# Service-Level-Agreement

# Portfolio

BAGHUS GmbH

# Zusammen mit BAGHUS zu einer rundum abgesicherten IT-Umgebung

Um Ihre Anforderungen vollumfänglich abdecken zu können kann aus einer Vielzahl an Service-Optionen gewählt werden, um somit ein passendes Leistungspaket erstellen zu können. dieses Paket bildet die Grundlage für ein gemeinsames SLA zwischen Ihnen und BAGHUS.

BAGHUS stellt hierfür für Sie Service-Optionen aus unterschiedlichen Bereichen (Services) bereit:

- Infrastruktur
- Windows-Server
- Firewall
- Mail
- Enterprise Client Management (ECM)
- Security Information and Event Management (SIEM)

Die Services enthalten alle wesentlichen Tätigkeiten der Service-Optionen, welche durch die BAGHUS momentan standardmäßig zur Verfügung gestellt werden.

Gerade in der IT ist es wichtig, situativ auf sich ändernde oder abweichende Umstände reagieren zu können. Um für ein stetiges Wachstum sorgen zu können ist es daher unerlässlich, dass BAGHUS mit Ihnen zusammen kontinuierlich und aktiv an der Weiterentwicklung arbeitet. Hierzu gehört auch, dass der Katalog jederzeit anhand Ihrer Systeme und -wünsche angepasst und bei Bedarf erweitert werden kann.

## Service-Level-Management

Beim Service-Level-Management (SLM) handelt es sich um eine ITIL-Prozess-Disziplin. Diese dient primär der Definition, Überwachung und Optimierung von Dienstleistungen. Eine wesentliche Funktion und Zielsetzung hierbei ist es, dauerhaft die Leistung der IT (bzw. Services) in Einklang mit den geschäftlichen Erwartungen zu bringen. Hierbei trägt das SLM die Verantwortung für die Effizienz der Prozessbeziehungen zwischen dem IT- und dem Geschäfts-Management. Um dies zu ermöglichen, wird ein einheitliches aber dennoch auf die sich ergebene Situation angepasstes Rahmenwerk der betroffenen Prozesse benötigt. Mit Hilfe eines Servicekataloges können hierbei Vereinbarungen, Verbindlichkeiten und Beziehungen beschrieben und verwaltet werden.

# Zusammen mit BAGHUS zu einer rundum abgesicherten IT-Umgebung

Damit die vereinbarten Service-Optionen vollumfänglich umgesetzt werden können gilt es, im Rahmen des Vertragsabschlusses, nötige Standards der BAGHUS bezüglich der betroffenen Services zu implementieren (beispielsweise im Windows-Bereich AD Hardening und Tiering).

Zudem wird für jeden bezogenen Service anhand der gewählten Service-Optionen eine Systemliste erstellt. Hierdurch soll sichergestellt werden, dass eine gemeinsame Basis geschaffen wird und jeder Vertragspartner den gleichen Kenntnisstand über die beinhalteten SLA-Vertragsgegenstände hat.

Um Ihnen einen bestmöglichen Überblick des BAGHUS Leistungsspektrum geben zu können unterteilt sich folgendes Dokument wie folgt:

Zuerst finden Sie eine Übersicht aller momentan gelebten Service-Optionen. Dieser folgt eine detaillierte Aufbereitung der standardmäßig durchgeführten Tätigkeiten je Service-Option.

Der folgenden Übersicht können die momentan von BAGHUS standardmäßig angebotenen Service-Optionen entnommen werden.

Bitte teilen Sie uns mit, wenn Sie Fragen oder weitere Informationen zu einem Service oder einer bestimmten Service-Option haben. Gerne vereinbaren wir dann einen Termin mit dem entsprechenden Fachbereich, um für Sie eine bestmögliche Anpassung an ihre Wünsche und Systeme durchführen zu können.

Sie können uns gerne telefonisch erreichen oder uns eine E-Mail zuschicken. Für letzteres können Sie auch gerne in der Tabelle die gewünschten Service-Optionen markieren (bspw. mit einem x) und uns zuschicken.

