IDC

Digital Trust: Die Grundlage für Digital Freedom

STUDIE VON:

Jennifer Glenn
Forschungsdirektorin,
Security and Trust Group, IDC

November 2022 | IDC Doc. #US49795922

Inhaltsverzeichnis

Klicken Sie auf Titel oder Seitenzahlen, um zu den einzelnen Abschnitten zu navigieren.

Digital Trust definieren

Die digitale Welt stellt uns eine riesige Menge an Informationen und Hilfsmitteln zur Verfügung. Geschäftsdaten und Benutzer werden für eine bessere Zusammenarbeit, effizientere Abläufe und mehr Innovation durch Geräte und Anwendungen verbunden. Private Geräte und Programme integrieren unsere persönlichen Informationen für alles, von der Finanzverwaltung und der Überwachung von Gesundheitsdaten bis hin zur Steuerung von Geräten und Online-Einkäufen. Allen Hilfsmitteln liegt die Infrastruktur der Verbindungen sowie die kontinuierliche Datenkommunikation über das Internet zugrunde. In Anbetracht der Bedeutung und der Abhängigkeit von diesen Hilfsmitteln für die Arbeit und das tägliche Leben können diese Verbindungen nicht ohne Folgen unterbrochen, beendet oder verändert werden. Dies erfordert ein hohes Maß an Schutz und Validierung der Einrichtungen und Daten, welche unsere digitale Infrastruktur ausmachen. Hier kommt Digital Trust zum Einsatz.

Digital Trust wird durch die strategische Implementierung von Technologie, Verfahren und Richtlinien erreicht, die es den Nutzern ermöglichen, sich furchtlos in ihrer digitalen Welt zu bewegen. Es ist eine Vorkehrung, um Vertrauen und Sicherheit zu schaffen, damit die digitalen Produkte und Dienstleistungen, auf die sich die Welt tagtäglich verlässt, sicher, da unverfälscht und geschützt, sind. Digital Trust bedeutet die Freiheit, zu arbeiten, sich zu vergnügen und sich mit der digitalen Welt zu verbinden, ohne sich zu sorgen, von bösartigen Akteuren beeinträchtigt zu werden.

Verstehen der Komponenten, welche Digital Trust Wirklichkeit werden lassen

Zwar ist Digital Trust von höchster Wichtigkeit, jedoch werden dessen Mechanismen oft als selbstverständlich angesehen. Wenn der durchschnittliche Verbraucher oder Geschäftskunde online navigiert, denkt er in der Regel nicht darüber nach, wie er Informationen oder Dienstleistungen erhält (obwohl das Vertrauen in die Marke leiden kann, wenn die gewünschten Informationen oder Dienstleistungen nicht verfügbar sind). Das *Wie* unserer digitalen Grundlagen wurde traditionell von IT-Fachleuten, welche sich den technischen Komplexitäten von Schlüsseltechnologien wie der Public Key Infrastructure (PKI) widmen, geschaffen und gemanagt.

