SecureBeam Q&A

In diesem Dokument finden Sie Antworten auf die häufigsten Fragen zu SecureBeam. Falls Sie weitere Fragen haben, wenden Sie sich bitte an Martin Vasko, Email: martin.vasko@securebeam.com.

Was ist SecureBeam?

SecureBeam ist ein völlig neuartiger Weg, mit dem Nutzer mehrere vorhandene Cloud-Dienste auf smarte Weise miteinander verbinden und dabei automatisch sicherer nutzen können. Hierzu teilt SecureBeam die Daten des jeweiligen Nutzers auf verschiedene Cloud-Speicher auf und speichert die Fragmente dort jeweils verschlüsselt.

Für den Benutzer ist dieser Vorgang transparent: Er nutzt einfach SecureBeam als seinen Cloud-Speicher. SecureBeam ist sozusagen eine Cloud in der Cloud und schafft einen neuen, größeren, sichereren Platz im Netz. Außerdem lassen sich alle Dateien auf sichere Weise mit Freunden und Kollegen tauschen.

Was ist der Unterschied zu Dropbox & Co?

SecureBeam ist kein eigener Cloud-Speicher, sondern setzt auf vorhandene Cloud-Speicher wie Dropbox auf und macht deren Speicherplatz auf einfachste Weise abhörsicher, ohne die Möglichkeiten für etwaige Zusammenarbeit einzuschränken.

Wer braucht SecureBeam?

Bei fast allen Cloud-Systemen werden die Dateien so gespeichert, dass die Betreiber und damit auch staatliche Behörden oder Hacker ungehindert Einblick in die Inhalte nehmen können. Ärzte, Anwälte, Steuerfachkräfte, Politiker, Journalisten und andere Berufsgruppen sollten daher auf keinen Fall unverschlüsselte Daten in Clouds speichern. Gleiches gilt für alle Arten von Geschäftsgeheimnissen in Unternehmen, vom Bauplan bis zum Vertrag. Private Nutzer wollen ihre privaten Fotos und persönlichen Dokumente ebenfalls nicht in der Hand unbefugter Dritter wissen, man denke hier an die jüngsten Vorfälle mit Nacktfotos aus gehackten Cloud-Speichern.

Kurzum: Jeder Benutzer von Cloud-Speichern benötigt SecureBeam. Dann kann er sicher sein, dass seine Daten in der Cloud wirklich sicher und geschützt sind.

Welche Cloud-Speicher unterstützt SecureBeam?
SecureBeam unterstützt derzeit die populären öffentlichen Cloud-Storage-Systeme Dropbox, Google Drive und Microsoft OneDrive. Auch die Unterstützung privater Cloud-Speicher wie ownCloud und AeroFS ist in Planung. Im nächsten Schritt folgen dann Box, CloudSafe, Egnyte, iCloud und SugarSync.

Was kostet SecureBeam?
SecureBeam verwendet ein Freemium-Modell. Die Grundversion unterstützt die Kombination der Cloud-Dienste Dropbox und Google Drive, was mit deren kostenlosem Angebot bereits bis zu 30 GByte Cloud-Speicher erschließen kann (Google Drive: 15, Dropbox: 2 bis 16 GB im Free-Plan).

Um sich zu finanzieren, verwendet SecureBeam In-App-Käufe. Damit lassen sich weitere Clouds aktivieren, etwa Box, iCloud, OneDrive oder SugarSync. Dann arbeitet als zusätzlicher Sicherheitsfaktor auch die redundante Speicherung von Daten.

Welche Betriebssysteme unterstützt SecureBeam?
SecureBeam gibt es bereits seit August 2014 als App für Android. Apps für iOS und Desktop-Betriebssysteme (Windows, Mac) werden Mitte November folgen, ebenso eine per Web nutzbare Desktop-Version.