## Service-Level-Agreements

Dies Ergebnisse dienen als Grundlage der Definitionen für Service-Level-Agreements (SLAs) zwischen IT-Service-Anbietern und IT-Service-Kunden. Sie werden benötigt, um die Schnittstelle zwischen Auftraggeber und Dienstleister festzulegen und um wiederkehrende Dienstleistungen einsteuern zu können. Ziel hierbei ist es, die Kontrollmöglichkeiten für den Auftraggeber transparent zu machen, indem zugesicherte Leistungseigenschaften wie etwa Leistungsumfang, Reaktionszeit und Schnelligkeit der Bearbeitung genau beschrieben werden.

| Service: Infrastruktur |
|---|
| ☐ Monatsreport: Infrastruktur |
| ☐ Backupsystem: Kontrolle |
| ☐ Backupsystem: Software |
| ☐ Backupsystem: Hardware |
| ☐ Backupsystem: Bändertausch |
| ☐ Backupsystem: Storage |
| ☐ Backupsystem: Restoretest |
| ☐ Virtualisierung: VMware Software |
| ☐ Virtualisierung: VMware Hardware |
| ☐ Virtualisierung: VMware Storage |
| ☐ Netzwerk: Switch Hardware |
| ☐ Netzwerk: Switch Restoretest |
| ☐ Netzwerk: WLAN-Hardware |
| ☐ Netzwerk: WLAN-Kennwörter |
| ☐ Linux: DokuWiki |
| ☐ Linux: Seafile |
| ☐ Hardware: USV-System |

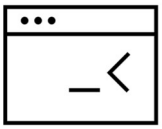
| Service: Windows-Server |
|---|
| ☐ Monatsreport: Windows-Server |
| ☐ Root-Domain: Windows |
| ☐ Root-Domain: DCs |
| ☐ Root-Domain: Member-Server |
| ☐ MARS-Agent: Backup |
| ☐ MARS-Agent: Restoretest |
| ☐ MARS-Agent: Softwarepflege |
| ☐ SQLBackupAndFTP: Backup |
| ☐ SQLBackupAndFTP: Restoretest |
| ☐ SQLBackupAndFTP: Softwarepflege |
| ☐ Monitoring: PRTG |
| ☐ MS SQL |
| ☐ MS SQL Express |
| ☐ MS SQL Advanced |
| ☐ Azure AD Connect |
| ☐ Password Safe |
| ☐ Regelmäßiger Wechsel lokaler Adminkennwörter auf den Servern und für Servicekonten |
| ☐ Defender for Identity |
| ☐ AD Hardening: Analyse AD und Azure AD auf aktuelle Best-Practices |
| ☐ AD Hardening/Tiering: Überprüfung von Kontrollbeziehungen und möglicher Angriffspfade |
| ☐ AD Hardening: Von Benutzer und Administratoren genutzte Kennwörter auf Kompromittierung und Qualität prüfen |
| ☐ KRBTGT-Kennwort regelmäßig ändern |
| ☐ NPS: Network Policy Server |
| ☐ Überprüfung Windows Firewall auf den Servern |
| ☐ Kundenspezifische Software: FineKey KeyWatcher |
| ☐ Kundenspezifische Software: RDP |

| Service: Firewall |
|---|
| ☐ Monatsreport: Firewall |
| ☐ Firewall: Restoretest |
| ☐ Firewall: Rechenzentrum |
| ☐ Firewall: Außenstandort |
| ☐ Firewall: Control Center |
| ☐ RSA |
| ☐ Firewall: Portscan |

| Service: Mail |
|---|
| ☐ Monatsreport: Mail |
| ☐ Exchange |
| ☐ Exchange Online |
| ☐ Mailsignatur: CodeTwo Signatur |
| ☐ Mailgateway: Barracuda E-Mail Gateway Defense |
| ☐ Mailarchiv: Message Archiver |
| ☐ Backup: Daten aus M365 |
| ☐ Restore: Daten aus dem M365-Backup |

| Service: ECM |
|---|
| ☐ Monatsreport: ECM |
| ☐ baramundi: Überwachung |
| ☐ baramundi: Bericht |
| ☐ Pflege bMS |
| ☐ Windows & O365 Updates |
| ☐ Virenschutz |
| ☐ Compliance: Mails |
| ☐ Compliance: Check |
| ☐ Compliance: Bericht |
| ☐ Pflege der kundenspezifischen Software |

| Service: SIEM |
|---|
| ☐ Monatsreport: SIEM |
| ☐ Sentinel: Check |
| ☐ Sentinel: Rules aktualisieren |
| ☐ Sentinel: Bericht |
| ☐ Sentinel: Agent Update |
| ☐ Sentinel: Berichtstellung von eingehenden Meldungen |
| ☐ Sentinel: Überprüfung Logserver |
| ☐ Softwarepflege: Kiwi Syslogserver |
| ☐ Unterstützung: Incident Response |
| ☐ Unterstützung: Phishing-Alert |



# Service: Infrastruktur

Für den Betrieb von Anwendungssoftware spielt die Verwendung von materieller sowie auch immateriellen Gütern eine immense Rolle. Hierbei kommt es vor allem auf die kombinierten Komponenten, die für Betrieb und Management von unternehmensspezifischen IT-Services und IT-Umgebungen nötig sind an. Demnach ist es unerlässlich, dass eine entsprechende Betreuung der entsprechenden Systeme stattfindet: dies betrifft die **Netzwerk-Infrastrukturdienste** (u.a., Switche, AccessPoints, Management-Tools, …), **Virtualisierungslösungen** (entweder via noris vDatacenter oder als on-Prem Hardware inkl. **Backup-Lösung**) sowie die nötigen **Linux-Server**.

