Fachpraktikum IT-Sicherheit: Betriebshandbuch k1599

Abzugeben am 03.09.2016

Betreuung durch Ralf Naues

Christoph Weißenborn[1], Jörg Ricardo Schumacher[1], Marc van Woerkom[1], Patrick Häbel[1], Sascha Girrulat[2], Silas Jansen[2], and Waldemar Schmidt[1]

[1]Gruppe 5 (Nord)
[2]Gruppe 10 (Süd)

Contents

Beschreibung der Systeme

Dateiserver Nord

Beschreibung	Stellt Dienste zum Austausch / Ablegen von Dateien im Netzwerk bereit: • zentrale Ablage von Dateien (Software, Dokumente, etc.) • zentrale Ablage von Backup-Dateien der anderen Services • SAMBA/SMB
Betriebsverantwortung	Gruppe 5
Server- / Gerätebasis	1 virtueller Server (Angemietet bei netcup GmbH)
Betriebssystem	Ubuntu 16.04
Besonderheiten	
Redundanzkonzept	Manuelle Redundanz über Dateiserver der Gruppe 10
Geforderte Verfügbarkeit	Gemäß Service-Level-Agreement (SLA)
Liefert Funktionen für	• Zertifikatsserver (Backup) • Webserver (Backup) • Mailserver (Backup) • Netz (Backup)
Benötigt Funktionen von	• Zertifikatsservern • Mailservern • Netz
Systemverwaltung / Administration	Erfolgt via Ansible. Direkter Zugriff ausschließlich per SSH (Passwort oder Zertifikat)
Backup	
Restore	

Dateiserver Süd

Beschreibung	Stellt Dienste zum Austausch / Ablegen von Dateien im Netzwerk bereit: • zentrale Ablage von Dateien (Software, Dokumente, etc.) • zentrale Ablage von Backup-Dateien der anderen Services • Dienste: SAMBA
Betriebsverantwortung	Gruppe 10
Server- / Gerätebasis	VServer CX20 von Hetzner
Betriebssystem	Debian GNU/Linux 8.5
Besonderheiten	
Redundanzkonzept	Manuelle Redundanz über Dateiserver der Gruppe 5
Geforderte Verfügbarkeit	Gemäß Service-Level-Agreement (SLA)
Liefert Funktionen für	• Zertifikatsserver (Backup) • Webserver (Backup) • Mailserver (Backup) • Netz (Backup)
Benötigt Funktionen von	• Zertifikatsservern • Mailservern • Netz
Systemverwaltung / Administration	Erfolgt via Ansible. Direkter Zugriff ausschließlich per SSH (Passwort oder Zertifikat)
Backup	
Restore	

Service Schnittstellen

Beschreibung der Serviceprozesse

Change Management

Das Change Management hat das Ziel, dass alle Anpassungen der IT-Infrastruktur kontrolliert, effizient und unter Minimierung von Risiken für den Betrieb bestehender Services durchgeführt werden.

Wir orientieren uns hier am Prozess aus der **IT Infrastructure Library (ITIL)**. Aus Ressourcengründen wurde auch hier auf eine pragmatische Lösung gesetzt - es wurden nur die Prozesse übernommen, welche für einen sicheren Betrieb der Umgebung aus unserer Sicht zwingend erforderlich sind. Auf eine Zertifizierung nach ISO/IEC 20000:2005 wurde daher verzichtet.

