REISSWOLF dok.suite.

IT-Sicherheit & -Technik

Inhalt

1. Für wen ist diese Dokumentation gedacht

Diese Dokumentation richtet sich an alle Partner und Kunden, die Informationen zum Betrieb, IT-Sicherheit und Datenschutz rund um dok.suite. benötigen. Wir haben uns bemüht, alle relevanten Fragen zum Themenkomplex hier zu beantworten. Sollten Sie darüber hinaus noch Fragen haben, stehen wir Ihnen natürlich gern zur Verfügung.

Die in diesem Dokument enthaltenen Informationen sind vertraulich zu behandeln! Die Inhalte dürfen genutzt werden, um

- im Rahmen einer Zusammenarbeit,
- eines gemeinsamen Projekts oder
- einer Neukunden-Akquise

Fragen zum Betrieb, der IT-Sicherheit oder des Datenschutzes zu beantworten und zu validieren.

2. Was ist dok. suite.?

- Ein webbasiertes, revisionssicheres digitales Archiv
- Eine Portallösung für den Dokumentenaustausch
- Auch als komfortable App für Android oder IOS von jedem Ort aus 24/7 verfügbar
- Eine Software als Dienstleistung - daher keine Investitionskosten für Hard- oder Software

3. Technische Betriebssicherheit im Rechenzentrum

Alle Komponenten in unserem Rechenzentrum sind redundant ausgelegt. Firewall, Server, Switche und die Backbone-Anbindung ans Internet sind jeweils mehrfach vorhanden.

Die Serverkomponenten (Festplatten, Netzteile etc.) verfügen über Hochverfügbarkeitstechnologie, die den unterbrechungsfreien Betrieb im Falle eines Ausfalls einer einzelnen Komponente sicherstellt.

Sämtliche Komponenten im Rechenzentrum und in den Servern unterliegen einem ständigen Monitoring und werden von uns überwacht, so dass Probleme frühzeitig erkannt werden können.

Unser Rechenzentrum verfügt über moderne Methoden zur Abwehr von DDoS-Angriffen. Gegen Brute-Force-Angriffe auf Benutzeraccounts sind automatische Account-Sperren eingerichtet. Die Systemkomponenten (Server) werden regelmäßig einer Schwachstellenanalyse unterzogen.

Das Rechenzentrum verfügt über eine redundante Stromzuführung, eine USV (unterbrechungsfreie Notstromversorgung) mit Batterie-Überbrückung für kurzfristige Stromausfälle und ein Diesel-Notstrom-Aggregat für längerfristige Stromausfälle.

Die Räume sind klimatisiert und mit einer Brandmeldeanlage sowie einer Gas-Feuerlöschanlage ausgestattet.

Der physische Zugang zu den Räumen des Rechenzentrums und der Hardware ist streng limitiert und unterliegt Personen-Zutrittskontrollen und einer ständigen Videoüberwachung.

Alle weiteren Details entnehmen Sie bitte der Anlage 1 (Technisch-organisatorische Maßnahmen nach Art. 32 Abs. 1 DSGVO) des Vertrags zur Auftragsdatenverarbeitung nach Art. 28 DSGVO. Hier

werden die unterschiedlichen Maßnahmen zur Zutritts-, Zugangs-, Zugriffskontrolle u.v.a. im Detail beschrieben.

4. Wartung und Verfügbarkeit

Für das Betriebssystem ist alle 4 Wochen ein Wartungsfenster vorgesehen, um Updates und Systemaktualisierungen einzuspielen. Sicherheitsrelevante, kritische Aktualisierungen werden bei Bedarf innerhalb eines Arbeitstages (mit deutschem Feiertagskalender) eingespielt.

Für die dok.suite.-Anwendung ist alle 3 Wochen ein Wartungsfenster vorgesehen, in dem die dok.suite.-Anwendung und seine Komponenten aktualisiert werden.

Jedes Wartungsfenster wird in der Zeit wird zwischen 22:00 Uhr und 05:00 Uhr MEZ geöffnet und hat im Normalfall eine Dauer von weniger als einer Stunde.

