Whitepaper

Haftungsrisiken für Unternehmen: Wer haftet und wie Sie Verstöße im Vorfeld verhindern

MATESO
PASSWORD SAFE

Vorwort

IT-Sicherheitsverstöße und Cyberangriffe sind gerade im Unternehmensbereich mittlerweile keine Seltenheit mehr. Kommt es aber im Ernstfall dazu und das eigene Unternehmen ist betroffen, kann die Geschäftsführung selbst in die Verantwortung gezogen werden – selbst, wenn diese von den Vorfällen gar nicht weiß und sich des Sicherheitsrisikos nicht bewusst war. Denn viele Unternehmen setzen sich mit IT-Sicherheit erst auseinander, wenn es dafür schon zu spät ist.

Dieses Dilemma bestätigt auch die Studie von VMware und Economist Intelligence Unit: Vielfach wird die Geschäftsführung für Cyberangriffe verantwortlich gemacht, die meist weder über Datenlecks und -verluste oder Sicherheitslücken informiert ist. Kein Wunder: Laut der Umfrage informiert jeder fünfte IT-Verantwortliche nicht die Unternehmensleitung über potentielle Sicherheitsvorfälle oder -lecks. Trotzdem sieht jeder Dritte diese in der Verantwortung, wenn es zu einem Vorfall kommt. Aber nur 11 Prozent der CEOs deutschlandweit sehen Cybersicherheit als essentielles Thema an. Wobei wiederum einer von drei CIOs einen Cyberangriff auf das eigene Unternehmen in den nächsten drei Monaten für wahrscheinlich hält und dieses zudem für dafür schlecht vorbereitet einstuft. Gründe dafür sind unter anderem veraltete IT-Sicherheitsmaßnahmen oder eine zu langsame Reaktionszeit auf Bedrohungen.

Dieses Whitepaper dient deshalb dazu, die Haftungsverantwortung sowie -risiken bei einem Sicherheitsvorfall oder Cyberangriff zu analysieren und zu bewerten, daraus Handlungsempfehlungen für Unternehmen zu ziehen und präventive Maßnahmen für diese abzuleiten.

Wir recherchieren unsere Beiträge sehr ausführlich. Die nachfolgenden Informationen stellen dennoch keine Rechtsberatung oder rechtsverbindliche Auskunft dar. Es handelt sich lediglich um einige Hinweise auf rechtliche Rahmenbedingungen.

»Unwissenheit schützt vor Strafe nicht – auch nicht vor Haftung.«

Haftungsverantwortung

Handelt es sich um einen Vorfall / Verstoß, der sich auf unzureichend dokumentierte oder umgesetzte IT-Sicherheit zurückführen lässt, so haftet an erster Stelle das Unternehmen selbst. Im weiteren Verlauf ist eine persönliche Haftung, die die Entscheider in der Unternehmensleitung betrifft, durchaus möglich, auf die im weiteren näher eingegangen wird.

KRITIS

Am 25.07.2015 ist das IT-Sicherheitsgesetz für Betreiber von »kritischen Infrastrukturen« (KRITIS) wie etwa Banken, Energieunternehmen oder Krankenhäuser in Kraft getreten. Diesem Gesetz nach sind diese verpflichtet, Mindeststandards für die IT-Sicherheit zu beachten, um ihre Systeme insbesondere vor Cyberangriffen zu schützen.

Kann ich Mitarbeitende haftbar machen, wenn der Vorfall durch ihr Verschulden zustande kam?

Ein Großteil von Sicherheitsverstößen kommt laut dem Cyber Security Intelligence Index von IBM durch Fehler von Mitarbeitenden zustande. Da aber ihre Haftung bei fahrlässigem Handeln beschränkt ist, ist der Rückgriff auf diese im Haftungsfall wenig vielversprechend. Das BAG hat für Arbeitnehmende auch bisher keine Haftungsquote festgelegt, die deren Jahresgehalt übersteigen und somit die durch einen Cyberangriff zustande kommenden Kosten kaum decken könnte. Dazu kommt, dass dieses Fehlverhalten laut Arbeitsrecht zuerst einmal nachgewiesen werden müsste. Das bedeutet, dass im Ernstfall Arbeitgeber für ihre Arbeitnehmer und deren Fehlverhalten haften. Kam es also beispielsweise zu einem Cyberangriff durch ein offen gelegtes Passwort, müsste zuerst einmal nachvollziehbar sein, wer dieses Passwort im Unternehmen kannte und wie er dieses verwaltet hat.