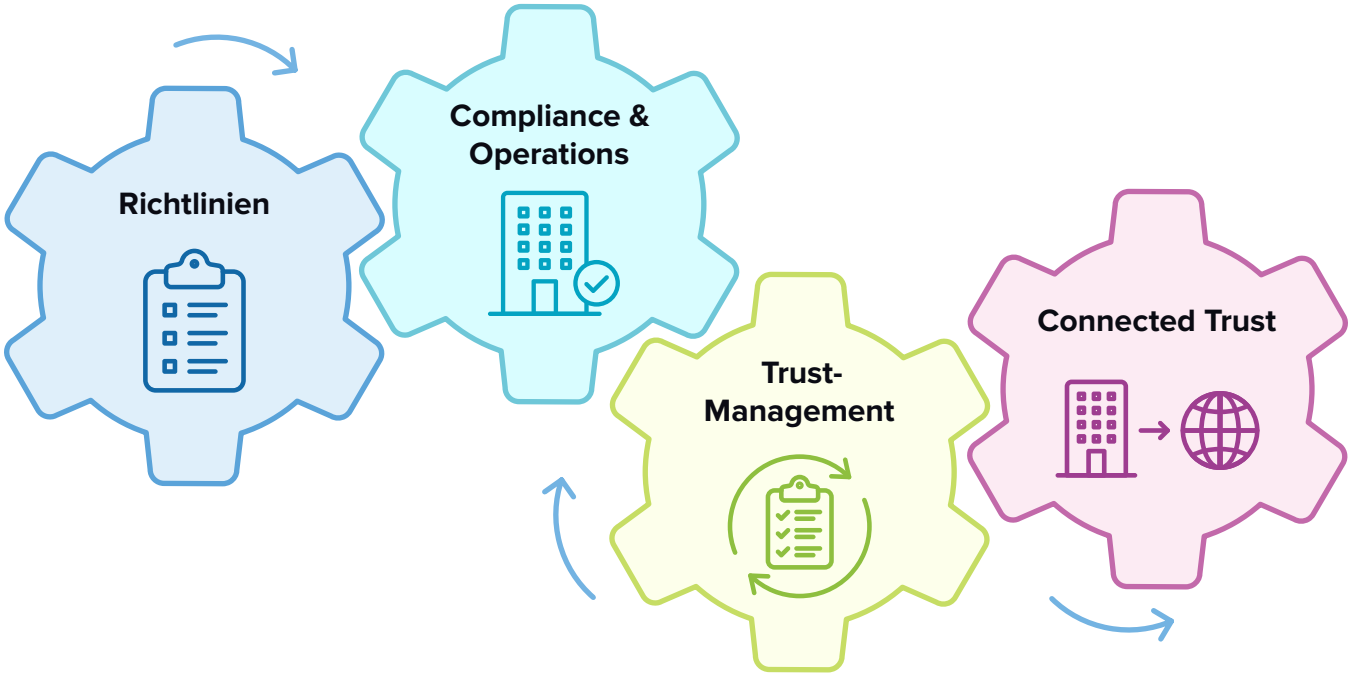
Eine PKI besteht aus der Infrastruktur (einschließlich der Regeln, Verfahren und Technologie), die für den Austausch kryptografischer Schlüsselinformationen zwischen Benutzern oder Geräten verwendet wird. Diese Schlüssel sind für die Ver- und Entschlüsselung von Daten während der Speicherung, bei der Übertragung an verschiedene Orte im Internet und/oder beim Verwenden für Anwendungen erforderlich.

Ein Schlüsselaustausch erfolgt heute einheitlich über digitale Zertifikate, welche mindestens aus einem Schlüssel und einer Signatur bestehen. Zur genauen Identifizierung der den Schlüssel kontrollierenden Einheit enthalten viele Zertifikate auch Identitätsinformationen. Der Einsatz von PKI ist für die Erleichterung der sicheren Online-Kommunikation und die Überprüfung der Signaturenintegrität unerlässlich und bildet die Grundlage zum Digital-Trust-Aufbau.

Allen strategischen Maßnahmen kommen eine klare Ausrichtung und Zielsetzung, messbare Ziele, ein starkes Management sowie eine solide Unterstützung zugute. Digital Trust bildet keine Ausnahme. Die vier in **Abbildung 1** dargestellten Komponenten bieten die Struktur und Definition für eine erfolgreiche Verwirklichung von Digital Trust.

ABBILDUNG 1

Die vier Komponenten des Digital Trust



Quelle: IDC, 2022

Richtlinien

In jedem System legen die entsprechenden Richtlinien einen Rahmen für das Zusammenwirken der Teilnehmer und die Mindestanforderungen für die Erstellung eines funktionierenden Projekts fest. Verschiedene Normungsgremien befassen sich mit Digital Trust für unterschiedliche Anwendungsfälle, bei denen digitale Zertifikate eine zentrale Rolle spielen. Unter anderem sind dies die Zertifizierungsstelle (CA)/Browser Forum, Matter, SAE International, Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI) sowie die Internet Corporation for Assigned Names and Numbers (ICANN). Über Änderungen oder Anpassungen der Richtlinienanforderungen auf dem Laufenden zu bleiben, kann eine Herausforderung sein. Aufsehenerregende Angriffe sowie Datenschutzanforderungen schärfen das Bewusstsein der Verbraucher für die zu schützenden Daten und/oder wie sie verwendet werden können. Dies wiederum veranlasst die Branchenverbände, Aktualisierungen und Änderungen an den Richtlinienanforderungen vorzunehmen.

