DER STAND DES DIGITALEN VERTRAUENS — UMFRAGE-ERGEBNISSE 2024

DIGITAL TRUST. ECHT GEMACHT.

SPITZENREITER

SCHLUSSLICHTER

PKI

COMPLIANCE

AUSFÄLLE

XX
WARNMELDUNGEN

IoT

BEST PRACTICES

digicert®

DER STAND DES DIGITALEN VERTRAUENS – UMFRAGEERGEBNISSE 2024

DigiCert führt seit 2022 jährliche Umfragen zum Stand des digitalen Vertrauens durch. Die digitale Transformation zieht sich durch jede Branche und digitales Vertrauen ist von entscheidender Bedeutung – schließlich müssen wir wissen, dass alle Transaktionen sicher sind. Und dazu muss dafür gesorgt sein, dass nur vertrauenswürdige Personen und Geräte eine Verbindung zu unseren Systemen und Umgebungen herstellen können.

Wie Jennifer Glenn, Research Director bei IDC, erklärt, ist digitales Vertrauen die Grundlage für eine sichere vernetzte Welt und Unternehmen müssen gewährleisten können, dass ihre Kundschaft, Belegschaft und Partner auf die Sicherheit ihrer Online-Geschäftsprozesse und -Interaktionen vertrauen können.

Als einer der weltweit führenden Anbieter digitaler Vertrauenslösungen sorgt DigiCert dafür, dass Unternehmen und Einzelpersonen digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind. Vor diesem Hintergrund wollten wir wissen, wie globale Unternehmen digitales Vertrauen wahrnehmen und wie weit ihre Initiativen zur Schaffung, Verwaltung und Ausweitung des digitalen Vertrauens bereits vorangeschritten sind.

Digital Trust – damals und heute

Bereits in unserer ersten Umfrage stuften 100 % der Teilnehmer digitales Vertrauen als wichtig ein und fast alle Unternehmen (99 %) hielten es für möglich, dass ihre KundInnen zum Wettbewerb abwandern würden, wenn sie das Vertrauen verlören. Dem stimmten die meisten VerbraucherInnen zu: Zwei Drittel (68 %) halten das digitale Vertrauen für einen wichtigen Faktor.

Unsere aktuelle Befragung zielte darauf ab, die Entwicklungen seit der ersten Umfrage genauer zu beleuchten. In diesem Bericht analysieren wir daher bestimmte Funktionen und Abläufe im Zusammenhang mit digitalem Vertrauen, um zu verstehen, inwieweit Unternehmen Digital-Trust-Initiativen bereits umgesetzt haben und diese weiter optimieren können.

Methodik

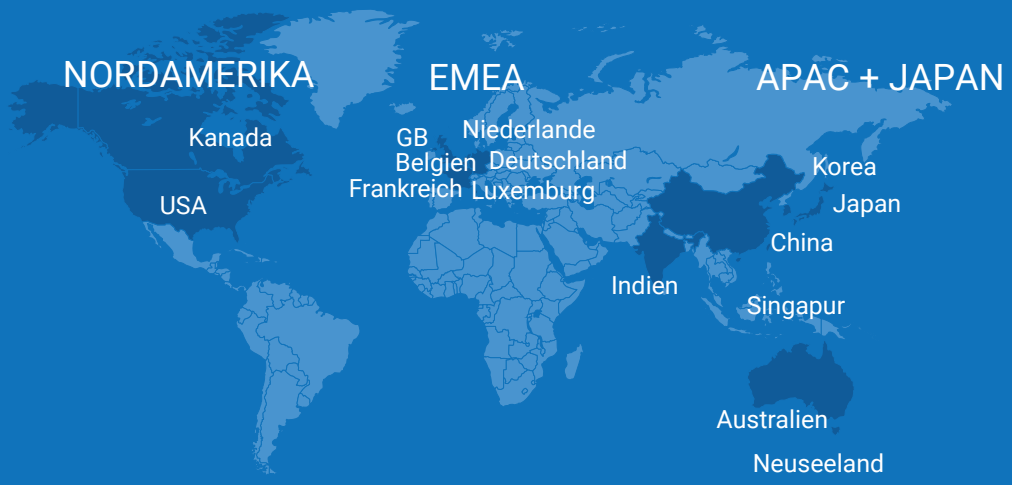
Im Rahmen der Umfrage zum Thema „Der Stand des digitalen Vertrauens 2024“ führte das in Dallas ansässige Marktforschungsunternehmen Eleven Research im letzten Quartal 2023 eine telefonische Befragung unter 300 Führungskräften in Unternehmen verschiedener Größen in den Regionen Nordamerika, EMEA und APJ durch.

Die Teilnehmer kamen aus verschiedenen Branchen wie Technologie, Fertigung und Finanzdienstleistungen und die Größe der befragten Unternehmen variierte zwischen 1.000 und mehr als 10.000 Mitarbeitenden.

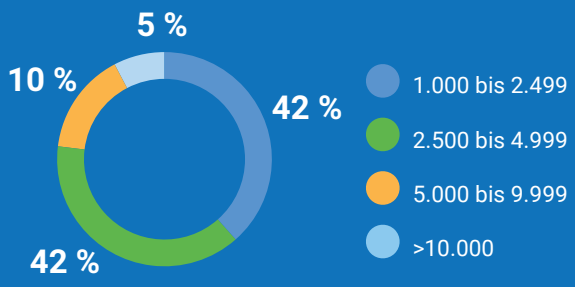
Um sich ein klares Bild von den Maßnahmen für das digitale Vertrauen zu verschaffen, konzentrierte sich Eleven Research auf Manager aus vier spezifischen Bereichen:

- Unternehmens-IT: Schutz der Kommunikation, Daten und des Zugriffs für Mitarbeitende, Anwendungen und Cloud-Umgebungen
- IoT und vernetzte Geräte: Schutz von Smart-Geräten und Anwendungen wie der Blutzuckerüberwachung
- Software: Schutz von Software und Anwendungen vor Manipulation und Lieferkettenangriffen
- E-Signaturen: Gewährleistung der Authentizität und Integrität von Dokumenten und Inhalten

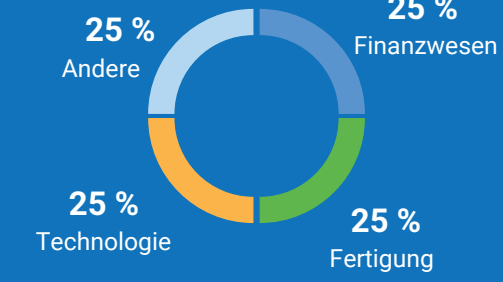
GEOGRAFISCHE AUFTEILUNG



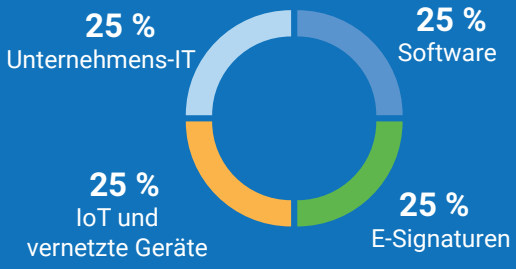
MITARBEITERZAHL



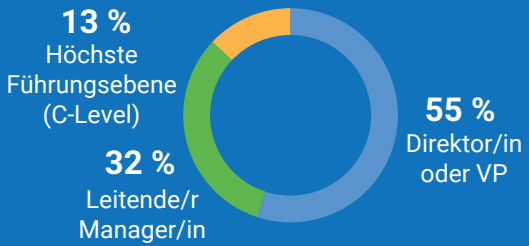
BRANCHE



VERANTWORTUNGSBEREICHE



POSITION



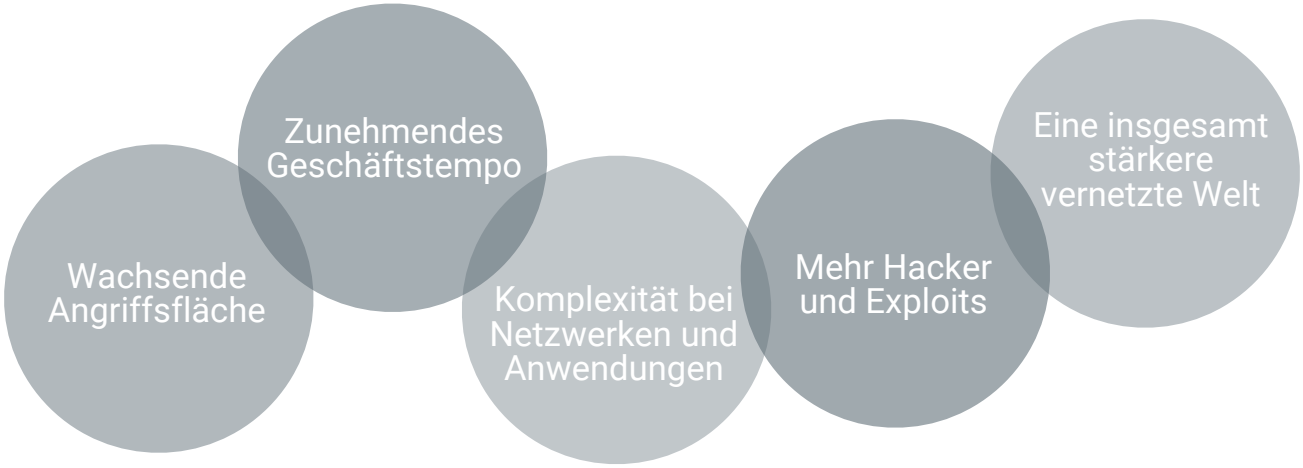
DAS DIGITALE VERTRAUEN STEHT WEITERHIN IM FOKUS

Die Umfrage des letzten Jahres zeigte, wie wichtig Unternehmen das digitale Vertrauen ist. Daher überrascht es nicht, dass dieses Thema nach wie vor einen extrem hohen Stellenwert bei den Geschäftsprioritäten einnimmt. Dafür gibt es drei konkrete Gründe:

- Die Anzahl der remote arbeitenden Beschäftigten ist heute höher als je zuvor.
- Der Umfang der digitalen Vernetzung ist gestiegen (zum Beispiel bei Edge-Netzwerken und in Bezug auf die Anbindung von Partnern und Kunden).
- Kunden fordern von Unternehmen, dass Digital-Trust-Prozesse umgesetzt werden.

