

# BEWÄLTIGUNG DER DIGITALEN HERAUSFORDERUNG

*Für ein sicheres, agiles und effizientes Unternehmen*

*„Vor drei Jahren erkannten wir, dass wir unsere Geschäftsabläufe transformieren müssen, um schneller auf Marktänderungen reagieren zu können, wenn wir auch in zehn Jahren noch erfolgreich sein wollen. Unsere Kunden waren online – und das mussten wir auch sein. Ich glaube, wenn wir das nicht getan hätten, wäre unser Unternehmen kein milliardenschwerer Konzern mehr, sondern ein ehemaliger großer Konzern, der gescheitert ist. Ich habe dem Aufsichtsrat damals gesagt, dass wir uns entweder auf die Cyber-Autobahn begeben müssen oder von der Konkurrenz überholt und abgehängt werden.“*

CEO, International Retail Conglomerate, Februar 2018

## EINLEITUNG

Wollen Sie, dass Ihr Unternehmen auch noch in drei Jahren erfolgreich ist? Das mag nach einer banalen Frage klingen, ist aber die zentrale Frage für alle heutigen Unternehmen. Die geschäftliche Transformation hin zu Teilnehmern auf dem digitalen Markt geschieht jetzt und ist eine Art Rennen. Unternehmen, welche die Grundlagen dieser neuen Welt akzeptieren, können die Chancen nutzen, während der Rest zurückbleibt. Vor allem müssen Unternehmen und ihre Kunden *sicher* bei ihren Aktivitäten sein und sich auf den Schutz ihrer Daten verlassen können.

In einem Umfeld, in dem Kundeninteraktionen langsam und kontrolliert verliefen, hatten Unternehmen den Luxus, Anwendungen und Serviceangebote jährlich oder halbjährlich aktualisieren zu können. Diese Zeiten sind allerdings vorbei! Die ständige Verfügbarkeit, die mit global verteilten und wachsenden Märkten verbunden ist, führt dazu, dass eine zunehmende Zahl von Kunden unterschiedliche und zum Teil widersprüchliche Anforderungen hat.

Alle Unternehmen bemühen sich darum, Kunden zu gewinnen, während die Wahrung der Loyalität ein bewegliches Ziel darstellt. Um Schritt halten zu können, müssen weniger agile Unternehmen ihre Ansichten hinsichtlich Innovationen sowie ihre Aufmerksamkeit auf einzelne Kunden, aus denen ihr Kundenstamm besteht, überdenken.

Konstante Innovationen und neue Angebote sind wichtige Anforderungen, wenn Unternehmen von Kunden wahrgenommen werden möchten. In vielen Einzelhandels- und Endverbrauchermärkten werden Kunden von Unternehmen mit neuen Releases bombardiert. Unternehmen, die Innovationen langsam und unflexibel auf den immer gleichen Kundenbedarf ausrichten, verlieren ihre Vorteile, die sie zuvor mittels Qualität oder Sortiment aufgebaut haben.

Auf dem heutigen Markt ist Kundenloyalität nur noch beschränkt vorhanden. Sie muss jeden Tag und jede Stunde gefördert und bestätigt werden.



Dieses umkämpfte Marktumfeld sorgt dafür, dass Flexibilität und schnelle Reaktionsfähigkeit auf Marktänderungen heute zu den wichtigsten Geschäftsanforderungen zählen. Dies in eine kommerzielle Oberfläche zu integrieren, die kostengünstig und sicher ist, stellt viele Unternehmen vor immense Probleme. In weniger flexiblen Unternehmen hat der Versuch, Geschäftsabläufe neu zu gestalten und vorhandene Infrastrukturen sowie Betriebsprozesse optimal zu nutzen, zu einem gegenteiligen Effekt und in manchen Fällen sogar zum kompletten Scheitern geführt.

Auf dem weltweiten digitalen Markt sind Innovation und Agilität Voraussetzung für die Gewinnung und Bindung von Kunden. Ohne diese Flexibilität werden Unternehmen nicht lange überleben. Sie werden einfach von der Konkurrenz überrollt.

---

## DIGITALE TRANSFORMATION

---

*„Wir sind in nur neun Monaten von der Familie Feuerstein bei den Jetsons angelangt.“*

David Giambruno, Senior VP & CIO, Tribune Media

Der Transformationszug kommt – und die Frage ist, ob Sie mitfahren. Der enorme Wandel bei der Ausführung von Geschäften setzt optimale Tools und gezielte Ausgaben voraus. Die Evaluierung der Komponenten, die in die Infrastruktur eines Unternehmens integriert werden, ist heute, da die gesamte Handelswelt in Aufruhr ist, von entscheidender Bedeutung.

Eine Abstimmung von Kundenanforderungen und Produktpaletten ist in dieser Situation unerlässlich, wird jedoch durch die Dringlichkeit erschwert. Unternehmen mit Produkten oder Dienstleistungen, die sich an einige dieser Herausforderungen richten, fällt es nicht leicht zu verstehen, wie sie mit ihrem Angebot Kunden am besten helfen können.

Die übergeordnete Anforderung in der wachsenden digitalen Geschäftswelt heißt Sicherheit. Dazu gehört nicht nur der Schutz der digitalen Ressourcen eines Unternehmens (z. B. Finanzen und Integrität der Verarbeitungssysteme), sondern auch die Sicherheit von Kundendaten. Bestandteil der Geschäfte im Internet ist die implizite Vertrauensbasis zwischen jenen, die Produkte und Dienstleistungen anbieten, und jenen, die sie kaufen. Jegliche Kundenloyalität und Erfolge im digitalen Bereich müssen auf dieser Vertrauensbasis aufbauen.