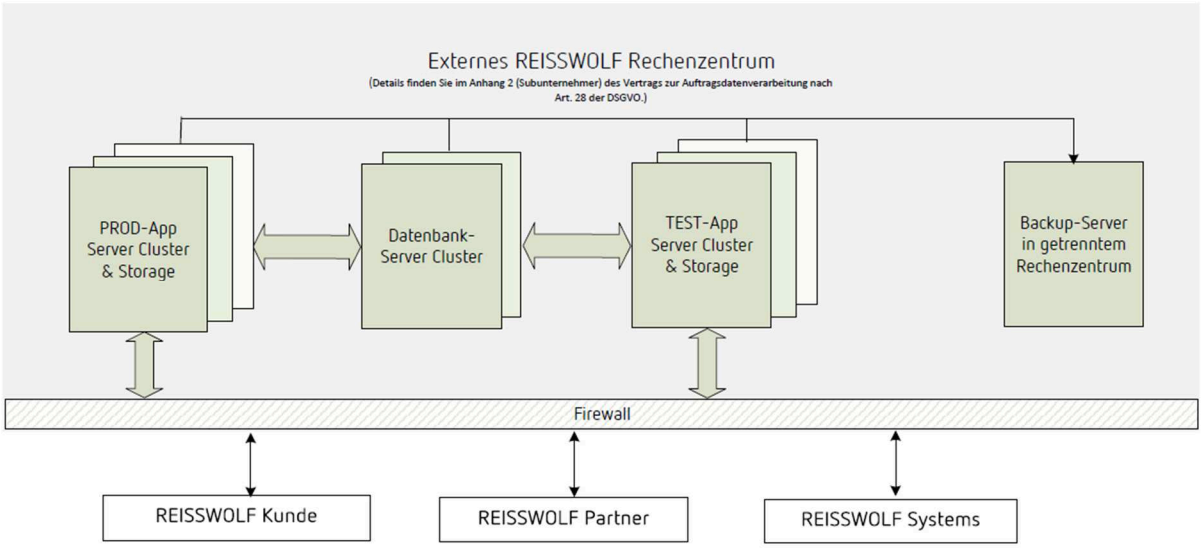
Eine regelmäßige automatisierte Schwachstellenanalyse wird auf allen von außen erreichbaren Servern durchgeführt. Der durchschnittliche Abstand zwischen den Schwachstellentests ist 4 Wochen. Die Ergebnisse und weitere Details der Schwachstellenanalyse finden Sie im Kapitel Ergebnisse der Schwachstellenanalyse (englisch) dieses Dokuments. Die Verfügbarkeit der Systeme soll durch die Tests nicht eingeschränkt werden.

Unabhängig von dem geplanten Wartungsfenster, gehen wir von einer Verfügbarkeit der Anwendung von 99,5% pro Monat aus.

Kennzahlen:

- Für die mittlere Dauer der Wiederherstellung des Systems nach einem Ausfall (Mean Time to Repair, MTTR) haben wir eine Stunde vorgesehen.
- Für den Betrieb von dok.suite. ist eine RPO-Zeit (Recovery Point Objective) von 24 Stunden definiert.
- Die RTO-Zeiten (Recovery Time Objective) sind mit einer Stunde definiert.

5. Architektur-Skizze des Rechenzentrum-Betriebes



6. Datensicherung & Backup

Die Anwendungs-, Datei-, und Datenbankserver werden stündlich gesichert. Zusätzlich erfolgt eine Komplettsicherung aller Maschinen alle 24 Stunden. Die Sicherungskopien der Datenbanken werden automatisiert an einem räumlich getrennten Ort abgelegt.

Aufbewahrungsfristen der Datensicherungen

Intervall	Dauer der Aufbewahrung
Stündliche Backups	24 Stunden
Tägliche Backups	14 Tage
Wöchentliche Backups	4 Woche
Monatliche Backups	12 Monate

7. Technische Datensicherheit

Die Server erzwingen für die Verbindung eine Transportverschlüsselung (TLS 1.2). Eine unverschlüsselte Verbindung zu unseren Servern ist nicht möglich.

Die Festplatten des Datenbank-Servers sind vollständig mit LUKS und einer Key-Länge von 256 Bit verschlüsselt.

Kundenindividuelle Richtlinien ermöglichen zusätzlich eine weitere Eingrenzung der Zugänge auf Basis von Netzwerkadressen oder Wochentagen und Tageszeiten.