Workflow

1. **Request for Change (RfC):** Ein Mitarbeiter der vereinten Backwerke stellt beim Change Manager einen formalen RfC. Dafür wird das Formular 5.1.1 genutzt. Der RfC enthält alle Informationen, die für die weitere Entscheidungsfindung wichtig sind.
2. **Change Advisory Board (CAB):** Das CAB besteht aus dem Change Manager und von ihm benannten weiteren Personen. Es muss nach Beantragung innerhalb von 7 Tagen zusammentreten und den RfC genehmigen - oder diesen alternativ, inklusive Begründung der Ablehnung, an den Antragsteller zurück übermitteln.
3. **Implementierung**: Genehmigte Changes werden zur Bearbeitung an die entsprechenden technischen Gruppen weitergegeben.
4. **Post Implementation Review:** Ziel ist es, die Effizienz der durchgeführten Maßnahmen sowie des dazugehörigen Prozesses zu durchleuchten. Dabei sollen sowohl die durchgeführte Veränderung als auch die dabei benutzten Methoden und Prozesse einer Ist-Soll-Analyse unterzogen werden. Bei größeren Changes spielen auch Kosten-Nutzen-Vergleiche, die Return on Investment (ROI)-Kalkulation sowie die Messung der Zielerreichung aus der geschäftlichen Perspektive eine Rolle. Der Change Manager legt hierzu Termine und Agenda fest und fordert dafür Unterstützung an.

Change Manager

Der Change-Manager ist verantwortlich für die Durchführung eines Changes in einer systematischen Art und Weise, nachdem die bekannten Risiken abgewogen

wurden. Er überwacht auch den Fortschritt des Changes. Der Change-Manager beurteilt die Requests for Change (RfC) zusammen mit dem Change Advisory Board (CAB). Change Manager ist **Sascha Girrulat**.

Standard Changes

Bei Standard Changes handelt es sich um häufig wiederkehrende Changes mit vergleichsweise geringem Risiko, deren Prozess vom CAB einmalig genehmigt wurde.

Das Verfahren zur erstmaligen Genehmigung eines Standard Changes ist das Gleiche wie bei herkömmlichen Changes. Wiederkehrende Standard Changes werden nicht durch einen RfC geleitet, sondern lediglich als Service Requests dokumentiert.

Genehmigte Standard Changes

Standard Change	Prozess
Betriebssystem Update Server	1. Aufnahme als Service Request im Ticketsystem 2. Überprüfung des Changelogs auf Risiken 3. Einspielen des Updates außerhalb der garantierten Betriebszeit (siehe Seite 11) oder Information aller Gruppen der Vereinigten Backwerke 48 Stunden vor Einspielen des Updates 4. Überprüfung des, durch den Server bereitgestellten, Services auf Funktion 5. Dokumentation im Ticketsystem.
Dateiserver Dienst Update Dateiserver:	1. Aufnahme als Service Request im Ticketsystem 2. Überprüfung des Changelogs auf Risiken 3. Einspielen des Updates außerhalb der garantierten Betriebszeit (siehe Seite 11) oder Information aller Gruppen der Vereinigten Backwerke 48 Stunden vor Einspielen des Updates 4. Überprüfung des, durch den Server bereitgestellten, Services auf Funktion 5. Dokumentation im Ticketsystem.

Benutzerkonten lokal (einrichten, ändern, Passwort zurücksetzen)	1. Änderung vornehmen in Ansible-Konfiguration 2. Einspielen der neuen Konfiguration auf beiden Servern 3. Betroffenen Nutzer über Änderungen informieren 4. Warten auf Rückmeldung des Nutzers (bei Einrichtung oder Änderung)
Offline Backup Dateiserver (1x wöchentlich, So)	1. Prüfung, ob aktueller Termineintrag noch in gemeinsamem Kalender vorhanden 2. Login auf dem Mumble Server des CSIRT 3. Bekanntgabe an alle Anwesenden, dass mit der Sicherung begonnen wird 4. Erstellen eines Client-lokalen Backups von einem der beiden Dateiserver, inklusive des tar.gz-Backups vom anderen Server auf eine externe Festplatte a. Sicherung der eigentlichen Anwender-Dateien b. Sicherung der Systemeinstellungen mittels tdbbackup /etc/samba/passdb.tdb i. smb.conf ii. secrets.tdb iii. tdbsam c. Integrität der Backup-DB prüfen mittels tdbbackup -v etc/samba/passdb.tdb d. Sicherung der verwendeten Software: Samba e. Sicherung der Protokolldateien: rsyslog 5. Trennen der externen Festplatte vom Computer 6. Löschen des aktuellen Termineintrags im gemeinsamen Kalender 7. Logout auf dem Mumble Server

