BRAINLOOP

SECURITY BRIEF | MyRoom

Sicheres Filesharing im Unternehmen und darüber hinaus

In einer immer mobileren Arbeitswelt stellen Verstöße gegen die Datensicherheit für viele Unternehmen ein großes Risiko dar. Viele dieser Verstöße entstehen durch weitverbreitete, unsichere Methoden, Informationen mit Dritten zu teilen.

Daher sollten Unternehmen die Voraussetzungen dafür schaffen, dass ihre Mitarbeiter wichtige und vertrauliche Informationen sicher teilen können. In besonderem Maß gilt das für streng regulierte Unternehmen. Laut einer Studie von Forrester Research besteht die globale Arbeitswelt zu etwa 29 % aus sogenannten Knowledge-Workers, welche üblicherweise drei oder mehr mobile Endgeräte nutzen, um jederzeit und überall auf ihre Informationen zuzugreifen.

Es ist diese Angewohnheit, die viel zur Verbreitung von Filesharing-Lösungen beigetragen hat, die allerdings lediglich den Ansprüchen von Privatanwendern genügen. Solche kundenorientierten Cloud-Lösungen sind heute bei vielen Angestellten beliebt und halten damit auch Einzug in die Netzwerke ihrer Arbeitgeber. Der Verlust von Daten und Compliance-Verstöße sind leider oft die Folge dieses Verhaltens.

Seit über 17 Jahren schützt die Brainloop AG höchstvertrauliche Dokumente von Unternehmen und unterstützt die Einhaltung von gesetzlichen Vorgaben und Compliance-Anforderungen. Somit bietet Brainloop allen Unternehmen eine Lösung, die
das Teilen und Synchronisieren von Dateien mit internen und externen Partnern nicht nur einfach macht, sondern auch höchsten Sicherheitsanforderungen genügt.

IM UNTERNEHMEN GELTEN ANDERE REGELN ALS BEIM PRIVATEN FILESHARING

- **Regel 1:** Die Daten gehören dem Unternehmen.
- **Regel 2:** Lokale Ablage (Laptop, Desktop und mobile Endgeräte) sollte als „feindliche Umgebung“ betrachtet und entsprechend geschützt werden.
- **Regel 3:** Der lokale Datenzugriff sollte für den Nutzer so einfach wie möglich sein.
- **Regel 4:** Das Unternehmen muss in der Lage sein, Zugriffsrechte auf lokal gespeicherte Daten jederzeit zu widerrufen (etwa beim Ausscheiden eines Mitarbeiters).
- **Regel 5:** Das Unternehmen muss in der Lage sein, alle Richtlinien anzupassen (etwa die Passwortstärke oder die maximal erlaubte Offline-Zeit).

HÖCHSTE SICHERHEITSSTANDARDS

Einhaltung von Datenschutzgesetzen
Alle Kundendaten werden in ISO-zertifizierten Rechenzentren in Deutschland gespeichert.

Schutz vor externen Zugriffen
Kein Hosting-Provider zwischen Brainloop und dem Kunden. Brainloop betreibt den Service völlig selbständig und stellt auch die Hardware und Software zur Verfügung. Die Rechenzentren steuern lediglich Rack-Stellplätze, Internetkonnektivität, Stromversorgung und Klimatisierung.

Verfügbarkeit
Daten werden stets redundant gespeichert, zwei Tier-3-Rechenzentren in mindestens 25 km Entfernung voneinander und dualer Dark-Fibre-Verbindung sowie jeweils voneinander unabhängige Internet-Konnektivität in einer Mindestbandbreite von 2 x 1 Gbit/s pro Rechenzentrum.

Provider Shielding
Kein Mitarbeiter der Brainloop AG hat Zugriff auf Dokumenteninhalte.

Administrator-Shielding
Selbst Administratoren auf Kundenseite sind vom Zugriff auf die Inhalte ausgeschlossen.

Key Management
Brainloop Dox nutzt eine große Anzahl kryptographischer Schlüssel. Diese Schlüssel werden mit Hilfe eines Key-Management-Systems (KMS) abgesichert.

Failover
Zwei Rechenzentren, Setup aktiv/passiv mit sofortiger Umschaltung, konsistente Datenhaltung über beide Rechenzentren.

Dark Fibre
Abhörsichere und dezidierte Verbindung zwischen den Rechenzentren.

Authentifizierung von Microservices
Die Architektur von Brainloop Dox verwendet das Microservice-Konzept. Dies bietet viele Vorteile wie Skalierbarkeit und höhere Resilienz der Lösung. Die verwendeten Microservices dürfen erst dann aufeinander zugreifen, wenn sie sich gegenseitig erfolgreich authentifiziert haben.