Ein weiterer wichtiger Aspekt bei der Ausführung von Geschäften in der digitalisierten Welt ist die Geschwindigkeit, mit der Unternehmen auf den Markt reagieren müssen. Egal ob es sich um Kundenbedarf nach neuen Leistungsmerkmalen oder Funktionen, das Erschließen neuer Märkte oder die Behebung von Problemen geht, müssen digitale Geschäftsteilnehmer die steigende Geschwindigkeit unterstützen können. Die Geschwindigkeitsfaktoren reichen von kürzeren Implementierungszeiten bis hin zu mehr betrieblicher Flexibilität, damit Unternehmen Prozesse leichter anpassen und besser mit Kunden kommunizieren können. Die Tage langsamer Reaktionen sind vorbei. Nur Unternehmen, die agil sind und sich rasch anpassen können, werden in dieser digitalen Welt Erfolg haben.

Die dritte Priorität digitaler Unternehmen ist die Kontrolle der Ausgaben. Für maximale Wirtschaftlichkeit werden die geringsten Kosten mit den erforderlichen Funktionen abgewogen, sodass ein schlankes und kostenbewusstes Unternehmen entsteht. Egal ob die Kosten mit der Bereitstellung von Waren und Dienstleistungen oder dem erforderlichen Schutz der Ressourcen zusammenhängen, entscheidet auch heute noch die Balance zwischen Einnahmen und Ausgaben über den Gesamtzustand und Erfolg digitaler Unternehmen.

Die digitale Transformation eines Unternehmens in einen starken Akteur auf dem Markt setzt koordinierte Veränderungen voraus, von denen viele gleichzeitig vorgenommen werden müssen. Darum ist es sinnvoll, den Weg mit dem bestmöglichen Fundament zu starten.

---

## **SICHERHEIT – SCHUTZ DES KUNDENVERTRAUENS**

---

*„Vertrauen im Cyberspace ist für Finanzunternehmen absolut essentiell. Konsistenz zwischen Sicherheit und Risiken ist ein Schlüsselfaktor für einen guten Ruf und Kundenvertrauen.“*

---

Stéphane Nappo, IBFS Global Chief Information Security Officer & Board Advisor,  
Paris, Frankreich

Kunden müssen darauf vertrauen können, dass Unternehmen Daten, die sie über sie sammeln und zur Ausführung der Geschäfte nutzen, zuverlässig schützen. Ein Versagen in diesem Bereich kann den Ruf von Unternehmen schneller beschädigen als jeder andere Faktor. Es wird als Verrat an der unausgesprochenen Vereinbarung zwischen Käufer und Verkäufer betrachtet.

Kunden, die sich von einem Unternehmen betrogen fühlen, kehren mit großer Wahrscheinlichkeit nicht mehr zurück. Laut einer Studie mit über 175.000 Unternehmen kehren 78 % der Kunden nach einer Datenschutzverletzung nicht zurück – es sei denn, das betroffene Unternehmen übernimmt sofort die Verantwortung und erklärt genau, was es tut, um die Schwachstellen zu beheben und den Schaden wiedergutzumachen. Versuche, den Vorfall zu vertuschen, bewerten 95 % der befragten Kunden als Zeichen der Geringschätzung. Oder wie es ein Umfrageteilnehmer in seinen Notizen ausdrückte: „Warum sollte ich Geschäfte mit einem Händler betreiben, der mich nicht als Person wahrnimmt? Warum sollte ich mit einem Unternehmen interagieren, das mich nicht zu schätzen weiß?“

*„Wir hatten gerade eine große Zahl von Servern ausgetauscht und viele Millionen Dollar für Wiederherstellungsservices ausgegeben, um die Probleme aufgrund eines Ransomware-Angriffs zu beheben, als wir erneut Ziel eines Angriffs wurden. Wir waren kurz davor, das Unternehmen aufgeben zu müssen. Ein Finanzunternehmen, das Kunden tagelang hintereinander nicht bedienen kann, verliert seinen Ruf, den es sich so hart erarbeitet hat. Wir haben Millionen von Dollar für die Wiederherstellung ausgegeben und schätzen, dass wir dabei lediglich zu 75 % erfolgreich waren. Wir haben nicht nur intern Millionen von Dollar ausgegeben, sondern werden auch Dutzende von Millionen Dollar in die Hand nehmen müssen, um Kunden zurückzugewinnen.“*

---

CIO – Mittelgroßer Finanzdienstleister

Wie viel ist das Überleben eines Unternehmens wert? Was würde ein Verlust von 35 % der Kundschaft für den Gewinn bedeuten? Das sind Fragen, die mit den Problemen und Ausgaben für Cybersicherheit abgewogen werden müssen. Wenn Kunden einem Unternehmen nicht vertrauen, warum sollten sie dann Geschäfte mit ihnen machen?

Die horrenden Datenschutzverletzungen, über die in den letzten Jahren in den Nachrichten berichtet wurde, haben die Gefahren auf dem digitalen Markt deutlich gemacht. Nicht nur sind Unternehmen bei der Ausführung ihrer Geschäfte konstanten Angriffen ausgesetzt. Wenn Angriffe erfolgreich sind, sind neben dem geistigen Eigentum und den Ressourcen von Unternehmen auch die Daten ihrer Kunden in Gefahr.