Zur Unterstützung bietet BAGHUS folgende Service-Optionen an, die sich aktuell standardmäßig im Leistungsumfang des Service Infrastruktur befinden:

## Monatsreport: Infrastruktur

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Ticketübersicht der im Monat angefallen Tätigkeiten
- Ticketübersicht der im Monat durchgeführten SLA-Leistungen
- Review und Übermittlung Komponentenverzeichnis

## Backupsystem: Kontrolle

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Kontrolle
  - der Sicherung in Veeam B&R
  - der Kopien der Sicherung in Veeam B&R
  - ggf. der Tape-Sicherung in Veeam B&R
  - ggf. des Status des Cleaning-Tapes
  - ggf. der vCenter Sicherung

## Backupsystem: Software

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Updates in Veeam B&R kontrollieren

## Backupsystem: Hardware

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Kontrolle
  - des iLO Eventlog Backupserver
  - des Systemzustands der Backupserver
  - der Versionen von iLO, SystemROM und weiteren Komponenten
  - des Systemzustands der TapeLibrary
  - der Versionen von TapeLibrary und Bandlaufwerk

## Backupsystem: Storage

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfen
  - des Systemzustands der Hardware
  - der Logfiles
  - auf Updates

## Backupsystem: Bändertausch

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Bänder tauschen
- Alte Bänder als „im Tresor“ markieren
- Neue Bänder als „Frei“ markieren

## Backupsystem: Restoretest

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Virtueller Server mit erstelltem Backup wiederherstellen (exemplarisch)
- vCenter mit erstelltem Backup wiederherstellen (exemplarisch)

## Virtualisierung: VMware Software

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfen
  - des Systemzustands der Hardware der vSphere Hosts
  - der Logfiles der vSphere Hosts
  - der Logfiles der vCenter
  - auf Updates für VMware vSphere
  - auf Updates für vCenter
  - der VMware-Tools

## Virtualisierung: VMware Hardware

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfen
  - der iLO-Eventlogs
  - der Integrated Management Logs
  - der Version von iLO und System ROM
  - einzelner Komponenten, u.a.
    - des Processors
    - der Memory
    - des Network
    - das Device Inventory
    - das Local Storage

## Virtualisierung: VMware Storage

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Alerts und Bestätigung dieser
  - der Capacity
  - des Volumes
  - der Disks
  - der Performance
  - der Activities
  - der Version der Storage und Disks auf Updates

## Netzwerk: Switch Hardware

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Erstellung eines Backups
- Überprüfung
  - des Systemzustands der Hardware
  - der Logfiles und des Status
  - auf Updates

## Netzwerk: Switch Restoretest

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Durchführung eines Restoretest

## Netzwerk: WLAN-Hardware

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung der Version der Firmware

## Netzwerk: WLAN-Kennwörter

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Änderung der WLAN-Kennwörter

## Linux: DokuWiki

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der DokuWiki Version
  - der Logfiles
  - des Betriebssystems
  - des freien Speichers

## Linux: Seafile

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Seafile Version
  - der Logfiles
  - des Betriebssystems
  - des freien Speichers

## Hardware: USV-System

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Logfiles
  - des Updatestatus
  - der Batterielaufzeit

# Service: Windows-Server

Windows-Server sind auf die gemeinsame Nutzung von Diensten durch mehrere Benutzer und die umfassende administrative Kontrolle von Datenspeichern, Anwendungen und Unternehmensnetzwerken ausgelegt. Daher umfasst dieser Service die Betreuung der gängigsten **Microsoft-Infrastrukturdienste** (Verzeichnisdienst, Windows-Server, Datenbanken etc.), ergänzt um regelmäßige Maßnahmen zur **Absicherung des Verzeichnisdienstes und der Identitäten**. Die Betreuung eines **Passwortmanagers** und des **Monitorings** runden das Paket ab.

