bitte', 'SWAT deaktivieren', 'Setup Ansible', 'Setup Ansible Repository', 'Auswahl Diagrammeditor', and 'Maßnahmen zum Passwortschutz'.
- Ideas:** Contains potential future tasks like 'SELinux?', 'watchdog', 'Absicherung des Servers', 'Monitoring? (ggf. SMS-Server)', 'fail2ban', and 'ssh key rolle hinzufügen'.

Each card in the columns includes a title, a description, a due date, and a list of assignees. The board interface includes a top navigation bar with the Trello logo, a search bar, and a user profile for 'Sascha Gurrulat'. The bottom of the board shows a 'Kalender' (Calendar) and 'Menü anzeigen' (Show menu) option.

Vorgehensmodell

13

Testen

Scrum

DoD – Definiton of Done

Mache die Regeln für den Prozess explizit¹

Dokumentation

4 Augen Prinzip

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

Projektorganisation

14

Was?

Reviews

Versionskontrolle

Git

Version Control: The Freedom to Delete¹

GitHub

Eigenverantwortlich

Kollaboration

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

Versionskontrolle

15

The screenshot shows the GitHub interface for the repository 'sagiru / Wilddiebe10'. At the top, there's a navigation bar with 'Pull requests', 'Issues', and 'Gist'. Below this, the repository name is displayed with options to 'Unwatch', 'Star' (0), and 'Fork' (2). A secondary navigation bar includes 'Code', 'Issues' (0), 'Pull requests' (1), 'Wiki', 'Pulse', 'Graphs', and 'Settings'. The main content area shows the repository name 'FaPra 1599 Uni Hagen' with an 'Edit' link. Below this, a summary bar indicates '306 commits', '5 branches', '1 release', and '6 contributors'. A row of buttons allows users to 'Create new file', 'Upload files', 'Find file', or 'Clone or download'. The file list shows various directories and files with their commit messages and timestamps. The 'README.md' file is highlighted, showing the repository name 'Wilddiebe10' with a 'build passing' status and the text 'FaPra 1599 Uni Hagen'.

This repository Search

Pull requests Issues Gist

sagiru / Wilddiebe10

Unwatch 6 Star 0 Fork 2

Code Issues 0 Pull requests 1 Wiki Pulse Graphs Settings

FaPra 1599 Uni Hagen — Edit

306 commits 5 branches 1 release 6 contributors

Branch: master New pull request

Create new file Upload files Find file Clone or download

WeissenbornC Keynote angelegt Latest commit a602c32 2 days ago

ansible	Backup: ensure host key of remote machine is known	3 days ago
docs	Added backup script (autostarted via cron)	4 days ago
keynote	Keynote angelegt	2 days ago
scripts	docs: Also update ansible appendix generation	5 days ago
.gitignore	docs: Remove and ignore superfluous files	4 days ago
.gitmodules	ansible-role-firewall: Add ansible-role-firewall as vendor submodule	a month ago
.travis.yml	tests: Remove tests for latex build because ubuntu 12.1 does not supp...	10 days ago
Makefile	docs: Also update ansible appendix generation	5 days ago
README.md	README: Add Buildstatus button on project page	29 days ago

README.md

Wilddiebe10 build passing

FaPra 1599 Uni Hagen

Projektorganisation

16

Zuverlässig

Ansible

Puppet

Versioniert

Konfigurationsmanagement

The Power of Automated Deployment¹

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

17

```
234 The command "make syntax-checks" exited with 0.
235 $ make ci
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)
274
```

69.38s

Konfigurationsmanagement

18

- 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

19

Syntax

Ansible
Best Practices

Qualitätssicherung

If It Hurts, Do it More Frequently,
and Bring the Pain Forward¹

Konventionen

Automatisiert

Testen

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

Qualitätssicherung

20

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

Bezeichnung	Beschreibung
k1599_anti_virus	ClamAV Virenschanner
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

21

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

22

Syntax

travis-ci

Automatisch

Testverfahren

ansible-spec

Always Run All Commit Tests Locally
before Committing, or Get
your CI Server to Do it for You¹