Die Auswirkungen von Sicherheitsverletzungen auf das Kundenvertrauen und spätere Umsätze wurden untersucht – und eine Analyse der Daten zeigt, dass nach einer signifikanten Verletzung bei betroffenen Unternehmen im Durchschnitt 41 % weniger Kunden kaufen.

Das hat einen unmittelbaren sowie langfristigen Einbruch der Umsätze zur Folge. Dadurch wird der bereits angegriffene Ruf des Unternehmens weiter beschädigt. Je nach den ergriffenen Maßnahmen kehren diese Kunden möglicherweise nie zurück. Und wenn sie es tun, dann nur im Anschluss an beträchtliche Ausgaben für Service, Ausrüstung und Personal, um das Vertrauen und Kunden zurückzugewinnen.

Die Ausgaben für die Rückgewinnung eines Kunden nach einer Sicherheitsverletzung können bis zu 18,6-mal so hoch wie die Kosten für seine ursprüngliche Gewinnung sein. Bei jeder Marktexpansion muss auf die Wiederherstellung des Rufs geachtet werden, damit neue Kunden genug Vertrauen haben, um mit dem Unternehmen auch nach dem offensichtlichen Sicherheitsproblem Geschäfte zu betreiben.

In anderen Worten: Ein erfolgreicher Hack kann für Unternehmen extrem teuer werden.

---

## **AGILITÄT – MARKTSENSIBILITÄT**

---

*„Es sind nicht mehr große Unternehmen, die kleine hinter sich lassen, sondern schnelle die langsamen.“*

Eric Pearson, CIO, International Hotel Group (IHG)

Eine der wichtigsten Kennzahlen zur Erfolgsmessung auf dem digitalen Markt ist die Fähigkeit, weltweit auf sich rasch wandelnde Zielgruppen reagieren zu können. Wenn es in dieser Landschaft zu Veränderungen kommt, können meist jene Unternehmen von den Chancen profitieren, die am schnellsten reagieren – um Marktanteile und Umsätze zu erhöhen.

Eine zunehmend mobile und verteilte digitale Mischung bringt für Unternehmen neue und komplexe Herausforderungen mit sich. Die Anforderungen dieser Herausforderungen variieren. Sie umfassen verschiedene Bereiche, wie die Skalierung zur Bewältigung plötzlicher Aktivitätsspitzen, die Förderung von Sicherheit zum Schutz von Prozessen und Daten sowie die Stabilisierung der Performance, um für konsistente Antwortzeiten zu sorgen und gleichzeitig Daten für die Personalisierung von Erkenntnissen und Transaktionen zu gewinnen.

In diesem Umfeld sind die verborgenen Schichten der Infrastruktur und Best Practices extrem wichtig. Die zugrunde liegenden IT- und Geschäftsentscheidungen sind entscheidender denn je, bleiben jedoch weiter unsichtbar. Die kombinierten Einflüsse dieser Eigenschaften ergeben eine Gesamtkennzahl für die Customer Experience (CX) – die Kundenerfahrung. Diese bestimmt sich über Marktanteile und schafft Kundenloyalität.

*„Vor zehn Jahren galten wir als innovatives Unternehmen, da wir unser Produktangebot zweimal im Jahr aktualisierten. Inzwischen hinken wir hinter der Konkurrenz zurück, da wir neue Releases nur alle sechs bis acht Wochen freigeben. Das Feedback, das wir von unseren Kunden erhalten, deutet darauf hin, dass wir mit dem Markt nicht mithalten können. Darum ist es absolut entscheidend, dass wir schneller reagieren können als die Konkurrenz, wenn wir unsere Kunden halten wollen. Kunden, die man einmal verloren hat, kommen so leicht und günstig nicht wieder. Kunden haben heute Erwartungen, die extrem subjektiv, unglaublich schnell und extrem kritisch sind. Unsere Fähigkeit, konstant Innovationen umzusetzen, ist wichtiger denn je.“*

CMO – Sehr großes Versicherungsunternehmen

Da immer mehr Geschäfte in Echtzeit ausgeführt werden, werden die Ergebnisse der Effektivität und Effizienz von IT-Infrastrukturen zunehmend sichtbar. Probleme mit Anwendungen, die auf mangelnde Qualität hinweisen, spiegeln sich in Kundenabwanderung und verlorenen Marktanteilen wieder. Langsame Antworten bei der Anwendungsperformance oder im Kundensupport können weitreichende, zum Teil katastrophale Folgen haben. Dabei geht es nicht nur um einen einmaligen Effekt auf Umsatz und Transaktionen, sondern einen längeren Trend bei der Reaktion von Kunden auf dem virtuellen Markt.

Die neue Sichtbarkeit der Qualität von bereitgestellten Services verändert die Weise, wie Unternehmen ihre IT-Infrastruktur auswählen. Wenn Probleme mit der Qualität enger mit den Einnahmen verknüpft sind, erfahren die Grundlagen zur Ermittlung der angemessenen Kosten und Ausgaben einen radikalen Wandel. Das bedeutet, dass es zu einem wichtigen evolutionären Schritt bei der Auswahl, Konfiguration und Verwaltung der IT-Infrastruktur kommt. Die operative Struktur wird reformiert, während sich die Vision der zugrunde liegenden Beziehung zwischen Computing, Speicher und IT-Mitarbeitern zur Unterstützung der Geschäfte wandelt. Die Komplexität von Cloud-Bereitstellung vs. eines standortbasierten Betriebs hat alles weiter verkompliziert.