DIE DREI WICHTIGSTEN FAKTOREN

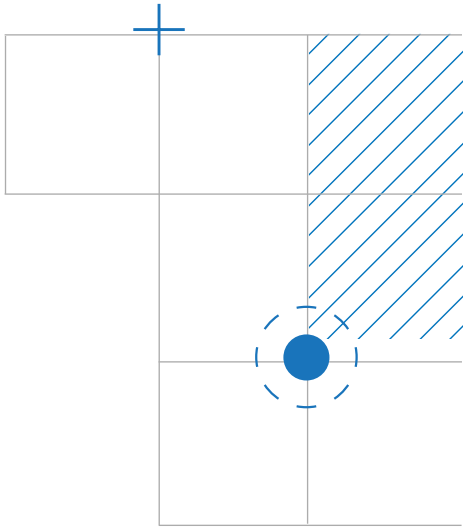
WEITERE FAKTOREN



Allerdings fällt es Unternehmen schwer, digitales Vertrauen aufzubauen, zu überwachen und zu verwalten, vor allem aufgrund der folgenden fünf Faktoren:

- **Unzureichender Wissensstand der Belegschaft:** Digital Trust ist ein relativ neues Konzept und nicht alle Mitarbeitenden besitzen die nötige Erfahrung bei der zentralisierten Umsetzung. Hinzu kommt, dass viele private PKIs bereits seit zehn Jahren bestehen, keine ausreichende Zuverlässigkeit bieten und ausfallanfällig sind. Das erschwert den Teams, in diesem Bereich die nötige Expertise aufzubauen.
- **Die zunehmende Komplexität von Netzwerken und Anwendungen:** Unternehmenstechnologie ist komplexer geworden. Im Netzwerkbereich sind Unternehmen über die herkömmlichen Rechenzentrums-, Zweigstellen- und Cloud-Umgebungen hinausgewachsen. Eine moderne Infrastruktur umfasst Edge-Netzwerke und Multi-Cloud-Architekturen und muss oft Tausende von mobilen Mitarbeitenden unterstützen.

  Anwendungen haben sich von monolithischen Strukturen zu stark verteilten Microservices-Architekturen entwickelt und ein Großteil der Services befindet sich nicht mehr unter der direkten Kontrolle des Unternehmens. In einer derart komplexen Landschaft digitales Vertrauen umzusetzen, ist außerordentlich schwierig.
- **Der schiere Umfang an Elementen, die Unternehmen schützen müssen:** Je weiter die digitale Transformation voranschreitet, desto mehr geschäftskritische digitale Assets gibt es. Damit wächst der Umfang dessen, was Sicherheitsteams schützen müssen, exponentiell an.
- **Fehlende Unterstützung durch die Führungsebene:** Faktoren wie die COVID-19-Pandemie und Inflation haben Führungskräfte dazu gezwungen, harte Entscheidungen zu treffen. Allein im Jahr 2023 mussten beispielsweise mehr als 240.000 Arbeitskräfte im Technologiesektor entlassen werden.[1] Unter solch schwierigen Bedingungen ist es nicht verwunderlich, dass dem Bereich Digital Trust auf der Chefetage mitunter nicht der verdiente Stellenwert zuteil kommt.
- **Die mühselige und zeitaufwendige Verwaltung der zunehmenden Anzahl kryptografischer Ressourcen:** Sowohl öffentliche als auch private Vertrauensdienste sind bei der Schaffung digitalen Vertrauens auf digitale Zertifikate angewiesen. Doch bei der Menge von digitalen Zertifikaten, die Unternehmen heute nutzen, gestaltet sich die Verwaltung als problematisch.



[1] Tech Crunch

FORTSCHRITTSAUFNAHME

Wie gut kommen Unternehmen bei der Umsetzung von Digital-Trust-Initiativen voran? Das lässt sich nicht so einfach beantworten, denn die Details sind komplex und nuanciert. Doch die kurze Antwort lautet: „Im Prinzip gut, aber noch lange nicht hervorragend."

Der Erfolg von Digital-Trust-Maßnahmen hängt davon ab, in welchem Bereich der Schwerpunkt liegt. Wir haben vier konkrete Bereiche untersucht, um zu erfahren, wie weit die Entwicklung in Unternehmen fortgeschritten ist:

- Unternehmens-IT
- IoT und vernetzte Geräte
- Software
- E-Signaturen
- E-Mail-Sicherheit
- Endpunktsicherheit

Digitales Vertrauen in der Praxis: Unternehmens-IT

Die Digital-Trust-Initiativen im Bereich der Unternehmens-IT liegen auch meist im Verantwortungsbereich der IT-Abteilung und umfassen in erster Linie:

- Zertifikatsverwaltung
- Identitäts- und Zugriffsmanagement

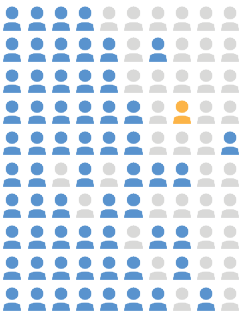
Selbst im Bereich der Unternehmens-IT, von dem man annehmen müsste, dass hier die größten Fortschritte verzeichnet werden, befinden sich die meisten Unternehmen in Bezug auf das digitale Vertrauen noch im Anfangsstadium. Nur sehr wenige (1 von 100) der Manager in diesem Bereich bezeichnen ihre digitalen Vertrauensmaßnahmen als „sehr ausgereift". 87 % der Befragten teilen außerdem mit, dass ihre Bemühungen isoliert sind.

Digitale Zertifikate ermöglichen die Authentifizierung und den Schutz der Kommunikation unter den Unternehmensnutzern und den von ihnen verwendeten Geräten wie Webservern und Smartphones. Die wachsende Größe und Komplexität der Unternehmensnetzwerke und Anwendungsbereiche machen eine stetig zunehmende Anzahl von Zertifikaten erforderlich.

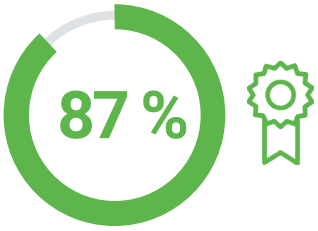
In etwa der Hälfte (52 %) der befragten Unternehmen werden Zertifikate von der IT-Abteilung verwaltet, bei einem Drittel (37 %) werden sie von anderen Teams und bei jedem neunten Unternehmen (11 %) gar nicht verwaltet.

In den meisten Unternehmen werden Zertifikate von höchstens fünf Abteilungen ausgestellt, doch die Mehrheit der Umfrageteilnehmer war der Ansicht, dass mehr Abteilungen dafür verantwortlich sein sollten.

Nur **1 von 100** Managern bezeichnet die internen Digital-Trust-Maßnahmen als „sehr ausgereift".



Die meisten empfinden sie als „einigermaßen ausgereift".

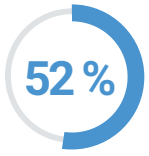


der Befragten bezeichnen ihre Bemühungen als isoliert.

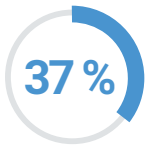
In den meisten Unternehmen werden Zertifikate von höchstens fünf Abteilungen ausgestellt.

Die Mehrheit findet, dass mehr Abteilungen Zertifikate ausstellen sollten.