Restore Dateiserver	1. Ein Mitglied der Gruppe mit Betriebsverantwortung für den entsprechenden Sever verifiziert, dass dieser tatsächlich nicht mehr wieder in Betrieb genommen werden kann 2. Neuinstallation des Betriebssystems auf dem Gleichen oder, falls dies nicht mehr möglich ist, auf einem anderen Server 3. Einrichtung des SSH Zugangs auf dem neuen System 4. Restore der Serverkonfiguration auf letzte funktionierende Ansible-Version (ggf. Anpassung der externen IP-Adresse) 5. Einspielen der Nutzerdaten aus dem letzten verfügbaren Backup (vom anderen Dateiserver) 6. Mindestens zwei Techniker der Dateiservergruppen bestätigen die Wiederverfügbarkeit der Daten 7. Information an alle Anwender der Vereinigten Backwerke über vorgenommenen Restore sowie an Change und Problem Manager 8. Dokumentation im Ticketsystem
Benutzer verlässt das Unternehmen	1. Aufnahme als Service Request im Ticketsystem 2. Löschen ggf. vorhandener lokaler Konten auf den Dateiservern 3. Löschen der persönlichen Benutzerfreigaben auf beiden Dateiservern 4. Dokumentation im Ticketsystem

Emergency Changes

Ein Sonderfall des Changes, der nicht den üblichen Prozess durchläuft sondern sofort, notfalls auch unter erheblichem Risiko und ohne weitere Genehmigung vom CAB, meist zur Abwendung größeren Schadens durchgeführt wird. *Bei einem Change dieser Art benötigt der durchführende Techniker nur die Zustimmung eines weiteren Technikers innerhalb der IT-Gruppen.* Vorrangig ist hier auf eine Notsituation reagieren zu können. Entsprechende weitere Genehmigungen und Tests werden erst nach dem Change durchgeführt.

Die durchgeführten Emergency Changes sind jedoch umgehend nach der Wiederherstellung des normalen Betriebes zu dokumentieren und die betroffenen Gruppen sowie der Change Manager sind zeitnah zu informieren.

Incident Management

Unter einem Incident / einer Störung versteht man nach IT Infrastructure Library (ITIL) ein Ereignis, das nicht zum standardmäßigen Betrieb eines Services gehört und das tatsächlich oder potenziell eine Unterbrechung dieses Services oder eine Minderung der vereinbarten Qualität verursacht.

IT-Incident Management umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf solche Ereignisse. Ziel des Incident-Management-Prozesses ist die schnellstmögliche Wiederherstellung der Service-Leistung (auch mit Workarounds).

Benutzerservice

Um den Anwendern einen Single Point of Contact für alle IT-Anliegen zur Verfügung zu stellen, haben wir einen Benutzerservice eingerichtet. Der Benutzerservice hat die Aufgabe Anwenderanfragen entgegen zu nehmen, im Ticketsystem anzulegen und das Ticket dann an die betroffenen Gruppen weiter zu vermitteln.

Workflow

1. **Meldung** des Incidents an:
   (Mitarbeiter des Benutzerservice können hier direkt mit 2. weiter machen)
2. **Aufnahme** und Bewertung des Incident im Ticketsystem
3. Falls die Anfrage direkt beantwortet/gelöst werden kann weiter mit 6. - sonst:
   Information per Mail an alle Mitglieder der betroffenen Gruppen
4. **Bearbeitung** des Incident in den Gruppen
5. Dokumentation des Bearbeitungsstandes im Ticketsystem
6. Nach Abschluss der Arbeiten
   a. Information an den Anfrager sowie aller direkt betroffenen Anwender
   b. **Dokumentation** der Lösung im Ticketsystem

IT Security Incident Management

IT Sicherheitsmanagement beinhaltet die Überwachung und Feststellung von Sicherheitsereignissen auf dem System und die angemessene Reaktion auf diese Ereignisse.

