Strategie zum Managed Service „hBOX.at“, Datenschutz und Sicherheit

1. Einleitung

Gratuliere zu Ihrer Entscheidung die hBOX zu verwenden! Sie setzen auf ein österreichisches Produkt, das nach strengen Kriterien überprüft und betrieben wird und die oberste Regel lautet dabei: „Achte auf die Sicherheit der Kundendaten!“. Dabei kommt es weder bei aktiven Daten, noch bei laufenden Datensicherungen zu einer Ablage außerhalb von Österreich, sofern es sich um eine bei uns gehostete Instanz handelt.

Die hBOX.at gibt es in den folgenden Ausprägungen:

- Hardware Appliance im Kundenrechenzentrum
- Virtuelle Appliance in der Virtualisierungsplattform des Kunden
- Managed Service aus den Rechenzentren dediziert

Auch wenn die wesentlichen Sicherheits-Features der hBOX auf jeden Fall zutreffen, haben Sie als Kunde natürlich die Möglichkeit eine hBOX – Appliance im Ausland zu betreiben, wenn Sie sich dafür entscheiden.
Das restliche Dokument bezieht sich im Wesentlichen auf das „Managed Service“, also bei Huemer gehostete Instanzen von hBOX.at.

2. Datenablage

Ohne Ausnahme kommt es bei hBOX.at nur in unseren österreichischen Rechenzentren zu einer Datenablage ihrer Daten.
Das bedeutet, dass auch Backups und inaktive Versionen Ihrer Appliances/Daten Österreich nicht verlassen. Damit stellen wir sicher, dass Ihre Daten keiner ausländischen Gesetzbarkeit ausgesetzt sind, mit Regeln die sie üblicher Weise nicht einmal kennen, geschweige sich daran halten können. Es gibt auch keinerlei Verträge mit ausländischen Unternehmen die diese Absicherung aufweichen würden.

Auf Wunsch des Kunden können alle Kundendaten mit einem nur dem Kunden bekannten, bzw. dem User des Kunden bekannten Schlüssel versehen werden und so auch den Zugriff von Administrator-Seite unterbinden.
Wenn der Kunde fremde Services (Googledrive, Dropbox, onedrive, S3,…) als zusätzlichen Datenstore einbinden dann gilt das nur für jene Verzeichnisse die diesen Services entsprechen natürlich nicht mehr. Generell hat der Kunde diese Möglichkeit, auch wenn wir davon abraten.
Weiters gibt es die Möglichkeit Daten nur für eine gewisse Zeit auf der hBOX abzulegen und danach automatisiert zu löschen. Viele Kunden nutzen dieses Feature um aus der hBOX eine Datendrehscheibe und keine Ablage zu machen.

3. Datenübertragung

Jede Datenübertragung von/zu hBOX.at erfolgt verschlüsselt und wird im Activity-Log verzeichnet. Dieser Log steht dem Benutzer für seine eigenen Daten und dem Site-Admin für die gesamte Instanz des Kunden zur Verfügung. Damit ist auch bei einer Überprüfung feststellbar, welche Daten angelegt, downgeloadet, gelöscht oder geshared wurden.

4. Datensicherung

Die Datensicherung erfolgt jede Nacht zwischen 20:00 und 4:00 Uhr. Sofern keine anderen Vereinbarungen mit dem Kunden getroffen wurden, werden die täglichen Backups 21 Tage aufbewahrt und danach gelöscht. Wie angemerkt, erfolgt die Datensicherung und die Aufbewahrung der Sicherungsdaten und Logs ausschließlich in Österreich.

5. Authentifizierung

Username und Passwort sind die wesentlichsten Mittel zur Authentifizierung der hBOX. Auf Wunsch des Kunden können Multifaktor-Authentifizierungs-Mechanismen des Kunden, oder dementsprechende Managed Services von Huemer Data Center verwendet werden um eine zusätzliche Absicherung des Zugriffes einzubauen.
Die zu Grunde liegende Userdatenbank ist üblicher Weise das Active Directory des Kunden oder die hBOX.at-Userdatenbank der Kundeninstanz. Die Passwortregeln die zum Tragen kommen, werden zu 100% vom Kunden bestimmt, wobei wir regelmäßiges Wechseln und starke Passwörter empfehlen.
Bei Brut-Force-Attacken, bei denen Dictionary-basiert versucht wird in User-Accounts einzudringen, wird der betroffene User bei jeden weiteren Versuch immer länger gesperrt.
Die Richtlinien, wie viele Fehlversuche erlaubt, wie lange die Sperre erfolgen soll und Mechanismen zur Absicherung der dahinter liegenden Userdatenbank werden mit dem Kunden abgestimmt und individuell etabliert.

