Sicherheitscheckliste Redmine

Mit wenig Aufwand sicherer Arbeiten

ALPHANODES

Gefahr / Risiko: Zugriff von außen durch unbefugte Dritte	
Maßnahme	**Umgesetzt?**
Mit stets aktueller Softwareversion arbeiten	☐
Redmine- und Systemupdates regelmäßig und zeitnah einspielen	☐
Redmine Anwendung über HTTPS Protokoll laufen lassen	☐
Redmine mit Apache HTTP Server absichern:	
• Zugang zur Redmine Administrationsoberfläche mittels Apache limitieren	☐
• Einsatz von „Fail2Ban“ um Loginversuche zu limitieren	☐
Sicheres Administratorkennwort verwenden und regelmäßig aktualisieren	☐
Link zur Redmine Instanz aus dem Suchmaschinenindex ausschließen	☐
Sicherheitsmonitoring für Redmine und Serverinstanz einsetzen um auffällige Aktivitäten schnell aufzudecken [1]	☐
Für die Anmeldung an Redmine die Option *„Authentifizierung erforderlich“* aktivieren	☐
Nur starke Passwörter erlauben. Hierzu Passwortmanager mit Passwortgenerator einsetzen [2]	☐
Option *„Erzwinge Passwortwechsel nach x Tagen“* für Redmine Anwender aktivieren	☐
Plugin Sicherheit:	
• Mit so wenig Plugins wie nötig arbeiten	☐
• Nur aktuelle, gepflegte Zusatzplugins aus vertrauenswürdigen Quellen installieren	☐
• Plugin Updates regelmäßig und zügig einspielen	☐
Gefahr / Risiko: Zugriff von innen durch unbefugte Mitarbeiter	
Maßnahme	**Umgesetzt?**
Benutzerrechte und Rollen richtig konfigurieren / Konfiguration regelmäßig prüfen	☐
Zugriffe ausgeschiedener Mitarbeiter sperren	☐
Anzahl an Administratoren streng limitieren (z.B. max. 3). Nicht jeder PM braucht auch Administratorrechte / -zugriffe	☐
Administratoren sollten für „normale“ Projektarbeiten einen eigenen Account mit weniger Rechten verwenden und solche Arbeiten nicht als „Admin“ übernehmen.	☐
Anzahl bestehender Administratoraccounts regelmäßig auf Notwendigkeit prüfen	☐
Gefahr / Risiko: Verlust von sensiblen Daten	
Maßnahme	**Umgesetzt?**
Ansprechpartner für den Notfall benennen	☐
Backup der Redmine Datenbankdateien erstellen	☐
Regelmäßige Security Audits einplanen für den Notfall:	
• Funktionsfähigkeit der Backup-Datei überprüfen	☐
• Fehlerfreies Einspielen des Backups testen	☐
• Festlegen wer hilft wann und wie	☐
• Festlegen wie der Schaden minimiert werden kann	☐

Die AlphaNodes GmbH ist Experte für **Open Source** und dem Multi-Projektmanagement Tool **Redmine**.
Das Unternehmen unterstützt Startups und Mittelstand optimal bei der Digitalisierung von Geschäftsprozessen mit Redmine, denn es vereint vieles unter einem Hut.
Wir hosten und betreuen jede Redmine Infrastruktur auch InHouse. Mit Fokus: Sicherheit und Performance.
Das spart Kosten, sorgt für mehr Datensicherheit und entlastet die eigene IT Fachabteilung.

[1]) https://alphanodes.com/de/server-monitoring
[2]) https://alphanodes.com/de/redmine-passwords

Ein Service der
AlphaNodes GmbH
Bavariafilmplatz 3
D-82031 Grünwald bei München

https://alphanodes.com/de

– Version 1.0 vom 02.06.2017 –