Zur Unterstützung bietet BAGHUS folgende Service-Optionen an, die sich aktuell standardmäßig im Leistungsumfang des Service Windows-Server befinden:

## Monatsreport: Windows-Server

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Ticketübersicht der im Monat angefallen Tätigkeiten
- Ticketübersicht der im Monat durchgeführten SLA-Leistungen
- Review und Übermittlung Komponentenverzeichnis
- Adminkonzept/Tätigkeitsbeschreibung
    - Tätigkeiten in Form eines Excel
    - Übersicht von noris
    - Azure Report
- Monitoringergebnisse
- Prüfung der Einhaltung des Löschkonzepts bzgl. Domänencontroller

## Root-Domain: Windows

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- DNS
  - Überprüfung Status und Logs
  - Test der DNS-Objektreplikation
- Replizierung
  - Überprüfung Status und Logs
  - Test der AD-Objektreplikation
- Überprüfung Status und Logs des NTP-Service (Zeitservice, Taktgeber für die Domäne)
- AD-Schema
  - Schema-Version auf Aktualität hin überprüfen
  - Ggf. erweitert um die Initiierung einer Aktualisierung
- Enterprise CA (interne Zertifizierungsstelle)
  - Prüfen auf abgelaufene Zertifikate und Bereinigung dieser
  - Prüfen auf fehlgeschlagene Zertifikatsanforderungen und ggf. Bereinigen dieser
  - Prüfen der von der CA generierten Logdaten
- Anfertigung manuelles Backup Enterprise CA mit allen relevanten Daten, um Enterprise CA wiederherstellen zu können

## Root-Domain: DCs

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

Überprüfung der von Windows auf dem AD-Service generierten Logs auf Auffälligkeiten. Abgleich mit kundenspezifischen „Known-Issues“.

- Anwendungsprotokoll
- Systemprotokoll
- Directory-Service-Protokoll
- DFS-Replikation in Hinblick auf Sysvol-Replizierung
- Active Directory Webdienste

## Root-Domain: Member-Server

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

Überprüfung der von Windows generierten Logs auf Auffälligkeiten. Abgleich mit kundenspezifischen „Known-Issues“.

- Anwendungsprotokoll (Windows-Dienste, Dienste RDS-Hosts, Fileserver/DFS)
- Systemprotokoll

## Backup: DC-Backup mit MARS-Agent

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Kontrolle des Backups bezüglich System-State und File-System.
- Turnusmäßiger Testrestore von Dateien auf dem Sysvol
- Dokumentation des Ergebnisses

## Restoretest: DC-Backup mit MARS-Agent

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Turnusmäßiger Testrestore von Dateien auf dem Sysvol
- Dokumentation des Ergebnisses

## Softwarepflege: MARS-Agent

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfen der Software auf Aktualität
- Bei Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## Backup: MS SQL-Datenbanken mit SQLBackupAndFTP

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfen Status täglicher Datensicherung von MS SQL-Datenbanken
- Turnusmäßiger Testrestore einer Datenbank
- Dokumentation der Ergebnisse

## Restoretest: MS SQL-Datenbanken mit SQLBackupAndFTP

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Turnusmäßiger Testrestore einer Datenbank
- Dokumentation der Ergebnisse

## Softwarepflege: SQLBackupAndFTP

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfen der Software auf Aktualität
- Bei Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## Monitoring: PRTG

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfung des Lizenzstatus
- Prüfung Updatestatus und ggf. Initiierung einer Aktualisierung
- Prüfung Betriebsstatus/Zustand

## MS SQL

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Ergebnisse und Logs MS SQL-Server
  - des Updatestatus MS SQL-Server und MS SQL-Management Studio
  - Backupstatus (Gegenprüfung zum Backup)
  - Datenbankintegrität
- Bei vorliegenden Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## MS SQL Express

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung des Updatestatus
- Bei vorliegenden Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## MS SQL Advanced

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Ergebnisse und Logs MS SQL-Server
  - des Updatestatus MS SQL-Server und MS SQL-Management Studio
  - Backupstatus (Gegenprüfung zum Backup)
  - Datenbankintegrität
- Bei vorliegenden Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## Azure AD Connect

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - des Synchronisierungsstatus
  - der Ereignisse und Logs
  - des Updatestatus
- Bei vorliegenden Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## Password Safe

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Ereignisse und Logs
  - des Updatestatus
  - des Backups (Gegenprüfung zum Backup)
- Bei vorliegenden Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## Regelmäßiger Wechsel lokaler Adminkennwörter auf den Servern und für Servicekonten

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Kontrolle der letzten Kennwortänderung durch Local Administrator Password Solution (LAPS) oder baramundi Script
- Manuelle Änderung von Kennwörtern
  - für Windows-Server außerhalb einer Domäne (z. B. DMZ-Server in einer Workgroup)
  - für verwendete Servicekonten und Durchführung der mit dem Kunden abgestimmten Nacharbeiten
- Dokumentation der Kennwörter und sicheres Verfahren für Notfälle