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

23

```
{
  "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)\n",
    "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

24

Current Branches Build History Pull Requests

More options

Default Branch

✓ master 182 builds	→ #223 passed about 4 hours ago	cb352ec Sascha Girrulat	✓	✓	✓	✓	✓
------------------------	------------------------------------	----------------------------	---	---	---	---	---

Active Branches

✓ rsyslog 3 builds	→ #146 passed 9 days ago	ee94b47 sijans	✓	✓	✓		
✓ ssh_keys 1 builds	→ #137 passed 10 days ago	2769d25 Sascha Girrulat	✓				
✓ user 9 builds	→ #87 passed 19 days ago	30e4021 Sascha Girrulat	✓	✗	✓	✓	✓
✓ integration 25 builds	→ #25 passed about a month ago	ab90f6b Sascha Girrulat	✓	✗	✗	✗	✓

Inactive Branches

✓ docu_released 1 builds	→ #217 passed 5 days ago	334c472 Christoph Weißenborn	✓				
✗ local/user 1 builds	→ #64 failed 22 days ago	9580607 Sascha Girrulat	✗				

Funkt. Grobkonzept

25

- Hardware
- Dateiservice

Funkt. Grobkonzept

26

Virtualisiert

Ubuntu 16.04 LTS

„Hardware“

netcup

Hetzner

Debian Gnu/Linux 8.5

Funkt. Grobkonzept

27

http(s)

OwnCloud

Dateiservice

WebDAV

Samba

FTP

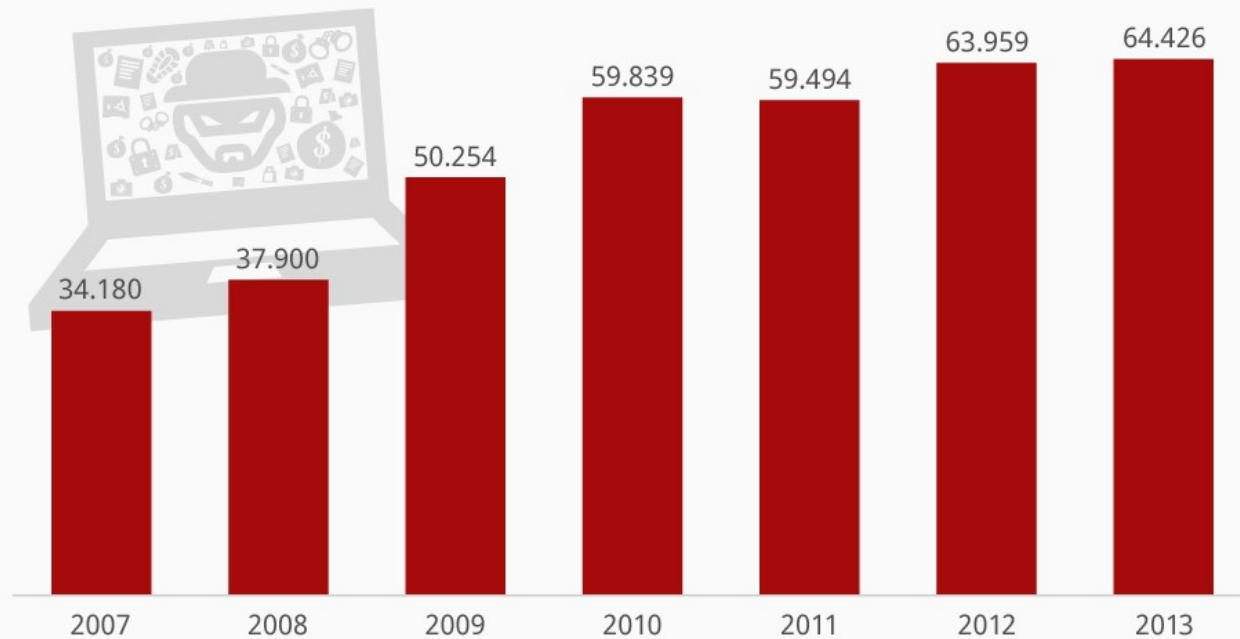
smb3

Sicherheitskonzept

28

Cybercrime boomt in Deutschland

Anzahl der Fälle von Cybercrime* in Deutschland 2007 bis 2013



* Straftaten, die unter Ausnutzung moderner Informations- & Kommunikationstechnik oder gegen diese begangen wurden

Sicherheitskonzept

29

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

BSI IT-Grundschutz

30



BSI IT-Grundschutz

31

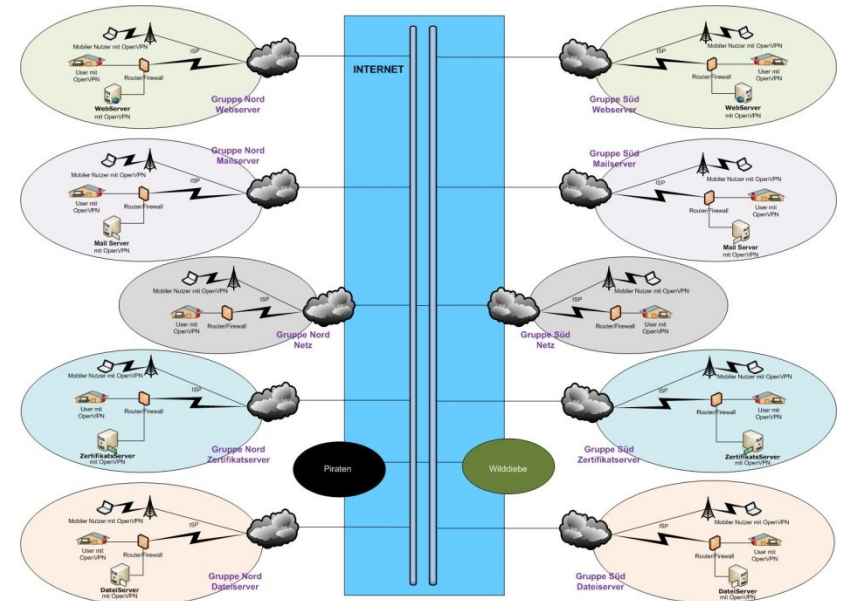
Strukturanalyse

Schutzbedarfsfeststellung

Maßnahmen

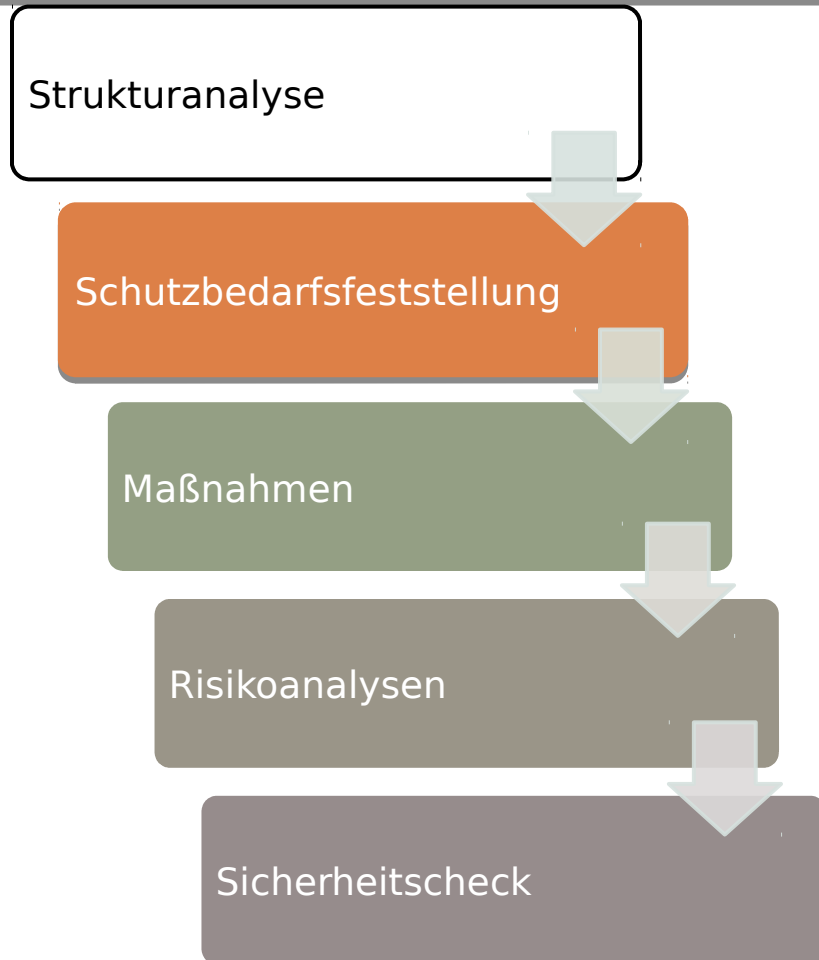
Risikoanalysen