Computer Security Incident Response Team (CSIRT)

Die Aufgaben des CSIRT sind

- die Überwachung der Systeme auf Sicherheitsvorfälle
- als zentraler Kommunikationsknoten für eingehende Sicherheitsereignisse und ausgehende Informationen über diese Ereignisse zu agieren
- Sicherheitsvorfälle zu dokumentieren
- Das Bewusstsein für sichere IT innerhalb der Vereinigten Backwerke zu schärfen, um Vorfällen vorzubeugen
- Externe System- und Netzwerkaudits zu unterstützen (etwa bei der Schwachstellenanalyse und Penetrationstests)
- sich über neue Angriffsvektoren und -strategien zu informieren
- Informationen über Sicherheitsupdates eingesetzter Software einzuholen und diese an die Administratoren der Services zu verbreiten
- Administratoren bei Sicherheitsfragen zu beraten
- bei Sicherheitsvorfällen zeitnah und angemessen die technische Reaktion der Vereinigten Backwerke zu koordinieren und diese umzusetzen

Jedes Teammitglied ist eigenständig verantwortlich für

- die Bereithaltung wichtiger Software-Werkzeuge und eines vom Vereinigten Backwerke Netz unabhängigen Computers mit Internet-Anschluss
- die Ablage wichtiger Notfallinformationen (IP-Adressen der Systeme, Passwörter, Betriebshandbuch, Kopien von CA Schlüsseln) offline an einer für

denjenigen gut zugänglichen, sicheren Stelle

- Die Überprüfung des Bürger-CERT auf aktuelle Sicherheitswarnmeldungen

Mitglieder

Aus Gruppe	Personen
Gruppe 5 (Datei Nord)	Christoph Weißenborn Jörg Ricardo Schumacher
Gruppe 10 (Datei Süd)	Sascha Girrulat Silas Jansen

Mumble Server

Bei einem Security Incident koordinieren sich die Mitglieder des CSIRT über den Ersten der im folgenden aufgelisteten Server. Falls dieser nicht verfügbar sein sollte, so koordinieren sie sich über den zweiten Server, usw.

Server	Login
Gruppe 10	IP/DNS: 78.46.200.193 User: <beliebig> Passwort: juXe1goi
Gruppe 5	IP: 5.45.103.136:64738 DNS: praktikum.ehanse.de:64738 User: <beliebig> Passwort: piratenwilddiebe
Last Resort	Skype, Google Hangout oder Telefonkonferenz (Achtung, hier keine Geschäftsgeheimnisse kommunizieren!)

Workflow

1. **Meldung** des Sicherheitsvorfalls durch Anwender, Administrator oder Monitoring an den Benutzerservice
2. Der Benutzerservice erstellt ein **Ticket** im Ticketsystem und nimmt eine **Erstbewertung** des Vorfalls vor. Falls es sich nach dieser Bewertung um einen möglichen Security Incident (gemäß) handelt, werden alle Mitglieder des CSIRT (per Mail und - soweit angegeben - telefonisch) informiert. Sie erhalten dabei auch die ID des Tickets (Zeilennummer im Ticketsystem).
3. Das CSIRT koordiniert die Reaktion über die Mumble Server. Dabei orientiert sich das Team an den folgenden Leitlinien:

a. Schaden begrenzen und weitere Risiken minimieren

b. Die Art und den Umfang der Kompromittierung feststellen

c. Beweise sichern

d. Weitere Stellen informieren, falls notwendig (CIO, Polizei, BSI, etc.)

e. Systeme wiederherstellen

f. Informationen für die Dokumentation zusammenstellen und strukturieren

g. Schaden und Kosten abschätzen

h. Reaktion überprüfen und Verfahren anpassen

Problem Management

Über das Problem-Management werden unbekannte Ursachen für tatsächliche und potentielle Störungen (Incidents) innerhalb der IT-Services untersucht und die Behebung gesteuert. Anders als das Incident Management arbeitet das Problem-Management sowohl reaktiv als auch proaktiv. Ein wesentliches Ziel ist hierbei die 'dauerhafte Problemlösung'.

Ein Problem ist so lange offen, wie seine Ursache und deren Behebung nicht erledigt sind; demgegenüber kann ein Incident geschlossen werden sobald die vom Anwender benötigte Funktionalität wieder hergestellt ist.