## Defender for Identity

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Agent-Version auf Aktualität prüfen
- Berichte erstellen und ggf. noch offene Warnungen auswerten
- Auswertung Microsoft Sicherheitsbewertung mit Quelle „Defender for Identity“
- Evaluierung von Neuerungen im Service, welche für Kunden relevant sein können und entsprechende Kommunikation von eventuell notwendigen Anpassungen

## Active Directory Hardening: Analyse AD und Azure AD auf aktuelle Best-Practices

Vorbemerkung: um diese Service-Option beziehen zu können ist seitens des Kunden zum einen die Beteiligung an einer Softwarelizenz für die Analyse nötig. Zum anderen wird ein vorgelagerter Workshop bzgl. AD-Hardening und eine initiale Umsetzung der ermittelten Maßnahmen durchgeführt.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Analyse AD und Azure AD auf aktuelle Best-Practices
- Dokumentation des Status, Beurteilung und Kommunikation von eventuell notwendigen Anpassungen

## Active Directory Hardening/Tiering: Überprüfungen von Kontrollbeziehungen und möglicher Angriffspfade

Vorbemerkung: um diese Service-Option beziehen zu können ist ein vorgelagerter Workshop bzgl. AD-Hardening und AD-Tiering nötig sowie eine initiale Umsetzung der ermittelten Maßnahmen.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

Regelmäßige Überprüfungen von Kontrollbeziehungen im Active Directory, u.a.

- Erkennung potenzieller Lateral-Movement-Pfade
- Erkennung von GPOs die Sicherheit/Integrität des Tiering/Hardening gefährden
- Validierung und Einhaltung des Tier-Modell
- Pflege der Alarmmechanismen für Änderungen an sensiblen Konten/Gruppen
- Bericht über den Status und ggf. Initiierung weiterer Verbesserungen

## Active Directory Hardening: Von Benutzer und Administratoren genutzte Kennwörter auf Kompromittierung und Qualität prüfen

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

Regelmäßige Überprüfung der im AC von den Benutzern und Administratoren verwendeten Kennwörter:

- Abgleich mit aktuellen Passwortlisten mit kompromittierten Kennwörtern
- Überprüfung
  - der Passwortqualität
  - auf Verwendung gleicher Kennwörter, z. B. für Benutzer- und Adminkonten
- Bericht über den Status und ggf. Initiierung weiterer Verbesserungen

## KRBTGT-Kennwort regelmäßig ändern

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

Änderungen des „KRBTGT“ Kennworts.

## NPS: Network Policy Server

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfen, ob ein Update oder technische Neuerungen vorliegen
- Überprüfung der Gültigkeitsdauer von Zertifikaten
- Systemstatus mit „health check script“ prüfen und dokumentieren

## Überprüfung Windows Firewall auf den Servern

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Durchführung Portscan in den Servernetzen, einschl. DMZ
- Abgleich der Ergebnisse (Portstatus) mit Dokumentation Windows-Firewall für alle Windows-Server

## Kundenspezifische Software: FineKey KeyWatcher

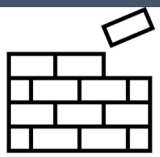
*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfung Windows IoT auf Updates
- Prüfung FineKey auf Updates

## Kundenspezifische Software: RDP

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfung Windows RDP Status (einschließlich Lizenzstatus)



# Service: Firewall

Eine Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Umso wichtiger ist es diesen Fluss entsprechend zu schützen und abzusichern. Dementsprechend ist die **Wartung und Pflege der Firewall-Systeme**, inklusive einem **Backup-System** oder auch eines **MultiFaktor-Systems** wie RSA nötig. Erweitert wird der Schutz durch eine **regelmäßige Prüfung der geöffneten Ports und Systeme** der Firewall-Anschlüsse.

Zur Unterstützung bietet BAGHUS folgende Service-Optionen an, die sich aktuell standardmäßig im Leistungsumfang des Service Firewall befinden:

## Monatsreport: Firewall

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Ticketübersicht der im Monat angefallen Tätigkeiten
- Ticketübersicht der im Monat durchgeführten SLA-Leistungen
- Review und Übermittlung Komponentenverzeichnis
- Report einer logischen Netzwerkübersicht
- Übersicht der blockierten Länder in der Firewall

## Firewall: Restoretest

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Firewall mit erstelltem „*.PCA“-Backup-File wiederherstellen (exemplarisch)

## Firewall: Rechenzentrum

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Erstellung eines Backups
- Überprüfung
  - der Firmwareversion
  - der Lizenz
  - der Events sowie deren Bereinigung
  - des Systemstatus
  - der VPN-Verbindungen
  - der Firewall und IPS

