

TALUS Informatik AG

Einsatz einer Zwei-Faktoren Authentifizierung in einem Rechenzentrum

Success Story

September 2014



Talus Informatik AG

Die Talus Informatik AG ist ein IT-Dienstleister mit heute 75 Mitarbeitenden am Firmenstandort Wiler bei Seedorf im Berner Seeland. Talus hat sich spezialisiert auf Gesamtlösungen für Städte, Gemeinden, Kirchgemeinden und Energieversorger (EVU). Das Service-Portfolio umfasst die integrierte Lösung NEST/IS-E mit ABACUS als ERP, Software im Bereich GEVER (CMIAXIOMA), Vorlagen-Management (officeatwork), Software und Dienstleistungen im Web-Bereich (CMS-Projekte, Mail- und Webhosting) sowie Dienstleistungen und Produkte im Hardware-Bereich. Ein Grossteil der eingesetzten Applikationen ist Swiss Made Software, was durch den Kundenstamm sehr geschätzt wird. Den Kunden bietet Talus auf Wunsch „Alles aus einer Hand“ - sei dies als Inhouse-Installation oder Full-Outsourcing im hauseigenen Rechenzentrum.

Für den sicheren Benutzerzugriff auf die bereitgestellten Citrix-Applikationen via Web Interface setzte die Talus in der Vergangenheit zwei unterschiedliche Lösungen ein. Diese basierten auf Hardware-Tokens oder auf X.509 Zertifikaten. Beide Lösungen sind kostenintensiv, da sowohl die Token als auch die Zertifikate nach einer bestimmten Zeit erneuert werden müssen. Bestellung, Kauf und Verteilung sind teilweise mühselig und fehleranfällig. Die Tokenlösung und ein Teil der zertifikatsbasierten Lösung wird nach ihrem Ablauf sukzessive auf die M.ID Suite der Firma Swiss SafeLab, Bern migriert. „Den grossen Nutzen sehen wir in den sinkenden Betriebskosten, der einfachen Administration und darin, dass der Kunde auch Devices ohne USB Schnittstelle nutzen kann, die er in Kombination mit Zertifikaten sonst nicht nutzen könnte“, so Michael Weissbach.

"Wir suchten eine Zwei-Faktoren Authentifizierungs-Lösung mit einem pragmatischen Lösungsansatz für unsere Kunden und für uns selber. Heute können wir schnell und ohne grossen technischen respektive administrativen Aufwand neue Benutzer aufschalten. Die M.ID Suite brachte den erwarteten Mehrwert."

*Michael Weissbach
Mitglied der Geschäftsleitung*



Firmensitz

Talus Informatik AG
Stückirain 10
CH-3266 Wiler bei Seedorf

www.talus.ch

Organisation

Lösungsanbieter für Gemeinden, Städte, Kirchgemeinden und Energieversorger.

Betrieb eines Kunden-RZ

Eigene Web-Abteilung mit Mail / Web Hosting

2012 Evaluation einer neuen Lösung

Evaluationsbericht von Hr. Weissbach, Geschäftsleitungsmitglied Talus Informatik: „Die neue Lösung wurde für die Nutzung durch Talus und ihre Kunden evaluiert. Bei den Kunden stand die einfache und rasche Abwicklung für eine Bestellung und Aufschaltung neuer Benutzer im Vordergrund. Die Lösung musste iPad, Android und andere Tablets unterstützen, da die Nutzung von USB-Tokens mit entsprechendem Zertifikat, aufgrund fehlender USB-Schnittstelle, sonst nicht möglich ist. Die dritte wichtige Anforderung war die Mehrfachredundanz, um eine maximale Verfügbarkeit ohne Mehrkosten sicherzustellen. Deshalb war für uns schnell klar, dass die neue Lösung ausschliesslich Software basiert sein musste.“

Die Evaluation der M.ID Suite war relativ einfach und basierte auf Produkt-Erfahrungen eigener Mitarbeiter sowie Referenzen der Firma Comset. Die Einführung bzw. Umstellung erfolgt nun schrittweise und ist noch nicht abgeschlossen. Wenn ein Token oder X.509 Zertifikat end of life ist wird der Benutzer wo immer möglich und sinnvoll auf M.ID migriert.“



Rechenzentrum / Dienstleistungsbereitstellung

Swiss SafeLab GmbH

Die Swiss SafeLab GmbH gehört zu den führenden Anbietern von Zwei-Faktoren-Authentisierungsprodukten und SMS Providing im Schweizer Markt. Das Schweizer Unternehmen wurde 2005 gegründet. Zu den Kunden zählen unter anderem die Stadt Bern, BKW Energie AG, Energie Wasser Bern (EWB) und das Schweizerische Rote Kreuz.

Mit der rein softwarebasierten Swiss SafeLab M.ID Suite kann sich ein Benutzer auf verschiedenste Arten von Remote am Firmennetz anmelden. Es stehen App, SMS, E-Mail, Telefon und Token zur Verfügung. Bei Verlust des Mobiltelefons findet via Fallback-Szenarien, wie das Versenden des OTP auf alternative Nummern, weiterhin eine sichere Authentifizierung statt. Die Benutzer-Anmeldung erfolgt über diverse Agenten, die den zweiten Faktor an den M.ID Server weiter geben. Der M.ID Server ist das Herzstück der Lösung, er prüft den zweiten Faktor und steuert das SMS Providing.

Swiss SafeLab GmbH

Neuengasse 20

CH-3011 Bern www.swiss-safelab.com

+41 31 932 31 86 info@swiss-safelab.com

Erfahrung / Ergebnis

F: Was gefällt Ihnen an der neuen Lösung?

A: Da wir auch die Logistik der Zwei-Faktoren Authentisierungslösung für unsere Kunden sicherstellen, gefällt uns der einfache Bestell-, Implementierungs- und Übergabeprozess. Es gibt kein Ablaufdatum und keine Zustellung von Equipment. Das bringt eindeutige zeitliche und monetäre Vorteile für uns und die Endkunden.

F: Wie haben die Beteiligten von der Lösung profitiert?

A: Wir sehen für Kunden wie Mitarbeiter einen grossen Mehrwert beim Einsatz von Tablets und Smartphones, um jederzeit auf Applikationen und Daten zuzugreifen. Der Zugriff ist unabhängig von zusätzlichen Tokens oder USB Sticks.

F: Was war speziell aus der Sicht eines Rechenzentrums wichtig?

A: Eine einheitliche und flexible Lösung, die der Kunde für unterschiedlichste Services nutzen kann. Was der Kunde nicht sieht ist die Gewährleistung einer sehr hohen Verfügbarkeit ohne entsprechende Mehrkosten.

F: Wie war die Zusammenarbeit mit Swiss SafeLab?

A: Wir haben heute eine sehr enge und partnerschaftliche Beziehung zu Swiss SafeLab. Swiss SafeLab führt heute ihre Reseller-Schulungen in unseren Schulungsräumen durch.