Die Cloud des SLTs und der Datenschutz

Problemstellung

Aktuell hat der SLT einen Webspace bei Strato gemietet, auf dem die Homepage des SLTs abgelegt ist. Zusätzlich soll nun darauf acuh noch eine Nextcloud installiert und genutzt werden.

Das ist insofern problematisch, dass in einem Bereich auf den Strato-Servern eine Joomla- und eine Nextcloud-Installation parallel laufen. Sollte die Joomla-Installation kompromittiert werden, hätte das direkten Einfluss auf die Sicherheit der Daten innerhalb der Nextcloud. Bei einem entsprechenden Einbruch (z.B. eine nicht geschlossene Sicherheitelücke), könnten daher Date aus der Cloud entwendet oder modifiziert werden. Dies liegt v.a. daran, dass seitens Strato keine Trennung der Dateien erfolgt.

Grundsätzlich sind verschiedene Lösungen denkbar, wie man dieses Dilemma umgeht oder löst. In jedem Fall ist eine Abwägung des Risikos mit dem geweiligen potentiellen Schaden gegen den Aufwand und den Nutzen vorzunehmen. Im folgenden sollen nun einige Varianten vorgestellt werden, wie das Problem gelöst werden kann mit den jeweiligen Vor- und Nachteilen.

Lösungsansätze

Grundsätzlich basieren die Lösungsansätze auf der Verschlüsselung der Daten und ggf der Trennung der einzelnen Funktionalitäten der Server.

Ende-zu-Ende Verschlüsseung – extern

Die erste Möglichkeit besteht in der Verschlüsselung auf den PCs der Nutzer. Dabei werden logischerweise keine Daten (idealerweise) auf der Cloud abgelegt, ohne dass diese verschlüsselt wären.

Vorteile	Nachteile
Höchste Sicherheit	Alle Benutzer müssen sich an die Regeln halten
Keinen Anspruch an den Server	Teilen von Inhalten an dritte ist komplexer
	Backup nur auf verschlüsselten Daten möglich

Interne Verschlüsselung Es gibt eine App in der Nextcloud, die E2E-Verschlüsselung realisieren soll. Diese App ist im Moment nicht stabil. Daher wird von den Entwicklern empfohlen, dass sie nicht produktiv verwendet wird.

Externe Verschlüsselung Es gibt diverse Programme zum transparenten Verschlüsseln von einem Verzeichnis. Dabei werden die Daten lokal mit einem NC-Clienten herunter geladen und dann mit einem separaten Tool die Verschlüsselung realisiert (daher extern).

Vorteile	Nachteile
	Alle Nutzer müssen sich auf einen Clienten einigen (OS-abh.!)
	Online können keine Daten verarbeitet werden, viele Apps daher ohne Funktion

Server-Seitige Verschlüsselung in Nextcloud

Eine weitere Möglichkeit besteht in der Server-seitigen Verschlüsselung. Dabei werden die Daten vom Nutzer empfangen und vor dem Ablegen auf dem jeweiligen Speicher (egal wo dieser genau ist) transparent vom Server verschlüsselt. Beim Lesen der Daten werden die Daten noch ebenso transparent entschlüsselt bevor sie an den Nutzer ausgeliefert werden.

Dabei ist wichtig, dass die Verschlüsselung durch die Nextcloud-Software realisiert wird. Dadurch ist es für den Administrator schwerer, die Daten der Cloud für ein Backup abzugreifen. Statt dessen kann man nur die

versschlüsselten Daten und den Schlüssel ablegen. Das Backup ist daher nicht direkt lesbar und damit ist es auch schwer nachzuvollziehen, ob es vollständig ist.

In diesem Fall gibt eine Vielzahl verschiedener Subvarianten, die nicht alle sinnvoll sind.