Die Kundenerfahrung von Endbenutzern basiert auf zwei unterschiedlichen Perspektiven, die beide gleich wichtig sind. Das intuitive Design der kundenorientierten Anwendung sowie der unsichtbaren Plattform, die sie bereitstellt, sind im Auge des Kunden nicht getrennt. Der Benutzer nimmt Anwendung und Plattform als Ganzes wahr und evaluiert entsprechend.

Wenn CEOs bemerken, dass sie Marktanteile verlieren oder die Rentabilität fällt, reduzieren sie in den meisten Fällen Kosten. Wenn man jedoch an die Kundenerfahrung denkt, muss bei der Auswahl der zu senkenden Kosten der Effekt auf die Marktwahrnehmung berücksichtigt werden. Während es früher überzeugende geschäftliche Argumente für die mögliche Einsparung von Einmalprodukten und preisgünstigen Komponenten gab, ist inzwischen klar, dass der Effekt der Systemzuverlässigkeit auf die Kundenerfahrung kurzfristige Ausgaben klar übersteigen kann.

Es gibt wichtige Faktoren für die Kundenerfahrung, die nichts mit Plattformen oder Anwendungen zu tun haben. Diese sind nicht minder wichtig für den Erfolg von Unternehmen, die im Cyberspace Geschäfte betreiben. Diese Dimensionen hängen mehr mit der betrieblichen Struktur und Prozessen zusammen als mit tatsächlichen Computern. Diese Dimensionen können grob eingeteilt werden in:

- Bedeutung des Endbenutzers für das Unternehmen
- Betrachtung des Kunden als Individuum
- Flexibilität bei der Bereitstellung individueller Reaktionen auf Endbenutzer

Alle drei sind damit verbunden, wie sehr Unternehmen ihre Kunden schätzen.

Der Support für die verborgene IT-Infrastruktur, welche als Grundlage für den Geschäftsbetrieb dient, lässt sich weiter aufschlüsseln. Das Ziel von Kompetenz, Wertschätzung und Marktfähigkeit entsteht durch eine abgestufte Unterstützungsstruktur, die Anwendungen und Daten, die Betriebsumgebung sowie die unterstützende IT-Infrastruktur umfasst.



Die Zusammensetzung der einzelnen Schichten kann sich positiv oder negativ auf die anderen Schichten auswirken. Da die Kundenerfahrung ein kombiniertes Ergebnis der Synergien zwischen allen Schichten ist, lässt sie sich nicht leicht auseinandernehmen, sodass man sich auf eine Komponente konzentrieren kann. Jede von ihnen kann eine sich ausbreitende Wirkung haben, die die äußeren Ringe von Geschäft und Kundeninteraktionen sowie die Kundenerfahrung beeinflusst. Egal ob es um die Anwendung geht, die eine Schnittstelle für Kundeninteraktionen bereitstellt, die Regel, die schnelle Kreditentscheidungen ermöglicht, oder die Hardware, die Daten schnell und konsistent zur Verfügung stellt, sind alle Schichten wichtig.

Als Grundlage für die sichtbare Kundenerfahrung dient die pünktliche Bereitstellung von Aktionen, bei denen der Endbenutzer im Mittelpunkt steht. Da die Kundenerfahrung einen direkten Einfluss auf die Nettoeinnahmen hat, wird sie auf dem virtuellen Markt immer wichtiger.

Die Erklärung für diesen Schwerpunkt lässt sich in einer grafischen Darstellung von 14.071 Sites erkennen, bei denen in den letzten sechs Monaten neue Anwendungen bereitgestellt wurden. Diese wurden anhand von Bewertungskategorien zur Kundenerfahrung – mit Werten von 0 bis 5 – angeordnet, was einem subjektiven Bereich entspricht, der die Erfahrung von mangelhaft bis hervorragend einstuft. Die durchschnittliche monatliche Umsatzänderung ausgehend von der Basis des ersten



Monats wird dargestellt, um aufzuzeigen, welche Auswirkungen die Kundenerfahrung auf den Cashflow und das Nettoeinkommen von Unternehmen hat.

Für die Auswirkungen wurden in Bezug auf den Startmonat Durchschnittswerte errechnet, es wird jedoch eine Beziehung zwischen Gesamtkundenerfahrung und Umsätzen deutlich. Bei Bereitstellungen mit einer suboptimalen Erfahrung zeigte sich, dass die Umsatzhöhe im Vergleich zu jenen Bereitstellungen mit einer besser wahrgenommenen Kundenerfahrung nie mehr aufholen konnte.

Die zwei folgenden Kundenzitate machen deutlich, wie radikal unterschiedlich das Bild an den entgegengesetzten Enden der Kundenerfahrung aussieht.

*„Unser neues Produktangebot für den Einzelhandel ging vor sieben Monaten online. Wir haben Millionen von Dollar für Werbekampagnen, Entwicklung und Hardware ausgegeben. Unsere Marketingabteilung hat hart gearbeitet, um für Öffentlichkeit zu sorgen, und alles sah gut aus... für die ersten drei Tage.*

*In der folgenden Woche erlebte das Gesamtsystem sechs Ausfälle – mit verllorener Verfügbarkeit von mindestens sechs Stunden. Die Probleme in sozialen Medien und für unsere Kundendienstabteilung waren enorm. Die optimistischen Einschätzungen nach den ersten drei Tagen wurden von den auftretenden Problemen völlig entwertet. Nachdem wir das eigentliche Problem erkannt hatten, konnten wir nicht schnell genug reagieren, um uns davon zu erholen.*

