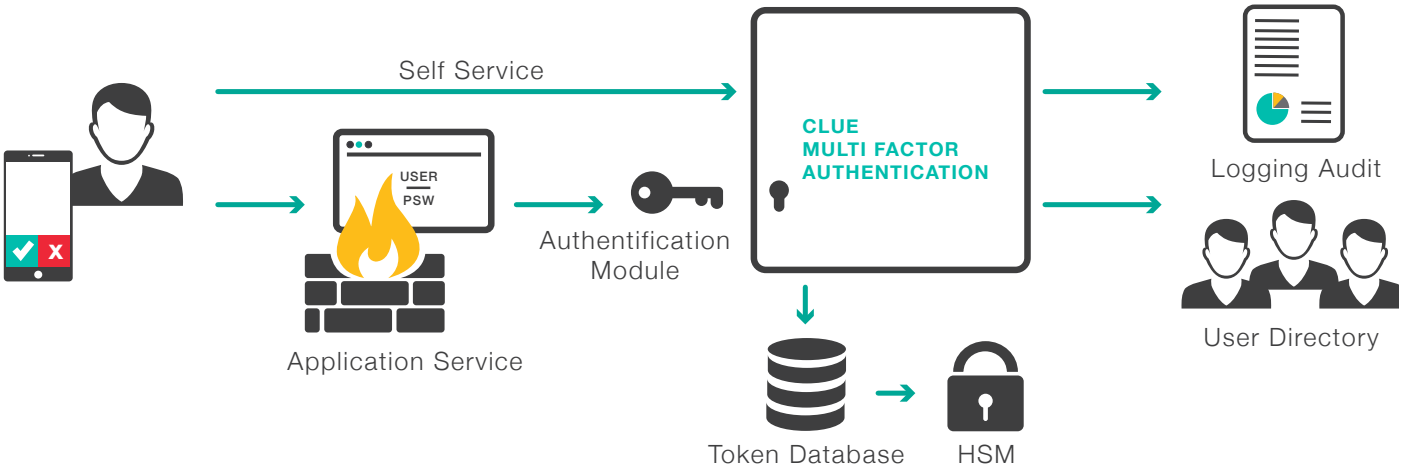
SECURITY SERVICES AG

CLUE

MULTI FACTOR AUTHENTICATION

Clue Multi Factor Authentication verifiziert die Identität der User bevor sich diese mit Ihren Applikationen und Systemen verbinden. Der Service ist einfach einzusetzen und bietet die nötige Flexibilität für den Einsatz für Sicheren Remote Access und die Integration in Applikationen.



EIN PASSWORT IST NICHT GENUG

Ein einzelnes Passwort hat als Zugangsschutz lange ausgedient, denn es weisst einige Schwachstellen auf. Passwörter sind leicht zu auszunutzen, da Menschen oft das selbe Passwort für viele Zugänge verwenden. So werden Passwörter mit anderen Anbietern geteilt und sind dadurch stärker von Passwort Diebstahl gefährdet. Durch zu komplexe Passwort Richtlinien werden Mitarbeiter ausserdem dazu bewegt, Passwörter nach unsicheren Mustern zu kreieren oder diese zu notieren.

MULTI TOKEN MANAGEMENT

Die Anforderungen an eine Multi Faktor Authentifizierung variieren je nach Anwendung stark. Aus diesem Grund ist eine hohe Flexibilität bei den möglichen Authentifizierungs-Methoden sehr wichtig, denn damit wird die Identität eines Benutzers oder einer Transaktion bestätigt. Daher unterstützen wir eine grosse Bandbreite an Token. Push-Token ermöglichen eine hohe Sicherheit und verbessern die Benutzerfreundlichkeit erheblich. QR-Token ist ebenfalls sehr benutzerfreundlich und kann in die Windows oder MacOSX Anmeldung sowie in Applikationen intregriert werden.

Ob klassisch mit Display oder als FIDO U2F Token eigenen sich Hardware Token für externe Mitarbeiter und hohe Sicherheitsanforderungen. Software Token für Smartphones und als SMS erfüllen die meisten Sicherheitsvorgaben und sind effizient und kostengünstig zu verwalten.

EFFIZIENTES MANAGEMENT

Eine der grössten Hürden beim Einsatz von Multi Factor Authentifizierungs Systemen ist die Verwaltung der User Token. Speziell in Umgebungen, in denen auf unterschiedliche Token Typen eingesetzt werden, entsteht im Rollout und im Betrieb ein erheblicher Betrieblicher Aufwand.