Alle Passwörter von Benutzern werden in der Datenbank einwegverschlüsselt (BCRYPT-Verfahren) abgelegt und sind weder für den Kunden noch für REISSWOLF wieder auslesbar.

Passwörter haben Mindestanforderungen an die Komplexität wie z.B. Länge, nicht fortlaufende Zeichen und die maximale Gültigkeit und die maximale Anzahl von fehlerhaften Login-Versuchen (wobei die beiden zuletzt genannten individuell je Kunde eingestellt werden können). Eine Prüfung

auf wiederverwendete Passwörter erfolgt. Die letzten 5 Passwörter können nicht noch einmal verwendet werden.

Alle weiteren Details entnehmen Sie bitte der Anlage 1 (Technisch-organisatorische Maßnahmen nach Art.32 Abs. 1 DSGVO) des Vertrags zur Auftragsdatenverarbeitung nach Art. 28 DSGVO. Hier werden die unterschiedlichen Maßnahmen zur Zutritts-, Zugangs-, Zugriffskontrolle u.v.a. im Detail beschrieben.

Die Anwendung, die Datenbank und das Betriebssystem erzeugen automatisiert technische Log-Dateien, in denen die Aktivitäten der verschiedenen System-Komponenten protokolliert werden. Diese Log-Dateien werden mit statistischen Methoden überwacht.

Im Fall eines ungewöhnlichen Verhaltens oder eines Fehlers werden die Log-Dateien auf Detailebene untersucht und ausgewertet. Die Log-Dateien werden nach 30 Tagen automatisch überschrieben.

8. Benutzerverwaltung

Die normale Authentifizierung erfolgt mit Username und Passwort.

Eine erweiterte Sicherheit kann mit einem optionalen 2-Faktor-Authentisierung eingerichtet werden.

Zur Steuerung der individuellen Berechtigung eines Benutzers, gibt es ein Rollen-Konzept in der Benutzerverwaltung. Jeder Benutzer kann einer oder mehreren Rollen zugewiesen werden. Eine detaillierte Aufstellung der Funktionen, die an eine Rolle gebunden sind, ist im Admin-Handbuch der Anwendung beschrieben.

Dok.suite. bestätigt Auftragseingänge und informiert über den Fortschritt von Aufträgen per E-Mail. Voraussetzung für den Empfang von E-Mails ist eine gültige E-Mail-Adresse. Damit die E-Mails nicht in Ihrem Spam-Filter hängen bleiben, fügen Sie bitte die Domain *.reisswolf.com als vertrauenswürdigen Absender in Ihrer Mailkonfiguration hinzu.

8.1 Einfache Authentifizierung

Neue Benutzer werden über die normale Authentifizierung, mit Username und Passwort, authentifiziert.

8.2 2-Faktor-Authentifizierung mit TOTP

Wir empfehlen Ihnen, den sog. TOTP (Time-based One-time Password) Algorithmus als Standard einzurichten. Einmal eingerichtet, wird alle 30 Sekunden ein sechsstelliger Code generiert, der nach der Eingabe des Passworts in einem zweiten Schritt eingegeben werden muss. Dieser 6-stellige Code kann von Apps unterschiedlicher Hersteller generiert werden. Hier eine kleine Auswahl an Anwendungen, um TOTP-Codes zu erzeugen:

- Google Authenticator for iOS und Android (erste und älteste Anwendung mit dieser Funktion)
- Microsoft Authenticator for iOS und Android
- FreeOTP for iOS und Android (Open-Source)
- Viele Passwort-Manager für Desktop PCs bieten ebenfalls die Möglichkeit ein TOTP-Code zu generieren, so dass der Passwort-Manager gleichzeitig zum zweiten Faktor wird. (z.B. keepass mit dem KeePassOTP Plugin)

9. Datenschutz

Sofern keine andere individuelle Vereinbarung getroffen wurde, werden sämtliche Server ausschließlich in Deutschland betrieben.

In der dok.suite. sind eigene Benutzer und Benutzergruppen einzurichten, um eine differenzierte Trennung von Funktionen und Rollen abzubilden. Damit hat jeder Benutzer nur die Funktion zur Verfügung, die er für seine Arbeit benötigt.

