Zendto was ist das .?

ZendTo ist ein webbasiertes System, dass mit vollständiger Sicherheit auf einem eigenen Server ausgeführt wird. Dateien werden 50% schneller und sicherer als per E-Mail gesendet.

Hauptmerkmale

- **Sichere Ver- und Entschlüsselung** von hochgeladenen Dateien mithilfe einer benutzerdefinierten Passphrase, um persönliche oder eingeschränkte Daten zu schützen
- **Prüfsummen** der hochgeladenen Dateien, um Streitigkeiten darüber zu vermeiden, welche Inhalte geliefert wurden
- Die Nutzer werden über die Verwendung und Verarbeitung ihrer Daten **gemäß den** Anforderungen der **DSGVO informiert**
- Sehr einfach zu bedienen, unterstützt **Drag-and-Drop-** Auswahl von Dateien zum Hochladen
- Keine festen Upload-Limits (Uploads von 20 GB oder mehr sind möglich)
- Integriert sich in bestehende Kundenservice-Ticket-Systeme
- **claimID** ist eine zufällige Zeichenfolge, die dem Benutzer für jede Abgabe als Schlüssel übergeben wird.
- **ClaimPasscode** ist die 2. zufällige Zeichenfolge, die dem Benutzer übergeben wird, damit die Details der Abgabe auf zwei verschiedene Arten gesendet werden können, falls dies aus Sicherheitsgründen erforderlich ist.
- **Passphrase (Geheimwort)** wird zur Ver- und Endschlüsselung genutzt jedoch nicht mitgespeichert.
- **Absender** wird angezeigt. Der vollständige Name des Erstellers der Abgabe.
- **Absender E-Mail** des Erstellers der Abgabe wird mitgeteilt.
- **Empfangsbestätigung** wird per E-Mail-Benachrichtigung an den Ersteller gesendet, wenn ein Empfänger die Abgabe abgeholt hat.
- **SenderIP** ist die vom Ersteller der Abgabe verwendete IP-Adresse. Zu Protokollierungszwecken wird diese erstellt.
- **Der Zeitstempel**, zu dem die Abgabe erstellt wurde.
- **Hinweise / Kurznotizen** können optional an die Abgabe angehängt werden Z.B Signatur

Überprüfung der Absenderadresse

Dies geschieht, indem jeder verifizierten E-Mail-Adresse ein Token zugewiesen wird, dass sie an ZendTo zurückgeben müssen, um zu beweisen, dass sie der Eigentümer der von ihnen verwendeten E-Mail-Adresse sind. Diese Token verfallen und werden auch sofort nach der Verwendung gelöscht, sodass keine Wiedergabeangriffe möglich sind.

Aufforderung zur Abgabe

Wenn ein Absender aufgefordert wurde, einige Dateien abzugeben, umgeht diese Person die Überprüfung der E-Mail-Adresse da angenommen wird, dass diese dem Endempfänger der Abgabe bekannt sind.

Das Token, das ihnen in der E-Mail-Nachricht übergeben wird, besteht aus 3 Wörtern, von denen jedes 3 oder 4 Buchstaben lang ist. Dies macht es sehr einfach, das Token per Telefon weiterzuleiten, wenn der Empfänger die Dateien dringend benötigt und nicht darauf warten kann, dass die E-Mail den Absender erreicht. Das Token kann vom Absender direkt in ein Webformular eingegeben werden.

Die Token verfallen nach einigen Stunden und werden sofort nach Gebrauch gelöscht, so dass keine Wiedergabeangriffe möglich sind.

Benutzerverwaltung

Einer der verfügbaren Authentifikatoren ist "Local", um die Anmeldeinformationen und den Namen jedes Benutzers zu speichern, der sich bei ZendTo anmelden darf. Dabei wird das

Kennwort selbst nicht gespeichert, sondern nur ein 1-Wege-Hash des Kennworts, der ausreicht, um den Anmeldeversuch zu verifizieren, der jedoch nicht mit dem Kennwort des Benutzers entschlüsselt werden kann.

Wenn ein Benutzer versucht, sich in zu kurzer Zeit zu oft erfolglos anzumelden, wird er für eine konfigurierbare Zeitspanne vollständig gesperrt. Dies vereitelt Versuche, mit ZendTo die Passwörter der Benutzer zu erraten.

Die Daten werden in der Tabelle "loginlog" gespeichert und geben nur an, wie oft ein Benutzer sich nicht nacheinander angemeldet hat und wann der erste erfolglose Versuch stattgefunden hat. Die Logdaten für den Benutzer werden gelöscht, sobald die Sperrzeit abgelaufen oder manuell aufgehoben worden ist, wodurch der Zähler für den Benutzer zurückgesetzt wird.

Verschlüsselungsstärken

Der Vorgang, bei dem ein Benutzer zum Hochladen einer Abgabe aufgefordert wird, umfasst die Erstellung einer Zeichenfolge aus 3 verschiedenen Wörtern mit jeweils 3 oder 4 Buchstaben. Da es im Englischen ungefähr 3000 solcher Wörter gibt, ergibt dies eine Anzahl möglicher Zeichenketten von ungefähr 3000 ^ 3 = 27.000.000.000 Möglichkeiten. Hier die zufällige Kombination zu finden innerhalb der Gültigkeit des Token ist mathematisch unmöglich.