Lassen sich Daten mit SecureBeam sharen?
Jede Datei kann mit allen Kontakten im jeweiligen System abhörsicher geteilt werden, auch mit mehreren gleichzeitig. SecureBeam initiiert dabei automatisch auch einen verschlüsselten Chat für den sicheren Austausch von Informationen zur Datei.

Erhöht SecureBeam die Speichergröße?
SecureBeam kann funktionsbedingt *nicht* die Größe der einzelnen Cloud-Speicher erhöhen. Doch durch die Kombination der verschiedenen Dienste addiert und erhöht sich die über SecureBeam sicher nutzbare Gesamtspeichergröße. Kombiniert man etwa Dropbox, Google Drive, Microsoft OneDrive mit jeweils 15 GByte, sind über SecureBeam 45 GByte nutzbar. Wo die Daten liegen, ist dabei aus Nutzerperspektive egal.

Belegt SecureBeam den kompletten Cloud-Speicher?
Der Benutzer hat stets die volle Kontrolle über seine Clouds. SecureBeam belegt nur so viel Speicher wie der Nutzer anfordert. Jeder Anwender stellt also selbst ein, wie groß der SecureBeam-Speicher ist und wie viel Prozent des SecureBeam-Speicherplatzes von welchem Dienst bezogen werden sollen. Die SecureBeam-App zeigt jederzeit an, wie viel Platz, den die in SecureBeam gespeicherten Dateien belegen, aktuell von welchem Cloud-Dienst bezogen werden.

Wie verschlüsselt SecureBeam seine Daten?
Zur Verschlüsselung von Dateien und Nachrichten nutzt SecureBeam eine AES-Verschlüsselung mit 256 Bit Schlüssellänge. Zum Austausch der dafür notwendigen Schlüssel implementiert SecureBeam asymmetrische RSA-Verschlüsselung mit 2048 Bit. Am Ende nutzt SecureBeam also ein hybrides Verschlüsselungskonzept, das die Geschwindigkeit symmetrischer Verschlüsselung mit der Sicherheit und Flexibilität einer Public-Key-Infrastruktur kombiniert.

SecureBeam steht in Kontakt mit dem Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein und arbeitet an einer **Zertifizierung von SecureBeam**.

Verschlüsselt SecureBeam auch Dateinamen?
SecureBeam verschlüsselt einzelne Dateien und lädt sie als kleine Speicherblöcke in unterschiedliche Cloudspeicher. Dabei werden auch die Dateinamen verschlüsselt und sind nur für den Urheber lesbar. Die von SecureBeam verwendeten kleinen Speicherblöcke lassen sich unabhängig voneinander schneller synchronisieren als zum Beispiel eine ineffizient große, verschlüsselte Container-Datei.

Wo liegen die Schlüssel?
SecureBeam etabliert eine eigene Infrastruktur für den Austausch öffentlicher Schlüssel. Der private Schlüssel liegt auf Android im sogenannten Keystore, auf iOS in der Keychain – das sind die jeweils verschlüsselten, speziell geschützten Speicherbereiche. Um ein neues Gerät zur SecureBeam-Cloud hinzuzufügen, muss der Nutzer ihm Zugang gewähren, wodurch es Teil der Infrastruktur wird.

Für die Business-Version ist ein eindeutiger Firmenschlüssel geplant. Dieses RSA-Schlüsselpaar können Unternehmen dann wahlweise auf eigenen Servern oder bei SecureBeam/expressFlow hinterlegen. Der Firmenschlüssel kann alle privaten Schlüssel aller der Firma zugehörigen Nutzer entschlüsseln; so hat das Unternehmen immer Zugriff auf verschlüsselte Daten, auch wenn ein Nutzer das Unternehmen verlassen hat.

Sind in SecureBeam gespeicherte Daten vor Fremdzugriff geschützter als in normalen Clouds?
Auf jeden Fall, und das gilt auch im Freemium-Modus. Alle Dateien werden nicht nur verschlüsselt, sondern auch in zufällige Fragmente zerlegt und auf die einzelnen Speicherdienste verteilt. Die Aufteilung einzelner Dateien erfolgt dabei stets schon in der SecureBeam-App. Das bedeutet, jeder Cloud-Speicher sieht nur Bruchstücke der Daten eines Benutzers – und auch diese nur verschlüsselt.