Kann ich Dienstleistende haftbar machen, wenn der Vorfall durch ihr Verschulden zustande kam?

Dienstleistende erfüllen meist nur die im Vertrag festgelegten vereinbarten Aufgaben als Hauptaufgaben. Somit ist eine Haftbarkeit dieser eher als erfolglos anzusehen. Diese vereinbarten Aufgaben können zudem auch nicht dem heutigen technischen Stand entsprechen (siehe Art. 24 Abs. 1 u. 2 DSGVO). Sofern also Dienstleistende nicht vertraglich dazu verpflichtet sind, dem »Stand der Technik« zu entsprechen und einen Nachweis darüber erbringen zu können, unterliegen diese nur der Nebenpflicht, die Geschäftsführung lediglich auf die erforderlichen technischen Maßnahmen (TOMs) hinzuweisen.

Wurde der Beratungspflicht nicht nachgekommen und die Aufklärungspflicht dadurch verletzt, kann bei Dienstleistenden theoretisch Schadenersatz eingefordert werden (siehe § 280 BGB). Gerade bei größeren Verträgen sind allerdings Haftungsgrenzen festgelegt, die Forderungsansprüche zusätzlich erschweren.

Art. 24 DSGVO Verantwortung des für die Verarbeitung Verantwortlichen

1. Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

2. Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

3. Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

Kann ich den Hersteller haftbar machen, wenn der Vorfall durch sein Verschulden zustande kam?

Kommt es zu einem Cyberangriff, liegt es nahe, die Schuld beim Hersteller der Software oder dessen Vertrieb zu sehen. Allerdings werden etwaige Sicherheitslücken meist erst nach dem Kauf erkannt und können nicht dem Hersteller angelastet werden, wenn die Software zum Kaufzeitpunkt dem »Stand der Technik« entsprach. Auch Zwischenhändler sind nicht zur Produktbeobachtung verpflichtet. Dies macht es umso wichtiger, die zu erwerbende Software genau zu analysieren und auf höchste Sicherheitsstandards zu achten. Wenn das Produkt etwa keine Backdoors hat und dem europäischen Datenschutzrecht unterliegt, sind Unternehmen somit besser abgesichert.

Bin ich als Geschäftsführer/-in haftbar?

Zum Schluss läuft es in puncto Haftung und finanziellem Ausgleich zumeist auf die Geschäftsführung zurück. Diese sollte sich dieser Tatsache und Gefahr sowie den potentiellen Auswirkungen für das Unternehmen, die existenzbedrohend sein können, daher jederzeit bewusst sein und dementsprechende Sicherheitsmaßnahmen aktiv anstoßen und überwachen. Die Geschäftsführung ist somit in der (Sorgfalt-)Pflicht, sich persönlich rechtstreu zu verhalten und zu gewährleisten, dass das Unternehmen nicht gegen Gesetze, Rechtsvorgaben und Richtlinien verstößt. Dazu gehört auch, personenbezogene Daten zu schützen und hierfür angemessene organisatorische Maßnahmen (TOMs) zu ergreifen. Sie ist somit verantwortlich dafür, dass die IT-Sicherheit unternehmensweit dem Stand der Technik entspricht.

FAQ

Kann ich mich gegen potentielle Bußgelder versichern lassen?

Schadenzahlungen für Bußgelder sind leider nicht versicherbar. Deshalb ist es umso wichtiger, dass sich die Geschäftsführung präventiv an die gesetzlichen Vorschriften hält, um derlei Strafen zu vermeiden.

Kann ich Haftungsbeschränkungen oder einen Haftungsausschluss laut AGB geltend machen?

