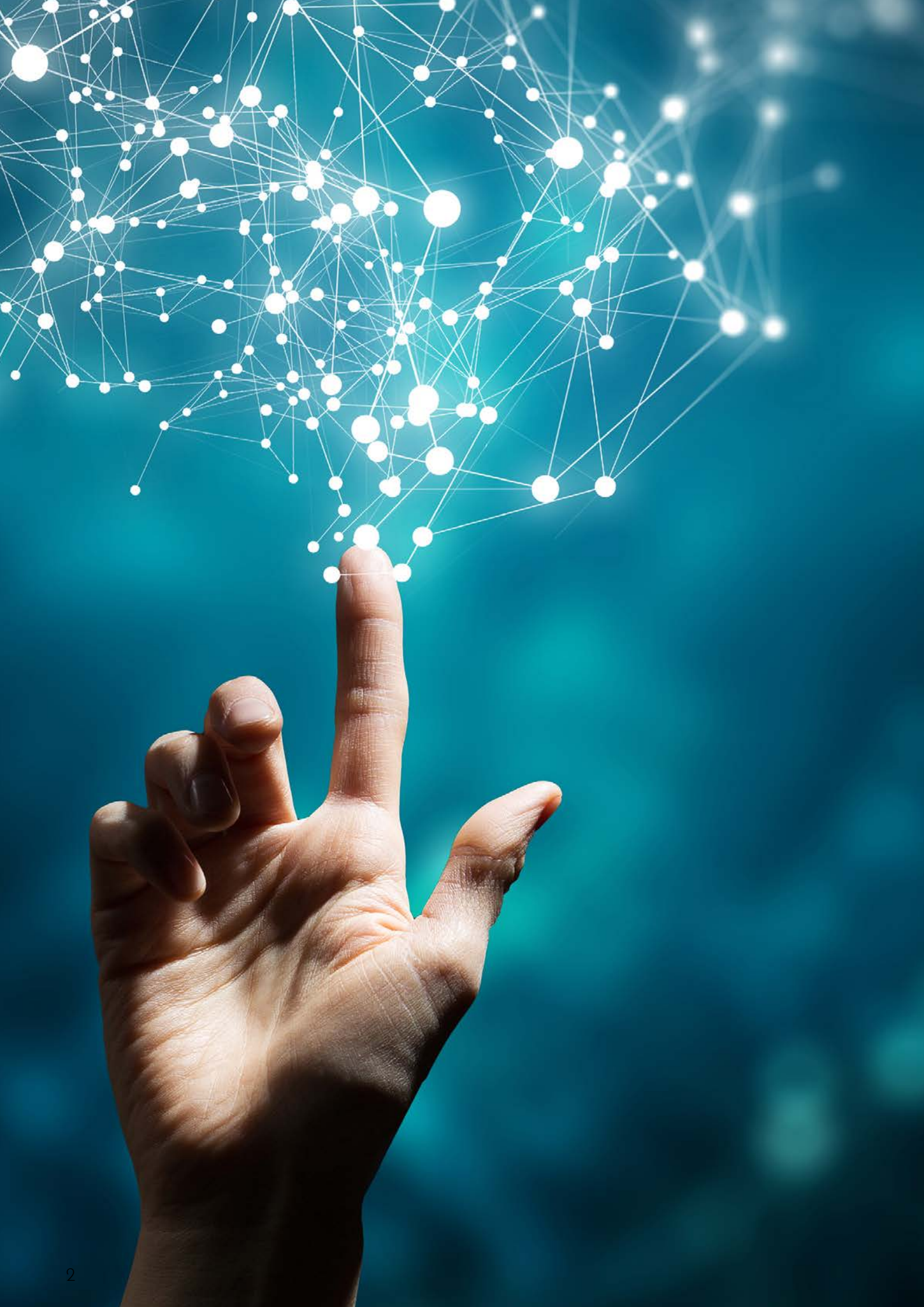
DOUBLE CLUE

DOUBLECLUE

Cleverly Secures Identities



70 % DER DEUTSCHEN UNTERNEHMEN WAREN 2019 VON CYBERSECURITY-ANGRIFFEN BETROFFEN.*

*Quelle: https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf

Häufig waren derartige Angriffe die (unbeabsichtigte) Mithilfe von Mitarbeitern zurückzuführen, etwa in dem diese aufgrund von Social Engineering-Kampagnen Zugangsdaten preisgegeben hatten. Doch auch schwache und mehrfachgenutzte Passwörter, unklare Zugriffsrichtlinien sowie fehlende Sicherheitsbarrieren bilden Schwachstellen, die Ihre Systeme für Cyberkriminelle attraktiv machen.

