



Specsavers

CASE STUDY

Die multinational aufgestellte Optikerkette Specsavers musste zügig den Fernzugriff auf ihre Netzwerk absichern und gleichzeitig das schnelle Wachstum des Unternehmens berücksichtigen. Der SafeNet Authentication Service erwies sich als die richtige Lösung.

Das Unternehmen

Specsavers wurde 1984 mit zwei Büros in Großbritannien gegründet. Heute unterhält das Unternehmen in Europa und dem asiatisch-pazifischen Raum 1.300 Niederlassungen mit 26.000 Beschäftigten. Specsavers hat einen guten Ruf als zuverlässiger und preiswerter Anbieter und setzt überwiegend auf ein Joint-Venture-Modell. Eine geringere Anzahl von Läden sind vollständig im Besitz des Unternehmens oder werden von Franchise-Partnern betrieben.

Vorteile

Zunächst wurde der SafeNet Authentication Service für eine Gruppe von 700 Benutzern eingeführt. Es zeigte sich, dass alle Anforderungen, die Specsavers anfänglich an die Sicherheitslösung stellte, erfüllt oder sogar übertroffen wurden.



Authentication SERVICE

Unternehmensanforderung: Optimale Sicherheit

Specsavers steht im Ruf, schnell auf Marktchancen zu reagieren. Ebenso zügig reagiert das Unternehmen auf mögliche Risiken. Specsavers ist sich über eventuelle Sicherheitsprobleme eines schnell wachsenden, multinationalen Unternehmens im Klaren. Aktuell greifen Hunderte von Anwendern jeden Tag remote auf zentrale Ressourcen wie E-Mail, Web-Anwendungen oder Finanzapplikationen zu. Um den Schutz der Unternehmensdaten zu gewährleisten, war eine Datensicherheitsstrategie notwendig.

Skalierbar, flexibel, einfach

Mit dem starken Wachstum der vergangenen zehn Jahre stieg auch die Zahl der Beschäftigten und damit der Bedarf nach einer sicheren Methode für den Fernzugriff. Specsavers benötigte somit eine Lösung, die:

- skalierbar ist und den Personalzuwachs in bestehenden und neuen Märkten abdeckt;
- flexibel genug ist, um den unterschiedlichen Nutzerprofilen und technischen Möglichkeiten gerecht zu werden;
- einfach zu administrieren ist;
- und die Kosten für Deployment und im laufenden Betrieb reduziert.

Lösung

Specsavers Wahl bei der Absicherung des Fernzugriffs auf die internen Anwendungen und Datenbanken fiel auf den SafeNet Authentication Service (SAS).

Mit SAS verfügt Specsavers nun über die Möglichkeit, Authentisierungs-Token weltweit und nach Bedarf über eine, abgestufte Benutzergruppenstruktur auszurollen. Die einzelnen Niederlassungen wurden im Portal des SafeNet Authentication Service als Gruppen angelegt. Die Zentrale von Specsavers kann so die Verwaltung der jeweiligen Gruppe an einen Administrator vor Ort delegieren.

Specsavers entschied sich für einen Mix verschiedener Token-Formate aus Hardware, Software und SMS, um den unterschiedlichen Benutzeranforderungen gerecht zu werden. Mit Einführung des SafeNet Authentication Service ermöglicht Specsavers seinen mobilen Mitarbeitern und Remote-Benutzern den einfachen, sicheren Zugang zu den Unternehmensressourcen und Anwendungen.

Skalierbarkeit und Empowerment

Das kurzfristige Ziel von Specsavers war es, mit dem Einsatz der Zwei-Faktor-Authentisierung in den Büros in Großbritannien und Irland zu starten und dann international auszuweiten.

Ein kritischer Aspekt, um das gesteckte Ziel zu erreichen, ist die Funktion der gestaffelten Benutzergruppen, mit der die Belastung für die zentrale IT-Abteilung bei Specsavers reduziert wird. Die Niederlassungen sind selbst für Zuweisung und Rücknahme der Token nach Bedarf verantwortlich. Der SafeNet Authentication Service die einzige Lösung am Markt, die dies ermöglicht. Specsavers kann dadurch von der Skalierbarkeit eines globalen Dienstes profitieren, anstatt verschiedene Server für die einzelnen Niederlassungen beschaffen und betreiben zu müssen.