Im Falle von digitalen Zertifikaten geben Unternehmen wie das CA/Browser Forum klare Richtlinien vor, wann eine Zertifizierungsstelle ein Zertifikat ausstellen kann, welchen Inhalt dieses Zertifikat hat und wann ein Zertifikat widerrufen werden muss. Die PKI-Standards variieren nach Anwendungsfall des Zertifikats sowie entsprechend der Bedeutung der zu sichernden Informationen.

Um die Grundlage für starkes Digital Trust für Ihr Unternehmen zu schaffen, ist es wichtig, den Überblick über die Anforderungen dieser Richtlinien und alle Änderungen zu behalten. Während einige Unternehmen die Standards selbst verfolgen und managen, verlassen sich die meisten bei der Wahrung auf ihre Zertifizierungsstellen. Unabhängig davon, wer die Verantwortung trägt, sollten gewandte Unternehmen über ein klares Verfahren verfügen, um auf dem neuesten Stand der Richtlinien zu bleiben. Sie sollten die Richtlinienänderungen für die Zertifikatsvalidierung nicht nur aufzeichnen und managen, sondern auch überprüfen.

Compliance und Operations

Es ist eine Sache, die Richtlinien zu kennen und zu verstehen. Die Einhaltung durch die einzelnen Teilnehmer zu regeln, kann jedoch eine ganz eigene Aufgabe sein. Die Einhaltung der Vorschriften (Compliance) kann auf zwei Arten gemessen werden. Zum einen gibt es die Möglichkeit, zu erfassen und darzustellen, wie gut Unternehmen die von den Normungsgremien festgelegten Richtlinien erfüllen. Aus der Sicht der Business Operations kann dies wie eine Checkliste aussehen, in der die erforderlichen Punkte zur Erfüllung der verschiedenen Richtlinien aufgeführt sind. Dies führt zur zweiten, einer internen Art der Messung. Wenn Sie zum Beispiel mehrere Teams haben, die Server- oder Gerätezertifikate erwerben, können diese Checklisten dazu beitragen, dass alle im Unternehmen auf demselben Stand sind. Digital Trust ist, bzw. sollte, eine unternehmensweite Aufgabe sein, und genau diese Beständigkeit ist ein wichtiges Instrument für jede Abteilung, ihren Erfolg an diesen Zielen zu messen.

Für die mit dem Unternehmen zusammenarbeitenden Zulieferer und/oder die Verbraucher, welche sich auf die Produkte oder Dienstleistungen verlassen, ist es ein klarer Beweis des Bekenntnisses an Qualität und Vertrauen, wenn sie das Verfolgen und Einhalten der Industriestandards durch das Unternehmen erkennen.

Trust-Management

Mit der Einhaltung von Industriestandards geht folgende Notwendigkeit einher: das Trust-Management über mehrere Anwendungsfälle hinweg, einschließlich von Schlüsseln, Identitäten und Zertifikaten, zu vereinheitlichen. Mehrere Teams können Zertifikate für verschiedene Zwecke erwerben. Auch wenn ein gutes Verständnis der Compliance für das Unternehmen Konsistenz bietet, kann jede Komponente des „Trusts“ einen anderen Lebenszyklus haben. TLS-Zertifikate sind beispielsweise bis zu 398 Tage gültig. Einige Programme verlangen hingegen eine dreijährige Schlüsselrotation. Jede Trust-Komponente muss verwaltet werden, um Verstöße gegen Compliance-Anforderungen zu vermeiden und die Sicherheit zu optimieren. Versäumnisse im Trust-Management können Aus- oder Zwischenfälle hervorrufen. Während ein einzelner Ausfall aufgrund eines abgelaufenen Zertifikats schlimm ist, kann der Ausfall eines wichtigen Systems einen Dominoeffekt auf andere Systeme auslösen. Damit kann es wiederum zu weitreichenden Problemen in anderen Bereichen des Unternehmens kommen, die auf dieses System angewiesen sind.

Eine der größten Herausforderungen beim Management digitaler Zertifikate ist die Sichtbarkeit. Wenn mehrere Abteilungen Zertifikate (öffentliche und private) erwerben, müssen Unternehmen bis zu Zehntausende von Zertifikaten verwalten. Laufen diese nicht über ein zentrales Verwaltungssystem, ist es fast unmöglich zu wissen, welche Systemzertifikate erneuert werden müssen oder ob sie die zuvor beschriebenen Compliance-Standards erfüllen. Außerdem ist die enorme Anzahl der im Umlauf befindlichen Zertifikate sehr schwer zu managen, sodass die Problemlösung der Sichtbarkeit eine Grundlage – oder zumindest eine Rechtfertigung – für die Automatisierung des Prozesses bieten kann.