IDENTITÄTEN IHRER MITARBEITER EFFEKTIV ABSICHERN

Die größte Schwachstelle in Ihrem Netzwerk bildet folglich der Mensch. Die Algorithmen und die KI, die Virenscannern und Threat Protection heute zugrunde liegen, sind so ausgereift, dass sie Schadsoftware gut erkennen und diese abfangen, bevor sie zur Bedrohung werden können.

Dem Menschen fällt dies jedoch schwer: Besonders unter Leistungs- und Zeitdruck sind Ihre Mitarbeiter geneigt, ohne genauere Prüfung einen Anhang zu öffnen oder einem Link zu folgen. Cyberkriminalität setzt daher auf die Interaktion mit dem Menschen – sei es aufgrund von Nachlässigkeit, (scheinbaren) Zwängen oder emotionaler Beeinflussung.

Untersuchungen zeigen, dass Daten und persönliche (Identifikations-)Informationen oft bereitwillig preisgegeben werden, wenn es gelingt, eine emotionale Beziehung aufzubauen – dieses sog. **Social Engineering** findet sich in Phishing-E-Mails ebenso wie in betrügerischen Telefonanrufen oder auf gefälschten Webseiten.

Mit der Einführung eines zweiten Faktors zur Verifikation einer Mitarbeiteridentität verhindern sie Identitätsmissbräuche zuverlässig. Denn nur, wer sich doppelt ausweisen kann – mit einem nur ihm bekannten 2. Faktor –, erhält Zugriff auf eine Datei oder ein System.

Daneben stellt ein eindeutiges und zielorientiertes Zugriffsmanagement sicher, dass nur diejenigen Mitarbeiter Zugriff auf sensible Bereiche Ihrer Unternehmens-IT haben, die diese auch wirklich benötigen. Dies ist insbesondere in Finanz-, HR- und IT-Abteilungen relevant, um mögliche Risiken für den Missbrauch von Daten und Systemen so gering wie möglich zu halten.

DoubleClue ist eine umfassende Software zur sicheren Verwaltung von Identitäten, Zugriffen und Passwörtern sowie zur zentralen Speicherung von sensiblen Daten.

DOUBLECLUE – ALLE FEATURES

DoubleClue schützt Ihr Firmennetzwerk zuverlässig vor unerlaubten und schädlichen Fremdzugriffen. Die Software verbindet modernstes Identity- & Access Management (IAM) mit State of the Art Multifaktor Authentifizierung (MFA) und verfügt standardmäßig über weitere Security-Funktionalitäten, die den Alltag und die Zusammenarbeit Ihrer Mitarbeiter erleichtern.

DOUBLECLUE BIETET IHNEN ACHT MÖGLICHKEITEN BEI DER AUTHENTIFIZIERUNG

- Passwort (als erster Faktor)
- Push Benachrichtigung (passwortlose Anmeldung mit der DoubleClue App)
- QR-Code (passwortlose Anmeldung mit DoubleClue in der DoubleClue App)
- OTP / One Time Passcode (auch offline)
- OTP Hardware Token
- FIDO Token (u. a. biometrisch)
- Voice Message
- SMS Passcode
- Desktop App mit Passcode (kein Smartphone benötigt)

IDENTITY & ACCESS MANAGEMENT

In der übersichtlichen IAM-Plattform verwalten Sie zentral Accounts, Identitäten und Zugriffe. Das Herzstück bildet das Zugriffsmanagement auf Systeme und Anwendungen mit automatisiertem Berechtigungsmanagement und adaptiven Zugriffsrichtlinien für Applikationen und Benutzergruppen. Dies erlaubt auch die Einrichtung eines sog. Privileged Access Managements (PAM).