Für Partner und Kunden werden Verträge zur Auftragsdatenverarbeitung nach Art. 28 der DSGVO geschlossen.

Unsere Datenschutzerklärung https://www.reisswolf.com/datenschutz-reisswolf-dok-suite/

10. Zertifizierung ISO 9001 und ISO/IEC 27001

Unser Qualitätsmanagementsystem (ISO 9001) als auch unser Informationssicherheits-managementsystem (ISO/IEC 27001) sind an unseren Standorten und im Betrieb mit unserer dok.suite.-Software zertifiziert. Alle Einzelnachweise sind auf unserer Homepage veröffentlicht.

https://www.reisswolf.com/reisswolf/zertifizierungen

11. Technische Systemvoraussetzungen

Die dok.suite.-Web-Anwendung ist über eine individualisierte ULR im Browser aufzurufen:

https://< InstanzName>.reisswolf.fit/ds/

Die genaue URL wird Ihnen mit Vertragsabschluss bzw. Einrichtung des Systems bekannt gegeben. Sind in der eigenen Umgebung nur zugelassene Web-Seiten für die Anwender aufrufbar, muss die Domain *.reisswolf.fit/ds ggf. noch zugelassen werden.

11.1 Dok.suite. Web-Anwendung für den Desktop-Arbeitsplatz

Die Anwendung dok.suite ist für die Nutzung mit folgenden Browsern freigegeben: Safari, Chrome, Firefox, Edge mit eingeschaltetem JavaScript.

Ohne installierte Addons. Cookies, Session- und Local-Storage im Browser müssen erlaubt sein.

Mindestens 2 GByte freier Arbeitsspeicher.
Wir empfehlen mindestens eine Full-HD Bildschirmauflösung (1920 × 1080 Pixel)
Internetverbindung mit einer Bandbreite von min. 50 Mbit/s.

11.2 Dok.suite. Web-Anwendung auf Tablets oder Handhelds

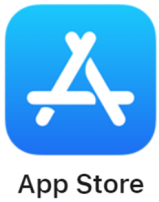
Die dok.suite.-Web-Anwendung ist grundsätzlich auch auf jedem Tablet oder Handheld lauffähig, da die Anwendung nur einen Web-Browser benötigt.

Da mobile Tablet- oder Handheld-Computer besonders auf geringen Energieverbrauch optimiert sind, ist bei dieser Geräteklasse besonders auf eine ausreichende CPU-Leitung zu achten. Hier sollten die CPUs mindestens einen Geekbench 5 Single-Core CPU Score von 750 erreichen (z.B. Apple A10 eines Apple iPad der 7. Generation oder vergleichbar).

Aufgrund der Bauform der Geräte (8 bis 12 Zoll Bildschirmgröße) kann es je nach Auflösung zu Einschränkungen in der Darstellung kommen.

11.3 Dok. suite. mobile App für Android und iOS

Die mobilen Apps werden über den Apple Play Store für iOS oder den Google Play Store für Android installiert.