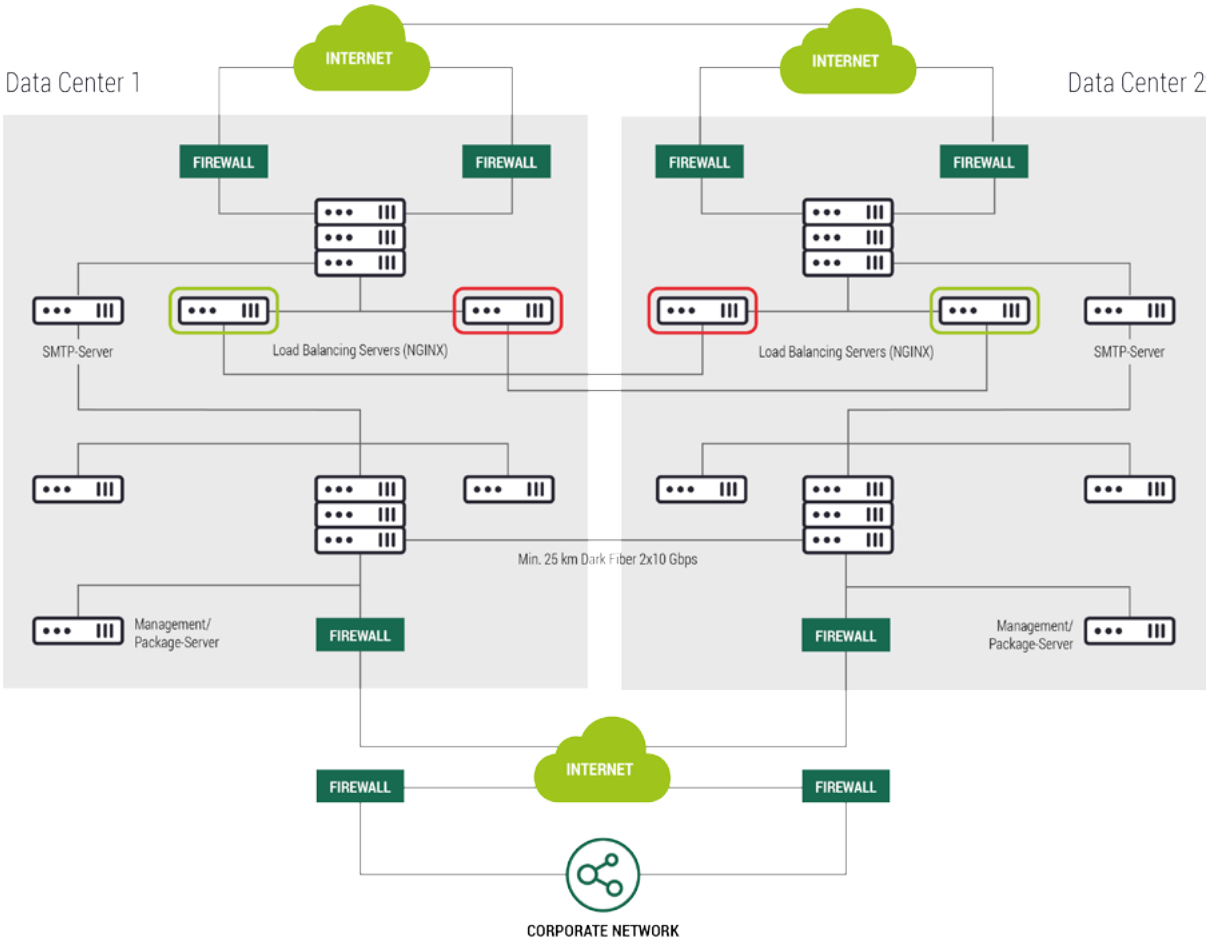
Interne Schutzmaßnahmen
Kein Mitarbeiter der Brainloop AG hat Zugriff auf Kundendokumente, die auf den operativen Servern gespeichert sind. Die Konfigurationen werden von einem „Team A“ durchgeführt, die Implementierung erfolgt durch ein eigenständiges „Team B“.

Integrität
Alle Dokumente werden per Fingerprint-Verfahren gekennzeichnet und redundant in mindestens zwei Rechenzentren gespeichert. Die Verschlüsselung mit AES-GCM gewährleistet die Integrität der verschlüsselten Daten.