Für Unternehmen, die Digital Trust nachweisen wollen, ist eine zentrale Zertifikatsverwaltung unerlässlich. Wie ein großer Technologieanbieter sagte: *„Wir benötigten eine Möglichkeit, alle Zertifikate des gesamten Unternehmens zu zentralisieren – nicht nur zur Erkennung vom bevorstehenden Ablauf, sondern auch zur Automatisierung des Erneuerungsprozesses. Beides hilft uns dabei, das Risiko eines für das Unternehmen katastrophalen Serviceausfalls zu verringern.“*

Connected Trust

Die letzte Komponente, welche Unternehmen für den Aufbau eines Digital-Trust-Netzes benötigen, ist die Ausweitung dieser Sicherheitsverantwortung und des -nachweises auf die wachsende Zahl von vernetzten Geräten, die den Markennamen und die Software des Unternehmens tragen, aber außerhalb seiner Kontrolle agieren. Dazu gehören Geräte wie die Hausautomatisierung und tragbare Geräte zur Gesundheitsüberwachung.

Bei dieser Geräteart stellen sich eine Reihe verschiedener operativer Herausforderungen. Wie bei den bereits erwähnten Komponenten kann es überwältigend sein, mit der erforderlichen Zertifikatanzahl für ein optimal funktionierendes IoT-Gerät (Internet of Things) Schritt zu halten. Jedes Gerät selbst kann unterschiedliche Zertifikate haben. Außerdem verfügen die Webanwendungen, Cloud-Dienste sowie Gateways, die eine Verbindung zum Gerät herstellen, über Zertifikate. Zur Gewährleistung der Gerätesicherheit sowie des Schutzes der übertragenen Daten, müssen alle Verbindungen ordnungsgemäß authentifiziert werden, auf die das Gerät angewiesen ist. Und zu guter Letzt muss das Gerät schnell und ohne Ausfallzeiten aktualisiert werden können. Eine sichere Kommunikation zwischen dem Gerät und dem Unternehmen ist hierfür unerlässlich.

Die Authentizitäts- und Sicherheitsgewährleistung sowie die Wahrung der Integrität des Codes werden nochmals deutlich wichtiger, wenn man diesen besonderen Gerätezweck bedenkt. Fehler in einem der oben genannten Bereiche können zu einem Serviceausfall führen. Dies wiederum würde nicht nur die Marke in ein negatives Licht rücken, sondern könnte auch zu rechtlichen Schritten führen.

Jeder dieser Bereiche ist ein wesentlicher Bestandteil des Digital-Trust-Netzes. Weisen Unternehmen in einem oder mehreren dieser Bereiche Defizite auf, ist Digital Trust unvollständig.

Die Vorteile einer strategischen Initiative für Digital Trust

In den letzten zehn Jahren hat sich die Sichtweise auf die Cybersicherheit von einer utilitaristischen zu einer strategischen Sichtweise gewandelt. Wahrscheinlich ist dies auf die öffentlichkeitswirksamen Ransomware-Angriffe und Datenschutzverletzungen zurückzuführen. Datenschutz- und Compliance-Vorschriften haben ebenfalls zu diesem Wandel beigetragen. Sie trugen außerdem dazu bei, die Aktivitäten der Sicherheitsteams in den Mittelpunkt zu rücken. Daher wurden Verschlüsselung, Schlüssel-Management und Zertifikate – wesentliche Grundelemente des Digital Trust – weitgehend einem kleinen Team innerhalb der IT-Abteilung überlassen.

Jahrelang hielten PKI-Administratoren und Kryptographie-Betriebsteams im Stillen unsere digitale Welt zusammen. Ihre Arbeit sowie ihre Erfolge werden oft nicht erkannt und/oder als Sicherheitsfunktion abgetan. Dies kann – und sollte – sich ändern, da die Sicherheit immer mehr in den Zuständigkeitsbereich der Exekutiv-Ebene rückt.