ZWEI-FAKTOR AUTHENTIFIZIERUNG

Die einfach umsetzbare Zwei-Faktor Authentifizierung verhindert An- und Eingriffe auf und in Ihr Netzwerk. DoubleClue bietet Ihnen dabei alle Möglichkeiten einer modernen, passwortlosen Anmeldung: Wählen Sie für Ihr Unternehmen aus verschiedenen Authentifizierungsmöglichkeiten die Variante, die am besten zu Ihnen passt.

SINGLE SIGN-ON (SSO) DOUBLECLUE MYAPPLICATIONS

Ihre Mitarbeiter arbeiten zeitgleich in verschiedenen Anwendungen, für die sie separate Accounts mit eigenen Zugangsdaten benötigen. Dank Single Sign-On genügt eine einzige Anmeldung in DoubleClue MyApplications, um Zugriff auf alle benötigten Applikationen zu erhalten – mit nur einem Klick.

PASSWORDSAFE MIT AUTOFILL-FUNKTION

Der DoubleClue PasswordSafe vereinfacht die Verwaltung vieler, selbst komplexer Passwörter erheblich. Speichern Sie Ihre Passwörter ganz einfach an einem Ort und greifen Sie gebündelt darauf zu – direkt aus der Webanwendung oder der mobilen App heraus. MFA und Verschlüsselung stellen sicher, dass die Passwörter in Ihrem Safe sicher verwahrt sind.

Dank Autofill können Sie sich ganz bequem aus der DoubleClue App heraus überall anmelden. Das erlaubt Ihnen die Vergabe von hochkomplexen, sicheren Passwörtern für jede Ihrer Anwendungen und Zugriffe.

DOUBLECLUE KEEPASS-PLUGIN

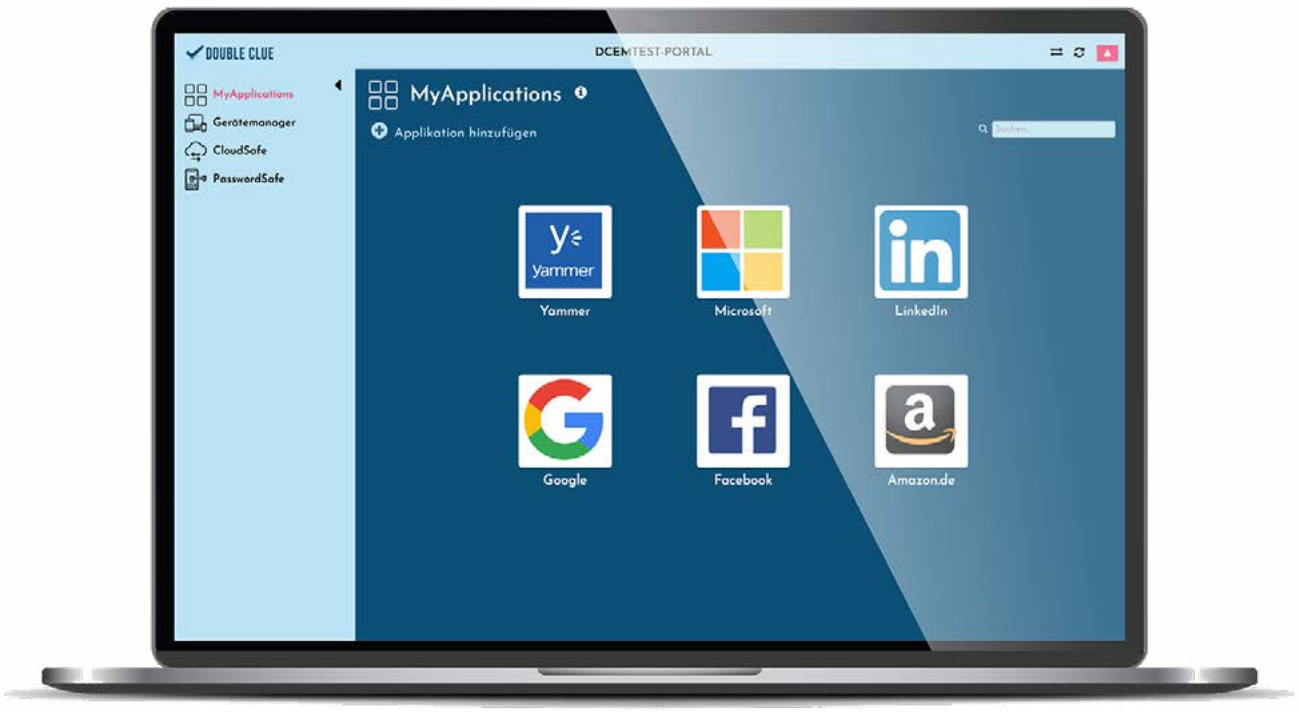
Dem weltweit beliebten OpenSource Passwortmanager KeePass fehlen standardmäßig zwei Dinge für die Nutzung im Unternehmensumfeld: Eine Multifaktor Authentifizierung sowie die Möglichkeit, Passwörter mit Kollegen, Partnern und Dienstleistern zu teilen. Das DoubleClue KeePass-Plugin erlaubt den einfachen Im- und Export von Passwort-(kdbx-)Dateien zwischen beiden Systemen.