Verantwortlich für die Zertifikatsverwaltung



IT



Andere Teams als die IT-Abteilung

Zertifikate werden nicht verwaltet

Die Ergebnisse: Unternehmens-IT

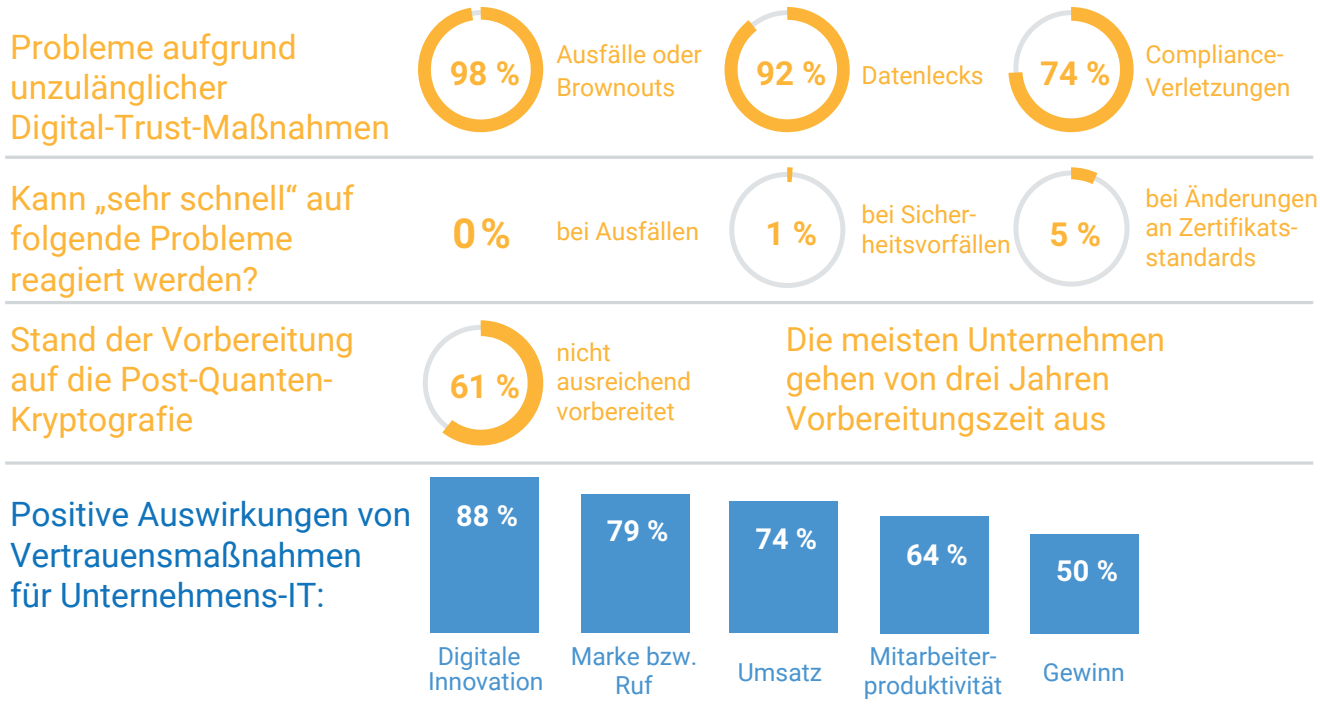
Wie erfolgreich wurden Digital-Trust-Initiativen bereits umgesetzt? Unsere Umfrage zeigt, dass hier noch starkes Verbesserungspotenzial besteht. Die Teilnehmer nennen zum Beispiel folgende Probleme im Zusammenhang mit unzulänglichen Digital-Trust-Maßnahmen:

- **Fast alle Teilnehmer (98 %)** haben mindestens gelegentlich mit Ausfällen und Brownouts zu kämpfen.
- **Die meisten Unternehmen (92 %)** haben Datenlecks zu verzeichnen.
- **Relativ viele (74 %)** melden Compliance-Verletzungen.

Außerdem wollten wir mehr zur Reaktionsschnelligkeit der Unternehmen wissen:

- **Kein Unternehmen** kann extrem schnell auf Ausfälle reagieren.
- **Kaum ein Unternehmen (1 %)** kann extrem schnell auf Sicherheitsvorfälle reagieren.
- **Nur wenige (5 %)** können extrem schnell auf Änderungen bei Zertifikatsstandards reagieren.
- **Die meisten (61 %)** sind nur unzulänglich auf das Post-Quanten-Zeitalter vorbereitet und gehen in der Regel davon aus, dass sie erst in drei Jahren so weit sind.

Trotz dieser Rückschläge betonen die Führungskräfte, dass die Digital-Trust-Initiativen im Bereich der Unternehmens-IT ihre Organisation insgesamt in verschiedenen Bereichen, von der digitalen Innovation bis hin zur Gewinnerzielung, voranbringen.



Digitales Vertrauen in der Praxis: IoT- und vernetzte Geräte

Bei diesem Themenpunkt haben wir uns auf Unternehmen konzentriert, die IoT- oder vernetzte Geräte herstellen und an Endkunden verkaufen. Die Produktpalette reicht von Werksensoren über Sportuhren bis hin zu Thermostaten für Wohnbereiche. Unsere Umfrage richtete sich an Mitarbeitende in den folgenden Verantwortungsfeldern:

- Authentifizierungsmechanismen für IoT- bzw. vernetzte Geräte
- Verschlüsselung auf IoT- bzw. vernetzten Geräten
- Signieren von Software- oder Firmware-Updates für IoT- bzw. vernetzte Geräte
- Kryptografie für den Schutz von IoT- bzw. vernetzten Geräten

Auch die Führungskräfte, die für das digitale Vertrauen bei IoT- und vernetzten Geräten verantwortlich sind, vermitteln die Botschaft: „Im Prinzip gut, aber noch lange nicht hervorragend“. Nur eine von sieben Führungskräften bezeichnet die Digital-Trust-Maßnahmen in diesem Bereich als „sehr ausgereift“. Die meisten sprechen von „einigermaßen ausgereift“.

Überraschenderweise werden **in den meisten Unternehmen (87 %)** personenbezogene Daten von IoT- bzw. vernetzten Geräten über unverschlüsselte Kanäle übermittelt.

In einem **Großteil der Firmen (88 %)** gibt es die Position des Chief Product Security Officer. In allen Fällen werden digitale Zertifikate für die Identifizierung von Geräten im laufenden Betrieb genutzt und eine starke Nutzerauthentifizierung ist ebenfalls üblich.

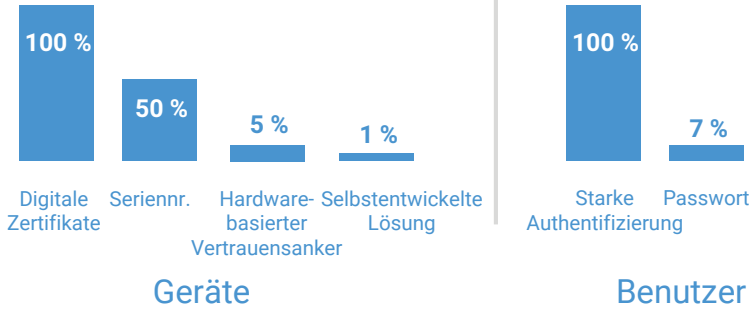
Nur **1 von 7** Managern bezeichnet die internen Digital-Trust-Maßnahmen als „sehr ausgereift“.

Die meisten empfinden sie als „einigermaßen ausgereift“.

übermitteln personenbezogene Daten von IoT- bzw. vernetzten Geräten über unverschlüsselte Kanäle.

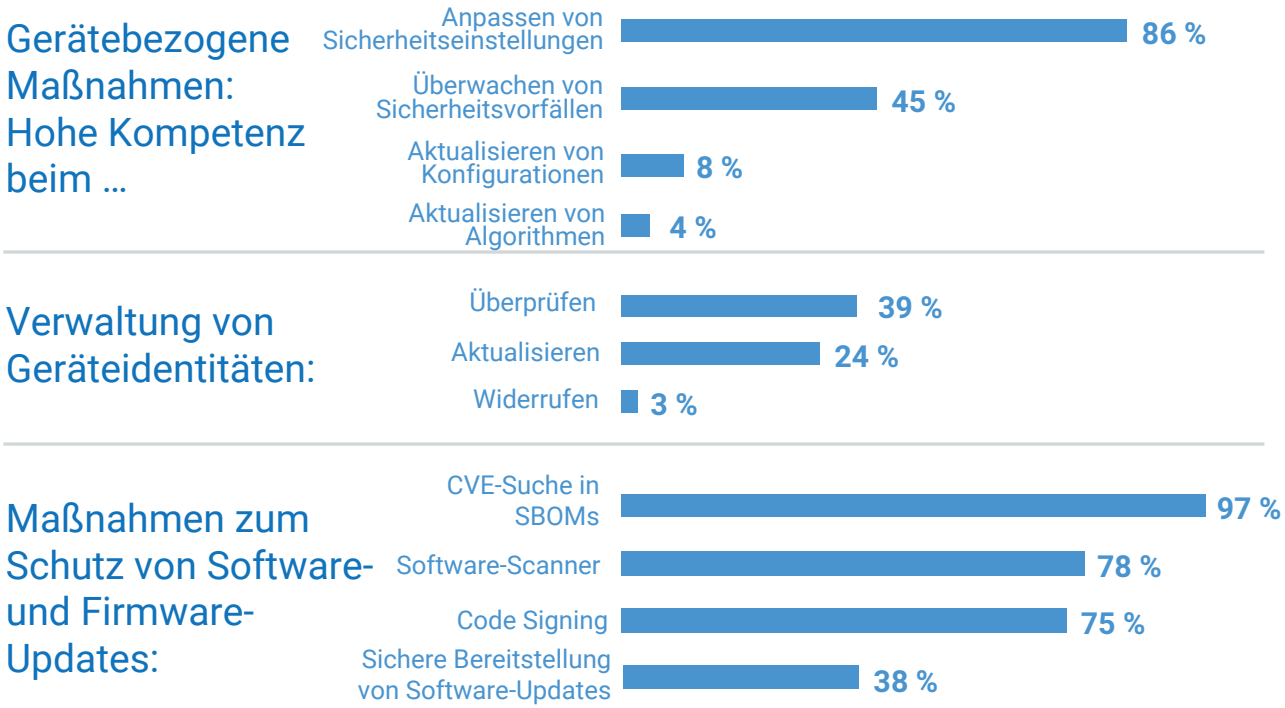
der Unternehmen lassen alle IoT- bzw. vernetzten Geräte vom Chief Product Security Officer oder einem zentralen Sicherheitsteam verwalten.