Sind in SecureBeam gespeicherte Daten sicherer vor Verlust als in normalen Clouds?
SecureBeam kann sicherer operieren als einzelne Clouds: Aktiviert der Nutzer durch In-App-Kauf die Redundanzfunktion, speichert SecureBeam die Daten in den Diensten redundant und schafft so eine extrem sichere und hochverfügbare Speicherlösung. Selbst ein Totalausfall eines beteiligten Cloud-Speicher-Dienstes hat keine Auswirkung auf die Daten in SecureBeam. Technisch verwendet die Redundanz das Verfahren, auf dem auch RAID5 basiert.

Was ist der Unterschied zu Cloud-Lösungen, die bereits Verschlüsselung anbieten?
Einige Cloud-Speicher-Angebote beinhalten eine Verschlüsselung, so dass die Inhalte im Cloud-Speicher sicher vor Fremdzugriff sind. Doch diese Lösungen arbeiten oft mit begrenztem Speicherangebot und speichern Dateien anders als SecureBeam weder redundant noch fragmentiert. Je nach Bezahlmodell fallen also Zugriffsschutz und Ausfallsicherheit geringer aus als bei SecureBeam. Zugleich sind diese Systeme oft schwer zu bedienen.

Ist SecureBeam für Unternehmen sinnvoll?
Unternehmen stehen heute vor dem Problem, dass die Nutzer Cloud-Speicher verwenden, obwohl dies bei vielen gängigen Diensten ein relevantes Sicherheitsproblem darstellt. Zugleich ist eine Blockade von Cloud-Speichern erfahrungsgemäß nur schwer durchzusetzen, einfach weil es so bequem ist.

Mit SecureBeam hingegen können Unternehmen öffentliche Cloud-Speicher (wie Dropbox) sicher nutzen, ohne die User zu gängeln. Firmen können außerdem auch (zusätzlich ebenso wie ausschließlich) Private-Cloud-Lösungen wie ownCloud oder AeroFS einbinden, mit denen sich firmen-eigenen private Clouds bilden lassen. Für Businesskunden existieren außerdem speziell angepasste Versionen von SecureBeam, etwa mit einer nahtlosen Integration firmeneigener Speicherlösungen wie Microsoft Sharepoint.

Wer steht hinter SecureBeam?
Entwickler des Systems ist die expressFlow GmbH mit Sitz in Wien. Gründer und Geschäftsführer des Unternehmens ist Dr. Martin Vasko. Bereits in seiner Dissertation behandelte er die optimale Abwicklung von automatischen Abläufen in Cloud-Systemen – mit spezieller Berücksichtigung auf Security (etwa den Schlüsselaustausch bei PKI-Umgebungen). Das – und das Fehlen einer clientseitigen Verschlüsselung bei Dropbox – motivierte Dr. Vasko zunächst zur Entwicklung einer Software namens „expressFlow“. SecureBeam ist eine komplette Neuentwicklung dieser Software, basierend auf dem expressFlow-Benutzerfeedback.

Die Arbeit an SecureBeam begann im Oktober 2013. Die im April 2014 gegründete expressFlow GmbH konnte verschiedene Investoren gewinnen. expressFlow erhielt eine Anschubfinanzierung

durch SevenVentures im Rahmen des ProSiebenSat.1-Accelerators und gewann den ContentPitch-Award des ZIT Wien. Es erfolgte eine Aufnahme in den dritten Badge des ProSiebenSat.1-Accelerators. Außerdem ist SecureBeam Finalist in der EIT ICT Labs Idea Challenge „Future Cloud“, qualifizierte sich als Alpha-Startup zum Web Summit 2014 und errang den Mercur Innovation Award 2014.