EVIDEN

Der ultimative Schutz vor Phishing-Angriffen

Grenzen der Multi-Faktor-Authentifizierung und effektive Maßnahmen

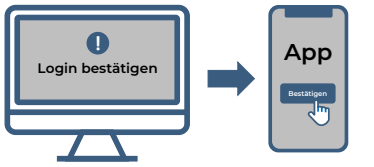
Über 90% aller Cyberangriffe beginnen mit einer Phishing-Mail

Am Anfang eines Phishing-Angriffs steht meist eine gefälschte E-Mail oder Messenger-Nachricht, die den Empfänger auf eine betrügerische Webseite lockt. Dort wird er zur Eingabe von Benutzername, Passwort und eventuell weiteren Geheiminformationen aufgefordert, die so in die Hände des Angreifers gelangen.

Die Erfolgswahrscheinlichkeit eines solchen Angriffs steigt, wenn die Nachricht den Anschein erweckt, von einem bekannten Anbieter oder Arbeitskollegen zu stammen. In den letzten Jahren hat die IT-Welt einen alarmierenden Anstieg von Phishing-Angriffen erlebt, was diese Technik zu einer der bedeutendsten Formen der Cyberkriminalität macht. Laut Forbes verursachte diese Methode allein im Jahr 2022 einen Schaden von über 500 Millionen Dollar.[1] CNBC berichtet zudem von einem Anstieg der Phishing-Angriffe zwischen Mai und Oktober 2022 um 61 % im Vergleich zum Vorjahr.[2] Über 90 % aller Cyberangriffe beginnen mit einer Phishing-Mail.

Von den vielen Tausend Phishing-Nachrichten, die ein Angreifer verschickt, führt oft nur eine zum Erfolg – das kann jedoch schon für einen wirkungsvollen Angriff ausreichen. Längst gibt es Tools, mit denen sich Phishing automatisieren lässt, wobei auch „Phishing as a Service" am Markt angeboten wird. Künstliche Intelligenz (KI) spielt hierbei eine wichtige Rolle und ermöglicht es Angreifern, innerhalb kürzester Zeit Hunderttausende maßgeschneiderter Phishing-Mails und gefälschter Webseiten zu erstellen.

Abbildung 1: Multi-Faktor-Authentifizierung sieht vor, dass mindestens zwei voneinander unabhängige Methoden gemeinsam zur Authentifizierung genutzt werden, beispielsweise PIN und TAN.



Transaktionsnummer wird zum Smartphone geschickt

Anwender bestätigt Login

Abbildung 2: Einer der Faktoren bei einer Multi-Faktor-Authentifizierung kann eine Transaktionsnummer sein, die der Nutzer aus einer Smartphone-App übernehmen muss.

Multi-Faktor-Authentifizierung schützt nicht unbedingt gegen Phishing

Multi-Faktor-Authentifizierung (MFA) ist ein bewährtes Konzept, das die Authentifizierung sicherer macht. MFA erfordert die Nutzung von mindestens zwei voneinander unabhängigen Authentifizierungsmethoden. In Sicherheitsrichtlinien wird oft die Nutzung von MFA gefordert, doch meist werden die genauen Anforderungen meist nicht definiert, obwohl es erhebliche Unterschiede zwischen den verschiedenen MFA-Varianten gibt.

Nicht ausreichend: Basic MFA: OTP/TAN, Mobile-App-Push-Benachrichtigung

Eine weit verbreitete Methode kombiniert das Passwort mit einer nur einmal verwendeten Transaktionsnummer (OTP/TAN). (Abbildung 1). Die Transaktionsnummer wird per SMS oder E-Mail an den Benutzer geschickt oder auf dessen Gerät generiert (Authenticator). Der Nutzer gibt sie dann in der Login-Maske zusätzlich zum Passwort ein. Alternativ kann eine Smartphone-App eine Push-Benachrichtigung senden, die eine Bestätigung des Nutzers anfordert (Abbildung 2).