## Firewall: Außenstandort

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Erstellung eines Backups
- Überprüfung
  - der Firmwareversion
  - der Lizenz
  - der Events sowie deren Bereinigung
  - des Systemstatus
  - der VPN-Verbindungen
  - der Firewall und IPS

## Firewall: Control Center

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Erstellung eines Backups
- Überprüfung
  - der Firmwareversion
  - der Lizenz
  - der Events sowie deren Bereinigung
  - des Systemstatus
- Im Downloadportal nach neuer Software suchen

## RSA

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - Version des RSA-Servers
  - des Zertifikatsstatus
  - des Linux Status

## Firewall: Portscan

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Kontrolle der externen Anschlüsse der einzelnen Firewalls auf offene Ports
- Überprüfung
  - der Events und deren Bereinigung
  - des Systemstatus

# Service: Mail

E-Mails gelten immer noch als eines der wichtigsten Kommunikationsmittel und sind gleichzeitig ein Einfallsweg für Malware. Ransomware, Phishing, virenversuchte Attachments und Spam sind konkrete Bedrohungen für die IT-Sicherheit. Um die Mail-Übertragungen absichern zu können unterstützt dieser Service durch **Dienstleistungen an Systemen**, die in einem modernen **Mailkonstrukt von Microsoft** benötigt werden. Abgerundet wird dies durch Produkte von Drittanbietern, u.a. in den Bereichen **zentral gesteuerte Mailsignaturen, Datensicherung, E-Mailarchivierung.**

Zur Unterstützung bietet BAGHUS folgende Service-Optionen an, die sich aktuell standardmäßig im Leistungsumfang des Service Mail befinden:

## Monatsreport Mail

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Ticketübersicht der im Monat angefallen Tätigkeiten
- Ticketübersicht der im Monat durchgeführten SLA-Leistungen
- Review und Übermittlung Komponentenverzeichnis
- ATP-Log vom Mailsecurity Gateway
- Prüfung der Einhaltung des Löschkonzepts bzgl. Message Archiver

## Exchange

Vorbemerkung: es werden nur Exchange-Installationen betreut, welche in einer hybriden Umgebung lokal ausschließlich zur Benutzerverwaltung genutzt werden und keine weiteren Dienste bereitstellen.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der lokalen Exchange Installationen auf Updates
  - der Adminlogs
- Bei vorliegenden Updates Beurteilung und ggf. Initiierung einer Aktualisierung

## Exchange Online

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Kapazitätsauslastung
  - der Adminlogs
  - auf eingerichtete Weiterleitungen
- Bericht über zugriffsberechtigte Benutzer auf Shared-Mailboxen für einen Review durch Datenverantwortliche

## Mailsignatur: CodeTwo Signatur

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung folgender Parameter
  - Betriebsstatus
  - Lizenzstatus
  - Prüfen auf Ankündigungen von Änderungen durch den Hersteller für kundenspezifischen Tenant

## Mailgateway: Barracuda E-Mail Gateway Defense

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung des Betriebsstatus, u.a.
  - auf Ankündigungen von Änderungen durch den Hersteller für kundenspezifische Tenants
  - des Status der Anbindung am Verzeichnisdienst
- Überprüfung des Lizenzstatus
- Überprüfung der Ereignisse und Logs
  - Stichprobenartige Auswertung geblockter E-Mails, um ggf. Schutzmechanismen anzupassen
  - ATP-Log auf ungewöhnliche Häufungen von Bedrohungen prüfen
  - Admin-Audit-Log zur Plausibilisierung von Konfigurationsänderungen

## Mailarchiv: Barracuda Message Archiver

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
  - der Ereignisse und Logs
  - des Betriebsstatus
  - des Updatestatus
  - des Lizenzstatus

## Backup: Daten aus Microsoft 365

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Kontrolle des Ergebnisses der täglichen Datensicherung von Kernservices, u.a.
  - SharePoint
  - OneDrive
  - Exchange Online
  - MS Teams

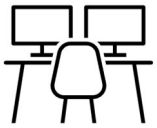
Sollte Veeam Backup for Microsoft 365 zum Einsatz kommen werden zusätzliche Tätigkeiten durchgeführt:

- Kapazitätsplanungen
- Prüfen auf Updates

## Restore: Daten aus Microsoft 365-Backup

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Testweise Wiederherstellung Objekten aus M365, u.a.
  - SharePoint
  - OneDrive
  - Exchange Online
  - MS Teams
- Dokumentation der Ergebnisse



# Service: Enterprise Client Management (ECM)

Der methodische Ansatz aller Maßnahmen zur Verwaltung und Steuerung der dezentralen IT-Infrastruktur (u.a., Arbeitsplatzrechner, Clients, Notebooks, Handys) unterstützt Unternehmen bei der Etablierung und des Erhalts eines unternehmensweit geltenden Standards. Hierzu zählen insbesondere die Verteilung und Installation von Software oder Betriebssystemen. Der Service ECM soll sicherstellen, dass BAGHUS durch die eigene Kompetenz die Weiterentwicklung des Kunden umfänglich unterstützen kann.