Vorteile	Nachteile
Der Server kennt die Verschlüsselung und kann daher Freigaben realisieren	Server muss alle notwendigen Daten zur Verschlüsselung besitzen, Angreifer auf Server kann alle Daten lesen Backup der Daten teilweise komplex und fehleranfällig

Daten gemeinsam mit Joomla auf einer Instanz Hierbei werden alle Daten zusammen auf einem Speicher (gemeinsam mit Joomla) abgelegt. Die dadurch gewonnene Sicherheit ist nicht vorhanden, da der Schlüssel zum entschlüsseln in diesem Falle auf dem selben Speicherbeireich liegen würde. Der Aufwand für einen Angreifer wäre nur minimal höher, als wenn die Daten in unverschlüsselter Form vorliegen würden.

Daher wird dieser Fall nicht weiter betrachtet

Daten gemeinsam mit Joomla, Cloud auf einem kleinen VPS Eine Möglichkeit wäre das Anmieten eines kleinen virtuellen Servers im Internet, der die Cloud zur Verfügung stellt. Die Daten werden dann eingebunden in den Speicherbereich der Cloud. Dazu muss auf dem "großen" Strato-Paket ein entsprechendes Paket installiert werden, dass dieses zulässt und die Daten auch korrekt ablegt.

Die Verschlüsselung würde auf der virtuellen Maschine statt finden. Damit wäre der Schlüssel für einen Angreifer auf den Strato-Server nicht erreichbar und die Daten nicht entschlüsselbar.

Aktuell gibt es mehrere Probleme bei dieser Lösung, die auf fehlerhaften Code oder Dokumentation hin weisen. Konkret sei auf die Issues 1 und 2 verwiesen. Es ist nicht klar, ob und ab wann diese Lösung realisiert werden kann.

Vorteile	Nachteile
Realisierung komplett in der Cloud-Software	Potentieller Bug in Cloud Performance externer Speicher nicht sehr gut, schwer einzuschätzen

Daten auf anderem Strato-Speicherbereich, Cloud auf kleinem VPS Strato bietet die Möglichkeit, Daten per SSH/SFTP einzubinden. Diese Variant besteht aus einem kleinen VPS und einem solchen HiDrive-Speicher.

Diese Variante ist sehr ähnlich zu S3 Storage, 2 Strato-Paketen oder externer Verschlüsselung.

Diese Variante ist bisher ungetestet.

Vorteile	Nachteile
Keine Probleme mit der Sicherheit von Joomla Realisierung komplett in der Cloud-Software	Zwei zusätzliche Pakete notwenidg Ungetestet, daher unsicher Performance eher fraglich, schwer einzuschätzen

Daten auf S3 Objekt-Speicher, Cloud auf kleinem VPS Alternativ zu klassischen Dateien in einer Dateistruktur können Dateien auch in einem sog. S3 Object-Storage ausgelagert werden. Das ist eine Art Datenbank für Dateien. Typischer Anbieter solcher Speicher-Instanzen ist Amazon. Alternativ bietet aber auch Strato mit HiDriveS3 ein entsprechendes Angebot an.

Die Preisgestaltung beim S3 Storage ist komplett verschieden zu den sonstigen Preisen. Hier zahlt man die wahre Nutzung der Daten und Bandbreite statt eines vorher definierten Fix-Preises.

Diese Variante ist bisher nicht getestet.

Vorteile	Nachteile
Typischerweise hohe Geschwindigkeit	Komplexere Preisstruktur
Realisierung komplett in der Cloud-Software	Bisher ungetestet, daher unsicher
Keine Probleme mit der Sicherheit der Jooma-Seite	2 zusätzliche Pakete notwendig
	Geschwindigkeit nicht sicher

Server-seitige Verschlüsselung extern der Nextcloud

Die Nextcloud erlaubt es auch, die Daten von irgendwo innerhalb des Servers zu speichern. Damit ist es acuh möglich, dass die Daten vom Betriebssystem (trabnsparent) verschlüsselt werden (s. gocrypfs). Damit die Daten dann auch an den entsprechendne Stellen landen, wo sie hin gehören, müssen entsprechende Programme im Betriebssystem eingesetzt werden.