DOUBLECLUE APP FÜR iOS & ANDROID

User erwarten heute eine hohe Usability. Daher bietet DoubleClue Ihnen die Möglichkeit, Passwörter und Approvals über eine moderne und übersichtliche App auf Ihrem mobilen Device zu verwalten.

DOUBLECLUE CLOUDSAFE

Wichtige und vertrauliche Dokumente sollten nie über unverschlüsselte E-Mails versendet werden. Der DoubleClue CloudSafe erlaubt Ihnen daher nicht nur die zentrale verschlüsselte Speicherung von sensiblen Daten in einem durch MFA geschützten, unzugänglichen Bereich innerhalb Ihrer eigenen IT-Infrastruktur. Er eröffnet Ihnen auch die Möglichkeit diesen Zugriff mit Ihren Mitarbeitern, Partnern oder Dienstleistern sicher zu teilen – ohne, dass Ihre Daten den Server verlassen.



HOHE INTEROPERABILITÄT

DoubleClue ist vollständig und unkompliziert in Ihre Infrastruktur integrierbar. Die Lösung unterstützt alle gängigen Protokolle und bindet On-Premises- sowie Cloud („as a Service") Dienste über gängige Standards ein. Die Lösung ist daher auch für hybride Umgebungen bestens geeignet.

- VPN- und Firewall-Absicherung über **RADIUS** (Remote Authentication Dial-In User Service)-Protokoll
- Einbindung von webbasierten Single Sign-On-Protokollen wie **SAML 2.0** (Security Assertion Markup Language) und **OpenID/ Oauth 2.0**
- Anbindung an offene Programmierschnittstellen für Webapplikationen über **APIs** (Application Programming Interface) bzw. **RESTful APIs**
- Authentifizierung von .NET-Plattformen und webbasierten MS-Produkten mittels **Directory Federation Services (ADFS)-Plugin**
- Sicherung von Microsoft Remotedesktop Verbindungen durch **Remote Gateway WebAccess-Plugin**
- Zugriff auf vorhandene **Active Directory**, z. B. Azure AD, LDAP Directories zum automatischen Import von Usern und Gruppen aus der Domain, inklusive Echtzeitsynchronisation

IHRE MÖGLICHKEITEN

OS LOG-IN ABSICHERN (WINDOWS/ MAC/ LINUX)

Jede Maschine benötigt ein Betriebssystem, um für Nutzer zugänglich zu werden. Kaum einem Nutzer ist bewusst, dass bereits vor dem eigentlichen Log-in eine schwerwiegende Sicherheitslücke vorliegt: Denn es ist möglich, den Log-in-Prozess zu umgehen.

DoubleClue ist in der Lage diese Lück für microsoft-, mac- und linuxbasierte Systeme zu schließen und somit nicht nur Ihre Useridentitäten abzusichern, sondern auch generell den Zugriff auf Ihr System zu verhindern. Insbesondere, wenn Sie keine Zugangsbeschränkungen zu Ihren Räumlichkeiten haben, sollten Sie lokale Zugriffe mit MFA absichern.