*Im ersten Monat erreichten die Umsätze nicht einmal 10 % der erwarteten Werte. Zudem mussten wir über 400.000 Dollar für eine rasche Lieferung von Ausrüstung, die Unterstützung von Anbietern und anderen Dienstleistern usw. ausgeben. Darüber hinaus mussten wir 150.000 Dollar in die Hand nehmen, um zu erklären, dass wir die Probleme gelöst hatten, ohne als komplett inkompetent dazustehen. Die Umsätze haben heute noch nicht einmal 50 % des Werts erreicht, den wir für den ersten Monat erwartet hatten, da unsere Kunden einfach nicht zurückkommen.“*

COO – Großer Einzelhändler

Die Risiken eines problematischen Starts müssen mit den Vorteilen abgewogen werden, die eine erfolgreiche und stabile Bereitstellung bieten kann. Die Chancen für Umsätze und neue Kunden sind immens. Um sich auf dem Markt richtig positionieren zu können, informieren sich Unternehmen über Methoden, die für sie geeignet sind.

*„Vor etwa neun Monaten haben wir eine neue Vertriebsprodukatanwendung bereitgestellt. Wir waren sehr zufrieden mit dem, was unsere Teams geleistet hatten, und freuten uns sehr, dass nach der Bereitstellung kaum Probleme auftraten. Der Markt reagierte äußerst positiv auf das neue System – mit klaren Folgen. Momentan sind unsere Umsätze 60 % höher als anfänglich geplant und*

*das System stellt inzwischen unseren rentabelsten Vertriebskanal dar. Wir versuchen, monatlich inkrementelle Änderungen und Erweiterungen zu implementieren, was die Entwicklung weiter unterstützt. Das Feedback der Kunden ist hervorragend, was natürlich hilfreich ist.“*

LOB VP – Services

Diese zwei unterschiedlichen Erfahrungen spiegeln sich in der großen Zahl von Kundenzitaten wieder, die im Rahmen der Datensammlung erfasst wurden, und machen die hohe Bedeutung der Kundenerfahrung für den geschäftlichen Erfolg sichtbar. Funktionalität, persönliche Orientierung und Performance der Kundenerfahrung werden von anderen Aspekten verstärkt, tendenziell jedoch als zentral für den Markterfolg wahrgenommen.

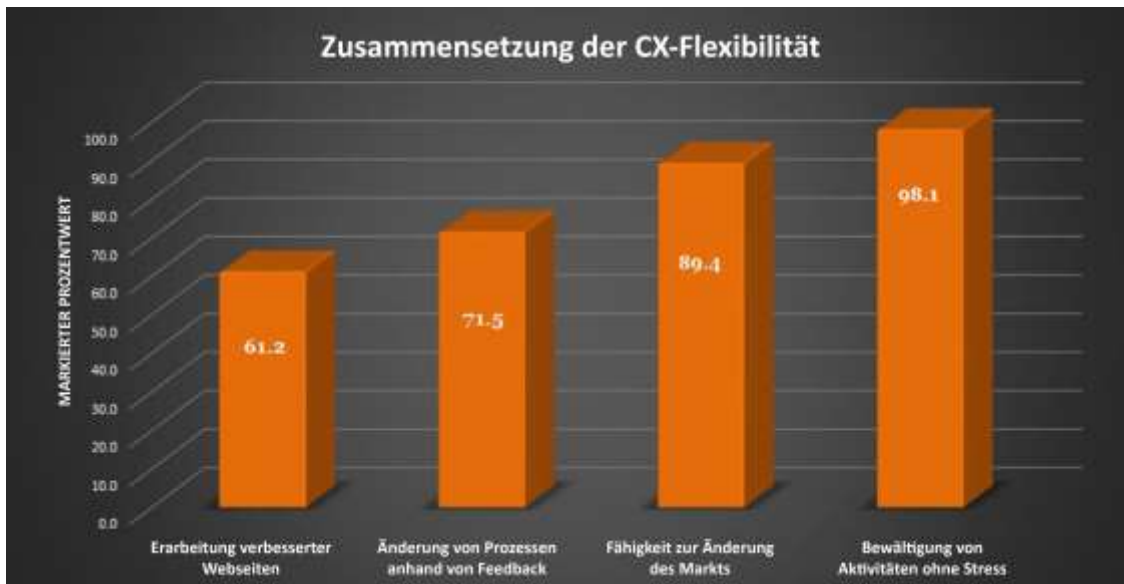
*„Es sind nicht die stärksten Spezies, die überleben, oder die intelligentesten. Es sind jene, die sich an Veränderungen am besten anpassen können.“*

Charles Darwin (1809-1882)

Der Markt verlangt Flexibilität. Wie genau diese Flexibilität aussieht, ist ebenfalls eine kombinierte Wahrnehmung. Daten von über 140.000 Endbenutzern weltweit hinsichtlich ihrer Erfahrungen auf dem digitalen Markt haben gezeigt, dass sich alle Flexibilität wünschen. Dieser Begriff weist jedoch unterschiedliche Kombinationen von reaktiven und proaktiven Bestandteilen auf. Das reaktive Element zeigt sich an der Bereitschaft eines Unternehmens, Schnittstellen, Regeln und Prozesse als Reaktion auf Kundenfeedback zu verändern. Das proaktive Element entspricht den kontinuierlichen Bemühungen, Kunden so schnell wie möglich das neueste „Spielzeug“ bereitzustellen.

