pro infirmis

BOLL
IT Security Distribution

PRO INFIRMIS SICHERT REMOTE-ZUGRIFF AUF DATEN UND APPLIKATIONEN MIT VASCO

STARKE AUTHENTISIERUNG

Im Bestreben, den Remote-Zugriff auf Daten und Applikationen wirksam zu schützen und zugriffsberechtigte Personen bei deren Anmeldung sicher zu authentisieren, setzt Pro Infirmis auf die moderne «Multi Factor Authentication»-Gesamtlösung von VASCO. Diese beinhaltet den Authentifizierungsserver IDENTIKEY und den OTP-Token DIGIPASS.

IDENTIKEY
Authentication Server

«Wer ist schon perfekt. Kommen Sie näher.» Mit dieser durch eine starke Bildsprache geprägten Kampagne macht Pro Infirmis auf beeindruckende Art und Weise auf die zentralen Themen ihrer Tätigkeit aufmerksam. Beispielsweise auf die Solidarität zwischen behinderten und nicht behinderten Menschen, auf das Recht aller Menschen, das Leben nach ihren Möglichkeiten selbstbestimmt und eigenverantwortlich zu gestalten, und auf die noch immer in vielen Lebensbereichen vorhandene Benachteiligung und Ausgrenzung von behinderten Menschen. Pro Infirmis, die grösste Fachorganisation für behinderte Menschen in der Schweiz, beschäftigt rund 600 Mitarbeitende, die jährlich über 140 000 Kontakte zu Menschen mit Behinderungen und deren Angehörigen wahrnehmen.

BERATUNG, BEGLEITUNG UND UNTERSTÜTZUNG VON MENSCHEN MIT BEHINDERUNG

Um möglichst nahe bei den Menschen mit Behinderung und deren Angehörigen zu sein, betreibt Pro Infirmis schweizweit 50 lokale Standorte mit durchschnittlich 12 bis 15 Arbeitsplätzen. Damit die Organisation trotz dezentraler Struktur von schlanken, effizienten, IT-gestützten Prozessen profitieren kann, setzt Pro Infirmis seit Jahren auf eine Citrix Terminal-Server-Lösung, auf

Citrix XenServer und Citrix Netscaler für den sicheren Remote-Zugriff. Die zentrale Infrastruktur wird in den zwei redundanten Rechencentern am Hauptsitz in Zürich betrieben und stellt den mittels «Managed VPN» eingebundenen Geschäftsstellen die benötigte IT-Power zur Verfügung. Zudem bietet sie die Möglichkeit, autorisierten Personen einen standort- und device-unabhängigen Zugang ins Firmennetzwerk bzw. Zugriffe auf Daten und Applikationen zu gewähren. Eine Option, die laut Marco Röthlisberger, Leiter Informatik bei Pro Infirmis, unter anderem für Mitarbeitende der Informatikabteilung wichtig ist. Dadurch sind diese in der Lage, auch ausserhalb der offiziellen Bürozeiten aus der Ferne Support- oder Upgrade-Services durchzuführen. Ein weiterer Anwendungsbereich ist laut Röthlisberger die Erschliessung von Kleinststandorten. «Dazu gehören u. a. sogenannte Sprechstundenstellen, wie wir sie beispielsweise in ausgewählten Spitälern betreiben. Dabei sind unsere Beraterinnen und Berater zu gewissen Zeiten im jeweiligen Spital vor Ort und bieten ihre Dienste lokal an. Damit diese Beratungstätigkeit in derselben Qualität und Ausgestaltung wie in einer eigenen Geschäftsstelle erbracht werden kann, benötigen die entsprechenden Mitarbeitenden via Spital-Infrastruktur einen gesicherten Remote-Zugriff auf unser Firmennetzwerk.»

SICHERER REMOTE-ZUGANG INS UNTERNEHMENSNETZWERK

Vor dem Hintergrund, dass für die erwähnten Anwendungen die alleinige Verwendung von Benutzername und Kennwort keine genügend hohe Zugangssicherheit gewährt, setzt Pro Infirmis seit geraumer Zeit auf eine sogenannte Zwei-Faktoren-Authentisierung. Dabei werden die User-spezifischen Credentials mit einer zusätzlichen Login-Komponente, einem nur einmal gültigen Passwort ergänzt (One Time Password, OTP). Da für die Anmeldung eine Kombination aus Wissen (Zugangsdaten) und Besitz (Token) erforderlich ist, bilden Einmalpasswörter eine wichtige Basis für den sicheren Netzwerk-Zugang und verhindern den unerlaubten Zugriff durch Dritte.