12. Service & Support (Incident-Management)

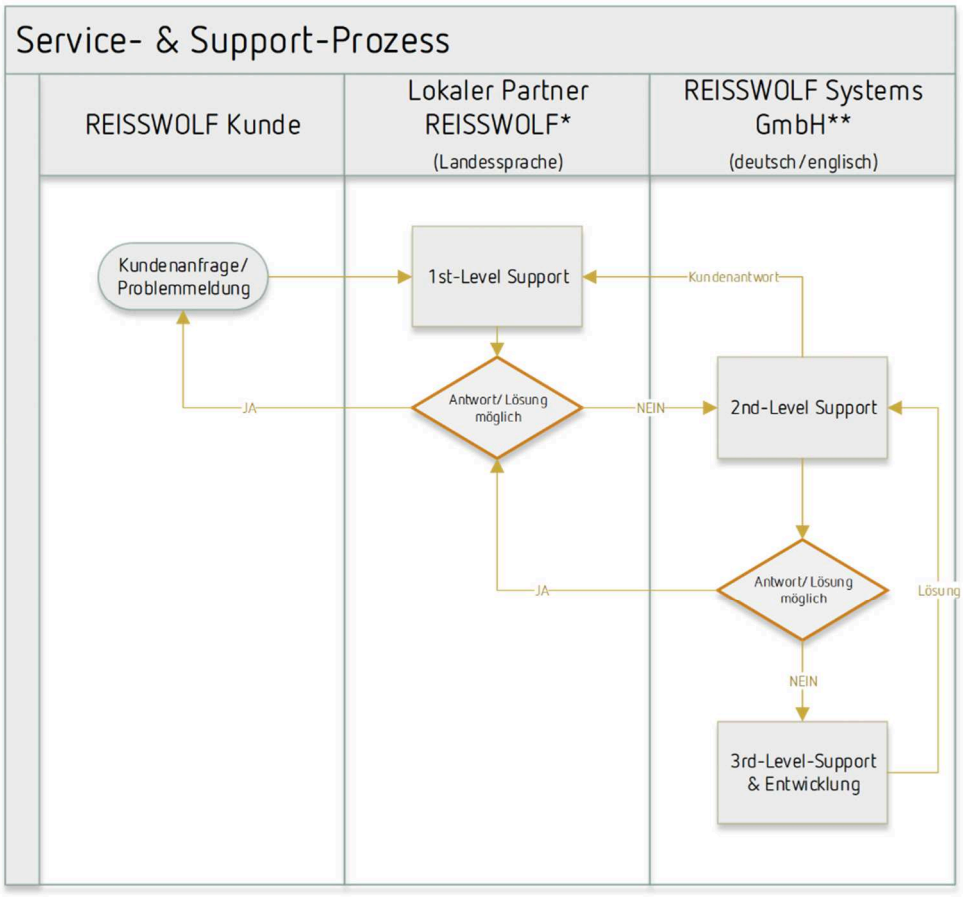
REISSWOLF stellt allen Nutzern der Anwendung dok.suite. eine Hotline für Fragen und die Aufnahme von Störungsmeldungen zur Verfügung. Alle Anfragen werden in einem Ticket-System nachverfolgt und dokumentiert.

Die Mitarbeiter sind telefonisch und per Mail zu erreichen. Die Kontaktdaten werden mit dem Vertragsabschluss zur Verfügung gestellt, sind aber auch in der Anwendung direkt verfügbar und im Handbuch beschrieben.

Um die Anwender optimal bei der Lösung von Problemen zu unterstützen, bieten wir einen Remote-Support via Teamviewer (https://www.teamviewer.com/de/) an.

Die weiteren Details (z.B. Reaktionszeiten, Verfügbarkeit usw.) sind im Software- und Wartungsvertrag geregelt.

Darstellung des Service & Support Prozesses:



* Betreiber eines Lagers/Lokaler Partner REISSWOLF
** Hotline-Zeiten: Mo-Do 09:00 – 17:00 MEZ; Fr 09:00-15:00 MEZ

13. WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) ist ein Protokoll zum Arbeiten mit Dokumenten und Ordnern. Sie können neben der Webapplikation von REISSWOLF dok.suite. eine WebDAV-Applikation verwenden, um ihre Dokumente zu verwalten. Ein Vorteil bei der Verwendung von WebDAV ist, dass Sie ganze Ordnerstrukturen hoch- und runterladen können. Ebenso bieten einige Applikationen von Drittherstellern eine Synchronisation von Ordnerstrukturen und Dokumenten auf lokalen Computern an.

Hinweis
Wir empfehlen als WebDAV-Client die Anwendung „Cyberduck".

https://cyberduck.io/webdav/

13.1 Berechtigungen und Versionierung

Bei der Verwendung von WebDAV sehen Sie dieselben Informationen wie in REISSWOLF dok.suite.

Versionierung von Dokumenten und Sicherung durch Berechtigungen werden auch bei der Verwendung von WebDAV durchgängig beibehalten.

