Sicherheitskonzept top.legal

Datum: Januar 2020

Einleitung

Angesichts der ernsten Bedrohungslage, in dem die sensiblen Daten vieler der weltweit bekanntesten Organisationen immer wieder offengelegt werden, ist die Aufmerksamkeit für das Thema Datensicherheit, weiterhin oft erschreckend gering. Während hochsensible Finanzinformationen oftmals streng kontrolliert werden, wird die Sicherheit anderer Daten oft vernachlässigt. Dies gilt auch für Rechtsinformationen, aus denen sich leicht Firmengeheimnisse und Strategien ableiten lassen.

Bei top.legal wird Datensicherheit groß geschrieben. Dabei verfolgen wir einen gesamtheitlichen Ansatz. Neben der Verschlüsselung und Sicherheit der EDV-Infrastruktur steht die Zugriffskontrolle auf Daten ganz oben.

Selektiver Benutzerzugang und Zugriffskontrolle

Die Zugriffskontrolle ist ein Sicherheitsmechanismus, der die Fähigkeit eines Benutzers regelt, sich mit einem Netzwerk zu verbinden, Ressourcen anzuzeigen und/oder eine Transaktion durchzuführen. Der Prozess umfasst die Identifizierung von Ressourcen, auf die Benutzer zugreifen dürfen, die Verwendung von Anmeldeinformationen zur Authentifizierung von Benutzern und die Autorisierung des Zugriffs auf die zugelassenen Ressourcen.

Bei top.legal sind Zugriffskontrolle und rollenbasierte Rechte das Herzstück unserer Softwarearchitektur. Benutzer können zu jedem Zeitpunkt nur auf Daten zugreifen, für die sie explizite Rechte haben. So ist jeder einzelne Datenbankeintrag durch ein passendes und eindeutiges Zugriffsrecht gesichert und kann nur bei Übereinstimmung der Sicherheitsdetails aufgerufen werden.

Die Zugriffsrechte auf top.legal sind zusätzlich granularisiert, so dass die Benutzer den Teams und Benutzern nur die Rechte zuweisen können, die sie für ihre Arbeit benötigen, und nicht mehr. Die Vergabe der geringsten Rechte an Benutzer vermeidet nicht nur neugierige Blicke auf sichere Daten, sondern macht auch versehentlichen Änderungen an Vorlagen durch unqualifiziertes Personal ein Ende.

Verschlüsselte Sicherheits-Token

Jede Benutzeranfrage an die Anwendung und die Datenbanken wird durch ein branchenüblichen Sicherheitszugriffstoken verifiziert. Der Token wird bei der Anmeldung

des Nutzers generiert und stündlich aktualisiert. Der Zugriffs-Token enthält eine JWT-Signatur, die bei der Signaturerstellung durch einen der zwei privaten RSA-Schlüssel auf den Servern verschlüsselt wird. Jeder Zugriff auf die Server muss den JWT-Signaturvalidierungsprozess durchlaufen und als nicht abgelaufen verifiziert werden. Nur registrierte Benutzer können ein gültiges JWT-Token erzeugen.

Selektiver und sicherer Zugang zur API

Das API-Gateway ist das Herzstück unserer API-Management-Lösung. Es fungiert als einziger Zugang zu unserem System und ermöglicht es mehreren APIs und Microservices, zusammenhängend zu agieren und dem Benutzer ein einheitliches Erlebnis zu bieten. Die wichtigste Rolle, die das API-Gateway spielt, ist die zuverlässige Verarbeitung jedes API-Aufrufs und die Überprüfung der Berechtigung der Anfrage.

Aus Sicherheitsgründen und der oben genannten Zulässigkeit von Anfragen sind alle Aufrufe an das top.legal API-Gateway nur dann zulässig, wenn die Anfrage mit einem gültigen Sicherheitstoken versehen ist. Die Sicherheitstoken werden verifiziert, bevor die Anfrage durch das Gateway geleitet wird. Ungültige Requests werden mit einer Fehlermeldung zurückgegeben, die eine unqualifizierte Verwendung verhindert.

Unser API-Gateway unterstützt Drosselungseinstellungen für jede Methode oder Route und schützt so unsere Backend-Systeme vor Distributed-Denial-of-Service (DDoS)-Angriffen, unabhängig davon, ob sie mit gefälschten Anfragen (Layer 7) oder SYN-Floods (Layer 3) angegriffen werden.

Trennung von Front-end Funktionalitäten

Wir sind der festen Überzeugung, dass eine Trennung der Zugriffsrechte, die durch unser sicheres API-Gateway und den selektiven Benutzerzugang auf unserem Backend gegeben ist, sich auch auf dem Frontend unserer Anwendung fortsetzen muss. Wir haben diesen Gedanken umgesetzt, indem wir Funktionalitäten aus dem Client-Frontend herausgenommen haben, die für einen bestimmten Benutzer nicht unbedingt erforderlich sind. Folglich hat jeder Benutzer nur Zugriff auf die Funktionen und Funktionalitäten, die für die Ausführung der für seine Rolle notwendigen Operationen notwendig sind.