Auch wenn diese Betrachtungsweise von Flexibilität eng mit Geschwindigkeit verbunden ist, ist das nicht alles. Der Teil, der nicht nur mit Geschwindigkeit verbunden ist, hat zwei Hauptaspekte. Zum einen geht es um die Sichtbarkeit des sich weiterentwickelnden und ändernden Angebots. Zum anderen geht es um Konsistenz bei der Bereitstellung.

Wie im Diagramm unten erkennbar kommt es auf die Flexibilität und Agilität von Unternehmen bei der Bewältigung unerwarteter Lasten an, ohne dass Kunden die Anstrengungen bemerken. Antwort- und Bereitstellungszeiten, die bei wiederholten Kundeninteraktionen ähnlich sind, führen dazu, dass die grundlegenden Erwartungen von Kunden erfüllt werden. Außerdem treten auf der Kundenseite minimale Probleme auf, die mit einer unbeständigen oder verzögerten Bereitstellung des gewünschten Services oder Angebots zusammenhängen. Wenn es dabei zu Inkonsistenzen kommt, gehen nachweisbar Kunden verloren.



Die Analyse der Kundenantworten hat gezeigt, dass die Erwartung von Flexibilität zentral für die Kundenerfahrung und somit auch den Erfolg in der digitalen Geschäftswelt ist. Das bedeutet, dass Unternehmen eine extrem flexible Entwicklungsabteilung, ein erweiterbares Team für den Kundensupport sowie Grundlage für eine ausfallsichere Verarbeitungsarchitektur benötigen.

Teil des neuen Paradigmas auf dem agilen digitalen Markt ist eine schnelle und sichtbare Reaktion auf Veränderungen. Der Wandel bei Anwendungen und Angebot kann auf Kundenfeedback, neue Vorschriften, veränderte Technologien anderer Anbieter und viele andere Faktoren zurückzuführen sein. Es reicht nicht mehr aus, dass Unternehmen die entsprechenden Änderungen vornehmen. Sie müssen auch ihre Bereitschaft signalisieren, auf die Wünsche ihrer Kunden einzugehen.

Bei dieser Sichtbarkeit geht es um die Erwartung der Kunden, von Unternehmen, mit denen sie interagieren, ernst genommen zu werden. Wenn es nicht mehr nur um freundliches Verkaufspersonal oder attraktive Ladengeschäfte geht, ist die Kommunikation der Unternehmenseinstellung hinsichtlich der Wahrnehmung von Kunden essentiell für die Kundenbindung.

Eine Vermittlung dieser Wahrnehmung im Cyberspace kann schwierig sein, ist jedoch so wichtig, dass Unternehmen diese Frage nicht ignorieren sollten.

---

## **KOSTEN – WIRTSCHAFTLICHKEIT**

---

Wirtschaftlichkeit ist die Fähigkeit eines Unternehmens, Produkte oder Dienstleistungen an Kunden oder Partner auf kosteneffiziente Weise bereitzustellen – unter Wahrung hoher Qualitätsstandards. Diese Kennzahl – manchmal als „effektive Ausgaben“ bezeichnet – lässt sich als Verhältnis zwischen den Investitionen in den Geschäftsbetrieb und den Ergebnissen des Geschäftsbetriebs betrachten. Steigt die Wirtschaftlichkeit, verbessert sich das Verhältnis zwischen Aufwand und Ergebnis. Die Berechnungen beruhen in der Regel auf Geld (Kosten), Personen (Personalzahl oder Full-Time-Equivalent/FTE) bzw. Zeit- und Arbeitsaufwand – stets im Vergleich zum Umsatz.

Die Dynamik digitaler Geschäfte erschwert diese Berechnung – vor allem aufgrund der fehlenden Fähigkeit der meisten Unternehmen, ihre geschäftlichen Ergebnisse mit der Reaktion von Kunden in Verbindung zu setzen. In einer Gruppe von über 190.000 Unternehmen hatten weniger als 1,4 % der Firmen eine formelle Methode zur Verknüpfung der geschäftlichen Resultate mit der Reaktion von Kunden. Das erschwert die Analyse von Verbesserungspotenzialen sowie des Nutzens von Wandel für das Unternehmen. Ohne ein ausreichendes Verständnis der Verbindung zwischen Kundenreaktion und Einnahmen befinden sich Unternehmen im Nachteil und geben möglicherweise deutlich mehr Geld für den kontinuierlichen Betrieb im Cyberspace aus als erforderlich.

Angesichts der geringeren Bedeutung physischer Standorte werden effiziente Ausgaben zu einem der wichtigsten Tools für die Erhöhung der Gewinne. Dies ist einer der größten Vorzüge des digitalen Markts. Wenn Unternehmen die Chancen dieser Umgebung nicht nutzen, werden es ihre Konkurrenten tun.

---

## **STRATEGIEN IM CYBERSPACE**

---

Entwicklung und Umfang der Gefahren im Cyberspace nehmen weiter an Geschwindigkeit zu – parallel zu den Chancen, die durch die neue Umgebung der digitalen Welt entstehen.



Für viele Unternehmen sind die Herausforderungen überwältigend. Sie haben Probleme mit der Etablierung der Grundlagen im Cyberbusiness und kämpfen mit ausfallenden Geräten, Sicherheitsverletzungen und wechselhafter Performance. Die ständigen Herausforderungen rauben Energie und Geld und führen zu deutlich mehr geschäftlicher Volatilität als in den Jahrzehnten davor.

Das neue Gesicht von Due Diligence und der Bedarf nach schnellen Marktreaktionen zeigen, wie unpassend vorhandene betriebliche Ansätze und Verfahren sind, wenn es um die Bewältigung des immer aggressiveren digitalen Marktumfelds geht.