„Wir haben nun mehr als zwei Jahre lang den SafeNet Authentication Service im Einsatz und mussten bisher weder Token noch Batterien ersetzen. Der Einsatz zuverlässiger, langlebiger Token senkt deutlich die Kosten und schont unsere Ressourcen. Wir profitieren schon jetzt davon.“

Angus Dorey, IT-Security Manager bei Specsavers

Langlebige Token

Specsavers nutzt eine Mischung aus Hardware-, Software- und SMS-Token. Software-Token eignen sich besonders für Anwender, die mit ihrem Desktop-PC oder einem Notebook arbeiten. Für Benutzer mit hohen Mobilitätsanforderungen wurden Blackberry-Token eingeführt. Und Anwender, die Hardware-basierende Token bevorzugen, wurden mit so genannten Keyfob-Token ausgestattet.

Soft- und SMS-Token senken erheblich die Kosten. Die Keyfob-Token verfügen zudem über fünf Jahre Garantie und haben kein Ablaufdatum. Sollte die Batterie leer sein, kann sie einfach vom Benutzer ersetzt werden. In der Vergangenheit waren Hardware-Token für Specsavers problematisch, da sie innerhalb von drei Jahren abliefen.

Geringere TCO

Specsavers vertraut auf die transparente jährliche Servicegebühr des SafeNet Authentication Service. Diese beinhaltet die Software-Komponenten und Anwendungen des Dienstes. Mit diesem Kostenmodell konnte Specsavers aufwändige Kalkulationen sowie Vorabinvestitionen in Hard- und Software ausräumen. Die Komplexität und Kosten der Implementierung und des laufenden Betriebs wurden gesenkt und die IT-Mitarbeiter bei Specsavers können sich auf lohnendere Tätigkeiten konzentrieren.

Ausblick

Im Rahmen der sich verändernden Vorgaben im Gesundheitswesen werden in naher Zukunft auch sensible Patientendaten für die Specsavers-Mitarbeiter aus der Ferne verfügbar sein. Specsavers ist sich sicher, dass die Zwei-Faktor-Authentisierung des SafeNet Authentication Service die gesetzlichen Vorgaben für den Remote-Zugriff auf solche Daten erfüllen wird.

„Der SafeNet Authentication Service eröffnet Specsavers einige Vorteile. Die gestaffelten Benutzergruppen ermöglichen es uns, Zwei-Faktor-Authentisierung global auszurollen, während die Administration lokal delegiert wird. Die Token erweisen sich als kostengünstiger und die Technologie bietet uns das höchste Sicherheitsniveau, das am Markt verfügbar ist. Das Feedback unserer Büros und der Endanwender war sehr positiv.“

Angus Dorey, IT-Security Manager bei Specsavers

Über SafeNet Authentication Service

Der SafeNet Authentication Service bietet vollständig automatisierte, hoch sichere Authentisierung „as a Service“ mit flexiblen Token-Optionen. Diese sind maßgeschneidert für den individuellen Bedarf Ihres Unternehmens und senken die Betriebskosten erheblich.

Starke Authentisierung leicht gemacht – dank der Flexibilität und Skalierbarkeit der automatisierten Workflows des SafeNet Authentication Service, seiner herstellerunabhängigen Token-Integration und umfassenden APIs. Zudem sind auch die Management-Funktionen vollständig automatisiert und anpassbar. Für eine nahtlose und bessere Benutzerfreundlichkeit.

Da keine Infrastruktur benötigt wird, ermöglicht der SafeNet Authentication Service die schnelle Migration auf eine mehrschichtige, mandantenfähige Cloud-Umgebung und schützt alles: Von Cloud-basierenden und vor Ort installierten Anwendungen über Netzwerke bis hin zu den Benutzern und Geräten.



Authentication SERVICE



THE
DATA
PROTECTION
COMPANY

Kontakt: Alle Niederlassungen und Kontaktinformationen finden Sie im Internet unter www.safenet-inc.com

Folgen Sie uns: www.safenet-inc.com/connected

©2012 SafeNet, Inc. Alle Rechte vorbehalten. SafeNet und das SafeNet Logo sind eingetragene Marken von SafeNet. Alle anderen Produktnamen sind eingetragene Marken ihrer jeweiligen Eigentümer. CS (DE) A4-11.13.12