Ansichten für den Zugriff auf zusätzliche Funktionen sind nur verfügbar, wenn sich die Rolle des Benutzers ändert oder wenn zusätzliche Rechte durch ein Upgrade oder eine bewusste Änderung durch einen Administrator verfügbar gemacht wurden.

Datei-Sicherheit

Alle hochgeladenen Dateien folgen den Prinzipien der geringsten Privilegien. Standardmäßig sind alle Dateien privat und geschützt und können nur von Benutzern mit expliziter Zugangsberechtigung aufgerufen werden. Alle über die Anwendung top.legal

hochgeladenen Dateien sind schreibgeschützt, es sei denn, es werden explizite Bearbeitungsrechte erteilt.

Alle Dateien werden über ein verschlüsseltes und sicheres Netzwerkprotokoll (TLS) hochgeladen, um potenzielle Angreifer daran zu hindern, den Netzwerkverkehr durch Person-in-the-Middle- oder ähnliche Angriffe zu belauschen oder zu manipulieren. Standardmäßig ist der öffentliche Zugriff auf die Dateispeicher ausgeschlossen.

Alle Dateien werden sofort redundant in mehreren unabhängigen Datenzentren gespeichert und bieten eine Haltbarkeit der Objekte von 99,99999999999% über ein bestimmtes Jahr. Diese Haltbarkeitsstufe entspricht einem durchschnittlichen jährlichen erwarteten Verlust von 0,00000000001% der Objekte. Wenn Sie zum Beispiel 10.000.000 Objekte mit Amazon S3 speichern, können Sie im Durchschnitt damit rechnen, dass ein einzelnes Objekt alle 10.000 Jahre verloren geht.

Sicherheitsprotokolle und Bereitstellung von Inhalten

Alle unsere Inhalte werden über TLS-Verbindungen ausgeliefert. Die Zertifikate werden regelmäßig und automatisch erneuert, um die neuesten Sicherheitsalgorithmen zu berücksichtigen und damit die Wahrscheinlichkeit von Man-in-the-Middle-Angriffen zu reduzieren.

Darüber hinaus bieten unsere Server eine ständig aktive Überwachung der Nutzeranfragen, die den eingehenden Datenverkehr prüft und eine Kombination aus Verkehrssignaturen, Anomalie-Algorithmen und anderen Analysetechniken verwendet, um bösartigen Datenverkehr in Echtzeit zu erkennen.

Das Senden und Abrufen von Informationen an unsere Backend-Systeme erfolgt über das TLS-Protokoll, um Abhören und Manipulation zu verhindern. TLS bietet zudem nicht nur Verschlüsselung für sensible Daten während der Übertragung, sondern überprüft auch die Identität der Verbindung zwischen Browser und der top.legal-Anwendung. Somit können Nutzer jederzeit zweifelsfrei feststellen, dass es sich beim Empfänger der Daten, um die top.legal Server handelt.

Vollständige Verschlüsselung

Alle Benutzerdaten, die in unseren Datenbanken gespeichert werden, sind im Ruhezustand vollständig verschlüsselt. Die Verschlüsselung im Ruhezustand bietet eine erhöhte Sicherheit, indem alle Benutzerdaten im Ruhezustand mit 256-bit Advanced Encryption Standard (AES-256) Schlüsseln verschlüsselt werden.

Während der Übertragung zwischen dem Browser und der Datenbank werden die Daten mit dem TLS-Protokoll verschlüsselt.

Datenspeicherung und mehrfache Redundanz

Unser Datenbankservice verteilt die Daten und den Datenverkehr automatisch auf eine ausreichende Anzahl von Servern, um den Durchsatz und die Speicheranforderungen zu bewältigen und gleichzeitig eine konsistente und schnelle Leistung zu gewährleisten. Alle unsere Daten werden auf Solid-State-Disks (SSDs) gespeichert und automatisch über mehrere unabhängige Verfügbarkeitszonen repliziert, wodurch eine hohe Verfügbarkeit und Datenhaltbarkeit gewährleistet wird.

Darüber hinaus erstellen wir kontinuierlich in regelmäßigen Abständen On-Demand-Backups, die ein vollständiges Backup der einzelnen Datenbanktabellen erstellen, und wir führen kontinuierliche Backups der Tabellen der letzten 35 Tage. Die Point-in-Time-Recovery hilft uns, unsere Tabellen vor versehentlichen Schreib- oder Löschvorgängen zu schützen.

DS-GVO Compliance

Unsere Maßnahmen zur DS-GVO Compliance entnehmen Sie bitte u.a. unseren technisch organisatorischen Maßnahme, die wir über folgenden Link öffentlich gemacht haben:

www.top.legal/de/toms