

# QIT Backupserver Bergfried



Unser Bergfried ist die moderne Lösung zur Langzeitsicherung in der bildgebenden Medizin: Stark verschlüsselte, unveränderbare Datenstände, geeignet für große Datenmengen und zusätzlich als Veeam® immutable Repository für Ihre virtuellen Maschinen nutzbar. Das System ist für höchste Sicherheit vollständig autark und vom normalen Praxisnetzwerk getrennt. Darüber hinaus ist es für Ihre IT komplett wartungsfrei. Wir unterstützen bei der Erstellung und Pflege Ihres Backup-Konzepts.

## VOLLWARTUNG UND ÜBERWACHUNG INKLUSIVE

Verwaltung und Systempflege erfolgt ausschließlich über unsere VPN-Infrastruktur und unsere mitgelieferte Verwaltungsbox, die via VPN mit unserem Backend verbunden ist. Dadurch wird maximale Sicherheit möglich: Kein Internet, keine Verbindungen vom lokalen Netz (zu sichernde Daten werden von Ihren Systemen abgeholt). Hardware und System-Logs werden ständig von uns überwacht. Bergfried bleibt dauerhaft vom Internet getrennt und für Angriffe im Praxisnetz praktisch unerreichbar.

## SICHER UND ZUVERLÄSSIG

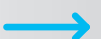
Bergfried basiert auf einem extrem abgesicherten Linux-System mit redundanter, selbst korrigierender und verschlüsselter Datenspeicherung sowie fortlaufend geprüfter Hardware. Wir überwachen Ihre Backups während der gesamten Lebenszeit und achten auf Veränderungen (z.B. Platz wird knapp, Backupzeiten reichen nicht mehr, Hardware-Lebensdauer nähert sich dem Ende, Temperatur weicht ab...).

## MASSGESCHNEIDERTES BACKUP-KONZEPT

Unsere Lösung umfasst nicht nur den Server selbst, sondern auch eine individuelle Beratung und Unterstützung bei der Erstellung, Umsetzung und Pflege Ihres Backup-Konzepts sowie die passende Dimensionierung der Bergfried-Hardware. Bergfried ist leistungsstark und kann bei Bedarf Daten sofort zurück liefern. Es ist auch möglich, eine weitere Kopie der Daten auf Bänder oder einem zweiten externen Bergfried zu erstellen.

## LEISTUNGSMERKMALE BACKUPSERVER BERGFRIED

- ✓ Maßgeschneidertes, dokumentiertes Backup-Konzept
- ✓ Über VPN und Verwaltungsbox voll administriert und überwacht, kein Wartungsaufwand für Sie
- ✓ Kein Internetzugang, keine Erreichbarkeit in Ihrem Netz, Datenverschlüsselung gegen Diebstahl
- ✓ Gehärtetes Linux-System nach CIS server level 2, restriktive Firewall aus- und eingehend
- ✓ Bergfried holt Daten aktiv von konfigurierten Quellen in Ihrem Netz
- ✓ Unveränderbare Datenstände (z.B. 30 Tage, 12 Monate, 5 Jahre)
- ✓ Option Veeam® *Immutable Repository* zur Sicherung Ihrer virtuellen Maschinen



## INFORMATIONEN FÜR SPEZIALISTEN



### FLEXIBLES SPEICHERVOLUMEN

Je nach Datenmenge und Anforderungen an die Sicherung – insbesondere die Anzahl der Stände bei dynamischen Datenbeständen – stehen verschiedene Größen des Bergfrieds zur Verfügung. Spätere Erweiterungen sind ebenfalls möglich. Wir ermitteln die passende Hardwareausstattung für Ihr Backup-Konzept.



### BACKUPKONZEPT INKLUSIVE

Wir unterstützen mit konkreten Vorlagen und *best-practice* Erfahrungen bei der Erstellung und Pflege eines Backup-Konzeptes wie es für jede kritische Infrastruktur erforderlich ist. Wir übernehmen hierfür Betriebsverantwortung und Sie erhalten tägliche Status-E-Mails. Dadurch wird Bergfried zu einem Backupsystem, das Ihre IT spürbar entlastet.



### VEEAM® IMMUTABLE REPOSITORY

Bergfried kann als sicherer *Veeam® Immutable Repository-Server* genutzt werden. Wir führen die Installation so durch, dass eine zertifikatgesicherte Kommunikation Ihres Veeam®-Servers zum Repository besteht. Wir unterstützen bei der Konfiguration Ihrer Veeam®-Backups und überwachen das Repository. Die Erreichbarkeit des Veeam®-Ports am Bergfried ist auf Ihren Veeam®-Server und die zuvor festgelegten Zeitslots begrenzt, um die Sicherheit weiter zu erhöhen.



### GEHÄRTETES LINUX

Das Serverbetriebssystem ist nach den Richtlinien des *Center for Internet Security (CIS server level 1, 2)* konfiguriert. Verwaltung, Überwachung und Updates erfolgen ausschließlich über ein gesichertes QIT Verwaltungs-VPN. Der Bergfried ist praktisch vollständig von den Netzwerken der Praxis getrennt: Nur für das Abholen von Daten öffnet die Firewall einzelne, stets nur ausgehende Ports. Snapshots der stark verschlüsselten Datenbestände sind für die unterprivilegierten Sicherungsprozesse unerreichbar.



### AKTIVE ABHOLUNG DER DATEN

Um maximale Sicherheit selbst in einem kompromittierten Netzwerk zu gewährleisten, lässt Bergfried keine eingehenden Netzwerkverbindungen zu (ggf. mit Ausnahme Ihres Veeam®-Backups). Statt dessen holt er regelmäßig Daten von Systemen in Ihrem Netzwerk ab. Zeitpunkte und verwendete Protokolle gibt das Backupkonzept vor, typisch sind Windows- oder *nfs*-Netzlaufwerke, sowie *rsync*-Server. Da von den kopierten Daten komplette Stände unveränderbar gesichert werden, bleiben beispielsweise auch im Original gelöschte oder bösartig verschlüsselte Daten verfügbar.



### BERGFRIED IST OFFLINE

Durch die komplette Schließung eingehender Ports am Bergfried ist dieser nur über das QIT VPN für Administration und Pflege erreichbar. Ausgehend schickt Bergfried Diagnose- und Statusdaten über eine gesondert gesteckte Verbindung zu unserer Verwaltungseinheit. Diese führt auch das Monitoring durch und ist ihrerseits nur über unser VPN erreichbar. Beide Verbindungen sind zertifikatbasiert und mit Zwei-Faktor-Authentifizierung abgesichert. In Hardware-Schadensfällen und für Neustarts (die mehrere manuelle Passworteingabe erfordern) können wir das System über die Verwaltungseinheit erreichen. Die Kombination dieser Eigenschaften macht den Bergfried in Ihrem LAN nahezu unangreifbar.

## QIT Systeme GmbH

Franz-Vollhard-Straße 5  
68167 Mannheim  
Deutschland

TEL +49 621 300 114 - 0  
FAX +49 621 300 114 - 99  
MAIL [info@qit-systeme.de](mailto:info@qit-systeme.de)  
WEB [www.qit-systeme.de](http://www.qit-systeme.de)