Sicherheitscheck



BSI IT-Grundschutz

32



- Betrachtet
- Vertraulichkeit
- Integrität
- Verfügbarkeit

BSI IT-Grundschutz

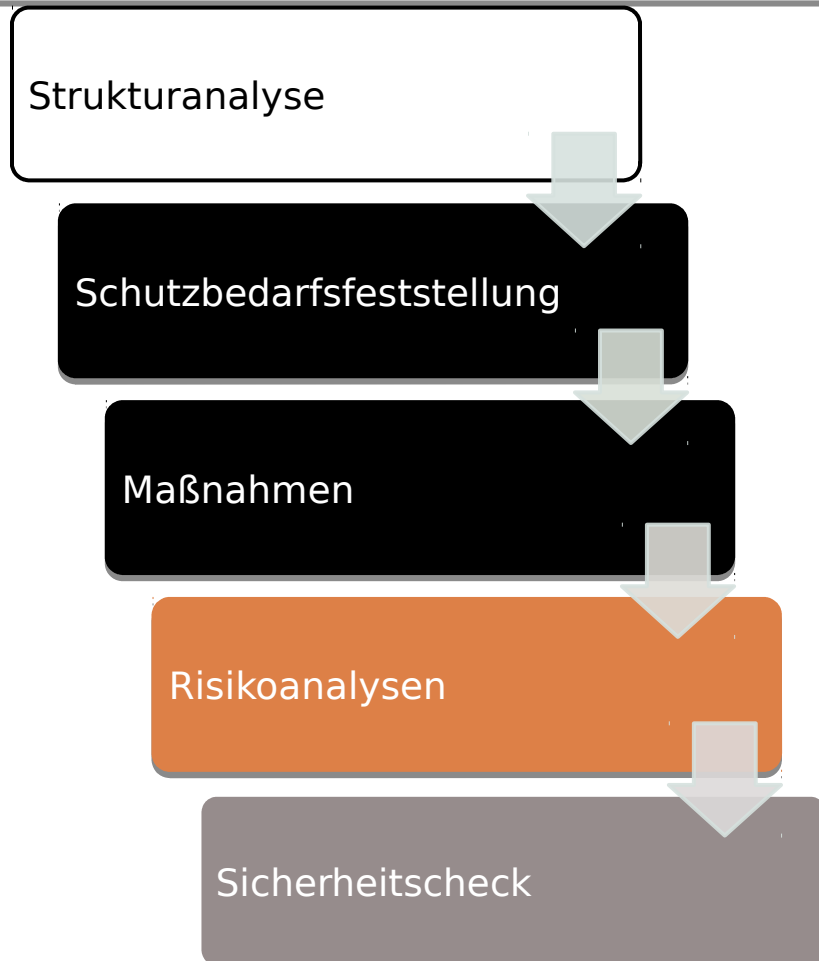
33



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

BSI IT-Grundschutz

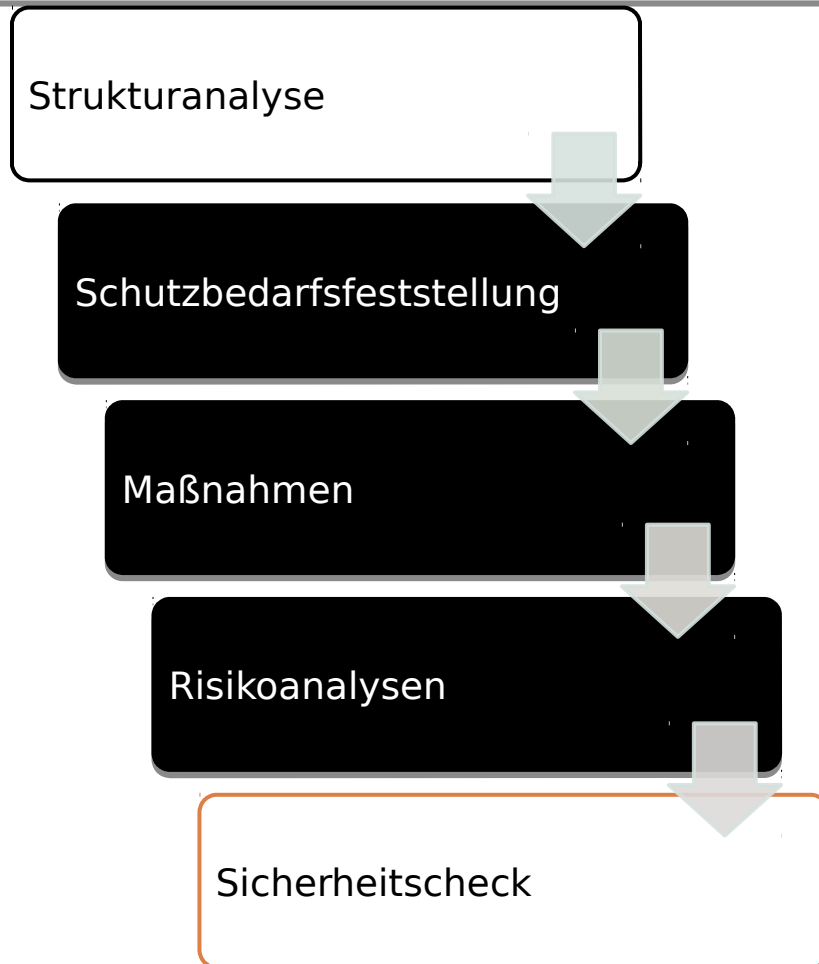
34



- Keine zentralen Management-Systeme
- Mumble-Server

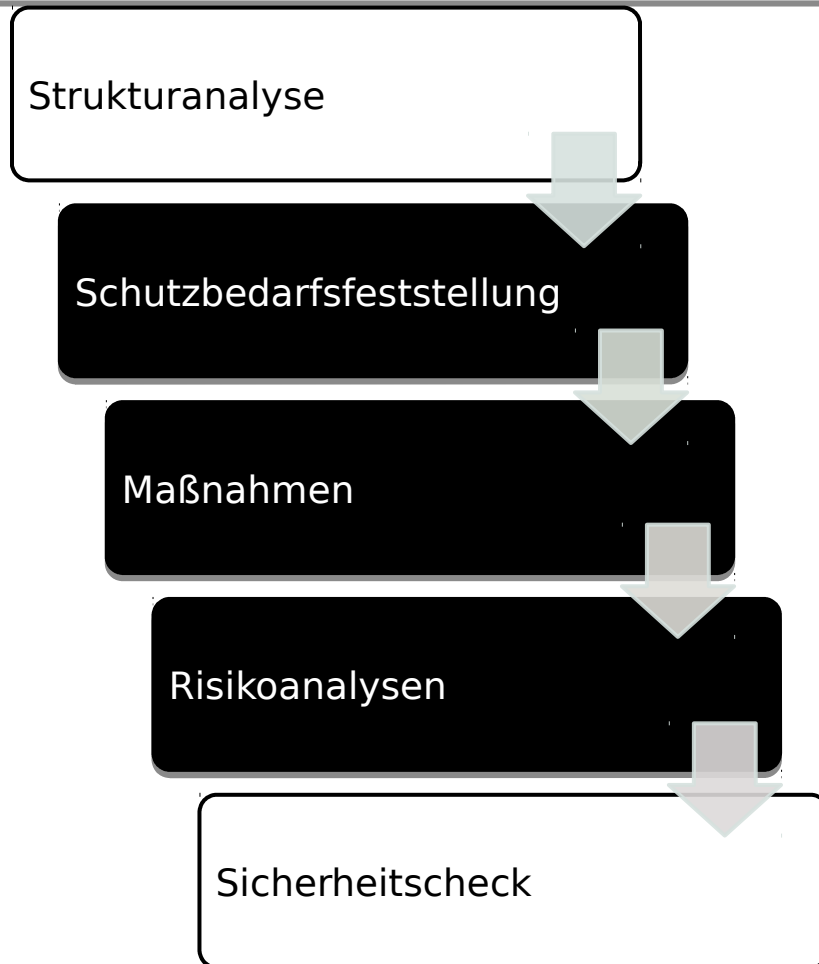
BSI IT-Grundschutz

35



BSI IT-Grundschutz

36



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

Sicherheitskonzept - Ergebnisse

37



Tech. Maßnahmen



Betriebshandbuch



Richtlinie für
Anwender



Tech. Maßnahmen

38

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



Betriebshandbuch

39

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



Leitlinie für Anwender

40

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

Security Index

41