Trotz Verwendung von AGB, die auch Haftungsbeschränkungen beinhalten, muss für die Folgen des Schadens aufgekommen werden, da zum Beispiel etwaige Liefertermine oder der Schutz von Kundendaten zu den Vertragspflichten gehören. Ein Haftungsausschuss wäre höchstens möglich, wenn es sich um eine individualvertragliche Vereinbarung handelt.

Haftungsrisiken

Aktiengesetz: Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder

Wenn die Geschäftsleitung oder der Vorstand ihren Pflichten zum Schutz der IT-Infrastruktur nicht nachkommen, können Ansprüche von der durch den Hackerangriff geschädigten Gesellschaft nach § 93 Abs. 2 Satz 1 AktG bzw. § 43 Abs. 2 GmbHG geltend gemacht werden. Dieser Paragraph kann Verwendung finden, wenn etwa die Geschäftsleitung nicht angemessen mit Risikovermeidungs- oder Risikoverminderungsmaßnahmen reagiert hat oder wenn sie trotz Hinweisen auf und dem Wissen über bestehende technische und organisatorische Defizite zum Schutz personenbezogener Daten untätig geblieben ist.

§ 93 Abs. 2 Satz 1 AktG GmbHG

»Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. (...) Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast.«

§ 43 Abs. 2 GmbHG

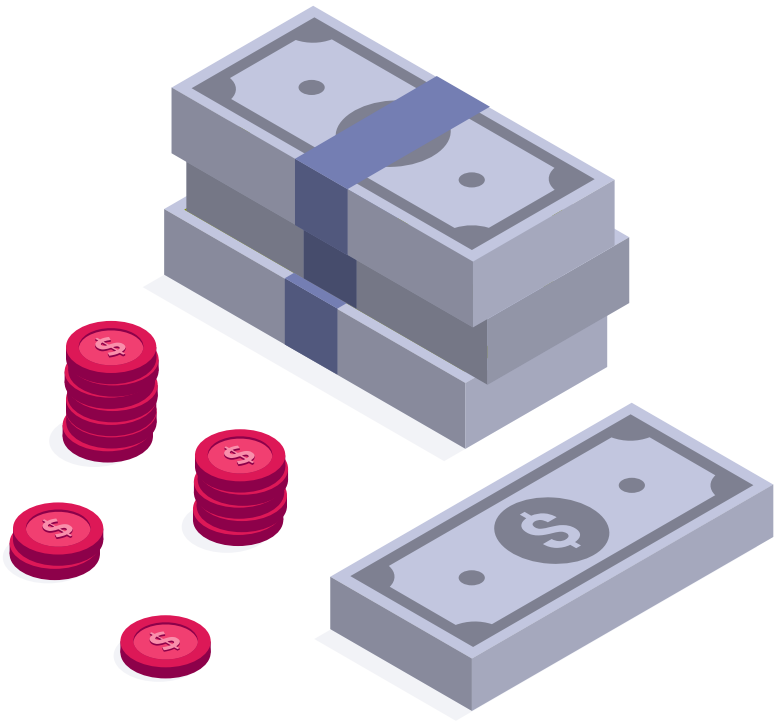
»Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden.«

Sorgfaltspflicht und -maßstab

Für die gängigen Unternehmensformen AG und GmbH wird der Sorgfaltsmaßstab (nach § 1297 ABGB) in die Betrachtung miteinbezogen. Nach diesem muss zuerst geprüft werden, ob eine Verletzung der Sorgfaltspflicht vorliegt und wie man sich in dieser speziellen Situation hätte verhalten müssen. An diesem Soll-Zustand wird daraufhin das tatsächliche Verhalten gemessen und bewertet – ob also der Täter hat Sorgfalt walten lassen oder ob er ein unerlaubtes Risiko geschaffen hat. Weicht er negativ von der Sorgfaltspflicht ab, kann ein behördliches Bußgeld auch dem einzelnen Mitglied der Geschäftsleitung auferlegt werden. Dieses kann sich bei einer Straftat laut Datenschutzrecht auf bis zu eine Million Euro belaufen.