Angesichts der Kundenanforderungen und geschäftlichen Gefahren ist Wandel dringend erforderlich. Letztendlich lässt sich der Bedarf nach Veränderungen an einer einzigen Frage festmachen.

*Wollen Sie, dass Ihr Unternehmen auch noch in drei Jahren erfolgreich ist?* Wenn die Antwort auf diese Frage ja lautet, ist ein Paradigmenwechsel erforderlich. Und dieser Wechsel muss dem Bedarf nach einer flexiblen Marktreaktion Rechnung tragen, die sicher ist und sich an die verschiedenen Anforderungen erfolgreicher digitaler Geschäfte anpassen lässt.

---

## LÖSUNGEN FÜR DIGITALE GESCHÄFTE

---

Die Strategien und Herausforderungen bei der Entwicklung eines Unternehmenspfads, der das Erreichen potenzieller Kunden im Cyberspace erleichtert, setzen ein Verständnis der unterschiedlichen Komponenten voraus, die in den Pfad integriert werden müssen. Das bedeutet, dass Informationen über geschäftliche und sicherheitsrelevante Abläufe sowie über deren Zusammenspiel benötigt werden.

Für das Verhalten spezifischer IT-Plattformlösungen, die eine optimale Kundenerfahrung ermöglichen und fördern, sowie die Härten des digitalen Geschäftsumfelds müssen sowohl technische als auch geschäftliche Aspekte berücksichtigt werden. Da die Auswirkungen der Plattformauswahl auf die Performance in der digitalen Geschäftswelt reflektiv und schwer zu messen sind, hat IBM Solitaire Interglobal Ltd. (SIL) damit beauftragt, eine objektive Analyse zum IBM LinuxONE Produkt zu erstellen.

SIL sammelt seit über 40 Jahren Daten über die Entwicklungen und das Produktionsverhalten auf dem Markt. Die Firma unterstützt über 6.000 Kunden und führt im Jahr mehr als 100 Millionen Prognosemodelle aus. Zudem erstellt SIL seit 22 Jahren den Global Security Watch (GSW). Durch diesen Mitgliederservice ist es SIL gelungen, ein Repository einzurichten, das über 550 PB an detaillierten Daten enthält. Diese Daten werden für Trends, Vergleiche und Schwellenwerte stündlich analysiert, um Unternehmen beim Erreichen ihrer Ziele zu helfen.

SIL hat zusätzliche Daten gesammelt, die sein umfangreiches Daten-Repository ergänzen, und Analysen durchgeführt, um die Vorteile und relativen Kosten von durch Kunden beschriebenen Produktionsumgebungen, in denen Unternehmen IBM LinuxONE nutzen, klar artikulieren zu können. Bei der Analyse ging es vor allem um den inkrementellen Nutzen (sowohl positiv als auch negativ) der Plattfornnutzung – und zwar aus geschäftlicher Perspektive. Mithilfe dieser Informationen können Führungskräfte die Verbindung zwischen der IT-Plattform und den Umsätzen sowie der Reaktion von Kunden in ihrem Unternehmen besser verstehen.

Digitale Geschäfte und Sicherheit müssen Hand in Hand gehen – darum müssen alle Analysen die enge Beziehung zwischen beiden berücksichtigen. SIL verfolgt geschäfts- und sicherheitsrelevante Aspekte bereits seit über 22 Jahren. Durch die Sammlung von Informationen über Global Security Watch (GSW) erhalten Tausende von Unternehmen kontinuierlich aktuelle Trend- und Risikodaten. Dieser konstante Strom an anonymen Daten über das, was heute eine entscheidende Landschaft für Unternehmen ist, hat über die Jahre als fruchtbare Grundlage für zahlreiche Studien gedient.

Eine kürzliche Studie hat gezeigt, dass sowohl die Geschwindigkeit des Marktbedarfs nach Wandel als auch die Zahl und Größe der aktiven Bedrohungen im Cyberspace parallel zueinander zugenommen haben. Mit dem größeren Marktpotenzial ist auch das Interesse der Kriminellen gestiegen. Egal ob diese Kriminellen von Staaten unterstützt werden, um die Stabilität anderer Staaten zu schwächen, oder finanzielle Interessen haben: Der Cyberspace ist für Unternehmen gleichzeitig hochinteressant und hochgefährlich.

GWS ist ein Service für Mitglieder, der die genaue Entwicklung von Sicherheitsbedrohungen und ihre Auswirkungen auf Unternehmen weltweit seit Jahrzehnten verfolgt und aktuell gemeldete Daten von über 12,1 Millionen Firmen erfasst. Die Daten aus GSW stellen eine reichhaltige Quelle an Informationen aus geschäftlicher Perspektive dar, die als Eingangsdaten für die Studie dienen und auf Produktionsdaten aus der realen Welt basieren. In GSW werden zwar Thread-Zahlen und andere genaue Merkmale erfasst, der Hauptfokus liegt jedoch auf den Folgen für den geschäftlichen Betrieb, den geschäftlichen Ressourcen sowie den Vorbeugungs- und Behebungskosten.

Mit Daten aus Umfragen zur Kundenerfahrung sowie Informationen über IT-Betrieb, geschäftliche Performance sowie Sicherheit hat SIL die Positionierung von IBM LinuxONE auf dem Markt für digitale Geschäfte untersucht. Die Ergebnisse der Analyse wurden in drei Bereiche zusammengefasst: Sicherheit, Agilität und Kosten. Diese Bereiche umfassen jene Hauptziele, die im Cyberspace aktive Unternehmen als besonders wichtig betrachten.