ABSICHERUNG HYBRIDER UMGEBUNGEN

Häufig verwenden Firmen einige ältere Applikationen On-Premises und neuere bereits in der Cloud. DoubleClue verbindet beide Welten, sodass Sie Ihre hybride Umgebung mit nur einem einzigen Tool absichern können. Sie müssen lediglich für Ihren Mandaten einen Agenten anlegen, um zwischen Cloud- und On-Premises-Umgebungen switchen zu können.

NUTZUNG DER VORHANDEN AD ZUR ERSTELLUNG VON ADAPTIVE POLICIES

DoubleClue greift auf Ihre vorhandene Active Directory zu. Sie benötigen keine aufwendige Neuanlage Ihrer Nutzerverzeichnisse, sondern können ganz bequem auf die vorhandenen Daten zurückgreifen. Mithilfe von Policies können Sie in DoubleClue User-Gruppen sowie zugehörige Zugangsrechte anlegen sowie erweiterte Regelungen erstellen. Etwa zu Timeouts, Restriktionen bei den Authentifizierungs-Methoden und die Einstufung sicherer Netzwerke, bei denen keine wiederholte Multifaktor Authentifizierung nötig ist.

MULTIMANDANTEN-FÄHIGKEIT ERLAUBT PRIVILEGED ACCESS MANAGEMENT

Komplexe Unternehmen mit einer sehr differenzieren Unternehmensstruktur benötigen eine größtmögliche Flexibilität bei der Installation. Daher ermöglicht DoubleClue Ihnen die Installation mehrerer, separater und komplett getrennter Mandanten zur übersichtlichen Zugriffsverwaltung. So können Sie neben internen Ressourcen auch strategische Partner oder Lieferanten sowie Kunden oder Freelancer mitanbinden.

Aufgrund dieser Mutlitmandanten-Fähigkeit erlaubt DoubleClue ebenfalls ein tiefes Privileged Access Management (PAM) zur Abtrennung separater, besonders schützenswerter Bereiche. Die Richtlinien hierfür können Sie individuell festlegen, je nach Datenschutz- und Compliancerichtlinien in Ihrem Unternehmen.

IHRE BENEFITS MIT DOUBLECLUE

STEIGERUNG DER MITARBEITERZUFRIEDENHEIT

Ein vereinfachter Anmeldeprozess erhöht die Produktivität und Akzeptanz Ihrer Mitarbeiter. Dank zentral gespeicherter Passwörter müssen sich die Vielzahl an komplexen Passwörtern nicht länger aktiv merken. Zudem können sich sich dank Single Sign-On mit einem Klick an ihrem PC und damit in ihren Applikationen anmelden. Das DoubleClue UserPortals erlaubt einen unterbrechungsfreien Wechsel in den Anwendungen.

Gleichzeitig können auch Ihre Admins auf komplexe Passwortrichtlinien zum Anmelden am PC verzichten. Selbst ein einfaches Passwort wird durch die zusätzliche MFA zu einem sicheren Log-in mit höchsten Sicherheitsanforderungen.

EXTERNE NETZWERKE SICHER ANBINDEN

Modernes Arbeiten bedeutet auch remote Work. Die zunehmende Digitalisierung bietet immer mehr Möglichkeiten des standortunabhängigen Arbeitens.

Unternehmen müssen sich darauf einstellen, dass sich Ihre IT in verschiedenen privaten wie öffentlichen Netzwerken befindet, auf die sie keinen Einfluss haben. Diese bilden jedoch ein mögliches Einfallstor für Viren und andere schädliche Applikationen.

DoubleClue ermöglicht Ihnen dank MFA und IAM die technische Absicherung dieser Netzwerke.

Besonders die dem Internet verbundenen Cloud-Tools, die z. B. der Zusammenarbeit oder Kommunikation dienen, sind ein zusätzliches Risiko in diesen Netzwerken. Insbesondere, wenn diese kurzfristig und ohne ausreichende Sicherheitsstandards eingeführt wurden oder gar auf privaten Devices genutzten werden.