Die Ursachen für das Problem werden analysiert und Maßnahmen zu ihrer Verhinderung oder Behebung entwickelt. Ergebnis dieser Analyse ist entweder ein Known Error (also die nun bekannte Ursache für eine Störung) oder ein Workaround (Umgehungslösung).

Im Problem-Management erarbeitete Workarounds können dem Incident Management zur Verfügung gestellt werden, um künftig für identische Störungen eine schnelle Wiederherstellung des betroffenen IT-Services zu ermöglichen.

Lösungen für bekannte Fehler (Known Errors) können als Änderungsanforderung (Request for Change) an das Change Management weitergeleitet werden.

Problems werden als solche im Ticketsystem dokumentiert.

Problem Manager

Der Problem Manager ist dafür verantwortlich, alle Problems über ihren gesamten Lebenszyklus zu verwalten. Seine vorrangigen Ziele bestehen darin, der Entstehung von Incidents vorzubeugen und die negativen Auswirkungen von Incidents, die nicht verhindert werden können, möglichst gering zu halten. Zu diesem Zweck pflegt er die Informationen zu Known Errors und Workarounds.

Festgelegte Problem Manager

Gruppe	Problem Manager
Gruppe 5 (Dateiserver)	Waldemar Schmidt
Gruppe 10 (Dateiserver)	Silas Jansen

Service Management

Service Level Agreement (SLA)

Der Begriff Service-Level-Agreement (SLA) bezeichnet die Schnittstelle zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen. Ziel ist es, die Kontrollmöglichkeiten für den Auftraggeber transparent zu machen indem zugesicherte Leistungseigenschaften, wie etwa Leistungsumfang, Reaktionszeit und Schnelligkeit, der Bearbeitung genau beschrieben werden. Wichtiger Bestandteil ist hierbei die Dienstgüte (Servicelevel), welche die vereinbarte Leistungsqualität beschreibt.

Serviceparameter	Geforderter Servicelevel
Garantierte Betriebszeit	Mo-Sa, 04:00-22:00 Uhr
Verfügbarkeit	mind. 99,0% (bezogen auf den Kalendermonat) Die max. Ausfalldauer pro Monat beträgt 7:10 Stunden.
Reaktionszeit	Security Incident: 2 Tage Incident (kritisch): 2 Tage Incident (normal): 2 Arbeitstage Problem: 14 Tage Infoanfrage: 2 Arbeitstage Service Request: 14 Tage
Entstörungszeit	Security Incident: 2 Tage Incident (kritisch): 3 Tage Incident (normal): 4 Arbeitstage Problem: - Infoanfrage: - Service Request: -

Klassifizierung von Events

Event	Beschreibung

Security Incident	Die Vertraulichkeit oder Integrität von Gütern, Informationen, Daten und IT-Services der Vereinigten Backwerke ist möglicherweise kompromittiert.
Störung (kritisch)	Ausfall eines Services *oder* erheblicher Teilausfall eines Services
Störung (normal)	Geringer Teilausfall eines Services oder einer Komponente (z.B. Nichtverfügbarkeit von Zusatz-Funktionen) *oder* Ausfall einer Redundanzkomponente *oder* Nichtverfügbarkeit eines Services für einen einzelnen Anwender
Problem	Unerwünschtes oder unerwartetes Verhalten eines Services, das aktuell ohne wesentliche Auswirkungen auf die Anwender ist
Infoanfrage	Informationsanfrage eines Anwenders, die ohne Änderung an den Systemen geklärt werden kann
Service Request	Anfrage eines Anwenders zur Bereitstellung eines neuen Services *oder* Anfrage eines Anwenders zur Bereitstellung einer bisher nicht realisierten Funktionalität eines bestehenden Services

Eskalationsprozedur

Eskalationen dienen in der Regel dazu, eine Störungsbearbeitung durch Einbeziehung höherer Instanzen zu beschleunigen, bzw. durch eine Erweiterung der Kompetenzen und Befugnisse zu ermöglichen.