Viele Angreifer haben sich jedoch darauf eingestellt und betreiben nun "Attacker in the Middle"-Phishing (AitM-Phishing) basierend auf einem Proxy-Server (Abbildung 3). AitM-Phishing ist heute weit verbreitet und ein fester Bestandteil zahlreicher Phishing-Toolkits. Mit dieser Technik kann ein Angreifer jede Information, die der Nutzer selbst eingibt, im Rahmen eines Phishing-Angriffs abgreifen. Der Angreifer kann diese Informationen sofort auf der Ziel-Website einspielen und sich so anstelle des Opfers authentifizieren. Auch wenn ein OTP alle 30 Sekunden abläuft, ist genügend Zeit, um den Angriff auszuführen. Ein geschulter Anwender könnte die falsche Identität des Proxy-Servers zwar entlarven, indem er das Zertifikat überprüft, doch in der Praxis wird dies selten passieren, da nur wenige Nutzer das erforderliche Know-how besitzen und den damit verbundenen Komfortverlust in Kauf nehmen.

Nur signaturbasierte MFA schützt gegen Phishing

Gegen Phishing kann MFA nur schützen, wenn mindestens ein Faktor der Authentifizierung auf einer Geheiminformation beruht, die nicht über das Netz geschickt wird. Dies ist insbesondere der Fall, wenn ein privater Schlüssel genutzt wird, der sicher gespeichert ist und nicht preisgegeben, sondern zur Erstellung einer digitalen Signatur verwendet wird. Es gibt im Wesentlichen zwei bewährte Technologien, die signaturbasierte MFA einbinden: Authentifizierung auf Basis digitaler Zertifikate („Certificate Based Authentication") und FIDO-Authentifizierung („Fast IDentity Online").

Phishing-sichere MFA durch private Signaturschlüssel

Die Authentifizierung auf Basis digitaler Signaturen ist eine wirkungsvolle Maßnahme gegen Phishing, da hierbei keine Geheiminformation über das Netz geschickt wird. Eine solche Authentifizierung läuft wie folgt ab (Abbildung 4):

1. Der Server sendet eine Challenge an den Client, die eine Zufallszahl, die aktuelle Uhrzeit und die URL des Servers enthält.
2. Der Client nutzt seinen privaten Schlüssel, um eine digitale Signatur zu erstellen. Der private Schlüssel ist durch einen anderen Faktor geschützt, wie z.B. eine PIN oder eine biometrische Information (Fingerabdruck oder Gesichtserkennung).). Der Client signiert die Challenge und sendet das Resultat als Response an den Server zurück. Die Response ist an die TLS-Verbindung gebunden und somit nur in dieser gültig. Ein Phishing-Angreifer, der eine separate TLS-Verbindung zum Server aufbauen muss, kann damit nichts anfangen.
3. Der Server prüft die Signatur. Wenn sie korrekt ist und zur TLS-Verbindung passt, ist die Authentifizierung erfolgreich.

1. https://www.forbes.com/advisor/business/phishing-statistics/
2. https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html