DATENZUGRIFF MIT INTERNEN & EXTERNEN KONTAKTEN TEILEN

Im Umfeld von Remote-Arbeit ist auch die Datenübertragung wichtiger und vor allem vertraulicher Dokumente gefährdet. Doch nicht nur Ihre in virtuellen Teams verteilte Mitarbeiter sind hier eine potenzielle Sicherheitslücke für Ihre IT oder vertraulichen Dokumente: Ebenso – und in vielleicht noch höherem Maße – sind es externe Stakeholder, die ein potenzielles Risiko darstellen. Denn: Wie garantieren Sie, dass dort ebenso hohe Sicherheitsstandards gelten wie in Ihrem Unternehmen?

Der integrierte DoubleClue CloudSafe speichert vertrauliche Unterlagen an einem zentralen und durch MFA gesicherten Ort in Ihrer private oder der deutschen DoubleClue Cloud. Diese zentrale verschlüsselte Speicherung ermöglicht es Ihnen, Mitarbeitern, externen Partnern, Lieferanten oder Freelancern Zugriff zu den dort aufbewahrten vertraulichen Dateien zu geben. Ohne, dass diese versendet werden oder gar Ihre Server verlassen müssen. Erteilen Sie externen wie internen Stakeholdern Zugriffs-, Schreib- oder nur Leserechte, sodass Sie sicher sein können, dass Ihre Daten vertraulich bleiben.

BLEIBEN SIE FLEXIBEL

Unsere Services bei Beratung, Implementierung, Roll-out und fortlaufendem Support

- Von der Stand-alone-Lizenz bis hin zum HWS Rundum-Sorglos-Paket: Wählen Sie das Lizenzmodell, das am besten zu Ihrem Business und Ihren Ressourcen passt, z. B.
  - Lifetime Managed MFA
  - Lifetime Managed Software Support
- Beratung zur Implementierungsstrategie vor Softwareeinführung
- Training der Administratoren und Anwenderkommunikation
- 90-tägige kostenlose Testversion mit Support
- Vollständige Begleitung von Implementierung und Roll-out

Bleiben Sie flexibel und wählen Sie das Lizenz- und Hostingmodell, das am besten zu Ihrem Unternehmen passt – On-Premises, oder in in der Cloud auf Servern in Deutschland.

Egal für welches Hostingmodell Sie sich entscheiden, die Funktionalitäten von DoubleClue sowie den zugehörigen Apps bleiben davon unberührt. Die DoubleClue App ermöglicht Ihren Mitarbeitern auch bei eigenem Hosting den Zugriff auf Ihre Daten – egal, wo sie sich gerade befinden.

Wir bieten unseren Kunden zudem vollumfängliche Serviceleistung im Zusammenhang mit der Einführung und Betreuung ihrer DoubleClue Applikationen. Den Grad der Betreuung können Sie flexibel auf Ihr Geschäftsmodell hin anpassen: Vom HWS Rund-um-Sorglos-Paket von Implementierung, Roll-out und Support bis hin zu individuell abgestimmten Serviceleistungen – wir beraten Sie gerne zur für Sie optimalen Umsetzung.

PASSEN SIE SICH NICHT AN DIE LÖSUNG AN, DIE LÖSUNG PASST SICH AN SIE AN.

BEISPIELHAFTER IMPLEMENTIERUNGSLEITFADEN BEI EINER ON-PREMISES-LIZENZ

Für Implementierung und Roll-out veranschlagen wir bei der Nutzung einer On-Premises-Lizenz (inkl. Testphase) maximal zwei Monate.

Die effektive Arbeitszeit ohne Testphase liegt je nach Firmengröße bei etwa 1–2 Wochen.

0,5-2 TAGE
Nach Ihrer Anfrage erhalten Sie von uns Ihre Installationsdaten zur Installation Ihrer DoubleClue-Applikation auf Ihren Servern. Der Zeitaufwand der technischen Implementierung richtet sich nach Komplexität Ihrer IT-Landschaft.

1 MONAT
Für die Testphase veranschlagen wir einen Monat. Je nach Wahl Ihres Supportumfanges, bieten wir Ihnen hier bereits Schulungen Ihrer Admins sowie die betreute Implementierung Ihrer Gesamtumgebung an.