Die bei Pro Infirmis in der Vergangenheit eingesetzte, auf Hardware-Token basierende OTP-Lösung hat sich zwar bewährt, wies laut Röthlisberger aber gewisse Nachteile auf: «Wir waren auf den ausschliesslichen Einsatz physischer Token begrenzt. Diese benötigen einerseits Platz und sind oft Teil überquellender Schlüsselanhänger. Andererseits dürfen die Aufwendungen für das Konfigurieren und das physische Versenden der Hardware-Token sowie das Handling von Ersatzlieferungen nicht unterschätzt werden. Kommt hinzu, dass unsere alte Lösung auf dem Prinzip der elektronischen Strichliste basierte, was bei unsachgemässem Handling zu Synchronisationsproblemen mit dem Server führte. Um Nachteile dieser Art auszuräumen, haben wir uns an die Evaluation einer neuen, zukunftsgerichteten Lösung gemacht, die nebst Hardware-Token auch SMS- und App-basierte Lösungen unterstützt. Diese machen sich die Tatsache zunutze, dass heute sämtliche User über ein Mobil- oder

> «Dank der SMS-basierenden OTP-Lösung von VASCO ist die Einbindung neuer User ein schneller, einfacher und kostengünstiger Prozess.»
>
> **MARCO RÖTHLISBERGER**
> Leiter Informatik, Pro Infirmis

VASCO – KOMPLETTLÖSUNG FÜR DIE STARKE AUTHENTISIERUNG

Mit dem Ziel, den (Remote-)Zugriff auf Daten und Applikationen wirksam zu schützen, zugriffsberechtigte Personen zu authentisieren und Transaktionen sowie Datentransfers vor Veränderungen und Diebstahl zu sichern, bietet VASCO eine leistungsfähige «Strong Authentication»-Gesamtlösung an. Diese adressiert Anwendungsbereiche wie Windows-Logon, Remote-Zugriffe via VPN, Einbindung mobiler Devices, Absicherung von Web-Anwendungen und wirksamen Schutz von Cloud-Services.

Die OTP-Lösung von VASCO besteht aus der Server-Software IDENTIKEY sowie aus Client-Komponenten (DIGIPASS):

IDENTIKEY

- Authentifizierungsserver für die Netzwerk- und Anwendungssicherheit mit Einmal-Passwörtern und digitaler Signatur
- Skalierbar – geeignet für Kleinstanwendungen bis hin zu Grossinstallationen
- Unterstützung unterschiedlichster Plattformen (Windows und Linux Server, virtualisierte Umgebungen)
- Nahtlose AD-(Active-Directory-)Einbindung sowie LDAP- und RADIUS-Unterstützung
- Inkl. Funktionen wie Primary-Backup und Replica-Server, Webfilter, Windows Desktop- und Netzwerk-Logon, SOAP, SBR etc.
- Mandantenfähig

DIGIPASS

- Hardware-, Mobile- und SMS-basierende Token
- Zeitbasierendes Verfahren: Jedes generierte One Time Password ist einmalig und nur für eine kurze Zeitperiode gültig
- Unterstützte Authentifizierungs-Technologien: One-Time-Passwörter (OTP), starke statische Passwörter (SSP) – gespeichert auf Digipass Smart Card oder Digipass Token
- Public Key Infrastructure (PKI) für Signaturen und Verschlüsselung

Smartphone verfügen, das in die Authentisierungslösung eingebunden werden kann. Sie ergänzen und ersetzen bisher benötigte Hardware-Token auf elegante Art und Weise.»

EINBINDUNG MOBILER DEVICES

Im Rahmen der Beschaffung einer neuen «Multi Factor Authentication»-Plattform hat sich Pro Infirmis für die Lösung von VASCO entschieden. Diese unterstützt alle denkbaren OTP-Token-Formen – so auch die SMS-basierte Variante. Dabei wird das One-Time-Passwort nicht durch einen physischen Token vor Ort, sondern durch einen zentralen Authentisierungsserver generiert und via SMS-Gateway an den jeweiligen User bzw. dessen Mobile-Phone übermittelt.

Die SMS-OTP-Lösung von VASCO führt laut Röthlisberger zu zahlreichen Vorzügen. Allen voran zu einer gesteigerten Effizienz und Geschwindigkeit bei der Einbindung neuer User. «Da müssen keine Hardware-Token konfiguriert und verschickt werden. Der Eintrag der neuen Handynummer im Active Directory und die Freigabe des Users im VASCO-Authentifizierungsserver reichen dazu aus. Zudem profitieren wir von wesentlich geringeren Kosten, da keine Beschaffungs- und Versandkosten für physische Token anfallen. Auch die Einführung der User ist denkbar einfach – nicht zuletzt aufgrund der Tatsache, dass SMS-OTPs in vielen E-Banking-Applikationen verwendet werden und somit bekannt und etabliert sind.» Wichtig für Röthlisberger und sein Team war auch die Möglichkeit eines Mischbetriebs. «Dies gab uns die Chance, die alten OTP-Token sukzessive durch die neue SMS-Lösung abzulösen.»