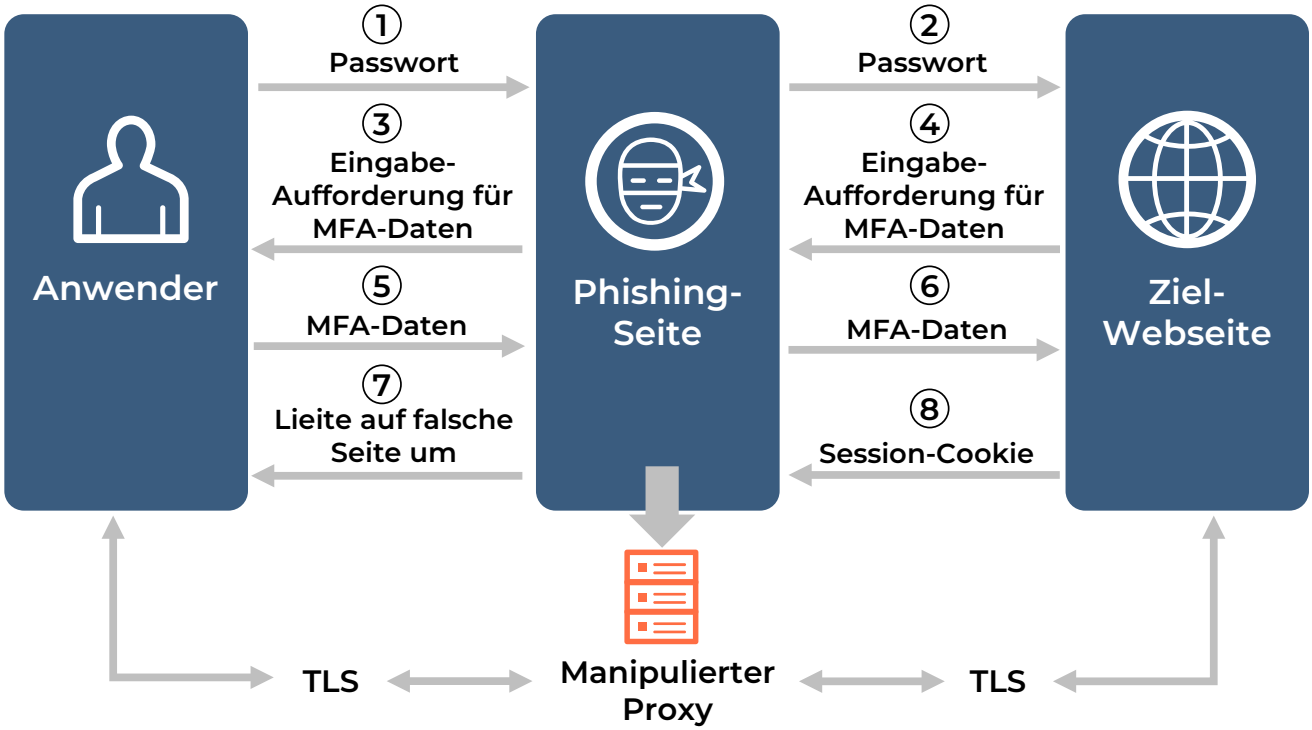


Abbildung 3: Ein Angreifer authentifiziert sich erfolgreich bei einer Ziel-Website über „Attacker in the Middle"-Phishing mit Wiederholung von Informationen auf beiden Seiten.