Die erfolgreiche Umsetzung von Digital Trust sollte nicht nur bei dieser kleinen Gruppe von IT-Administratoren liegen. Wie jede Cybersicherheitsinitiative liegt auch das Digital Trust in der Verantwortung des gesamten Unternehmens. Beim Einbeziehen des Digital Trust in die Neuausrichtung der gewünschten Geschäftsergebnisse können Unternehmen das gesamte Business zusammenbringen, um die folgenden Vorteile zu erzielen:

- **Verbesserte Kundenzufriedenheit und -bindung:** Laut der IDC-Studie *„Future Enterprise Resiliency and Spending Survey“* vom Juni 2022 stehen Kundenzufriedenheit und betriebliche Effizienz weltweit ganz oben auf der Liste geschäftlicher Prioritäten. Das bedeutet, den Kunden ein ideales Erlebnis zu bieten. Die von ihnen benötigten Geräte, Anwendungen und Dienste sollen verfügbar sein und optimal funktionieren.
- **Bessere operative Effizienz:** Die Bemühungen um Digital Trust können in Unternehmen zu mehr Effizienz führen. Das Zentralisieren des Zertifikatsmanagements bietet eine Grundlage für die Automatisierung sowie eine bessere Übersicht über die Zertifikatslandschaft. Beide Tätigkeiten tragen wesentlich zur Vernetzung und zum effizienten Betrieb der Geschäftssysteme bei.
- **Stärkere allgemeine Sicherheit:** Die Umsetzung der einzelnen Digital-Trust-Komponenten bedeutet, dass überall dort, wo sie benötigt werden, einheitliche Sicherheitskontrollen integriert werden müssen: bei den zur Kommunikation für die Zusammenarbeit der Mitarbeiter verwendeten Tools, bei den Servern, die kundenbezogene Informationen verarbeiten, sowie weltweit bei den IoT-Geräten.

DigiCert für Initiativen von Digital Trust in Betracht ziehen

Unternehmen werden bei der Bewältigung einzelner Komponenten dieses Digital-Trust-Netzes durch eine Vielzahl von Anbietern und Beratern unterstützt. Dabei ist die Wahl des richtigen Partners unabdingbar.

DigiCert wurde 2003 gegründet und stellt als globaler Digital-Trust-Anbieter umfassende Lösungen zur Verfügung, die es Unternehmen und Verbrauchern ermöglichen, sich auf die Sicherheit ihrer digitalen Daten zu verlassen. Mit seinen Grundpfeilern Identität, Authentifizierung, Verschlüsselung und Integrität bietet DigiCert die nötigen Komponenten für Digital Trust: Richtlinien, Compliance und Operations, Trust-Management und erweitertes Vertrauen in digitale Ökosysteme. Als Branchenführer trägt DigiCert zur Entwicklung globaler Standards für Digital Trust bei und ist unter anderem führend im CA/Browser Forum, bei Matter, SAE, IETF und NIST. DigiCert unterstützt eine Vielzahl von Branchen und hilft bei der Ausarbeitung und Umsetzung von Digital-Trust-Richtlinien im Rahmen der Zusammenarbeit zwischen mehreren Anbietern. Zur Gewährleistung von Compliance, Betriebszeit und Zuverlässigkeit verfügt das Unternehmen über 20 Niederlassungen weltweit und setzt global verteilte Rechenzentren ein.

Die DigiCert ONE Plattform bietet ein einheitliches Trust-Management, um regionalen und lokalen Anforderungen gerecht zu werden. DigiCert ONE und seine Manager-Module unterstützen Unternehmen bei der Vereinheitlichung des Trust-Managements für die Zertifikatslandschaft und bieten umfassende Berichtsfunktionen, Erkennung und Automatisierung sowie tiefgreifende Integrationen mit Partner-Tools. DigiCert ONE dehnt Trust auch auf Software-Lieferketten, vernetzte Geräte-Ökosysteme sowie Dokumente und elektronische Signaturen aus und ist als On-Premise-, Cloud-, DigiCert-hosted- oder Hybrid-Bereitstellungsmodell verfügbar. Mit der kürzlichen Übernahme von Mocana hat DigiCert den gesamten Lebenszyklus von Geräten von der Herstellung über die Produktion bis hin zur Verwendung gesichert.