Zusätzliche Schutzmaßnahmen
Kundenseitige Speicherung von Access Tokens unter höchsten Sicherheitsvorkehrungen. Dafür verschlüsselt Brainloop die Access Tokens mit einem sicheren Schlüssel, der aus der Passphrase des Benutzers abgeleitet wird. Folglich wird niemand ohne Kenntnis der jeweiligen Passphrase den Access Token extrahieren können, selbst wenn Angreifer vollständigen Zugriff auf den Host erlangen konnten. Certificate Pinning wird die Kunden zukünftig befähigen, die Gültigkeit eines Server-Kundenzertifikats zu validieren.

GCM (Galois/Counter Mode)
Das GCM Verfahren verhindert eine randomisierte Manipulation von verschlüsselten Dokumenten, welche zu fehlerhaften Inhalten führen würde.

Firewall und Load Balancing
Das Load Balancing und die BSI-zertifizierte Firewall werden ausschließlich von Mitarbeitern der Brainloop AG betrieben.



APPLIKATIONS-SICHERHEIT

Neben einer hochgradig sicheren Architektur bietet Brainloop Dox-Technologie Unternehmen eine Reihe von Funktionalitäten für die Verwaltung von Sicherheitsrichtlinien. So können Unternehmen den Zugang zu ihren Daten stets kontrollieren und Zugriffe nachverfolgen.

Zwei-Faktor-Authentifizierung

Der Zugriff auf Brainloop Dox-basierte Lösungen, wie Brainloop MyRoom, ist durch eine tokenbasierte Authentifizierung abgesichert. Dabei wird dem Benutzer eine einmalig gültige TAN per E-Mail oder SMS zugestellt. Alternativ erzeugt der Brainloop-Authenticator eine zeitbasierte TAN (TOTP) die Zugang in MyRoom gewährt.

Brainloop Authenticator

Der Brainloop Authenticator ist eine auf dem TOTP-Standard basierende Authentifizierungsmöglichkeit die sowohl online als auch offline funktioniert. Komfortabler als in Apps von Drittanbietern agiert dieses Brainloop-Anmeldeverfahren online. Es entfällt das lästige Eintippen der vom Server benötigten TAN.

Passwortsicherheit

Passwörter müssen aus mindestens acht Zeichen bestehen und zwei der drei folgenden Charakteristika aufweisen: Groß-/Kleinschreibung, Ziffern, Sonderzeichen Administratoren haben die Möglichkeit, Passwort-Policies zu definieren wie zum Beispiel die Passwort-Stärke, Gültigkeitsdauer von Passwörtern oder User-Lock-Out für x Minuten nach y Fehlversuchen. Die Regeln die für den Passwortgebrauch gesetzt werden, gelten auch für Passwörter die auf geschützte Links vergeben werden.

Lokaler Zugangscode
Für die Anmeldung an Dox-Clients und -Apps ist ein zusätzlicher 8-stelliger Zugangscode erforderlich.

Schutz beim Versand von Links
Benutzer können Links zu geteilten Dokumenten mit einem Passwort oder einer SMS-TAN schützen. Dabei kann der Absender selbst wählen, auf welchem Weg das Passwort übermittelt werden soll.

Schutz von Ordnern
Bei der Freigabe von Ordnern kann der Eigentümer zwischen drei Arten der Berechtigung wählen (Leser, Editor, Miteigentümer) sowie optional einen zusätzlichen TAN-Schutz (E-Mail, SMS oder Brainloop Authenticator) für die Freigabe, ein Verfallsdatum und die Möglichkeit, bereits gewährte Berechtigungen zu ändern oder zu widerrufen.

Rollenbasierte Berechtigungen
Bei der Freigabe von Ordnern können Benutzer Berechtigungen nach Rollen vergeben: Leser, Editor, Miteigentümer.

Audit im 4-Augen-Prinzip (optional)
Im Falle eines Verdachts, dass sich ein Nutzer von Brainloop MyRoom nicht an Compliance Regeln gehalten haben könnte, ist es möglich, einen Audit im 4-Augen-Prinzip zu initiieren. Dazu lädt ein Administrator einen Auditor ein um Einsicht in die Meta-Daten und Inhalte (optional) des verdächtigten Accounts zu erhalten.

Session-Time-Out
Sitzungen werden nach 60 Minuten Inaktivität automatisch beendet.

Vertraulichkeit
Alle Inhalte werden durch 256-Bit AES-GCM Verschlüsselung auf Server, Clients und Apps geschützt; 256-Bit TLS 1.2-Verschlüsselung der Inhalte im Transfer; Verschlüsselung der Metadaten.