2 WOCHEN
Roll-out nach erfolgreicher Implementierung; innerhalb dieser 2 Wochen erhalten Ihre Mitarbeiter Informationen zum Umgang mit der Software. Die eigentliche Registrierung erfolgt für den User in zwei Schritten:

- Erhalt einer E-Mail mit der Dokumentation sowie anschließende Installation der DoubleClue App (Desktop oder mobil)
- Registrierung in der App mittels QR-Code oder Dateneingabe

2 WOCHEN
Hypercare-Betreuung durch die HWS, um einen reibungslosen Roll-out und eine hohe Userakzeptanz zu gewährleisten.

BEISPIELHAFTER IMPLEMENTIERUNGSLEITFADEN BEI EINER SaaS-LIZENZ

Für Implementierung und Roll-out veranschlagen wir bei der Nutzung einer SaaS-Lizenz (inkl. Testphase) maximal zwei Monate.

Die effektive Arbeitszeit ohne Testphase liegt je nach Firmengröße bei etwa 1–2 Wochen.

ZERO-TIME
Nach Ihrer Anfrage erhalten Sie von uns eine E-Mail mit der URL und Ihren Einwahldaten zu Ihrem DoubleClue-Mandanten in unserer deutschen Hochsicherheitscloud. Sie können DoubleClue nun vollständig nutzen.

1 MONAT
Für die Testphase veranschlagen wir einen Monat. Je nach Wahl Ihres Supportumfanges, bieten wir Ihnen hier bereits Schulungen Ihrer Admins sowie die betreute Implementierung Ihrer Gesamtumgebung an.

0,5 – 2 TAGE
Technische Implementierung; Zeitaufwand je nach Komplexität Ihrer IT-Landschaft

2 WOCHEN
Roll-out nach erfolgreicher Implementierung; innerhalb dieser 2 Wochen erhalten Ihre Mitarbeiter Informationen zum Umgang mit der Software. Die eigentliche Registrierung erfolgt für den User in zwei Schritten:

- Erhalt einer E-Mail mit der Dokumentation sowie anschließende Installation der DoubleClue App (Desktop oder mobil)
- Registrierung in der App mittels QR-Code oder Dateneingabe

2 WOCHEN
Hypercare-Betreuung durch die HWS, um einen reibungslosen Roll-out und eine hohe Userakzeptanz zu gewährleisten.

FALLBEISPIELE

VPN-ABSICHERUNG FÜR REMOTE WORK IN ÖFFENTLICHEN EINRICHTUNGEN

Unser Kunde aus dem Bereich Politik/ öffentliche Einrichtungen benötigte eine Absicherung seiner im Homeoffice arbeitenden Mitarbeiter mittels Multifaktor Authentifizierung. In diesem sensiblen Bereich ist besonders die Absicherung von Referenten während digitaler Konferenzen zu brisanten politischen Themen relevant, um ein Mithören auszuschließen.

Das eigentliche Firmennetzwerk wurde bereits zuvor mit VPN ausgestattet. DoubleClue ermöglicht dank des in der Lösung integrierten RADIUS-Protokolls eine tiefe technische Absicherung von VPNs mit aufgesetzter Multifaktor Authentifizierung. So ist gewährleistet, dass ein unbefugter keinen Zugriff auf das sichere VPN-Netzwerk hat - inklusive des Anbieters und Betreibers des VPN-Clients.

Aufgrund der vorhandenen IT-Infrastruktur konnten wir die Implementierung, die Testphase, die Review-Phase sowie den Go-live in jeweils etwa zwei Stunden durchführen.

ABSICHERUNG LEITNETZWERK KRITISCHE INFRASTRUKTUR

Unser Kunde aus dem Bereich Energieversorgung benötigte für sein Leitnetzwerk im Bereich Wasser-, Strom- und Gasversorgung eine starke, von der restlichen Infrasturktur abgetrennte Absicherung mittels MFA und IAM. Das schließt sowohl remote Arbeitsplätze als auch PCs in der Fläche ein, da letztere durch schwache Zugangskontrollen potenziell zugänglich waren.

Aufgrund der Anforderungen unseres Kunden konnten wir drei Usergruppen identifizieren, die jeweils individuelle Zugriffsrichtlinien benötigten. Neben der Standardabsicherung normaler User haben wir mit DoubleClue besonders schützenswerte User definiert und diesen mittels eines sog. PAMs (Privileged Access Managment) strengere Access- und Authentifizierungslösungen bei den besonders kritischen Systemen zugeordnet.