So werden aktive Geräte und Nutzer identifiziert:



Wir baten die Teilnehmer, ihr Unternehmen hinsichtlich verschiedener Aspekte in Bezug auf IoT- und vernetzte Geräte zu bewerten. Beim Gerätemanagement variieren die internen Leistungen stark: Die Verwaltung der Sicherheitseinstellungen wird sehr gut gemeistert, die Überwachung von sicherheitsrelevanten Ereignissen ist durchschnittlich, aber das Anwenden von Geräte-Updates lässt stark zu wünschen übrig.

Auch die Verwaltung von Geräte-Identitäten ist eher unzureichend, besonders das Widerrufen von Identitäten. Was allerdings positiv eingeschätzt wird, ist der Schutz von Software (obwohl die sichere Bereitstellung von Software-Updates noch verbesserungswürdig ist).



Die Ergebnisse: IoT- und vernetzte Geräte

Diese Stärken (und Schwächen) erklären, dass die befragten Hersteller von IoT- und vernetzten Geräten sich folgenden Herausforderungen gegenübersehen:

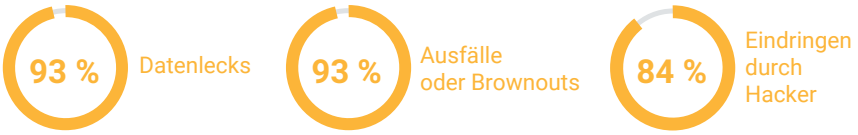
- **Die meisten Unternehmen (93 %)** hatten Datenlecks zu verzeichnen – oftmals, weil die von ihnen hergestellten Geräte leicht für den Zugang zum Netzwerk missbraucht werden konnten.
- **Die meisten Unternehmen (93 %)** erlitten sowohl Ausfälle als auch Brownouts.
- In Anlehnung an den ersten Punkt gaben **84 %** der befragten Unternehmen an, schon einmal Hackern zum Opfer gefallen zu sein.

Es gab aber auch positive Resultate aufgrund der Vertrauensmaßnahmen für IoT- und vernetzte Geräte:

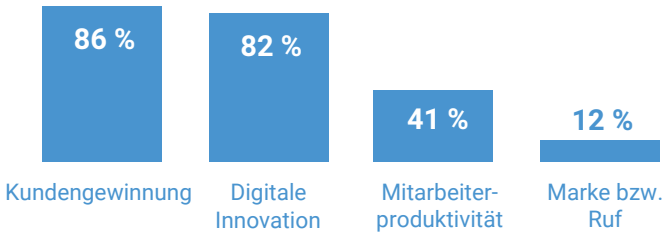
- **86 %** der Teilnehmer führen Erfolge bei der Kundengewinnung auf diese Maßnahmen zurück.
- **82 %** der Teilnehmer schreiben diesen Maßnahmen Fortschritte bei der digitalen Innovation zu.

Insgesamt wird deutlich, dass sich die Hersteller von IoT- und vernetzten Geräten stärker auf ihre Digital-Trust-Initiativen konzentrieren müssen.

Probleme aufgrund unzulänglicher Digital-Trust-Maßnahmen



Positive Auswirkungen von Vertrauensmaßnahmen für IoT- und vernetzte Geräte:



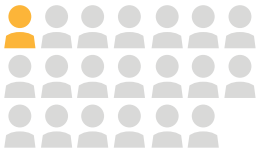
Digitales Vertrauen in der Praxis: Software

Mit Digital-Trust-Maßnahmen für Software wird dafür gesorgt, dass die an Kunden ausgelieferte Software vertrauenswürdig ist. Auch hier lautet das Fazit der Befragung: „Im Prinzip gut, aber noch lange nicht hervorragend“. Nur 1 von 20 Managern (5 %) bezeichnet die internen Digital-Trust-Maßnahmen für Software als „sehr ausgereift“. In welchen Bereichen Code Signing angewendet wird, unterscheidet sich von Unternehmen zu Unternehmen:

- **Fast alle Umfrageteilnehmer (99 %)** signieren Softwarequellcode.
- **84 %** signieren binäre Softwaredateien.
- **62 %** signieren Build-Skripte und Infrastrukturkonfigurationen.
- **33 %** signieren Container- und serverlose Umgebungen.
- **Die meisten Unternehmen (67 %)** speichern private Code-Signing-Schlüssel auf nach FIPS-140-2 zertifizierten Geräten.

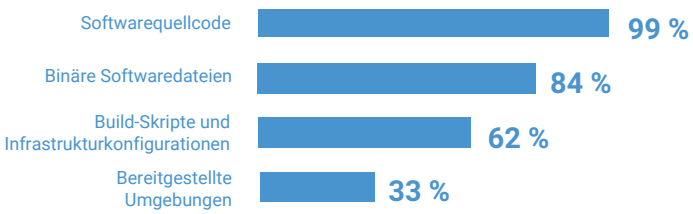
Keins der befragten Unternehmen wäre nach eigenen Angaben in der Lage, im Falle eines Sicherheitsvorfalls alle zu einem bestimmten privaten Code-Signing-Schlüssel gehörenden Anwendungen sehr schnell zu identifizieren.

Nur **1 von 20** Managern bezeichnet die internen Digital-Trust-Maßnahmen als „sehr ausgereift“.

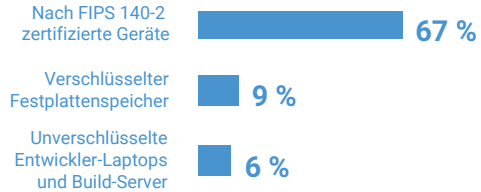


Die meisten empfinden sie als „einigermaßen ausgereift“.

Code Signing wird genutzt für:



Speicherorte für private Code-Signing-Schlüssel:



Würde ein privater Code-Signing-Schlüssel kompromittiert, könnte **KEINS** der befragten Unternehmen alle damit signierten Anwendungen schnell und einfach aufspüren.

Fast alle Umfrageteilnehmer erstellen regelmäßig eine SBOM für die hergestellte Software.

Fast alle Unternehmen haben risiko- und sicherheitsbezogene sowie rechtliche Anforderungen für Drittanbietersoftware.

Die Ergebnisse: Software

Wie steht es um die Compliance mit für Software relevanten gesetzlichen Vorschriften? Diese Frage beantwortete nur 1 von 8 der befragten Unternehmen mit „sehr gut“. Darüber hinaus wurde eine ganze Reihe von Problemen in Bezug auf Digital-Trust-Maßnahmen für Software gemeldet:

- **86 %** der Befragten erwähnten Datenlecks.
- **80 %** meldeten eine Kompromittierung der Build-Infrastruktur.
- **79 %** gaben an, dass Software aufgrund eines abgelaufenen Code-Signing-Zertifikats plötzlich nicht mehr funktionierte.
- **78 %** lieferten Software aus, die mit Malware infiziert war oder eine Sicherheitslücke enthielt.
- **75 %** konnten einen Veröffentlichungstermin nicht einhalten, weil ein Code-Signing-Problem oder Malware gefunden wurde.

Kunden müssen sich auf die Integrität von Unternehmenssoftware verlassen können, aber der für den Schutz sämtlicher Code-Signing-Schlüssel erforderliche Aufwand ist enorm.

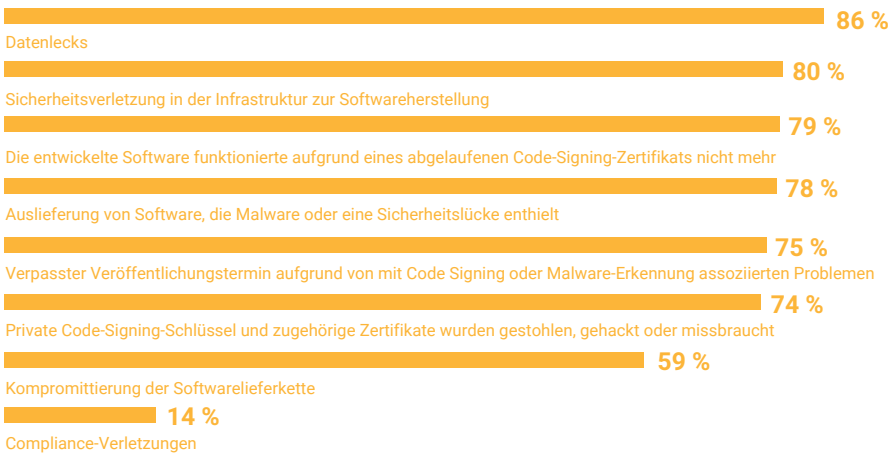
Nur wenige Hersteller gaben an, dass sie leicht eine Liste mit den Softwarekomponenten zusammenstellen können, die bei der Fertigung der Software genutzt werden.