Nebst der von Pro Infirmis genutzten SMS-OTP-Lösung stellt VASCO mit «Digipass for Mobile» auch eine App-basierte Authentifizierungs-Lösung zur Verfügung. Dabei wird das Passwort vom jeweiligen Smartphone selbst zeitabhängig generiert, was konsequenterweise die Installation einer App bedingt. Dieser Prozess ist denkbar einfach. Für den Rollout beziehungsweise für den Download der dedizierten Applikationen stellt VASCO komfortable «Application Provisioning Services» zur Verfügung. Übermittelt die berechtigte Person ihre Mobilenummer an den Server, erhält sie anschliessend eine SMS, mit deren Hilfe sich die Authentisierungs-Software verschlüsselt downloaden lässt. Ist der Download erfolgreich abgeschlossen und die App installiert, kann die Aktivierung bei der IT-Abteilung angefordert werden.

> «Die Kombination aus der umfassenden Authentifizierungslösung von VASCO mit dem breit abgestützten Know-how unseres Lösungspartners Steffen Informatik ist ein wahrer Gewinn.»
>
> **MARCO RÖTHLISBERGER**
> Leiter Informatik, Pro Infirmis

NAHTLOSE INTEGRATION

Trotz umfassender Funktionalität lässt sich die Enterprise-taugliche Authentifizierungslösung von VASCO einfach und schnell in bestehende Umgebungen und Applikationen einbinden. Dazu stellt der Authentifizierungsserver «IDENTIKEY» komfortable «Plug and play»-Funktionalitäten zur Verfügung und unterstützt sowohl Radius- als auch Web- und SOAP-Schnittstellen. Ob als Virtual- oder Hardware-Appliance – beide Varianten ermöglichen ein zentralisiertes, komfortables User-Management. So steht dem Administrator eine einheitliche Konsole für Funktionen wie Benutzerverwaltung, Token-Management, Auditing und Reports zur Verfügung. Für Röthlisberger ist klar: «Mit VASCO setzen wir aufs beste Pferd – bei moderaten Kosten und einer transparenten und kundenfreundlichen Lizenzstrategie. Kommt hinzu, dass wir für die Planung und die Implementierung der OTP-Lösung von VASCO auf das Know-how und die Erfahrung unseres langjährigen IT-Partners Steffen Informatik zurückgreifen konnten. Das gab uns die Gewissheit, das Projekt zeit-, fach- und budgetgerecht umsetzen zu können.»

PRO INFIRMIS

Pro Infirmis ist Kompetenzzentrum für Fragen rund um Behinderung. Der schweizweit tätige Verein setzt sich dafür ein, dass Menschen mit einer Behinderung ihr Leben selbständig und selbstbestimmt führen, aktiv am sozialen Leben teilnehmen können und nicht benachteiligt werden. Pro Infirmis berät, begleitet und unterstützt mit ihren über 600 Mitarbeitenden an rund 50 Standorten sowohl die Menschen mit Behinderung selbst als auch ihre Angehörigen sowie Fachpersonen. Die soziale Institution bietet weitreichende Dienstleistungen an. Dazu gehören Sozialberatung, Assistenzberatung, begleitetes Wohnen, finanzielle Direkthilfe und die Beratung für hindernisfreies Bauen.

STEFFEN INFORMATIK AG

Steffen Informatik ist ein führendes Informatik-Dienstleistungsunternehmen in der Schweiz. Das 1989 gegründete, bis heute inhabergeführte Unternehmen mit Niederlassungen in Mägenwil, Pratteln, Zug, Gümligen und St.Gallen bietet innovative, nachhaltige IT-Lösungen in den Bereichen Infrastructure- und Cloud-Solutions sowie weitreichende Consulting-Services. Diese reichen von der Beratung über die Umsetzung bis hin zum Betrieb kompletter IT-Infrastrukturen.

Steffen Informatik weist eine bemerkenswerte Entwicklung auf. Heute profitieren mehrere Hundert Kunden in der Schweiz vom Know-how und Engagement der rund 120 qualifizierten Mitarbeitenden der Steffen Informatik sowie von höchsten Partnerzertifizierungen bei den marktführenden Herstellern.

pro infirmis

STEFFEN INFORMATIK

BOLL
IT Security Distribution

STARKE PARTNER

KUNDE	REALISATION	DISTRIBUTION
pro Infirmis	**Steffen Informatik AG**	**Boll Engineering AG**
8032 Zürich	**5506 Mägenwil**	**5430 Wettingen**
www.proinfirmis.ch	www.steffeninf.ch	www.boll.ch