Vor allem durch den **Einsatz, die Pflege und Wartung** des baramundi Tools und die kontinuierliche Überarbeitung zum Erhalt der festgelegten **Compliance** sollen Freiräume für die interne IT geschaffen werden, um sich somit besser auf das eigene Kerngeschäft konzentrieren zu können.

Vorab aber noch eine kurze Information bzgl. der Service-Optionen:

- baramundi: Überwachung
- baramundi/Compliance Bericht
- Compliance Mails

Hier besteht die Möglichkeit zwischen zwei Optionen zu wählen:

- **Option 1: Überprüfung und manuelle Freigabe**
  Die Überprüfung und Meldung anfallender Tätigkeiten finden durch den Auftragnehmer statt. Zur Bearbeitung der Tätigkeiten und aufwandsbezogenen Abrechnung wird die Freigabe des Auftraggebers benötigt.

- **Option 2: Überprüfung und automatische Freigabe**
  Die Überprüfung und Meldung anfallender Tätigkeiten finden durch den Auftragnehmer statt. Die Bearbeitung der Tätigkeiten wird automatisch eingesteuert und aufwandsbezogen abgerechnet.

Zur Unterstützung bietet BAGHUS folgende Service-Optionen an, die sich aktuell standardmäßig im Leistungsumfang des Service ECM befinden:

## Monatsreport: ECM

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Ticketübersicht der im Monat angefallen Tätigkeiten
- Ticketübersicht der im Monat durchgeführten SLA-Leistungen
- Review und Übermittlung Komponentenverzeichnis
- Report über die Virenschutz Logins

## baramundi: Überwachung

Diese Service-Option kann entweder mit Option 1 oder Option 2 bezogen werden.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
    - der Jobs auf Fehler, sowohl allgemein als auch speziell MSW und updatebezogene Jobs
    - von dynamischen Gruppen, u.a.
        - Office 365 Versionsnummer
        - Microsoft fehlende Sicherheitspatche Server/Clients
        - Updateinventur älter 14 Tage bzw. keine vorhanden
        - Last Contact > 30 Tage
        - Kein Virenschutz installiert (z.B. ApexOne/TrendMicro)
        - usw.
    - baramundi Service und DIP
- baramundi Katalog Downloads prüfen

## baramundi: Bericht

Diese Service-Option kann entweder mit Option 1 oder Option 2 bezogen werden.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Dieser Bericht enthält u.a. folgende Punkte
    - Ausgabe aktueller Patch- und Softwarestände der betreuten Systeme
    - Windows Release IDs
    - Letzter Kontakt
    - Windows-Update-Zustand
    - Bitlockerverschlüsselungen
    - usw.

## Pflege bMS

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Managed Software prüfen auf ältere Versionen
- BAGHUS managed SW aktualisieren (u.a. MS Teams, MS OneDrive, Plantronics Hub, Nvidia Treiber, TeamViewer aus MSW, etc.)
- Deaktivierte Clients prüfen
- Bereinigen von baramundi Patchmanagement
- Kontrolle baramundi Gateway
- baramundi Version
    - auf neue Releases überprüfen
    - updaten, wenn eine neue Version verfügbar ist
- Mobile Devices prüfen (Betriebssystemversion)

## Windows & O365 Updates

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Sicherstellung
    - des Updateprozesses für Windows & O365 Updates
    - der Verfügbarkeit der Quellen
- Pflege der dynamischen Gruppen

## Virenschutz

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
    - der Virenschutzversion auf verfügbare Updates
    - der Aktualität und Erreichbarkeit der Agents auf verwalteten Systemen

## Compliance: Mails

Diese Service-Option kann entweder mit Option 1 oder Option 2 bezogen werden.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Laufende Überwachung und Qualifizierung von eingehenden CVE und sonstige Informationen über Sicherheitslücken aus den verfügbaren Quellen
- Ableitung von etwaig notwendigen Maßnahmen
- Bereitstellung der Informationen

## Compliance: Check

Vorbemerkung:

- diese Service-Option kann
  - nur in Zusammenhang mit Option 2 bezogen werden
  - nur bezogen werden, wenn in baramundi das Compliance Modul zusätzlich gebucht wurde

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfen, erhalten und verbessern des Compliance Scorings
- Erstellung und Prüfung eigen erstellter Standards mit eigenen Konfigurationsregeln

## Compliance: Bericht

Vorbemerkung:

- Diese Service-Option kann
  - entweder mit Option 1 oder Option 2 bezogen werden.
  - nur bezogen werden, wenn in baramundi das Compliance Modul zusätzlich gebucht wurde

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

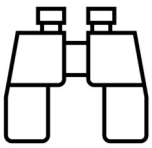
- Bericht über vorhandene Sicherheitslücken
- Erweiterung um u.a. folgende Punkte
  - CVE-Meldungen
  - Aufbereitung, zur besseren Übersicht
  - Compliance Scoring
  - usw.