Dennoch betonen die für Digital Trust bei der Softwareentwicklung zuständigen Führungskräfte, dass ihre Initiativen in zwei Bereichen für das Unternehmen insgesamt förderlich sind (digitale Innovation und Mitarbeiterproduktivität).

verzeichnen „sehr gute“ Ergebnisse bei der Compliance mit den für Software relevanten gesetzlichen Vorschriften.

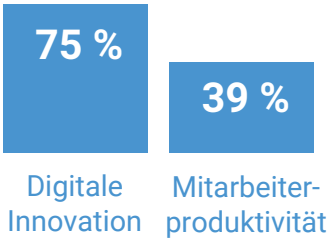
(also die meisten) schneiden in diesem Bereich „eher gut“ ab.

Probleme aufgrund unzulänglicher Digital-Trust-Maßnahmen



können „sehr leicht“ eine Liste mit den Softwarekomponenten und Konfigurationen zusammenstellen, die bei der Fertigung der Software genutzt werden

Positive Auswirkungen von Vertrauensmaß-nahmen für Software:



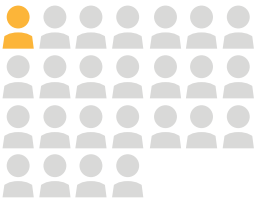
Digitales Vertrauen in der Praxis: E-Signaturen

Mithilfe von Document-Signing-Zertifikaten können Einzelpersonen, Teams und Abteilungen elektronische, digitale Signaturen zu Dokumenten in verschiedenen Dateiformaten hinzufügen, um ihre Identität zu bestätigen. Dadurch wird sichergestellt, dass Dokumente nicht geändert werden und sensible Informationen geschützt sind.

Wir baten die Umfrageteilnehmer, den Reifegrad ihrer Digital-Trust-Initiativen für E-Signaturen zu bewerten, und nur 1 von 25 Unternehmen (4 %) gab hier „sehr ausgereift“ an. Das ist die schwächste Bewertung bei den vier von uns untersuchten Bereichen. Es hat sich gezeigt, dass E-Signaturen in den meisten Fällen nicht von IT-Personal verwaltet werden, sondern von anderen Mitarbeitenden und Teams – zum Beispiel aus der Rechtsabteilung, dem Personalwesen oder dem Einkauf. Nur 1 von 8 dieser Mitarbeitenden besitzt ein gutes Verständnis der Unterschiede zwischen einfachen E-Signaturen und zertifikatsbasierten elektronischen Signaturen.

- **Knapp die Hälfte (48 %)** der befragten Unternehmen nutzt elektronische Siegel für Dokumente (z. B. zu Rechts-, Vertriebs- oder Beschaffungszwecken).
- **Die meisten (86 %)** nutzen digitale Signaturen mit Zertifikaten, die von vertrauenswürdigen Dritten ausgestellt werden, zur Identifizierung von Unterzeichnern.

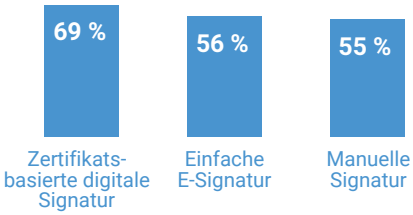
Nur **1 von 25** Umfrageteilnehmern bezeichnet die internen Digital-Trust-Maßnahmen als „sehr ausgereift“.



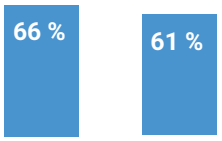
Die meisten empfinden sie als „einigermaßen ausgereift“.

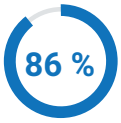
besitzen ein gutes Verständnis der Unterschiede zwischen einfachen E-Signaturen und zertifikatsbasierten digitalen Signaturen.

Art der verwendeten Signaturen:

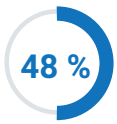


Art der verwendeten E-Signaturen:



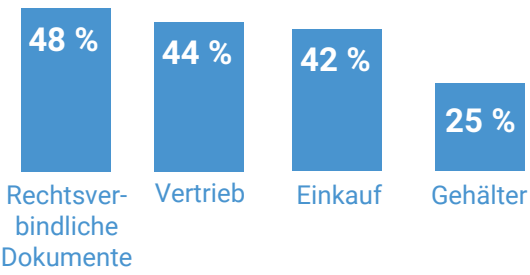


nutzen digitale Signaturen mit Zertifikaten, die von vertrauens-würdigen Dritten ausgestellt werden, zur Identifizierung von Unterzeichnern.



Die Hälfte der Befragten nutzt elektronische Siegel für Dokumente.

Die gängigsten Anwendungs-bereiche:



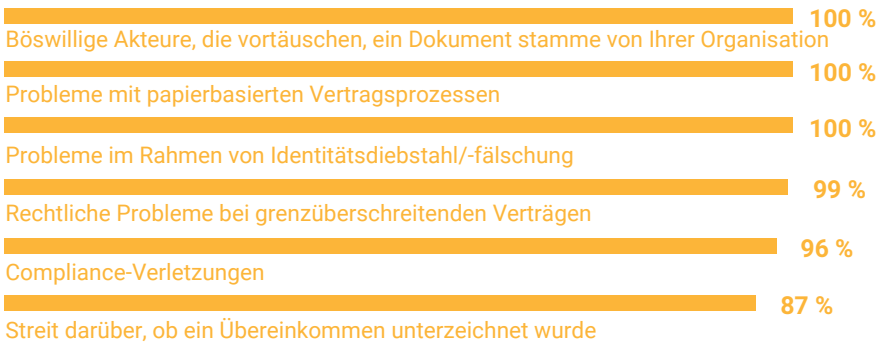
Die Ergebnisse: E-Signaturen

In dieser Gruppe finden sich die meisten Zwischenfälle aufgrund von Digital-Trust-Problemen:

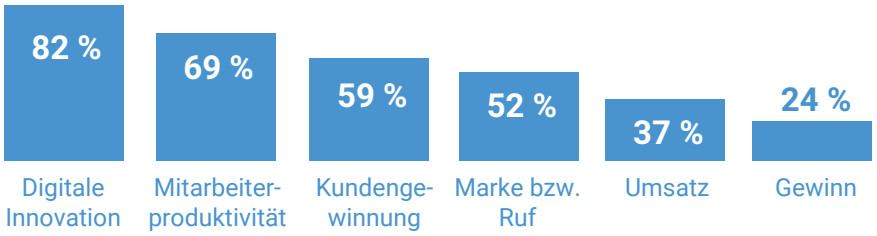
- **100 %** der Befragten meldeten, dass böswillige Akteure vorgetäuscht hätten, ein Dokument stamme von ihrer Organisation.
- **100 %** gaben Probleme mit papierbasierten Vertragsprozessen an.
- **100 %** nannten Probleme im Rahmen von Identitätsdiebstahl/-fälschung.
- Fast alle **(99 %)** Umfrageteilnehmer verzeichneten rechtliche Probleme bei grenzüberschreitenden Verträgen.
- **96 %** meldeten Compliance-Verletzungen.
- **87 %** hatten bereits Streit darüber, ob ein Übereinkommen unterzeichnet wurde.

Doch trotz dieser Herausforderungen waren sich die Befragten einig, dass ihre Initiativen positive Auswirkungen auf das Unternehmen insgesamt haben, unter anderem bei der digitalen Innovation, Produktivität und Kundengewinnung.

Probleme aufgrund unzulänglicher Digital-Trust-Maßnahmen



Positive Auswirkungen von Vertrauensmaßnahmen für E-Signaturen:



EINBLICKE VON KENNERN IN SACHEN DIGITALES VERTRAUEN

In den vorherigen Abschnitten haben wir die Ergebnisse in Bezug auf die Gesamtheit der befragten Unternehmen präsentiert. Dabei schnitten einige Unternehmen besser bzw. schlechter ab als der Durchschnitt.

Das wollten wir näher untersuchen und haben die Ergebnisse daher in Kategorien aufgeteilt und verglichen. Dazu haben wir jeder Frage, für die es eindeutige Ergebnisse gab, eine Punktezahl zugewiesen. Dabei handelte es sich um Fragen wie „Haben Sie schon einmal ein Datenleck erlitten?“ und „Wie schnell können Sie auf Sicherheitsverletzungen reagieren?“ Für ein positives Ergebnis gab es Pluspunkte, für ein negative Ergebnis Minuspunkte. Dann haben wir die Punktzahlen addiert und jedem teilnehmenden Unternehmen eine Gesamtpunktzahl zugewiesen.

Unternehmen mit einer Gesamtpunktzahl im oberen Drittel (unter den höchsten 33 Prozent) bezeichnen wir als „Spitzenreiter“. Die Unternehmen im unteren Drittel nennen wir „Schlusslichter“.

Im Folgenden sehen wir uns die Unterschiede zwischen den beiden Gruppen in Bezug auf die Maßnahmen und Ergebnisse für die vier Digital-Trust-Segmente an.