Eskaliert wird sobald sich abzeichnet, dass die definierte Entstörzeit nicht eingehalten werden kann - oder spätestens, wenn sie überschritten wurde. An weitere Eskalationsebenen wird eskaliert, wenn die jeweilige Eskalationsebene mit ihren Kompetenzen und Befugnissen nicht mehr ausreichend zur Behebung der Störung beitragen kann.

Da Problems, Infoanfragen und Service Requests keiner definierten Entstörzeit unterliegen, für ihre Lösung jedoch ggf. dennoch eine Eskalation erforderlich ist, sollte diese - soweit möglich - einvernehmlich vorgenommen werden.

Eskalationsstufe	Verantwortlicher Ansprechpartner
Normalfall	**Benutzerservice** Tel.: +49 228-3875 8003 Mail: gruppe5@mayerbrot.intern
1. Eskalation	**Problem Manager** siehe Festgelegte Problem Manager
2. Eskalation	**CIO** Ralf Naues Tel.: NA Mail: k1599@fernuni-hagen.de

Service Manager

Für die Umsetzung des Servicemanagements wird ein IT Service Manager eingesetzt. Für alle Belange der Anwender, die für die Steuerung der Serviceleistungen relevant sind, steht der Service Manager zur Verfügung. Er leistet in dieser Funktion jedoch keinen operativen Service und ist keine Eskalationsinstanz bei akuten Vorfällen. Er überwacht die Einhaltung der SLAs. Wichtige Informationsquellen hierfür sind Einträge im Ticketsystem sowie persönliches Feedback von Leitungsbereich, Anwendern und IT Gruppen.

Service Manager ist

Christoph Weißenborn

Tel.: +49151-12045346

Mail: christoph.weissenborn@live.de

Beschreibung der Betriebsprozesse

Einmalige Betriebsprozesse (ausgelöst durch Event)

Komplett bekannte, wiederkehrende Betriebsprozesse, welche Änderungen an den Systemen erfordern, sind als Genehmigte Standard Changes beschrieben. Bei den folgenden Prozessen handelt es sich daher nur um allgemeine Leitlinien für im Vorfeld nicht bekannte Maßnahmen:

Allgemeiner Change Dateiserver

- Nach jeder Änderung an der Datei smb.conf muss zunächst mit dem Programm testparm geprüft werden, ob die Syntax der Konfigurationsdatei

korrekt ist. Syntaxfehler in der Konfigurationsdatei können sonst dazu führen, dass der Server nicht neu startet oder Sicherheitslücken entstehen.

Einbindung externer Programme in SAMBA (Dateiserver)

- Es ist sicherzustellen, dass nur Programme, die keine schadhafte Funktion besitzen von Samba aufgerufen werden. Mit dem Kommando
  user> testparm -vs | grep -E "(command =)|(script =)|(exec =)|\ (panic action =)|(program =)"
  werden alle Parameter ausgegeben, die für die Einbindung externer Programme in Samba verantwortlich sind. Zusätzlich zu den Parametern werden die momentan gültigen Werte angezeigt.

Zyklische Reviews

Service Review

Zyklus	1x im Quartal
Verantwortlich	Service Manager
Teilnehmer	• Service Manager • Problem Manager • ein Mitglied jeder am Betriebshandbuch teilnehmenden IT Gruppe • ein Mitglied des CSIRT • weitere Administratoren auf Anfrage des Service Managers
Agenda	• Einhaltung der SLAs • Anzahl und Status der Incidents im Betrachtungszeitraum • Entwicklung der Servicequalität • geplante (oder sich im Ablauf ergebende) Änderungen am Service Management

IT Security Review

Zyklus	Jährlich
Verantwortlich	CIO
Teilnehmer	• CIO • Alle Mitglieder des CSIRT • weitere Administratoren auf Anfrage des CIO • Geschäftsleitung auf Anfrage des CIO
Agenda	• Wirksamkeit und Aktualität von Regelungen zur Datensicherheit • Wirksamkeit und Aktualität von Regelungen zum Datenschutz • Review von Sicherheitsvorfällen im Betrachtungszeitraum • Überprüfung der Einhaltung gesetzlicher Vorschriften (Lizensierung, etc.) • Bürger-CERT Meldungen und Bearbeitung im letzten Jahr • Organisation einer IT Sicherheitskampagne alle 2-3 Jahre