Kosten durch Cyberangriffe

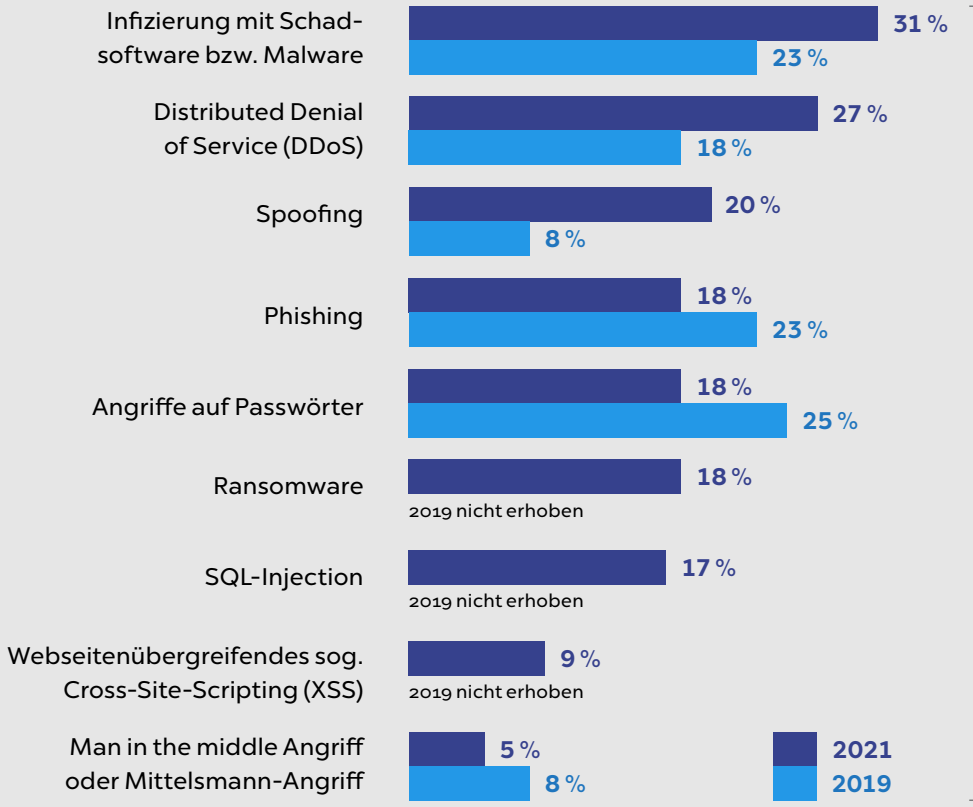
Die Kosten, die durch den Schaden eines Cyberangriffs anfallen, beziehen sich nicht nur auf das Wiederherstellen von Betriebssystemen. Vor allem wirtschaftliche Folgen und die daraus resultierenden Umsatzeinbußen sowie langfristige Wertverluste oder auch Kosten, die ein Unternehmen zur Ursachenforschung miteinkalkulieren muss, können diese exponentiell wachsen lassen. Dazu kommen Ausgaben für eine etwaige juristische Beratung sowie potentielle Bußgelder. Derlei unerwartete Aufwände können noch beträchtlich steigen, wenn Schadensersatzzahlungen (§ 280 Abs. 1, 2; 286 BGB) durch Dritte geltend gemacht werden können. Dies geschieht, wenn durch den Cyberangriff Deadlines nicht mehr eingehalten werden können und es etwa zu Lieferverzügen oder sogar -ausfällen kommt. Auch bei einem Datenverlust oder -diebstahl wird die Vertraulichkeitspflicht des Unternehmens verletzt und Schadensersatzzahlungen werden fällig. Summa summarum können die sich tatsächlich belaufenden Kosten nach einem Cyberangriff schnell existenzbedrohend für Unternehmen werden.



Wie wahrscheinlich ist es, dass mein Unternehmen angegriffen wird?

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?