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

Security Index

42

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

Security Index

43

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

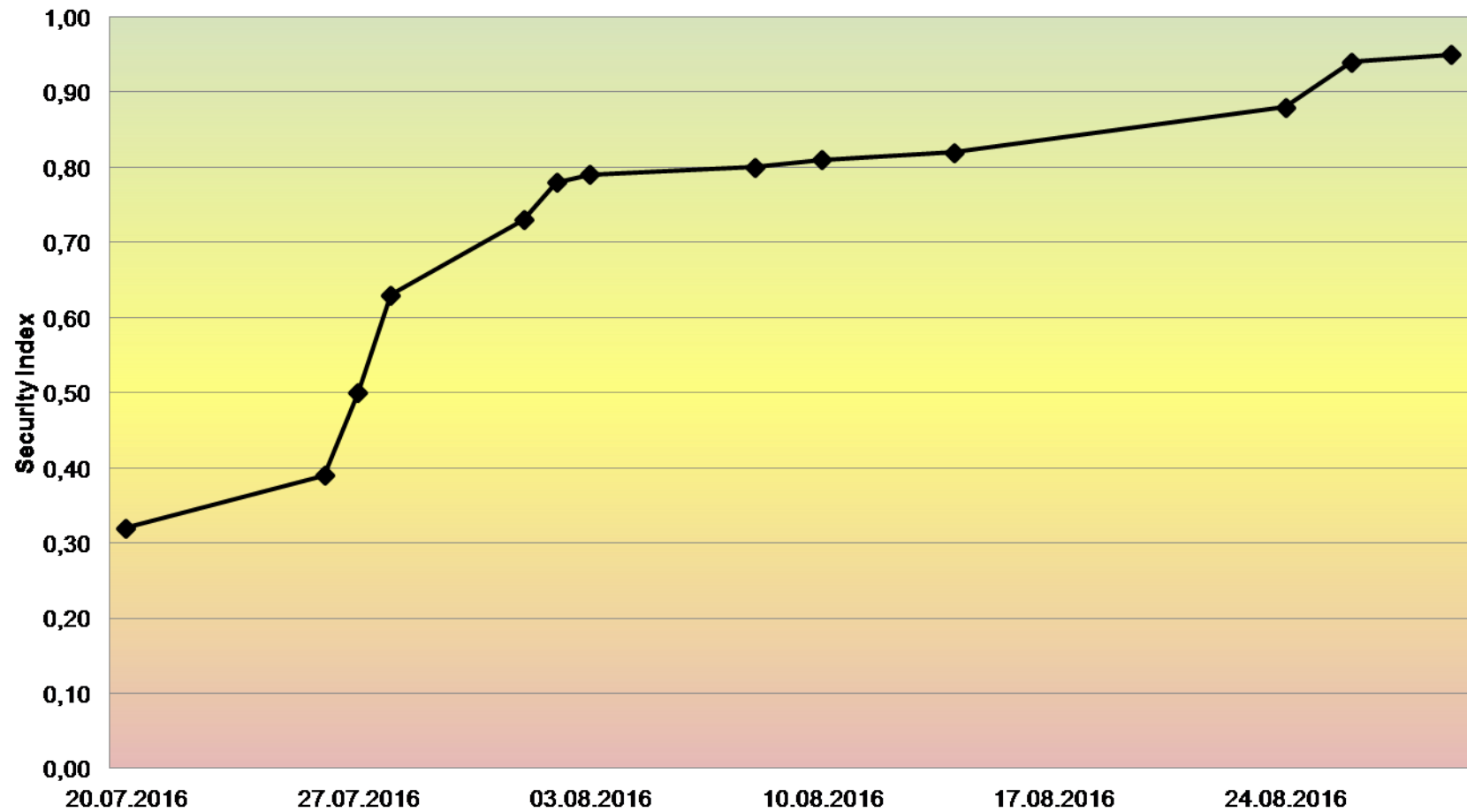
Security Index

44

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

Security Index

45



Datensicherungskonzept

46

- Sicherung & Wiederherstellung
- Vorgehensweise
- Sicherheitsaspekte

Datensicherungskonzept

47

Sicherung & Wiederherstellung

Datensicherungskonzept

48

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

Datensicherungskonzept

49

- 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

50

Vorgehensweise

Datensicherungskonzept

51

- 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

52

Sicherheitsaspekte

Datensicherungskonzept

53

- Backup-Skript enthält sensible Informationen
→ root:root 0700
- Ansible: Alle sensiblen Informationen im Vault
- Unverschlüsseltes Archiv wird nach dem Verschlüsseln wieder gelöscht

Systembeschreibung

54

- OpenVPN & Namensauflösung
- Samba
- Virens Scanner
- Firewall
- Benutzerverwaltung
- Secure Shell
- Logging
- Quota

VPN & DNS

55

- Basis: Konfigurations-Templates der Netz-Gruppen
- Server-Zertifikate und Passwörter im Vault
 - werden nach `/etc/openvpn/certs` kopiert
- Systemd-Dienst

VPN & DNS

56

- 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

57

- 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

58

- 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

59

- 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

60

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

Virens Scanner

61

- 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

Virens Scanner

62

- 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
```