13.2 Konfiguration von WebDAV-Applikationen

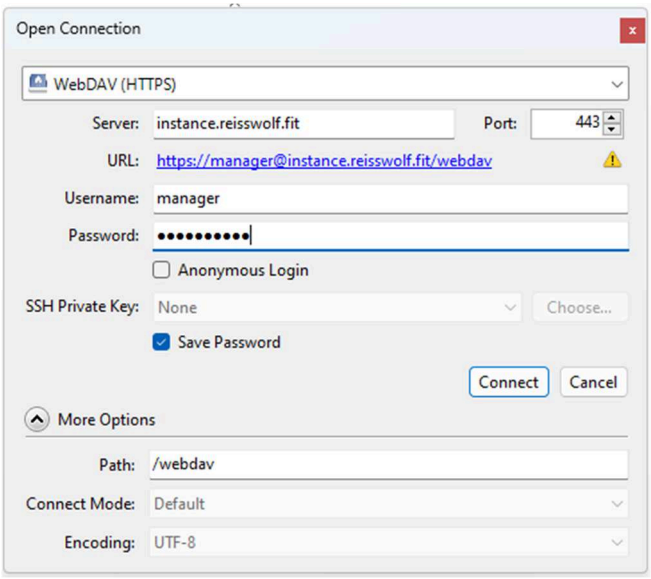


Abb. WebDAV - Einrichtung „Neue Verbindung" (Beispieldarstellung WebDAV von Cyberduck)

Damit WebDAV mit Ihrer REISSWOLF dok.suite. Instanz kommunizieren kann und Sie darüber Dateien und Ordner hoch und runterladen können, muss WebDAV zuvor eingerichtet werden. Hinterlegen Sie in Ihrer WebDAV Applikation diese Verbindungsdaten:

- Verbindungsart: WebDAV (HTTPS)
- Server: Addresse der dok.suite. Instanz
- Port: 443
- Benutzername und Passwort: Ihre benutzerdaten für den login

- Pfad: /webdav

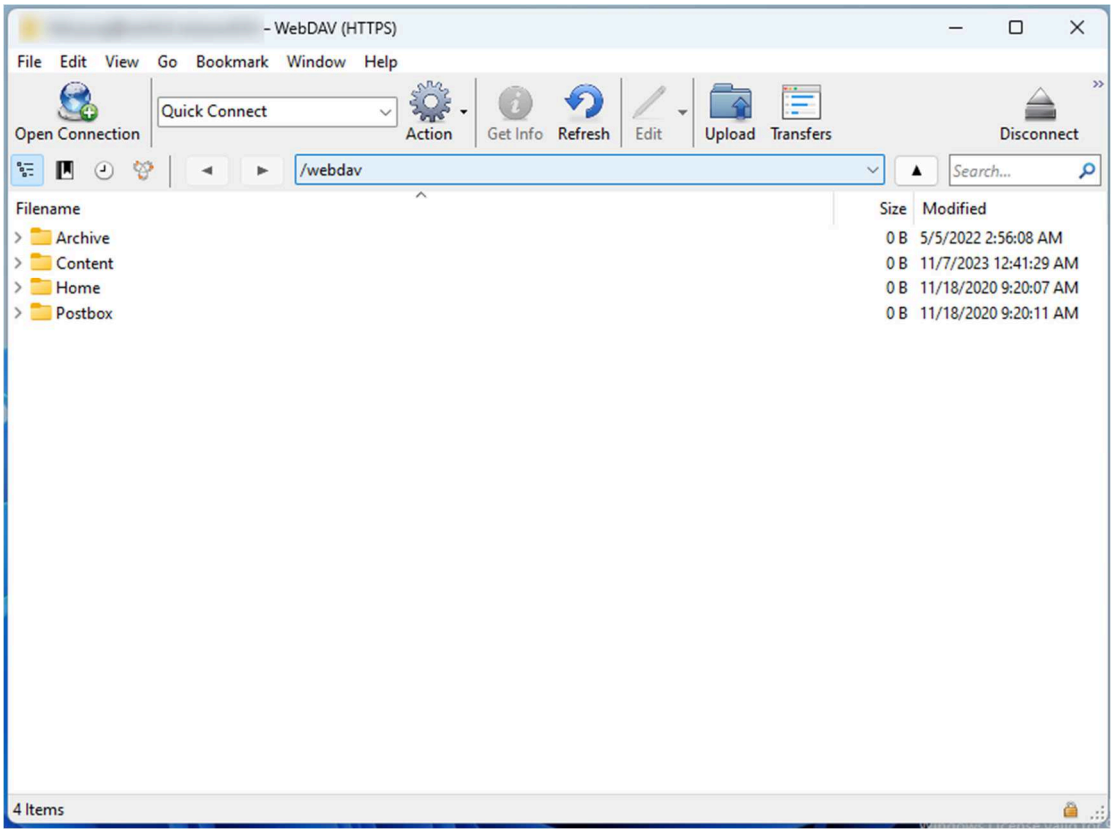


Abb. Anzeige Ordnerstruktur in WebDAV (Beispieldarstellung WebDAV von Cyberduck)

Nachdem Sie die Verbindung hergestellt haben, sehen Sie die Ordner und Dokumente, die Sie auch in REISSWOLF dok.suite. aufgrund der vergebenen Berechtigungen sehen können.