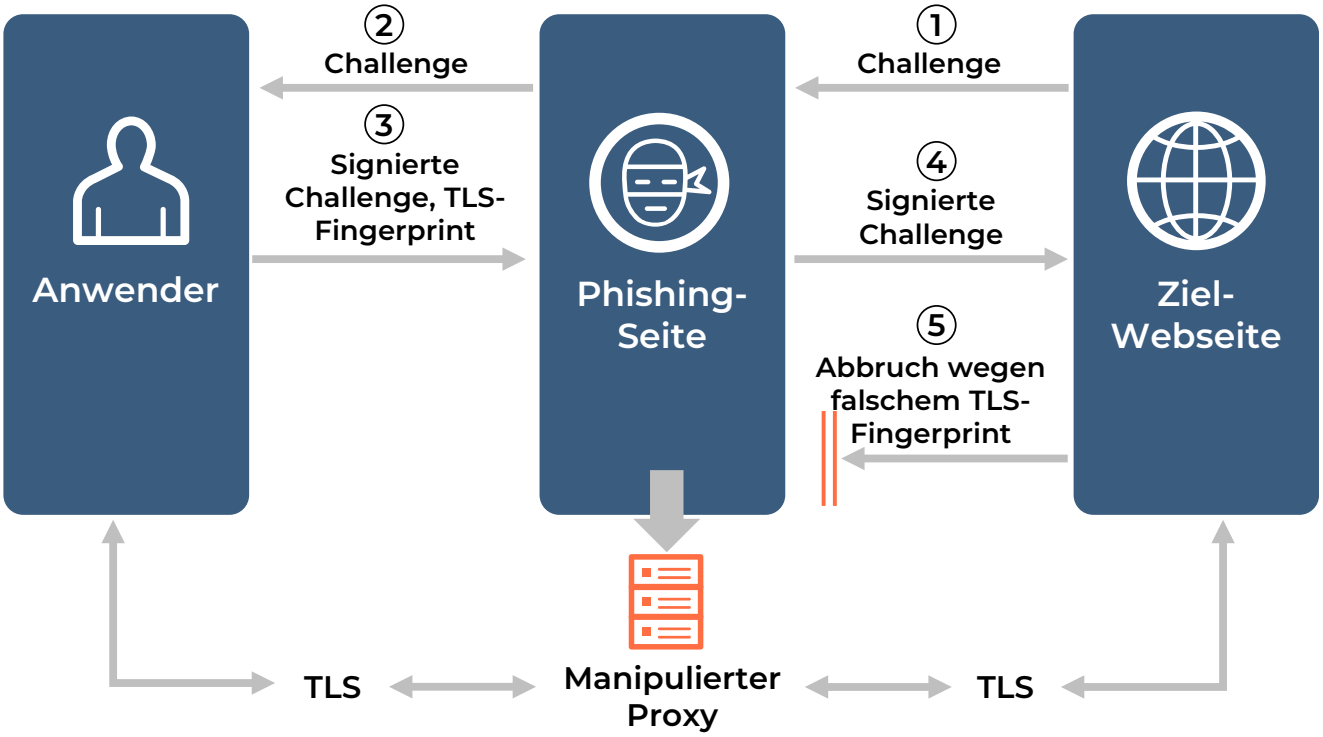


Abbildung 4: Phishing-sichere MFA schützt vor „Attacker in the Middle"-Angriffen.

Phishing-sichere MFA-Authentifizierung

Zertifikatsbasierte Authentifizierung

- ✓ Basiert nicht auf Passwörtern
- ! Benötigt eine Public-Key-Infrastruktur
- ✓ Digitale Zertifikate (von Zertifizierungsstelle signiert) sichern Authentizität
- ✓ Wird von zahlreichen Betriebssystemen, Browsern und anderen Komponenten unterstützt
- ✓ Zentrale Sperrung von Zertifikaten möglich
- ✓ Für E-Mail- und Dateiverschlüsselung nutzbar
- ✓ Auch für vertrauenswürdige digitale Signaturen nutzbar
- ✓ Zentralisiertes Management
- ✓ Unterschiedliche Smartcard-Formfaktoren möglich
- ✓ Key Recovery möglich

FIDO-Authentifizierung

- ✓ Basiert nicht auf Passwörtern
- ! Benötigt Out-of-Band-erstellte Vertrauensbeziehung
- ✗ Separates Schlüsselpaar für jeden Kommunikationspartner
- ✗ Keine zentrale Schlüsselsperrung
- ✗ Nicht für E-Mail- und Dateiverschlüsselung nutzbar
- ✗ Nicht für vertrauenswürdige digitale Signaturen nutzbar
- ✗ Kein zentralisiertes Management
- ✓ Unterschiedliche Smartcard-Formfaktoren möglich
- ✗ Key Recovery nicht möglich

Damit eine MFA mit privaten Signaturschlüsseln funktioniert, müssen die zugehörigen öffentlichen Signaturschlüsseln vertrauenswürdig sein. Für diesen Zweck gibt es zwei Ansätze: Zum einen können digitale Zertifikate und eine Public-Key-Infrastruktur (PKI) genutzt werden. Zum anderen kann das Rahmenwerk der FIDO zum Einsatz kommen. Die Vor- und Nachteile der beiden Varianten werden in der obigen Tabelle beschrieben.

Sowohl Zertifikate als auch FIDO eignen sich zum Erreichen des höchsten Authenticator Assurance Levels 3 (AAL3), das in den NIST SP 800-63 Digital Identity Guidelines definiert ist, und des Authentication Level of Assurance 4 (LoA4), das in der ISO/IEC 29115-Norm definiert ist, die eIDAS Identity Assurance HIGH ermöglicht.

Hohe Sicherheit ist günstig und unkompliziert

Die zertifikatsbasierte Authentifizierung galt früher als teure Lösung, die hauptsächlich von Behörden mit hohen Sicherheitsanforderungen und im Verteidigungssektor verwendet wurde. Diese Ansicht ist inzwischen jedoch überholt.[3] Eviden bietet beispielsweise eine abonnementbasierte PKI, die nur geringe anfängliche Investitionen erfordert. Automatisierungstools für die Ausstellung, Erneuerung und Verwaltung von Zertifikaten, haben den Bedarf an spezialisiertem Personal reduziert und die Betriebskosten gesenkt. Eviden Virtual Smartcards können das in Laptops vorhandene Trusted Platform Module (TPM) nutzen, um Private Schlüssel zu schützen, wodurch die Beschaffung von Smartcards oder Token nicht notwendig ist.