Durch das Self Service Portal kann die Verwaltung der Token teilweise oder ganz an die User in einem festgelegten Rahmen übergeben werden. Für eine flüssige Migration stehen Passthrough Token zur Verfügung, welche User, welche noch nicht umgestellt wurden, weiter auf die abzulösenden Token zurückgreifen lässt.

SECURITY SERVICES AG

CLUE

MULTI FACTOR AUTHENTICATION FEATURES

TOKEN
Das modulare System erlaubt eine breite Unterstützung von Token Technologien und Typen. Es werden App Token, Hardware Token, QR-Token, SMS und weitere unterstützt. Es werden offene Standards wie auch Hersteller spezifische Technologien eingesetzt.

SELF SERVICE
Per Selfservice Portal ist es dem User über einen gesicherten Zugang direkt möglich, Push Token, App Token und QR Token auszurollen, zu aktivieren und zu deaktivieren oder den User Pin neu zu setzen. Alle möglichen Optionen können mit Richtlinien gesteuert werden.

MODULE
Neben einer RADIUS Schnittstelle für Remote Access Systeme stehen Module für die Betriebssysteme Windows, MacOS und Linux zur Verfügung. Auch SAML für moderne Authentifizierungslösungen und eine API Schnittstelle für die direkte Integration in Applikationen sind verfügbar.

API
Durch einen API-First Ansatz erhalten Sie unlimitierte Möglichkeiten im Einsatz von Multi-Factor-Authentication. Die Integration in ihre Management Tools, User Self Service Portale, Produkte und Applikationen bringen volle Flexibilität und niedrige Kosten in der Implementation und Entwicklung.

USER DATENBANKEN
Um sich nahtlos in bestehende IT Infrastrukturen und Applikationen zu integrieren, wird eine vielzahl von Schnittstellen unterstützt. Dazu zählt unter anderem LDAP und Microsoft Active Directory. Zur Anbindung von Webapplikationen stehen SQL und JSON basierte Resolver bereit.

HSM
Jegliches vertrauliche Material ist verschlüsselt abgelegt. Auf Wunsch kann ein zusätzliches Hardware Security Module (HSM) eingesetzt werden. Dadurch wird sichergestellt, dass alle Schlüssel sicher und unabhängig von Ihrer Infrastruktur generiert und verwaltet werden.

MULTI FACTOR AUTHENTICATION SERVICE

Clue Multi Factor Authentication ermöglicht den sicheren Einsatz von Remote Access Systemen und sichert den Zugang zu lokalen und Cloud Applikationen und eliminiert dadurch einen der grössten Angriffsvektoren auf Ihre IT-Systeme. Gemeinsam mit Ihnen erarbeiten unsere Security Experten ein passendes Authentifizierungs-Konzept und implementieren die dafür benötigten Tools. Wir leisten den vollen Betrieb der erforderlichen Appliances, wie z.B. das regelmässige Backup, Release und Lifecycle Management als auch das Monitoring von Health und Security Events.

CLUE-LESS?

Clue Managed Services erweitern Ihr Team mit Security Experten, um die Absicherung Ihres Unternehmens zu verstärken. Die smarte Kombination aus bewehrten Produkten, unseren massgeschneiderten Erweiterungen und unserem persönlichen Support helfen Ihre Anforderungen bei einem niedrigen TCO zu erfüllen. Durch die monatlichen Servicegebühren entfallen für Sie hohe Investitionen sowie Trainingskosten und ermöglichen Ihnen den modularen Einsatz dieses Services.

NÄCHSTE SCHRITTE

Sie möchten den Zugang zu Ihren Systemen und Applikationen in Ihrem Unternehmen gegen unerlauten Zugriff schützen? Sie entwickeln Applikationen und Services und möchten die Integration von sicherer Authentifizierung schnell und unkompliziert durchführen? Sprechen Sie uns auf Multi Factor Authentication an. Gerne beraten wir Sie und zeigen Ihnen eine auf Ihre Anforderungen angepasste und sichere Umsetzung auf.

CLUE SECURITY SERVICES AG | NEUHOFSTRASSE 5A | CH-6340 BAAR | +41 44 667 77 66 | INFO@CLUE.CH | WWW.CLUE.CH