Vorteile	Nachteile
Bessere Kontrolle über die Daten	Root-(v)Server notwendig
Performance wahrscheinlich besser als bei Implementierung in PHP/Nextcloud	Erfahrung bei der Einrichtung nötig, aktuell vorhanden
Backup und Migration unproblematisch	
Daten durch Angriff auf Joomla nicht gefährdet	

Speicherung der Daten im bisherigen Strato-Webspace Es kann neben der Jooma-Installation noch eine weitere Software installiert werden, die ein Einbinden des Speichers in einen anderen Rechner erlaubt. Dies entspricht dem entsprechenden Fall im vorgehenden Kapitel.

Deiser Fall wurde bisher nicht praktisch getestet.

Vorteile	Nachteile
keine weiteren Pakete notwendig	Performance wahrscheinlich nicht ideal, aber schwer einzuschätzen

Speicherung in einem SSH/SFTP/S3 Speicherbereich Die Fälle zur Nutzung weiterer Dienste von Strato lassen sich ebenso extern einbinden. Auch diese Fälle sind im Moment ungetestet.

Separater Speicherbereich

Wenn der Speicher komplett von Joomla getrennt ist, kann man theoretisch auch auf die Verschlüsselung verzichten. Dies betrifft natürlich nur den Angriff via Joomla.

Wenn die Cloud-Software einen Fehler enthält, der einen Angreifer einlässt, wird das natürlich von keinem der hier beschriebenen Verfahren verhindert. Hier ist allerhöchstens noch anzumerken, dass der Hoster theoretisch Zugriff auf die Daten nehmen kann und das ggf vertraglich geregelt werden müsste.

Weiteres Strato-Paket Das Problem der Trennung der Daten kann auch auf Strato abgewiegelt werden. Dazu muss aber ein weiteres Paket gebucht werden ähnlich wie wenn ein neuer Kunde registriert wird.

Vorteile	Nachteile
Implementierung wird von Strato übernommen	Weiteres recht teures Paket notwendig
	Keine Verschlüsselung, daher Auftragsdatenverarbeitung muss realisiert werden

Direkter Speicher auf privat zur Verfügung gestelltem Rechner Theoretisch kann ich auch einen Speicher zur Verfügung stellen. Dieser ist aber weger hoch verfügbar noch kann ich irgend eine Weise von Zertifizierung vorweisen.

Wenn die Daten bei mir abgelegt werden sollen, müssten die genauen Anforderungen noch einmal geklärt werden. Erst danach kann ich sagen, ob ich diese auch einhalten kann

Vorteile	Nachteile
Kostengünstig	Klare Regelungen nicht gegben Keine hohe Bandbreite, keine garantierte Verfügbarkeit

Gemeinsamer Speicherbereich

Der letzte Fall wäre die Nutzung des Strato-Webspaces ohne eine Verschlüsselung durch die Cloud. Die Daten sind in diesem Falle gegen einen Angriff auf Joomla potentiell gefährdet.

Hierbei ist der Ansatz, die Cloud und Joomla immer aktuell zu halten und die Anzahl der Erweiterungen in Joomla minimal zu halten. Damit sollte die mögliche Angriffsfläche verringert werden.

Vorteile	Nachteile
Einfache, direkte Implementierung Verhältnismäßig schnelle Performance	Sicherheit deutlich reduziert

Abstrakte Analyse

Speicherbackend

Bezeichnung	Vor-/Nachteile
Im "großen" Speicher neben Joomla	Potentielles Risiko bei Bug in Joomla, kein zusätzliches Paket notwendig, wahrscheinlich schlechte Performance
In einem HiDrive via SSH/SFTP	Realisierung noch nicht getestet, weiteres Paket notwendig
In einem S3 Object Storage	komplexe Preisstruktur, hohe Geschwindigkeit, keine Erfarungen bisher
In privatem Speicher von CWolf	günstig, recht schnell einzurichten

Verschlüsselung der Daten

Bezeichnung	Vor-/Nachteile
keine	geringste Sicherheit, kein Schutz der Daten im Hintergrund
NC-intern	Implementierung in PHP daher potentiell langsamer, Realisierung in der Cloud vermeidet extere Abhängigkeiten
NC-extern (im OS)	einfaches Backup, Extraktion der Daten aus Nextcloud möglich, Root-Server nötig
Ende zu Ende	hohe Sicherheit, mehr Anforderungen an die Nutzer