Herausforderungen und Chancen

Geschäftsergebnisse und -prioritäten auf der Grundlage traditionell „technischer“ Konzepte wie PKI neu zu definieren, wird eine Herausforderung darstellen. Für viele Unternehmensleiter sind PKI und die anderen Elemente des Digital Trust einfach ein Teil der Kosten bzw. des Prozesses für die Geschäftstätigkeit im Internet. PKI wird fast wie ein Dienstprogramm – und zwar ein sehr technisches – betrachtet. Sie müssen oder wollen es nicht verstehen, denn der vorherrschende Gedanke ist: *Warum sollten wir etwas ändern, wenn es doch gut zu funktionieren scheint?*

Für Sicherheitsteams und PKI-Administratoren ist dies die Gelegenheit, den Wert von PKI zu vermitteln und ein Digital-Trust-Netz aufzubauen. Damit lassen nicht sich nur die Risiken im Zusammenhang mit Fehltritten im Netzwerk reduzieren, auch können Prozesse insgesamt effizienter gestaltet werden.

Schlussfolgerung

Digital Trust ist mehr als nur der Einsatz bestimmter Technologien. Für eine vorbildliche Umsetzung von Digital Trust müssen Unternehmen die Struktur, die Prozesse und die entsprechenden Aktivitäten verstehen und aktiv bereitstellen. Dazu gehören das Schritthalten mit den Änderungen der Industriestandards, die Gewährleistung der Einhaltung der regulatorischen Anforderungen in jedem Land, das Management des Lebenszyklus digitaler Vertrauenstechnologien sowie die Ausweitung des Vertrauens in digitale Ökosysteme. Unabhängig von ihrer Größe ist dies für viele Unternehmen ein bedeutendes Unterfangen, welches qualifizierte Mitarbeiter, viel Zeit und Budget erfordert. Unternehmen, die sich dem Digital Trust verschrieben haben, sollten prüfen, ob sie jede der zuvor beschriebenen Komponenten implementieren und managen können. Gegebenenfalls sollten sie einen Partner suchen, der sie bei der Verwaltung eines oder mehrerer dieser Prozesse unterstützt. Es verlangt einen Bewusstseinswandel, insbesondere in den Führungsetagen. Für Unternehmen, die ihre Bemühungen auf Digital Trust konzentrieren – und es zu einer strategischen Notwendigkeit für das Unternehmen machen – sind die Vorteile jedoch beachtlich. Sie schließen zuverlässige Betriebszeiten, ein geringeres Risiko der Datenkompromittierung und ein größeres Vertrauen der Benutzer ein.

Über die Analystin

Jennifer Glenn
Forschungsdirektorin, Security and Trust Group, IDC

Jennifer Glenn ist Forschungsdirektorin bei der IDC Security and Trust Group. Zudem ist sie für den Bereich Informations- und Datensicherheit verantwortlich. Zu Jennifers Kernkompetenzen gehört ein breites Spektrum an Technologien, darunter Messaging-Sicherheit, Management sensibler Daten, Verschlüsselung, Tokenisierung, Rechteverwaltung, Schlüssel-Management und Zertifikate. Im Rahmen dieser Untersuchung zeigt Jennifer die entscheidende Rolle der Datensicherheit bei wichtigen Unternehmensinitiativen wie der Schaffung von Kundenvertrauen und der digitalen Transformation auf.

Weitere Informationen über Jennifer Glenn

Nachricht vom Sponsor

DigiCert arbeitet weltweit mit führenden Unternehmen an Digital-Trust-Initiativen, welche reale Ergebnisse erzielen.

Wenn Sie erfahren möchten, wie DigiCert Ihre Ziele unterstützen kann, wenden Sie sich an sales@digicert.com.

IDC Custom Solutions

Diese Veröffentlichung wurde von IDC Custom Solutions erstellt. Als weltweit führender Anbieter von Marktinformationen, Beratungsdiensten und Veranstaltungen für die Märkte der Informationstechnologie, Telekommunikation und Unterhaltungselektronik unterstützt die Custom Solutions Group von IDC ihre Kunden bei der Planung, Vermarktung, dem Verkauf und dem Erfolg auf dem internationalen Markt. Wir erstellen umsetzbare Marktinformationen und einflussreiche Content-Marketing-Programme, die messbare Ergebnisse liefern.

IDC @idc @idc idc.com