Cyberangriffe haben bei

86%

der Unternehmen einen Schaden verursacht – **2019** waren es erst **70 %.**

Quelle: Bitkom Research 2021

Alle befragten Unternehmen (2021: n = 1.067; 2019: n =1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre

Kosten durch DSGVO-Verstöße

Wurden Daten nicht DSGVO-konform verarbeitet, haftet das Daten-verarbeitende Unternehmen für daraus resultierende (im-)materielle Schäden. Der immaterielle Schaden kann dabei – vor allem, wenn personenbezogene Daten gestohlen wurden – schnell den materiellen Schaden übersteigen. Laut BSI-Gesetz werden Ordnungswidrigkeiten mit Bußgeldern von bis zu 100.000 € belegt. Handelt es sich allerdings um DSGVO-Sicherheitsverstöße, können Strafen um einiges drastischer ausfallen. Sie werden anteilig am weltweiten Jahresumsatz des vergangenen Geschäftsjahres des Unternehmens gerechnet – bis zu 4 % dessen oder bis zu 20 Millionen Euro. Dass diese Bußgelder tatsächlich realistisch sind, zeigen die DSGVO-Verstöße des Unternehmens Deutsche Wohnen, für das im Jahr 2019 14,5 Millionen Euro Strafe verhängt wurde, da sensible Mieterdaten rechtswidrig gespeichert wurden. Auch für Google wurde im Jahr 2020 eine Strafe von über 50 Millionen aufgrund undurchsichtiger Privatsphäre-Einstellungen festgelegt. Wäre die Strafe von Google am Vorjahresumsatz als Höchstsatz festgelegt worden, hätte sie mit 3,7 Milliarden Euro sogar noch um einiges höher ausfallen können.

Gemäß Art. 32 der Datenschutz-Grundverordnung (DSGVO) haben Unternehmen, die personenbezogene Daten erheben, verarbeiten oder nutzen »angemessene technische und organisatorische Maßnahmen« (TOMs) zu treffen.

»Wie hohe Strafen können auf mein Unternehmen zukommen?«

Faustregel:

$$\frac{\text{Jahresumsatz}}{365} \times 10$$

Vergleich unterschiedlicher Rechtsformen

Die Rechtsform ist von entscheidender Bedeutung für die Haftung des Unternehmens. Von dieser hängen mitunter auch die Besteuerung und die Verteilung der Führungsverantwortlichkeit ab. Entnehmen Sie deshalb dieser Übersicht, bei welchen Rechtsformen eine Haftung mit Privatvermögen in jedem Fall oder nur bedingt möglich ist.

Einzelunternehmen Eingetragene/r Kaufmann /-frau	GbR / OHG	GmbH / UG / AG	KG	Ltd.
→ unbeschränkte Haftung mit Privatvermögen	→ gesamtschuldnerische Haftung mit Privatvermögen	→ beschränkte Haftung in Höhe des Gesellschaftsvermögens	→ Haftung des persönlich haftenden Gesellschafters in Höhe der Einlage	→ Haftung mit Privatvermögen

Prävention und Vorgehen

Um das eigene Unternehmen und dessen Daten und Geheimnisse zu schützen, aber auch, um eine eigene Haftung zu umgehen, ist es essentiell, die bestehenden Cybersicherheitsmaßnahmen und Gesetze wie das IT-Sicherheitsgesetz zu befolgen und die daraus resultierenden Pflichten bestmöglich umzusetzen. Um die interne IT-Sicherheit besser einschätzen und verbessern zu können, sind eine enge Zusammenarbeit sowie ein regelmäßiger Abgleich mit der IT und stellvertretend dafür der IT-Leitung unabdingbar. Da die meisten Cyberangriffe auf Fehler von Mitarbeitenden zurückzuführen sind, ist auch ein Investment in Sicherheitstrainings, um die Awareness zu verbessern, ein wichtiges Mittel in der Prävention.

Einführung von klaren Standards, Tools & Prozessen

Wenn Unternehmen keine klaren Richtlinien für Mitarbeitende formulieren und ausrollen, werden diese weiterhin (zumeist unwissend) gegen Gesetze verstoßen. Deshalb ist es umso wichtiger, Standards in die Praxis umzusetzen und Mitarbeitende nicht mit deren Umsetzung alleine zu lassen. IT-Sicherheits-Tools wie Password Manager können dabei helfen, Sicherheitslücken zu schließen und aktiv zu mehr und unternehmensweiter Cyberhygiene beizutragen. Zudem werden in Password Managern wie Password Safe alle Aktionen dokumentiert, sodass auch im Falle eines Sicherheitsvorfalls nachverfolgt werden kann, wer wann auf welche Zugangsdaten Zugriff hatte. Diese Dokumentation ist auch essentiell, wenn es darum geht, die eigene Haftungsverantwortlichkeit auszuschließen.

