

SHINE

Whitepaper



IT Consulting
Betriebsautomatisierung
Enterprise Web Applications

Projekt	SHINE
Branche	Agentur / Textil
Laufzeit	6 Monate

Situation

Der Auftraggeber bildet seine Mitarbeiter mit einer internen Exzellenzinitiative konsequent weiter. Dazu stellt er umfangreiches Schulungsmaterial zur Verfügung, in dem unter anderem auch sensibles Fakten- und Prozess-Know-How des Konzerns vermittelt werden. Diese Unterlagen, die umfangreiches Multimedia-Material enthalten, müssen zeitnah nach Veröffentlichung in vielen Ländern der Welt allen relevanten Mitarbeitern zur Verfügung stehen. Bedingt durch die teilweise unzureichende Netzwerkbandbreite kann dieses Material oft nicht ad-hoc aus dem Netz bezogen werden, sondern muss per Update verteilt und lokal gespeichert werden. Wegen der inhaltlichen Sensibilität müssen die Daten sowohl bei Transport als auch bei der lokalen Speicherung stark verschlüsselt sein. Um eine zufällige oder absichtliche Weitergabe an Dritte zu verhindern, sollen die Materialien zusätzlich personalisiert werden.

Aufgabe

Dr. Hagen & Partner wurden beauftragt, in Kooperation mit der Multimedia-Agentur, die die Schulungsmaterialien herstellt, eine Lösung auf Basis von firmeneigenen USB-Sticks zu entwickeln, die sowohl als Speichermedium für die Daten dienen als auch die notwendige Software für Zugriff und Update enthalten können. Jeder Stick soll im System registriert und einem Nutzer zugeordnet sein. Nur mit dem richtigen Stick und korrekten Zugangsdaten darf der Mitarbeiter auf die Daten zugreifen.

Das bereits existierende Schulungsmodul auf Basis von Flash musste in die Lösung eingebunden werden; es sollte sowohl online als auch offline gleichermaßen funktionieren. Das System soll 48 Stunden offline funktionieren, anschließend aber wieder eine Anmeldung im Netz (und ggf. zwingende Updates) verlangen. Auf Serverseite soll eine webbasierte Oberfläche die Pflege der Daten, die Zuweisung von verschiedenen Datensätzen zu Sticks/Mitarbeitern sowie die Kontrolle über die Sticks erlauben.

Im Notfall soll das System verlorene oder gestohlene Sticks per Remotebefehl löschen können.

Vorgehen

Auf Basis der bereits beschafften USB-Sticks und des Flash-Moduls wurde von uns zunächst ein Vorprojekt durchgeführt, um die technische Machbarkeit des Projekts sicher zu stellen. Dabei wurden Schlüsselkomponenten identifiziert, mit denen das Projekt umgesetzt werden konnte.

Anschließend wurde in Zusammenarbeit mit der Multimedia-Agentur eine Gesamtlösung konzipiert, spezifiziert und dem Auftraggeber vorgestellt. Im Rahmen der anschließenden Beratung konnten noch letzte Korrekturen an den technischen Randbedingungen im Konzept berücksichtigt werden.

Die Software wurde innerhalb weniger Wochen realisiert, getestet und an die Multimedia-Agentur ausgeliefert, die den Betrieb der Plattform übernimmt. In mehreren Integrations- und Lasttests konnte dargestellt werden, dass das System einwandfrei funktioniert, die Daten gegen übliche Entschlüsselungsangriffe geschützt und die Personalisierung nicht ohne weiteres zu Entfernen ist. In einer Teststellung konnten wir den Kunden von der Leistung des Systems überzeugen.

Den abschließenden Roll-Out haben wir gemeinsam mit der Multimedia-Agentur begleitet. Das System ist seit 2012 im produktiven Einsatz und wird intensiv genutzt.

Technik

Das entstandene System besteht aus mehreren Modulen. Die Serverseite wurde auf Basis von C#/.NET/MVC & Bootstrap entwickelt, auf Client-Seite kommt eine WPF-Anwendung zum Einsatz.

Auf Serverseite können die vorhandenen Dokumente in verschiedene Sprachen gepflegt und in Lernmodulen einzelnen Usern zugewiesen werden. Eine Update-Historie gibt Aufschluss über den Stand der Verbreitung aktualisierter Daten. Eine Umstellung einzelner Sticks auf verschiedene Lernmodule ist möglich; die neuen Daten werden im Hintergrund automatisch ausgeliefert.

Die Client-Anwendung startet automatisch vom USB-Stick aus und installiert nach erfolgreicher Authentifizierung des Nutzers einen Treiber für den Zugriff auf die verschlüsselten Dateien.

Die auf dem USB-Stick ausgelieferten Daten werden während der ersten Registrierung des Sticks von einem systeminternen Auslieferungsschlüssel auf einen persönlich Private Key des Nutzers umgeschlüsselt; während dieses Prozesses werden die Daten bereits personalisiert, so dass Daten und Stick nach der Erstanmeldung eindeutig dem User zuzuordnen und nur von ihm zu entschlüsseln sind.

Der Flash-Client startet nach der Authentifizierung ebenfalls automatisch vom USB-Stick und kann, so lange der Stick aktiv ist, über den Zugriffstreiber transparent auf die verschlüsselten Daten zurückgreifen. Für den Benutzer ist der Vorgang nicht ersichtlich, der Flash-Client verhält sich online wie offline völlig gleich. Der Zugriff auf entschlüsselte Dateien via Datei-Explorer ist hingegen nicht möglich; auch dann nicht, wenn die Datei gerade geöffnet ist.