13.3 Arbeiten mit WebDAV

Um Dateien und Ordner per WebDAV in REISSWOLF dok.suite. hochzuladen, ziehen Sie die benötigten Daten einfach in die WebDAV Anwendung und lassen Sie die Daten auf dem Ordner los, in den Sie diese einfügen möchten.

Mit WebDAV können Sie:

- mehrere Dateien gleichzeitig in einen Ordner ablegen
- komplette Ordnerstrukturen mit den darin enthaltenen Daten in dok.suite. ablegen
- Dateien und Ordner verschieben
- Dateien und Ordner löschen
- Dateien und Ordner umbenennen

Mit einem Doppelklick können Sie Dateien öffnen, bearbeiten und anschließend wieder speichern. Die Änderungen werden als neue Revision automatisch in REISSWOLF dok.suite. hochgeladen.

14. Dok.suite. API (Application Programming Interface)

14.1 Was ist die dok.suite. API?

Die dok.suite. API ist eine Programmierschnittstelle, die für den Datentransfer und die Steuerung von dok.suite. genutzt werden kann. Über die API kann eine technische Schnittstelle zu eigenen IT-Systemen realisiert werden. Mit einer technischen Schnittstelle können Arbeitsabläufe rationalisiert und organisiert werden.

14.2 Lizenz-, Wartungs- und Nutzungsbedingungen der API

1. Die Nutzung der API ist ohne zusätzliche Lizenz- oder Mietkosten möglich
2. Die Nutzung erfolgt auf eigenes Risiko.
3. Die Funktion der API sind vertraulich zu behandeln. Eine Weitergabe an Dritte ist ohne Zustimmung durch die REISSWOLF Systems nicht gestattet
4. Fragen rund um die API-Nutzung sind in jedem Fall mit den üblichen dok.suite.-Support-Kosten verbunden und führen auch in jedem Fall zu einer Rechnung, unabhängig davon, ob es sich um ein Verständnisproblem oder eine Fehleranalyse handelt
5. Für den Kunden-Support der API ist kein eigener Vertrag vorgesehen. Deshalb gibt es keine verbindlichen Reaktions- oder Lösungszeiten bei Anfragen zu/oder Fehlern in der API.
6. Wir bitten darum, Anfragen zur API-Nutzung immer mit einem Termin zu verbinden, damit wir die Verfügbarkeit unserer Entwickler einrichten können. Ein Termin mit einem unserer Entwickler ist möglich, benötigt aber immer ein Vorlauf von einigen Tagen.
7. Wir bieten keine Unterstützung in einer Programmiersprache wie Python, Java, .NET, C#, C++, Ruby o.ä. an. Fragen zu konkreten API-Aufrufen oder Parametern müssen als einfacher curl -Aufruf bereitgestellt werden. Bei Fragen oder Problemen, die in anderen Anwendungen oder Programmiersprachen entstehen, können wir nicht helfen.
8. Die API kann parallele Zugriffe verwalten, wir möchten aber dringend darum bitten, die Anzahl der parallelen Zugriffe zu begrenzen oder (besser) die API-Anfragen nur seriell (nacheinander) auszuführen. Massiv-Parallele Zugriffe von einem einzelnen Nutzer können unter Umständen die Verfügbarkeit der dok.suite.-Anwendung für andere Anwender reduzieren. Wenn wir feststellen, dass ein Nutzer massiv parallele Zugriffe verwendet und die Performance des Gesamtsystems darunter leidet, behalten wir uns vor, dessen Zugang ohne Vorankündigung oder Warnung zu sperren. Die Freigabe des Zugangs erfolgt erst wieder, nachdem sichergestellt ist, dass das Verhalten nicht wieder auftreten kann.
9. Wir versuchen, die Änderung an der API gering zu halten. Der Anwender hat aber kein Recht auf eine stabile API. Änderungen an der API werden von uns OHNE vorherige Ankündigung durchgeführt. Änderungen an der API können dazu führen, dass die eigene Anwendung nicht mehr funktioniert. Der Nutzer hat kein Recht auf eine Korrektur.
10. Die API-Dokumentation steht nur in englischer Sprache zur Verfügung.