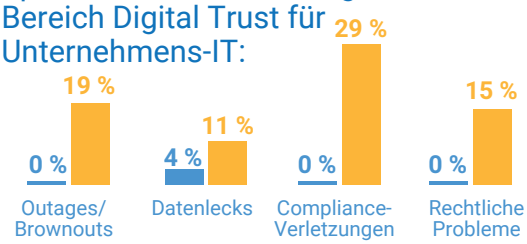
Digital Trust für Unternehmens-IT

In diesem Segment schneiden die Spitzenreiter im Vergleich wesentlich besser ab und haben sehr viel weniger Probleme in Bezug auf Digital-Trust-Initiativen in der Unternehmens-IT: Sie haben kaum mit Ausfällen, Datenlecks, Compliance-Verletzungen oder rechtlichen Problemen zu kämpfen.

Rund drei Viertel der Spitzenreiter (74 %) geben an, dass sie sehr schnell auf Ausfälle reagieren können (im Vergleich zu nur 59 % der Schlusslichter).

Die Spitzenreiter geben mit fast sechsmal höherer Wahrscheinlichkeit an, dass sie auf das Quantenzeitalter vorbereitet sind **(59 % im Vergleich zu 11 % bei den Schlusslichtern)**.

Spitzenreiter haben weniger Probleme im Bereich Digital Trust für Unternehmens-IT:



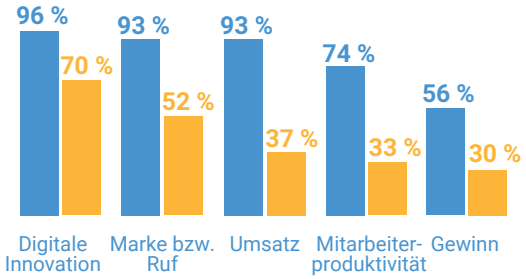
Schnellere Reaktion bei Ausfällen

Besser auf PQC vorbereitet

Beschleunigte PQC-Bereitschaft

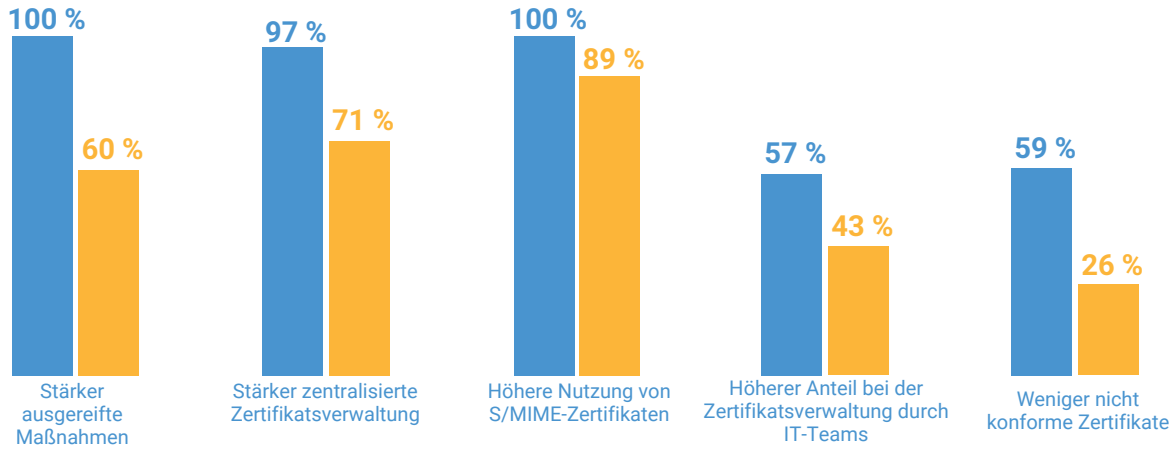
Zwei Jahre bei den Spitzenreitern, drei Jahre bei den Schlusslichtern

Klare Vorteile durch Digital-Trust-Maßnahmen für Unternehmens-IT bei den Spitzenreitern:



Was machen die Spitzenreiter anders?

100 % der Spitzenreiter bei Digital Trust für Unternehmens-IT bezeichnen die Initiativen in ihrem Unternehmen als „sehr ausgereift“. Sie setzen stärker auf Zentralisierung, nutzen S/MIME-Zertifikate für eine sichere E-Mail-Kommunikation und haben die Zertifikatsverwaltung der IT-Abteilung übertragen. Außerdem haben sie weniger nicht konforme Zertifikate.

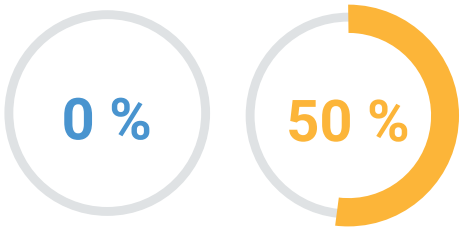


Digital Trust für IoT- und vernetzte Geräte

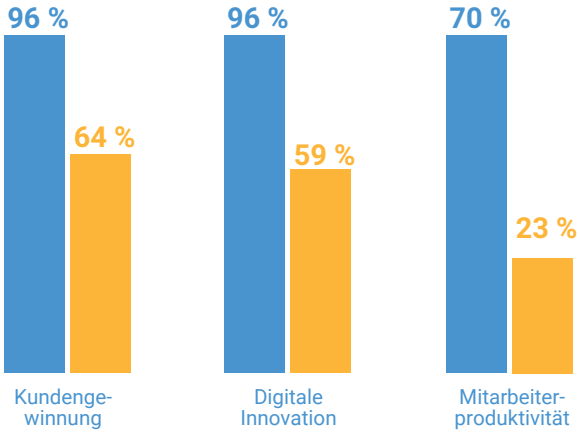
Als Nächstes haben wir uns die Antworten der Verantwortlichen im Bereich Digital Trust für IoT- und vernetzte Geräte angesehen. Auch hier waren die Spitzenreiter den Schlusslichtern wieder spürbar voraus. Die Spitzenreiter vermerkten keine Compliance-Probleme in ihrem Bereich, die Hälfte **(50 %)** der Schlusslichter hingegen schon.

Außerdem waren die Spitzenreiter der Ansicht, dass ihre Digital-Trust-Initiativen für IoT- und vernetzte Geräte einen wesentlichen Beitrag zum Unternehmenserfolg leisten: Fast alle Teilnehmer (96 %) hoben hier die Bereiche Kundengewinnung und digitale Innovation und die meisten (70 %) die Mitarbeiterproduktivität hervor. Dem gegenüber stehen jeweils 64 %, 59 % und 23 % für die Schlusslichter.

Weniger Compliance-Verletzungen



Klare Vorteile durch Digital-Trust-Maßnahmen für IoT-Geräte:

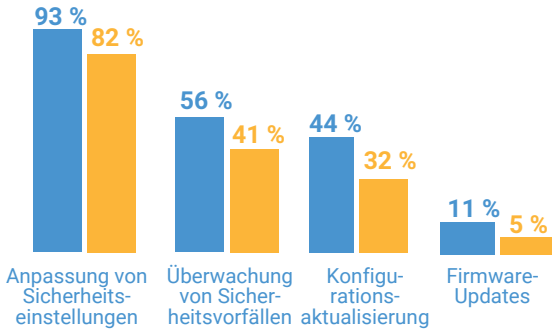


Wie wirken sich die Unterschiede in der Praxis aus?

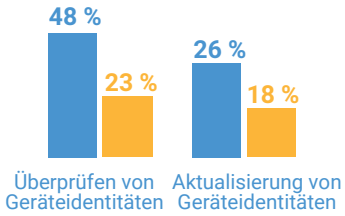
Den Spitzenreitern fällt es leichter, Geräte in Betriebsumgebungen zu überwachen und Änderungen daran vorzunehmen. Auch mit der Kontrolle und Aktualisierung von Geräteidentitäten haben sie weniger Probleme.

Ein weiterer Unterschied zeigt sich darin, wie gut die Unternehmen auf Probleme im Bereich Digital Trust für IoT-Geräte vorbereitet sind: KEIN Umfrageteilnehmer aus der Kategorie der Schlusslichter gab hier „sehr gut vorbereitet“ an (im Gegensatz zu 19 % bei den Spitzenreitern).