Organisation von Sicherheits-Teams und -Strukturen

Um präventiv gegen Cyberangriffe vorzugehen, eignen sich dedizierte Personen oder Teams im Unternehmen, die sich um die praktische Umsetzung von Sicherheitsrichtlinien kümmern. Diese Security Promoter sollen dazu dienen, ein regelkonformes Sicherheitsverhalten am Arbeitsplatz vorzuleben – etwa, indem Passwörter nur noch über einen Password Manager sichtgeschützt zur Verfügung gestellt und geteilt werden. Als sogenannte Power User können sie anderen Mitarbeitenden aber auch den Einstieg in komplexere Security Tools erleichtern und somit menschliches Fehlverhalten reduzieren.

Fazit

Von Brute Force über Social Engineering bis hin zu Man-in-the Middle-Attacken: Im Zeitalter der Digitalisierung sind Unternehmen so vielen Bedrohungen ausgesetzt, dass man schon ein IT-Spezialist sein muss, um diese Gefahren in ihrer Gänze zu erkennen. Trotzdem bleibt es dabei, dass die Cybersicherheit in Unternehmen der Geschäftsführung mit einer weitreichenden Berufshaftung unterliegt. Sie obliegt damit auch der Verantwortung, für eine IT-Sicherheit nach dem »Stand der Technik« zu sorgen und Cybergefahren zu analysieren, einzugrenzen und effektiv vorzubeugen. Die Geschäftsführung ist also auch in der Pflicht notwendige Tools bereitzustellen, die das Risiko eines Angriffs oder Sicherheitsvorfalls minimieren können.

Ohne einen professionellen Password Manager ist es für Unternehmen heutzutage schwer, die Sicherheit im Umgang mit Zugangsdaten zu gewährleisten und auch zu belegen. Eine unternehmensweite Lösung zur Verwaltung, Sicherung und Überwachung von Zugangsdaten ist deshalb mehr als sinnvoll, um sich gegen Haftungsrisiken zu schützen – vor allem, wenn man bedenkt, dass Passwörter mitunter den größten Risikofaktor für die IT-Sicherheit darstellen. Darüber hinaus bieten Password Manager weitere Vorteile wie Zeitersparnis durch automatisierte Logins und Password Resets. Denn schlussendlich geht es auch beim Thema Sicherheit um Effizienz und Produktivität in Unternehmen.

Unternehmen haften für ihre Beschäftigten – zu jedem Zeitpunkt und auch trotz Unkenntnis. Deshalb muss die Geschäftsführung dem Thema Cybersicherheit schon frühzeitig aufmerksam begegnen und mit den notwendigen Tools und Prozessen Vorsorge treffen.

Autorin:

Kristina Kaya
Product Marketing Managerin

Die MATESO GmbH ist ein führendes deutsches IT-Unternehmen, das sich seit der Firmengründung in 2006 erfolgreich im DACH-Raum etabliert hat. Die entwickelte Passwort-Sicherheitslösung Password Safe wird durch ihr weltweites Partnernetzwerk international vertrieben. Namhafte Referenzen bezeugen den Technologie- und Know-how-Vorsprung der IT-Software.

Heute verzeichnet das stetig wachsende Unternehmen branchenübergreifend über 10.000 Firmenkunden mit mehreren Millionen Anwendern weltweit – darunter 21 Firmen der Dax 40.

Pioneer im Enterprise Password Management

Password Safe dient Unternehmen als zentraler digitaler Tresor zur Sicherung,Verwaltung und Überwachung von sensiblen Daten wie Passwörtern, Dokumenten und Geheimnissen.

MATESO GmbH
Daimlerstraße 15
86356 Neusäß
GERMANY
Web www.passwordsafe.de
Email marketing@passwordsafe.de
Phone +49 821 74 77 87-0

MATESO
PASSWORD SAFE