## Pflege der kundenspezifischen Software

Vorbemerkung: mit Bezug dieser Service-Option wird vorab eine kundenspezifische Softwareliste erarbeitet, die als Grundlage bei der Überprüfung dient.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Prüfen der Verfügbarkeit neuer Softwareversionen anhand der kundenspezifischen Softwareliste



# Service: Security Information and Event Management (SIEM)

Ein SIEM kombiniert die zwei Konzepte Security Information Management und Security Event Management für die Echtzeitanalyse von Sicherheitsalarmen aus einer Vielzahl von Quellen. Hierbei handelt es sich um ein einzelnes Security-Management-System, das volle Sichtbarkeit und Transparenz zu Aktivitäten innerhalb eines Netzwerks bietet. Somit kann in Echtzeit auf Bedrohungen reagiert werden, um die Einhaltung der Compliance-Anforderungen sicherzustellen. Vor allem die kontinuierliche **Überprüfung und Wartung der Systeme** soll diesen Prozess der allumfänglichen Absicherung bestärken.

Zur Unterstützung bietet BAGHUS folgende Service-Optionen an, die sich aktuell standardmäßig im Leistungsumfang des Service SIEM befinden:

## Monatsreport: SIEM

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Ticketübersicht der im Monat angefallen Tätigkeiten
- Ticketübersicht der im Monat durchgeführten SLA-Leistungen

## Sentinel: Check

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Regelmäßige Prüfung der Vollständigkeit des SIEM-Systems

## Sentinel: Rules aktualisieren

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Regelmäßige Aktualisierung der Analytic Rules des SIEM-Systems
- Dokumentation der angepassten Rules

## Sentinel: Bericht

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Regelmäßiges Reporting der im Sentinel angebundenen Systeme
- Einarbeitung der Dokumentation
    - der monatlichen Rules-Anpassungen
    - welche Updateversion momentan eingesetzt wird

## Sentinel: Agent Update

Vorabinformation: Weitergabe der Update-Informationen für Systeme außerhalb der Betreuung durch BAGHUS liegt in Kundenverantwortung

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung auf anstehende Updates seitens Windows und Linux
- Initialisierung durch Benachrichtigung an Kunden
- Aufwandsbezogene Bearbeitung (analog Option 2 Service ECM)

## Sentinel: Berichtserstellung von eingehenden Meldungen

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Berichterstellung über die eingegangenen Meldungen des externen SOC-Team
- Aufbereitung enthält unter anderem
    - Reaktionszeiten
    - Lösungszeiten
    - Ticketbeschreibungen
    - Lösungsbeschreibungen

## Sentinel: Überprüfung Logserver

Linux-Server mit Syslog und Anbindung an Sentinel.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
    - der Logs
    - des freien Speichers
    - auf Updates

## Softwarepflege: Kiwi Syslogserver

Windows-Server mit Syslog

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Überprüfung
    - der Logs
    - auf Updates

## Unterstützung: Incident Response

Alle anfallenden Tätigkeiten werden aufwandsbezogen verrechnet.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

Wenn bei einem Verdacht oder Vorfall ein Serviceobjekt der BAGHUS (siehe Systemliste des jeweiligen Services) betroffen ist, unterstützt die BAGHUS den Kunden wie folgt:

- Überprüfung der Logdateien
- Zusammen mit dem organisatorischen Ansprechpartner des Kunden Informationen über das Ereignis aufarbeiten, damit diese durch den Kunden an dessen Cybersecurity-Versicherung übergeben werden können
- Koordination und Einplanung mit deren Spezialisten über erforderliche Tätigkeiten

## Unterstützung: Phishing-Alert

Alle anfallenden Tätigkeiten werden aufwandsbezogen verrechnet.

*Die Tätigkeiten dieser Service-Option ergeben folgenden Leistungsumfang:*

- Unterstützung nach einer Meldung des Kunden
- Überprüfung des Vorfalls
- Ableitung anfallender Tätigkeiten die zur Behebung nötig sind