Datensicherung Review

Zyklus	1x im Quartal
Verantwortlich	Alle Mitarbeiter Gruppe 5 und 10
Teilnehmer	• Gruppe 5 • Gruppe 10 • Ein Mitarbeiter des CSIRT
Agenda	• Test Restore aus dem Backup • Funktionierte das Backup im Betrachtungszeitraum wie definiert? • Volumina und Backupzeiten noch im Rahmen des Datensicherungskonzeptes?

Anlagen

Formulare

Request for Change (RfC)

Betroffener Service
Grund für den Change: Voraussichtliche Auswirkungen: Rollbackszenario für den Fall eines Fehlschlags: Priorität: Beteiligte IT Gruppen: Beteiligte Anwendergruppen: Vorhersehbare Risiken: Zeitplan zur Durchführung:

Aufnahme eines Services / Gruppe in Betriebshandbuch

Bezeichnung des Services*	
Serverdaten*	Beschreibung: Server- / Gerätebasis: Betriebssystem: Besonderheiten: Redundanzkonzept: Geforderte Verfügbarkeit: Systemverwaltung / Administration: Backup: Restore:
Service Management	Wollt ihr am gemeinsamen SLA teilnehmen? (Unser Vorschlag: Verfügbarkeit Mo-Sa, 04:00-22:00 Uhr, 99%)

Incident Management	Der Benutzerservice nimmt Mails entgegen, trägt sie ins bereitgestellte Ticketsystem ein und informiert die betroffenen Gruppen über das neue Ticket. Wollt ihr am gemeinsamen Benutzerservice teilnehmen? Welche Gruppenmitglieder nehmen am Benutzerservice teil?
IT Security Incident Management	Das Computer Security Incident Response Team (CSIRT) reagiert gemeinsam auf Sicherheitsvorfälle und behandelt diese angemessen. Wollt ihr am gemeinsamen CSIRT teilnehmen? Welche Gruppenmitglieder nehmen am CSIRT teil?
Problem Management	Wollt ihr am gemeinsamen Problem Management teilnehmen? Wer wird für eure Gruppe Problem Manager?
Change Management	Wollt ihr am gemeinsamen Change Management (nach ITIL) teilnehmen? Möchtet ihr dafür jemanden als Change Manager benennen? Welche Standard Changes möchtet ihr mit aufnehmen lassen? (Mit Ablaufbeschreibung)

Mit * gekennzeichnete Informationen sind Pflicht. Alle anderen Angaben optional.

Organisatorische Informationen

Technisch relevante Gesetze und Verordnungen

- Telekommunikationsgesetz (TKG)
- Telekommunikationsüberwachungsverordnung (TKüV)
- Urheberrechtsgesetz (UrhG)
- Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation
- Elektro- und Elektronikgerätegesetz (ElektroG)
- Signaturgesetz (SigG)

Technische Informationen

Liste der IP Adressen und DNS-Namen pro Gerät

Service	Intern IP	Intern DNS	Extern IP	Extern DNS
Nord VPN/DNS	10.8.1.1 /24	VPNNord.MayerBrot.intern		
Nord Web	10.8.1.20 /24	WebNord.MayerBrot.intern		
Nord File	10.8.1.30 /24	FileNord.MayerBrot.intern	5.45.103.136	praktikum.ehanse.de
Nord CA	10.8.1.40 /24	CaNord.MayerBrot.intern	46.101.99.119	ca-nord.fachpraktikum-1599.de
Nord Mail	10.8.1.50 /24	MailNord.MayerBrot.intern		
Süd VPN	10.8.3.1 /24			
Süd Web	/24			
Süd File	10.8.3.14 /24	fileserver.mueller-backwaren.de	138.201.175.250	static.250.175.201.138.clients.your-server.de
Süd CA	10.8.3.26 /24	ca.mueller-backwaren.de		caserv-mueller.westeurope.cloudapp.azure.com
Süd Mail	/24			