Alle technischen Details finden Sie in dem Dokument „REISSWOLF dok. suite. public API". Fragen Sie ggf. Ihren Support oder Ihren Vertriebspartner nach dem Dokument.

15. Ergebnisse der Schwachstellenanalyse (englisch)

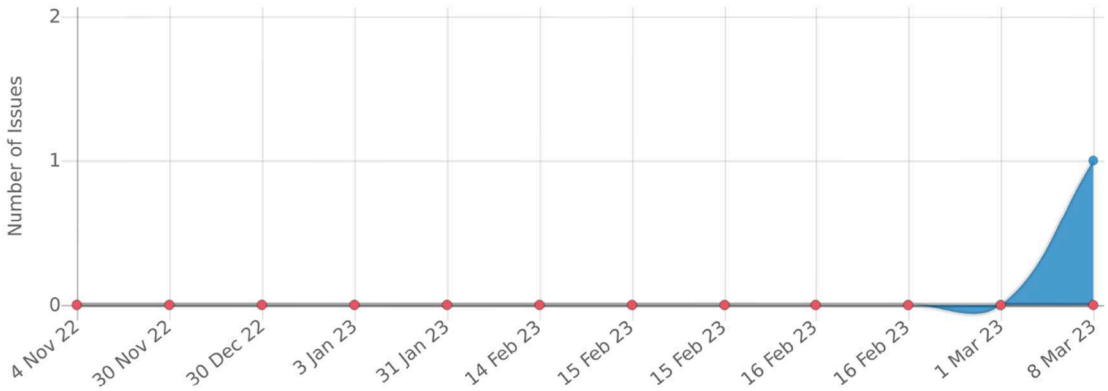
Scan Summary: **mscom IT Systems GmbH**
Targets: **23.88.8.85, 23.88.8.86, 23.88.8.84**
8 March 2023

Low
Threat Level

Low severity issues can not directly be exploited by an attacker, but may increase the ease of exploiting more severe issues in future. Fixing these issues may help protect against weaknesses that are not publicly known, or be used as one component in a highly targeted attack by the most sophisticated and well resourced attackers.

0	0	0	1
Critical issues	**High** issues	**Medium** issues	**Low** issues

Exposure over time



Differences since last assessment

New issues discovered		Previous issues remediated		Direction of travel
Critical	0	Critical	0	0
High	0	High	0	0
Medium	0	Medium	0	0
Low	0	Low	0	0

Total checks	Targets	Issues discovered
17,315	3	1

Here are some examples of what we checked your targets and their reachable webpages for.

Vulnerable software & hardware

- Web servers, e.g. Apache, Nginx
- Mail servers, e.g. Exim
- Development software, e.g. PHP
- Network monitoring software, e.g. Zabbix, Nagios
- Networking systems, e.g. Cisco ASA
- Content management systems, e.g. Drupal, Wordpress
- Other well-known weaknesses, e.g. 'Log4Shell' and 'Shellshock'

Web Application Vulnerabilities

- Checks for multiple OWASP Top Ten issues
- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- Local/remote file inclusion
- Web server misconfigurations
- Directory/path traversal, directory listing & unintentionally exposed content

Attack Surface Reduction

Our service is designed to help you reduce your attack surface and identify systems and software which do not need to be exposed to the Internet, such as:

- Publicly exposed databases
- Administrative interfaces
- Sensitive services, e.g. SMB
- Network monitoring software

Information Leakage

Checks for information which your systems are reporting to end-users which should remain private. This information includes data which could be used to assist in the mounting of further attacks, such as:

- Local directory path information
- Internal IP Addresses

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

REISSWOLF Systems GmbH
Wilhelm-Bergner-Straße 3 A
21509 Glinde
Internet: www.reisswolf.com