Virens Scanner

63

- 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 Virens Scanners, da die zeitnahe Pflege der Signaturen und Software sehr aufwendig ist

Firewall

64

- 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

65

- 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

66

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

Logging

67

(sudo|do su)

logrotate

tcp

SSL

Rsyslog

k1599_rsyslog_client

Nord

k1599_rsyslog_server

Süd

Rsyslog - Server

68

root@filenord: /var/log/rsyslog-k1599

sascha@discostu: ~/git/uni/Wilddiebe10/docs

root@filenord: /var/log/rsyslog-k1599

root@filenord: /var/log/rsyslog-k1599 64x36

root@filenord:/var/log/rsyslog-k1599# tree 10*

10.8.1.30

- auth.log
- auth.log-20160901
- cron.log
- daemon.log
- debug
- kern.log
- kern.log-20160904
- mail
- mail.info
- messages
- messages-20160901
- syslog
- user.log
- warn

10.8.3.14

- auth.log
- auth.log-20160903
- cron.log
- daemon.log
- debug
- kern.log
- messages
- messages-20160901
- syslog
- user.log
- warn

0 directories, 25 files

root@filenord:/var/log/rsyslog-k1599#

root@filesued: /var/log/rsyslog-k1599 64x36

root@filesued /var/log/rsyslog-k1599 # tree 10*

10.8.1.30

- auth.log
- auth.log-20160901
- cron.log
- daemon.log
- debug
- kern.log
- kern.log-20160904
- mail
- mail.info
- messages
- messages-20160901
- syslog
- user.log
- warn

10.8.3.14

- auth.log
- auth.log-20160831
- cron.log
- daemon.log
- debug
- kern.log
- messages
- messages-20160831
- syslog
- user.log
- warn

0 directories, 25 files

root@filesued /var/log/rsyslog-k1599 #

Rsyslog - Server

69

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","fileservers.mueller-backwaren.de"]
)

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

Quota

70

- 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

71

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

Ausblick – Dateiserver

72

- Folgende Maßnahmen müssten für produktive Umgebungen umgesetzt werden

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

Fazit

73

- 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

74

- Von uns
- für uns