Multi-Faktor-Authentifizierung kann sich bereits im ersten Jahr amortisieren. Dies liegt unter anderem daran, dass die Anwender Zeit sparen, wenn sie sich keine Passwörter merken müssen. Untersuchungen zeigen, dass Passwörter erhebliche Kosten verursachen. Forrester Research hat ermittelt, dass jedes Zurücksetzen eines Passworts 70 Dollar kostet.[4]

Auch die IT-Abteilung profitiert von der passwortlosen Multi-Faktor-Authentifizierung, da die Anzahl der Helpdesk-Anrufe aufgrund vergessener oder gesperrter Passwörter sinkt. Digitale Zertifikate bieten darüber hinaus weitere Vorteile. Insbesondere lassen sie sich zum digitalen Signieren verwenden, was die Vereinfachung zahlreicher Geschäftsprozesse ermöglicht.

3. https://www.bbc.com/worklife/article/20161219-tech-issues-kill-productivity-but-dont-rush-to-call-it
4. https://www.forbes.com/sites/forbestechcouncil/2023/03/23/embracing-the-end-of-the-password-here-and-now/

Lösungen von Eviden Digital Identity

Eviden ist ein international tätiges Unternehmen, das sich auf die Geschäftsbereiche Digital, Cloud sowie Big Data und Sicherheit spezialisiert hat. Als weltweit führender Anbieter für datengesteuerte, vertrauenswürdige und nachhaltige digitale Transformation ist Eviden ein Vorreiter der nächsten Generation digitaler Unternehmen. Das Unternehmen hat weltweit führende Positionen in den Bereichen Digital, Cloud, Daten, Advanced Computing und Sicherheit inne.

Eviden Digital Identity bietet umfassende Lösungen zur Sicherung elektronischer Identitäten mit kryptografischen Technologien und Anwendungen.

Phishing-sichere MFA-Authentifizierung von Eviden

Eviden Digital Identity bietet ein Portfolio von Lösungen zur Phishing-sicheren MFA-Authentifizierung. Der Kunde hat vielfältige Optionen, um diese Lösungen in die bestehende IT-Umgebung zu integrieren.

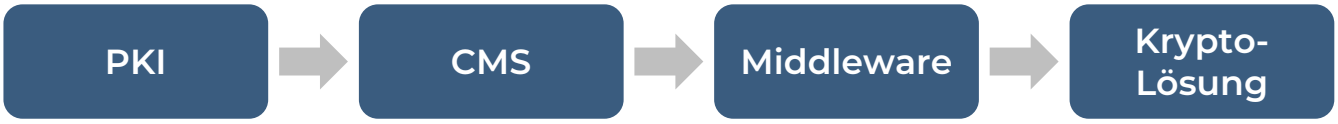


Abbildung 5: Die für MFA genutzten Zertifikate werden durch eine Middleware und bei Bedarf mit einem Credential Management System an die kryptografischen Komponenten gekoppelt.

Entscheidet sich der Kunde für eine MFA mit digitalen Zertifikaten, kann eine bereits vorhandene PKI genutzt werden. Alternativ lässt sich mit IDnomic PKI von Eviden eine neue PKI mit wenig Aufwand aufbauen. IDnomic PKI ist als „On Premise"-Lösung verfügbar, oder der Kunde kann ein Cloud-basierendes „Software as a Service"-Modell nutzen. Die Zertifikate werden durch eine Middleware und bei Bedarf mit einem Credential Management System an die kryptografischen Komponenten gekoppelt (Abbildung 5). Je nach Anforderung können hierbei ebenfalls bereits existierende Lösungen genutzt werden. Eviden bietet für diesen Zweck mehrere bewährte Produkte an, darunter die Smartcard-Middleware cryptovision SCinterface und das Credential Management System IDnomic CMS.

Die für eine Public-Key-Infrastruktur notwendigen kryptografischen Schlüssel werden in einer geschützten Hardware gespeichert, beispielsweise einer Smartcard. Die Middleware cryptovision SCinterface VSC ermöglicht es außerdem, das in jedem Endgerät vorhandene Trusted Platform Module (TPM) zur Schlüsselspeicherung und damit als virtuelle Smartcard zu nutzen.