Bessere Fähigkeit zur Anpassung von Geräten im laufenden Betrieb:



Überlegenheit in den folgenden Bereichen:



Besser vorbereitet auf Digital-Trust-Probleme bei IoT-Geräten:

Digital Trust für Software

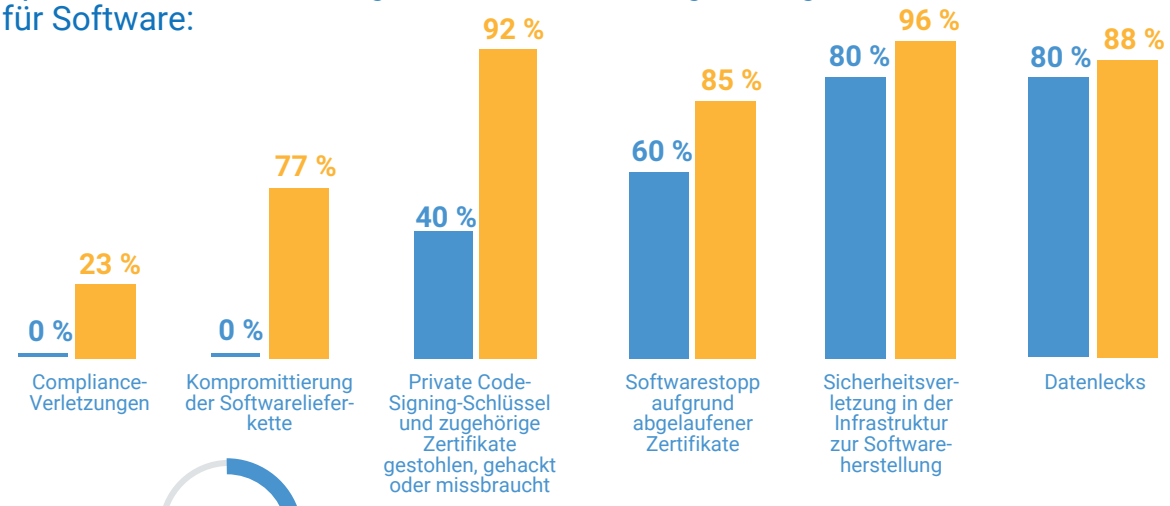
Auch in diesem Bereich kommen die Spitzenreiter besser zurecht als die Schlusslichter und melden wesentlich weniger Probleme. Beispielsweise führte kein Spitzenreiter Compliance-Verletzungen oder eine Kompromittierung der Softwarelieferkette an (im Vergleich zu 23 % bzw. 77 % bei den Schlusslichtern).

Jeder fünfte **(20 %)** Spitzenreiter stuft seine Digital-Trust-Maßnahmen für Software als „sehr ausgereift" ein, was KEINES der Schlusslichter von sich sagt.

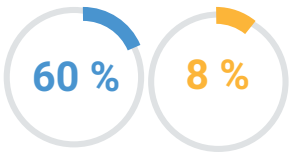
Auch bei der Einhaltung der für Software relevanten gesetzlichen Vorschriften liegen die Spitzenreiter vorn (60 % im Vergleich zu nur 8 % der Schlusslichter).

Darüber hinaus ist der Anteil der Unternehmen, die positive Auswirkungen ihrer softwarebezogenen Digital-Trust-Maßnahmen sehen (insbesondere in den Bereichen digitale Innovation, Kundengewinnung und Mitarbeiterproduktivität), bei den Spitzenreitern höher als bei den Schlusslichtern.

Spitzenreiter haben weniger Probleme in Bezug auf Digital-Trust-Maßnahmen für Software:

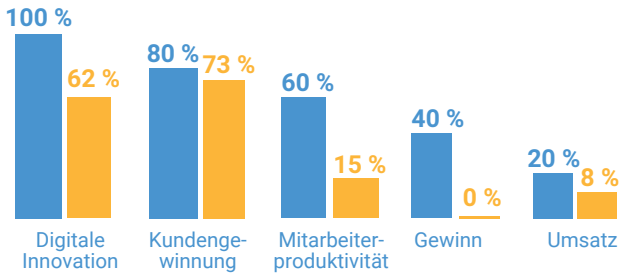


Spitzenreiter mit „sehr ausgereiften" Digital-Trust-Maßnahmen für Software (0 % bei den Schlusslichtern)



„Sehr gute" Compliance mit den gesetzlichen Vorschriften bei den Spitzenreitern

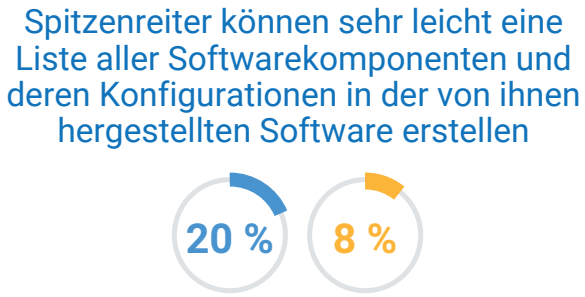
Klare Vorteile durch Digital-Trust-Maßnahmen für Software:



Wodurch zeichnen sich die Spitzenreiter aus?

Die Spitzenreiter nutzen mit doppelt so hoher Wahrscheinlichkeit formelle Genehmigungsprozesse für den Zugriff auf kryptografische Schlüssel (80 % im Vergleich zu 38 % bei den Schlusslichtern).

Außerdem finden mehr Spitzenreiter es „sehr einfach“, eine Liste aller Softwarekomponenten und deren Konfigurationen in der von ihnen hergestellten Software zu erstellen (20 % im Vergleich zu nur 8 % bei den Schlusslichtern).



Digital Trust für E-Signaturen

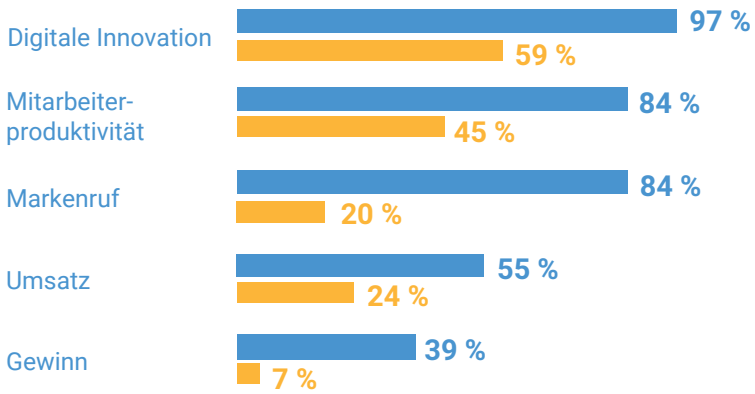
Zuletzt haben wir die Antworten der Verantwortlichen für elektronische Signaturen analysiert. Dabei handelt es sich vor allem um Manager aus dem Personalwesen, der Rechtsabteilung, dem Vertrieb und anderen nicht-technischen Bereichen. Da E-Signaturen meist nicht von IT-Fachkräften verwaltet werden, fehlt mitunter die erforderliche technische Expertise, und das zeigt sich bei den Ergebnissen.

So geben beispielsweise mehr Spitzenreiter als Schlusslichter an, „sehr ausgereifte" Digital-Trust-Prozesse für E-Signaturen zu nutzen, aber selbst da ist die Anzahl insgesamt sehr gering (10 %). Die Spitzenreiter sehen weniger Probleme in Bezug auf Digital Trust für E-Signaturen, dafür aber mehr Vorteile als die Schlusslichter.

der Spitzenreiter haben „sehr ausgereifte" Digital-Trust-Maßnahmen für E-Signaturen (0 % bei den Schlusslichtern)

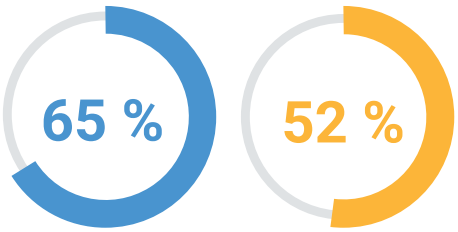
Weniger Digital-Trust-Probleme für E-Signaturen bei den Spitzenreitern:

Klare Vorteile durch der Digital-Trust-Maßnahmen für E-Signaturen:



Wodurch zeichnen sich die Spitzenreiter aus?

Die Unterschiede zwischen Spitzenreitern und Schlusslichtern lassen sich in erster Linie darauf zurückführen, dass die Spitzenreiter einen höheren Reifegrad in Bezug auf das Verständnis, die Implementierung und die Verwaltung von Richtlinien und Governance bei E-Signaturen und elektronischen Siegeln besitzen.



Spitzenreiter haben einen höheren Reifegrad in Bezug auf das Verständnis, die Implementierung und die Verwaltung von Richtlinien und Governance bei E-Signaturen und elektronischen Siegeln.

DIE EINSCHÄTZUNG VON DIGICERT

Je umfassender die Bedrohungslandschaft wird, desto größer ist die Spannweite zwischen den Unternehmen, die Digital Trust erfolgreich umsetzen, und denjenigen, die noch sehr viel Arbeit vor sich haben. Unsere Ergebnisse lassen erkennen, dass sowohl die Spitzenreiter als auch die Schlusslichter in diesem Bereich bei der Selbsteinschätzung sehr realistisch sind. Doch unsere Umfrage zeigt auch, dass sich Führungskräfte im Mittelfeld häufig fälschlicherweise in Sicherheit wiegen – und somit vielleicht am meisten gefährdet sind. Wenn sich Nachlässigkeit einschleicht und sich die Kluft weiter vertieft, kann dies gravierende Folgen haben.

Mit welchen Maßnahmen können Unternehmen also das digitale Vertrauen insgesamt stärken und auf welche Bereiche – wie Unternehmens-IT, Software, Geräte und Dokumentation – sollten sie sich besonders konzentrieren?