6. Zugriffsmöglichkeiten

Sofern der Kunde keine weiteren, individuellen Möglichkeiten vereinbart hat, oder explizite Wege sperren lässt gibt es folgende Möglichkeiten der Interaktion zwischen Benutzer und hBOX.at:

- Webserver/Browser
- Mobiler hBOX Client (Android, iOS, Windows Mobile)
- hBOX PC-Client für Synchronisation von einzelnen Bereichen oder der gesamten User-hBOX
- Foundation-Zugriff zwischen hBOX-Instanzen von unterschiedlichen Unternehmen
- Windows-Betriebssystem auf Basis Webdav
- Offene Webdav-basierende „Standard-Clients“ für Mobiles, Windows, Linux oder Mac

Primär empfehlen wir den Webzugriff oder die angebotenen hBOX-Clients, die in Funktion und Sicherheit geprüft und laufend aktualisiert werden.
Zwischen Unternehmen ist die Foundation die komfortabelste Variante um Daten auszutauschen oder eine Zusammenarbeit zu etablieren. Rechte auf gemeinsame Daten können granular pro Benutzer in beiden Unternehmen gepflegt werden.
Bei der Verwendung von Fremdclients gilt: Solange die Hersteller sich an die RFC-Konformität bei Protokollen und Authentifizierung halten sollte es funktionieren. Wir können aber diesbezüglich nichts versprechen und raten davon ab.

7. Daten teilen

Sofern vom Site-Admin nicht unterbunden, kann ein hBOX – Benutzer seine Daten mit fremden Kontakten außerhalb von hBOX.at teilen.
Dabei ist es möglich ein (ggf. starkes) Passwort zu setzen, eine zeitliche Einschränkung einzubauen wie lange die geteilte Datei zur Verfügung stehen soll und ob die Datei auch verändert oder nur gelesen werden darf. Der Benutzer kann einen Bereich seiner hBOX als Upload-Area definieren um einem Fremdkontakt die Möglichkeit zu geben Daten anzuliefern.

8. Viren/Ransomware und versehentlich gelöschte Daten und Inhalte

Auf der hBOX abgelegt Daten werden auf Kundenwunsch auch virengescanned. Welche Scanning-Engine dabei zur Verwendung kommt wird ebenfalls zwischen Kunde und Huemer vereinbart. Betroffene Dateien werden quarantänisiert und können in der Norm nach Entfernung der Schadsoftware wieder verwendet werden.

Unabhängig davon sind die Daten in der hBOX aber generell vor Schadsoftware geschützt, weil jede Veränderung von Daten reversibel ist (Versionierung), gelöschte Dateien wieder hergestellt werden können (undelete).

Wenn mehrere Personen zur gleichen Zeit die selbe Datei bearbeiten (was bei der Synchronisation von Daten leicht passieren kann) kann es durch mehrere Inkarnationen eines Files zu einem Konflikt kommen. hBOX.at erkennt diesen Konflikt und erzeugt eine „conflict“-Datei mit Vermerk des betroffenen Benutzers und Zeitpunkt des Konfliktes. Damit können eventuell neuere Absätze in einem Dokument später eingepflegt werden.

9. Verdacht auf Verlust der Usercredentials

Wurden Username/Passwort von einer fremden Person ausgespäht, oder sonst in Erfahrung gebracht ist schnelles Handeln angebracht.
Das wichtigste ist eine Kontaktaufnahme mit dem Site-Admin, der die weitere Vorgangsweise beurteilen kann.

Als kurzer Überblick:

Passwort erspäht: Passwort ändern.

Passwort von einer fremden Person bereits geändert: Analyse der Aktivitäten des betroffenen Accounts.

> **Download von einzelnen Dateien oder Verzeichnissen**: Passwort ändern, IP-Adresse und Zeitpunkt des Transfers erheben und ggf. Behörden einschalten.
>
> **Aktive Synchronisation mit Fremdgerät**: Remote Löschen der Daten veranlassen, ggf. Behörden einschalten.

Ein umgehender Kontakt mit dem Site-Admin ist auf jeden Fall obligatorisch.

10. Schlussworte

Bitte beherzigen Sie die Hinweise und Empfehlungen in diesem Dokument um eine optimale „User-Experience“ zu erleben.

Darüber hinaus bieten die Userdokumentation, die direkt-Hilfe in hBOX.at und unsere Youtube-Tutorial-Reihe wichtige Hinweise für ein ungetrübtes Arbeiten mit der hBOX.