Weiter nutzt der Kunde auf seinen Rechnern ein Windows-Betriebssystem. DoubleClue sichert die Windows-Log-ins sodass ein Umgehen des Anmeldeprozesses nicht möglich ist. Ergänzend wurde eine starke Multifaktor Authentifizierung für alle User verpflichtend.

SICHERE DIGITALISIERUNG IM MITTELSTAND

Unser mittelständischer Kunde aus der Stahlindustrie benötigte Hilfe bei der Absicherung seiner Digitalisierungsstrategie. Durch den Ausbau von Remote-Arbeit wurden cloudbasierten Kommunikations- und Kollaborationstools sowie ein neues VPN-Tool eingeführt.

DoubleClue schützt nun VPN-Verbindung technisch und vereinheitlicht gleichzeitig den Anmeldeprozess mit MFA im Netzwerk und den angeschlossenen Maschinen.

Daneben benötigte der Kunde ein spezielle Absicherung des Personalservers, auf dem alle Mitarbeiterdaten gespeichert sind. Die hohen Sicherheitsanforderungen an Datenschutz im Personalbereich machten eine technische Abtrennung der Personalabteilung von der übrigen Idee notwendig. Mittels eines eigenen Mandanten wurde die Personalabteilung vom Rest der IT abgetrennt. Durch die strenge Zugriffsbeschränkung kann lediglich der Personalleiter nach Verifizierung der eigenen Identität auf diesen Mandanten zugreifen.

DIGITALISIERUNG VON MEDIZINISCHEN EINRICHTUNGEN

Unsere Kunden im Bereich medizinische Einrichtung benötigen eine umfassende Software zur Begleitung ihrer Digitalisierung. Denn die verbesserte Vernetzung insbesondere mit Cloud- oder Software-as-a-Service-Anwendungen steigern das Gefahrenpotenzial aufgrund ihrer Offenheit zum Internet um ein Vielfaches. Gleichzeitig handelt es sich bei Patienten- und Gesundheitsdaten um besonders schützenswerte Dokumente.

Auch die gemeinschaftliche Nutzung von Maschinen und Anwendungen wird durch die DoubleClue-Lösung abgebildet. DoubleClue bietet im Bereich des Zugriffs- und Identitätsmanagement umfassende Lösungen für Authentifizierung an gemeinsam genutzten Geräten. Hierdurch garantiert DoubleClue höchste Sicherheitsstandards bei gleichzeitig gewohnt unterbrechungsfreien Anmelde- und Arbeitsabläufen.

DoubleClue ist die umfassende Software zum Identitätsmanagement im Krankenhaus, die höchste IT-Security-Ansprüche mit erstklassiger Usability verbindet.

HWS GRUPPE

HWS INFORMATIONSSYSTEME GMBH

Die HWS Gruppe bietet ihren Kunden umfassende IT-Dienstleistungen, Softwareentwicklung und Beratungen, insbesondere in den Bereichen IT-Infrastruktur, Cloud Operations und Identity Protection. Mehr als 150 Mitarbeiter aus Neustadt an der Aisch (Mittelfranken) und dem Nearshore Delivery Center auf Malta unterstützen sowohl DAX Konzerne als auch den gehobenen Mittelstand bei ganzheitlichen IT-Projekten. Dank eines progressiven und fordernden Serviceansatzes überzeugen wir seit mehr als 20 Jahren als verlässlicher und nahbarer Partner.

IT Security made in Germany!

Unsere umfassenden IT-Security Lösung „DoubleClue" ermöglicht Unternehmen weltweit ein sicheres Identitäts- und Zugriffsmanagement sowie eine starke Multifaktor Authentifizierungslösung.

Erfahren Sie mehr über uns sowie unsere Dienstleistungen und Softwareprodukte unter **hws-gruppe.de** & **doubleclue.com**.

Allianz für Cyber-Sicherheit
Partner

HWS INFORMATIONSSYSTEME GMBH
Wilhelmstr. 16 | 91413 Neustadt a. d. Aisch | +49 (0)9161 6239 200 | requests@doubleclue.com | doubleclue.com