Sicherheitsabwehrmaßnahmen

ZendTo wurde von Grund auf mit Blick auf die Sicherheit entwickelt, so dass es nicht für Angriffe auf seine Weboberfläche offen ist. Hier sind einige der Maßnahmen, die zur Verteidigung ergriffen wurden:

- Benutzer, die sich nicht anmelden können (d.h. Benutzer, die nicht registriert sind), können nur Dateien an Personen senden, wenn sie dazu aufgefordert werden. Es kann nicht dazu verwendet werden, um Dateien von einem Nichtmitglied an ein anderes Nichtmitglied zu senden.
- Die gesamte Kommunikation über das Web wird verschlüsselt mit SSL erfolgen.
- Der gesamte Authentifizierungsverkehr zwischen dem ZendTo Server und seinen Authentifizierern wird mit SSL verschlüsselt werden.
- Benutzerkennwörter werden nicht gespeichert. Stattdessen wird ein Einwort-Hash der Passwörter gespeichert, der ausreicht, um Benutzer zu authentifizieren.
- Alle eingegebenen Benutzernamen werden mit einem konfigurierbaren regulären Ausdruck verglichen, wodurch LDAP-Injection-Angriffe (Potenzielle nicht vertrauenswürdige Eingaben) vermieden werden.
- Alle eingegebenen E-Mail-Adressen werden gegen einen regulären Ausdruck geprüft, wodurch Angriffe auf das E-Mail-Routing durch Methoden wie "%" in einer Adresse ausgeschlossen werden.
- Alle in einem Webformular eingegebenen Werte sind so codiert, dass sie nicht-alphabetische Zeichen verarbeiten können, wodurch SQL-Injection- und HTML-Injection-Angriffe (Potenzielle nicht vertrauenswürdige Eingaben) vermieden werden.
- Alle in einem Webformular eingegebenen Werte werden mit konfigurierbaren regulären Ausdrücken verglichen, um unbekannte Angriffe auszuschließen.
- Da es in PHP geschrieben ist, werden die meisten Pufferüberlaufangriffe eliminiert.
- Die Dateinamen der Benutzer werden niemals direkt im Dateispeicher verwendet, in dem alle aktuellen Dateien gespeichert sind. Sie werden alle durch zufällige Zeichenfolgen ersetzt, sodass das Durchsuchen des Dateisystems für einen Benutzer, der Zugriff auf das Dateisystem hat, nur sehr wenige nützliche Informationen liefert. (nicht name.pdf sondern xge&ds8kf1).
- Alle Aktivitäten werden sowohl von ZendTo als auch vom Webserver protokolliert.
- Alle an einer Abgabe oder Abholung beteiligten IP-Adressen werden protokolliert und an den Benutzer gesendet, sodass Angriffsversuche nachvollziehbar sind.
- In allen E-Mail-Nachrichten an Benutzer wird deutlich hervorgehoben, dass sie dem Link in der Nachricht nur folgen müssen, wenn sie damit gerechnet haben, dass sie diese erhalten und wenn nicht, sie vollständig zu ignorieren.

- Nicht authentifizierte Benutzer müssen nachweisen, dass sie die E-Mail-Adresse besitzen, die sie verwenden möchten, indem sie einen Authentifizierungsschlüssel vorlegen, der ihnen per E-Mail zugesandt wird.
- Alle Authentifizierungstokens dürfen nur einmal verwendet werden, um Wiedergabeangriffe auszuschließen.
- Alle "Request for Dropoff" -Token dürfen nur einmal verwendet werden, um Wiedergabeangriffe auszuschließen.
- Wiederholte fehlgeschlagene Anmeldeversuche in einem konfigurierbaren Zeitraum führen dazu, dass der Benutzer für einen konfigurierbaren Zeitraum gesperrt wird, wodurch Brutal-Force-Angriffe zum Löschen von Kennwörtern vermieden werden.
- Alle hochgeladenen Dateien werden auf Viren überprüft und die gesamte Abgabe wird abgelehnt, wenn festgestellt wird, dass eine Datei infiziert ist.
- Der Ausfall des Virenscanners führt dazu, dass alle Abgaben abgelehnt werden, wodurch Angriffe ausgeschlossen werden, die versuchen, den Virenscanner zu umgehen, indem er zerstört wird.
- Alle hochgeladenen Daten können durch den User manuell gelöscht werden, wenn diese abgerufen wurden.
- Das System löscht alle alten Daten nach einer voreingestellten Zeit.
  Z.B älter als 14 Tage.

Additional settings (zusätzliche Einstellungen für VIP Kundenpakete)

Folgende Einstellungen sind möglich .

- Eingrenzung der IP Adresse damit sich ausschliesslich Mitarbeiter nur mit ihrer dienstl. IP Adresse einloggen können.
- Bibliothek für Alle oder jeden einzelnen Nutzer. Dient dazu um wiederholende Dateien nicht immer erneut hochladen zu müssen, sondern gleich aus der Bibliothek einzufügen. Sinnvoll bei Dateien mit mehreren Megabyte Größe.
- Passphrase/Geheimwort
  - AUS 2. Authentifizierung entfällt
  - EIN / AUS ist eingeschaltet kann aber ausgeschaltet werden
  - EIN Geheimwort ist immer erforderlich.(aktiv)
- Geheimwort wird nicht gespeichert und muss anderweitig an den Empfänger übertragen werden. Bei Anforderungen wird das Geheimwort nur von dem anfordernden Benutzer vergeben. Der Aufgeforderte gib die Daten ab welche automatisch mit dem Geheimwort verschlüsselt werden.