Für Kunden, die Smartcards verwenden wollen, ist das bewährte Produkt CardOS von Eviden eine sehr sichere Option mit einem Sicherheitschip und einem Smartcard-Betriebssystem, das in der EU entwickelt und zertifiziert wurde. Es ist in zwei Formfaktoren erhältlich: als Token mit USB- und NFC-Schnittstelle und als traditionelle Chipkarte mit Kontakt- und NFC-Schnittstelle. CardOS unterstützt nicht nur PKI-Funktionen, sondern kann auch mit FIDO-Schlüsseln umgehen und ist für diesen Zweck zertifiziert. Damit ist auch eine phishing-sichere MFA-Authentifizierung in der FIDO-Variante mit CardOS möglich. Die beiden Ansätze können auch kombiniert werden: So kann der Kunde z.B. die zertifikatsbasierte Authentifizierung für Ressourcen innerhalb des Unternehmens nutzen und hat zusätzlich die Möglichkeit, FIDO für den Zugriff auf Systeme außerhalb der eigenen PKI zu nutzen.

Phishing zuvorkommen mit S/MIME

Da die Mehrheit der Phishing-Angriffe über E-Mails erfolgt, gewinnen signierte E-Mails als Sicherheitsmaßnahme zunehmend an Bedeutung im Unternehmen. Das hierfür üblicherweise verwendete Format ist S/MIME. Durch die Signatur wird die Integrität der E-Mail und die Identität des Senders sichergestellt.

Mit cryptovision GreenShield bietet Eviden eine umfassende Lösung für die sichere und vertrauenswürdige E-Mail-Kommunikation. Detaillierte Informationen dazu finden Sie online.[5]

5. https://www.cryptovision.com/de/produkte/security-applications/greenshield/

Sie wollen mehr über unser Angebot erfahren? Kontaktieren Sie uns:

cv-info@eviden.com

www.cryptovision.com

Unser Beratungsteam setzt sich gerne mit Ihnen in Verbindung.

Eviden
cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Deutschland
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

EVIDEN

Eviden[1]

Eviden ist ein Technologieunternehmen der nächsten Generation im Bereich der datengesteuerten, vertrauenswürdigen und nachhaltigen digitalen Transformation mit einem starken Portfolio an patentierten Lösungen. Mit weltweit führenden Positionen in den Märkten für Advanced Computing, Sicherheit, KI, Cloud und digitale Plattformen bietet Eviden fundiertes Fachwissen für alle Branchen in mehr als 47 Ländern. Eviden vereint 53.000 Talente und erweitert die Möglichkeiten von Daten und Technologien über das gesamte digitale Kontinuum hinweg, heute und für kommende Generationen. Eviden ist ein Unternehmen der Atos-Gruppe mit einem Jahresumsatz von ca. 5 Mrd. €.

[1] Eviden ist mit den folgenden Marken vertreten: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden ist eine eingetragene Marke. © Eviden SAS, 2023.

Atos

Atos ist ein weltweit führendes Unternehmen im Bereich der digitalen Transformation mit 105.000 Mitarbeitern und einem Jahresumsatz von ca. 11 Mrd. EUR. Als europäische Nummer eins in den Bereichen Cybersicherheit, Cloud und High-Performance Computing bietet die Gruppe maßgeschneiderte End-to-End-Lösungen für alle Branchen in 69 Ländern. Als Pionier bei Dienstleistungen und Produkten zur Dekarbonisierung setzt sich Atos für eine sichere und dekarbonisierte digitale Welt für seine Kunden ein. Atos ist eine SE (Societas Europaea) und an der Euronext Paris notiert.

Das Ziel von Atos ist es, die Zukunft des Informationsraums mitzugestalten. Seine Kompetenzen und Dienstleistungen unterstützen die Entwicklung von Wissen, Bildung und Forschung in einem multikulturellen Ansatz und tragen zur Entwicklung wissenschaftlicher und technologischer Spitzenleistungen bei. Weltweit ermöglicht die Gruppe ihren Kunden und Mitarbeitern sowie den Mitgliedern der Gesellschaft insgesamt, in einem sicheren und geschützten Informationsraum zu leben, zu arbeiten und sich nachhaltig zu entwickeln.

eviden.com

 20240802