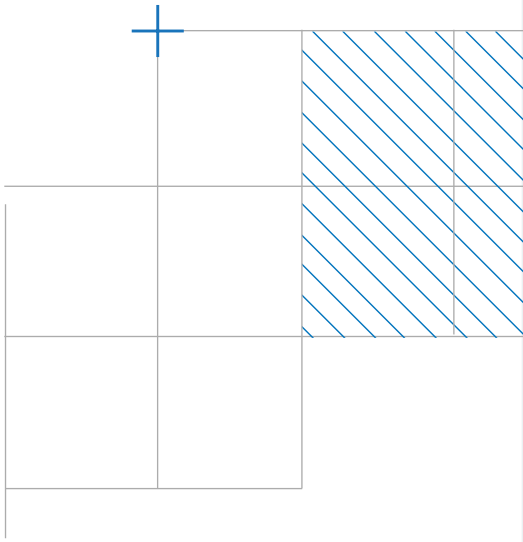
Als einer der weltweit führenden Anbieter digitaler Vertrauenslösungen sorgt DigiCert dafür, dass Unternehmen und Einzelpersonen digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur sicher und geschützt ist. DigiCert ist bereits seit über 20 Jahren im Bereich Digital Trust tätig und unsere Erfahrung zeigt, dass alle Unternehmen mit den folgenden Schritten ähnliche Erfolge wie die Spitzenreiter erzielen können:

Verwalten Sie Ihren Bestand.

Das Motto „Was man nicht sehen kann, kann man auch nicht verwalten“ trifft auch auf den Bereich Digital Trust zu. Verschaffen Sie sich einen ausführlichen Überblick darüber, wie kryptografische Schlüssel in Ihrem Unternehmen erstellt, geschützt und genutzt werden. Natürlich können Sie zu diesem Zweck Ihre Geschäftsprozesse manuell identifizieren und verwalten, aber es gibt auch Technologielösungen, die es Ihnen ermöglichen, Ihre Umgebung kontinuierlich im Blick zu behalten und Daten aus anderen Quellen, wie Systemen für das Management von IT-Ressourcen, zu nutzen.

Definieren Sie Richtlinien.

Es gibt eine ganze Reihe von Richtlinien zur Unterstützung von Digital Trust. Beispielsweise sollten Unternehmen Richtlinien für die Authentifizierung von Benutzern und Geräten einrichten – und zwar für die Belegschaft an Unternehmensstandorten genauso wie für mobile Mitarbeitende. Ermitteln Sie, welche Richtlinien für die Einhaltung rechtlicher Vorschriften erforderlich sind. Das gilt insbesondere für die Hersteller medizinischer Geräte und Unternehmen in anderen stark regulierten Branchen. Anbieter von geschäftskritischer Software müssen Richtlinien zum Schutz der Softwarelieferkette festlegen. Ein weiterer wichtiger Aspekt ist das Anstoßen oder Ausweiten von Zero-Trust-Initiativen. Das gilt vor allem für cloudnative Workloads, die für die Verarbeitung sensibler oder strengen Regeln unterworfener Daten genutzt werden. Und zu guter Letzt sind noch die allgemeinen unternehmensinternen Richtlinien für Kryptografie und PKIs zu beachten.



Zentralisieren Sie das PKI-Management.

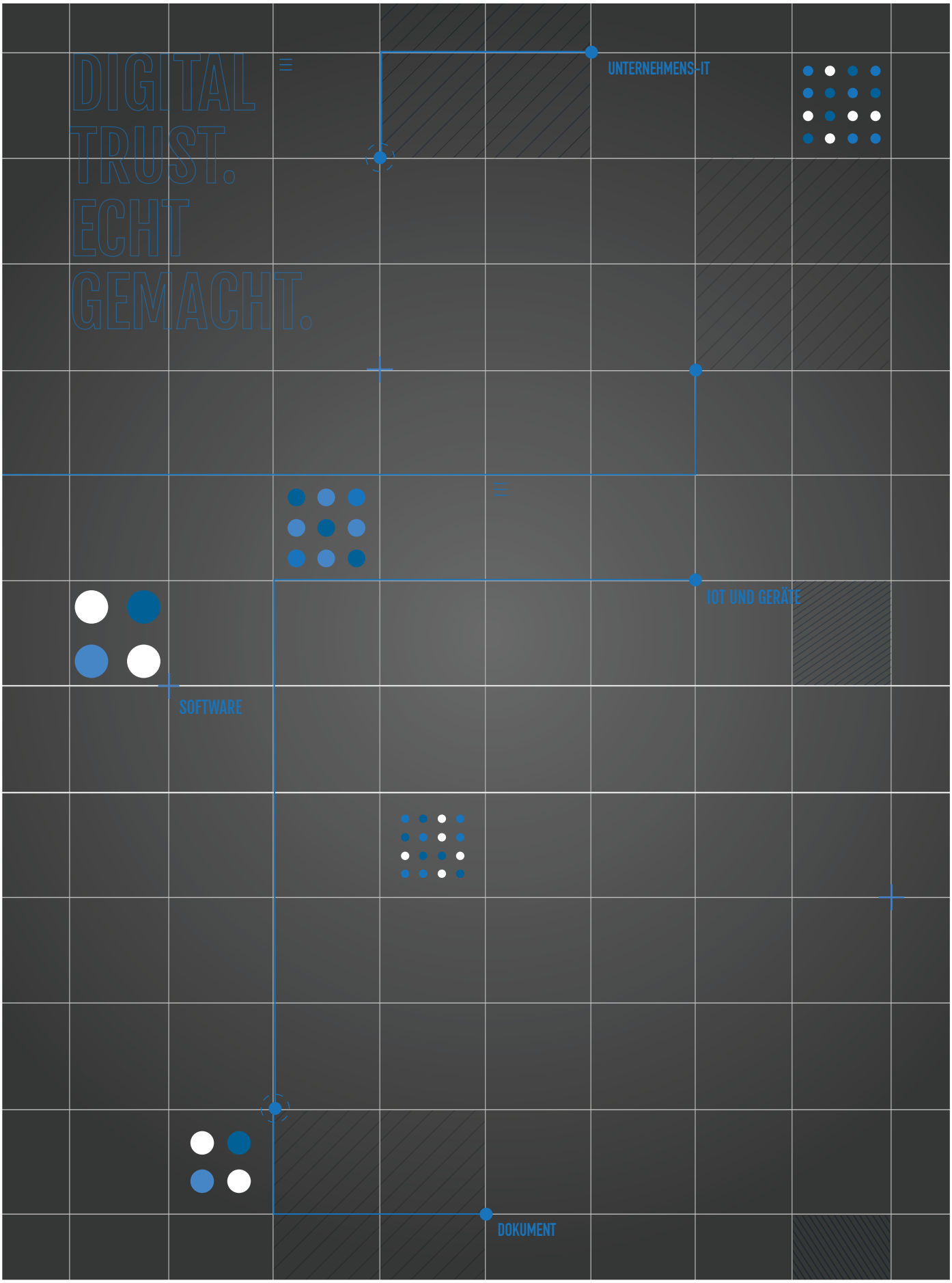
Unternehmen benötigen ein gewisses Maß an Krypto-Flexibilität, also die Fähigkeit, kryptografische Ressourcen schnell aktualisieren und anpassen zu können. Wenn Sie Ihr Unternehmen gegen zukünftige Störungen und die Risiken von morgen absichern möchten, sollten Sie Tools für die zentralisierte Verwaltung und Automatisierung Ihrer digitalen Zertifikate und PKIs einführen. Diese bieten zahlreiche Vorteile wie stärkere Sicherheit, mehr Effizienz und vereinfachte Verwaltungsprozesse.

Setzen Sie Prioritäten basierend auf den Auswirkungen auf das Unternehmen.

Überprüfen Sie Ihren Bestand, um Ressourcen im Zusammenhang mit geschäftskritischen Anwendungen und Prozessen zu identifizieren. Diese Bereiche verdienen als Erstes Ihre Aufmerksamkeit. Beheben Sie zunächst alle Sicherheitslücken und Schwachstellen und implementieren Sie anschließend Lösungen, die die Aufgaben zur Förderung des digitalen Vertrauens erleichtern. Ermöglichen Sie zum Beispiel Nutzern, ihre Geräte automatisch und ohne Eingriff des IT-Teams für den sicheren Remote-Zugriff zu konfigurieren. Unterstützen Sie die schnelle, sichere Ausstellung und Installation von Serverzertifikaten zum Schutz von Daten und Kommunikationsstrukturen, um die Cloud-Sicherheit insgesamt zu stärken.

Fazit

Unternehmen, die Digital-Trust-Initiativen Priorität einräumen, stärken ihre Marke, reduzieren die Cybersicherheitsrisiken und verbessern die betriebliche Effizienz. Durch robuste Sicherheitsmaßnahmen und transparente Governance-Praktiken sorgen sie bei Kunden, Partnern und Stakeholdern für Vertrauen. Durch den Aufbau des digitalen Vertrauens ermöglichen Sie den effektiven Umgang mit den Komplexitäten des regulatorischen Umfelds, stellen die Einhaltung von Vorschriften sicher und senken sowohl die rechtlichen als auch die finanziellen Risiken für Ihr Unternehmen. Ihre Vorteile? Umfassend abgesicherte Daten, bessere Resilienz und Schutz vor neuen Bedrohungen in der digitalen Welt von heute.


DIGITAL
TRUST.
ECHT
GEMACHT.
UNTERNEHMENS-IT
IOT UND GERÄTE
SOFTWARE
DOKUMENT