---

## **SICHERHEIT UND RISIKEN**

---

Risiken bei der Bereitstellung hängen mit verschiedenen Bereichen zusammen. Das größte von ihnen sind jedoch erfolgreiche Einbrüche in Systeme und Infrastrukturen von Unternehmen. Sicherheitsverletzungen zu verhindern ist die Hauptaufgabe von Sicherheitspersonal in digitalen Firmen.

Für diese Mitarbeiter gibt es keine akzeptablen Verluste. Jede Sicherheitsverletzung, jeder Einbruch, jede Überwindung der Schutzschale kann potenziell katastrophale Folgen haben. Während die Zahl der Angriffe stündlich zunimmt, sind Unternehmen wiederholt Versuchen ausgesetzt, Daten zu zerstören oder zu stehlen bzw. den Geschäftsbetrieb zu unterbrechen.

In diesem Kampf spielen die grundlegenden Eigenschaften der Infrastruktur eine zentrale Rolle. Das gilt besonders dann, wenn die zugrunde liegende Architektur der Technologie darauf ausgerichtet ist, Hackern das Leben zu erschweren.

Im Allgemeinen sind Hacker Opportunisten. Genauso wie sich Räuber einfache Opfer aussuchen, greifen viele Hacker leichte Ziele an. Seitdem auch das organisierte Verbrechen im Cyberspace aktiv ist, hat die Komplexität noch einmal deutlich zugenommen. Für diese Kriminellen liegt der Schwerpunkt weniger auf einfachen Zielen, sondern auf solchen, die den höchsten Profit versprechen. Zudem beteiligen sich im Rahmen eines inoffiziellen Cyberkriegs immer mehr Staaten an Diebstahl und Zerstörung. Diese drei verschiedenen Profile von Cyberkriminellen haben die Komplexität der Gefahren im Cyberspace noch einmal erhöht.

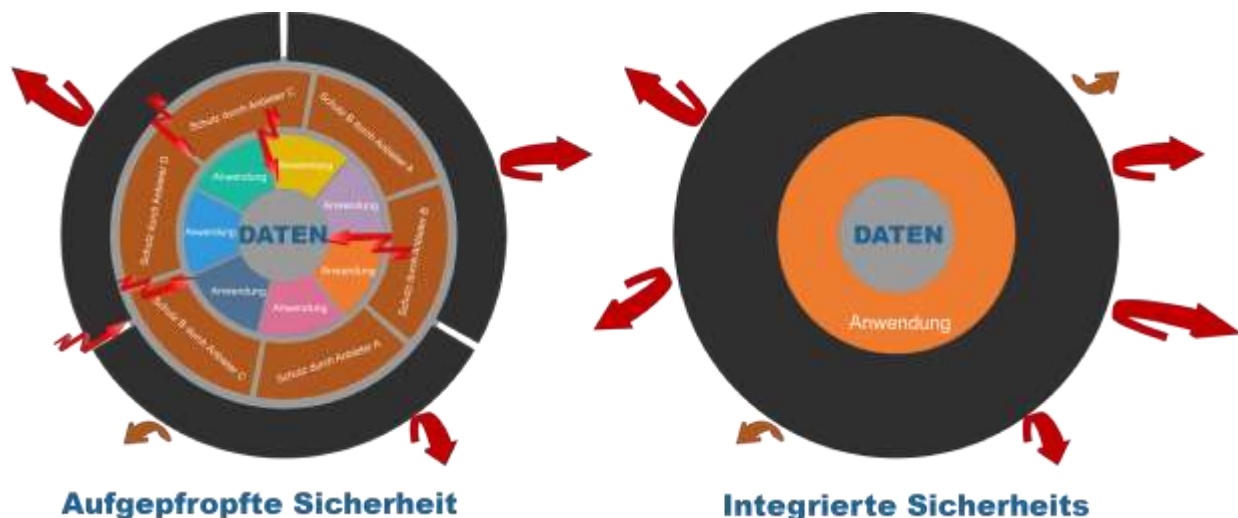
Wenn eine Überwindung der Schutzmaßnahmen zu schwierig ist, wenden sich Hacker leichteren Opfern zu. Außerdem hat die Hacker-Community neue und ausgeklügelte Tools und Verfahren entwickelt, darunter virtuelle Roboter, die sich ununterbrochen an Sicherheitsmaßnahmen abarbeiten, bis sie eine Lücke finden. Hier spielen die Unterschiede bei den Architekturen eine wichtige Rolle.

## AUFGEFROPFTE VERSUS INTEGRIERTE SICHERHEIT

Viele der auf dem Markt erhältlichen Architekturen basieren auf einer Philosophie der aufgepfropften Einbindung von Sicherheit. Einzelne Unternehmen können entscheiden, wie sie für ihren Schutz sorgen, und dabei zwischen Unmengen an Produkten wählen.

Das Problem mit aufgepfropfter Sicherheit ist, dass es stets Verbindungen gibt – Stellen, an denen eine Schutzlösung mit einem anderen Produkt kommunizieren muss. Dadurch entstehen automatisch Schwachstellen und Möglichkeiten für Hacker, in Systeme einzudringen. Das ist jedoch grundlegender Bestandteil des Designs und wird von entsprechenden Unternehmen als „Flexibilität und Wahlfreiheit“ betrachtet.

Eine Alternative zu aufgepfropfter Sicherheit ist ein vollständig integrierter Stack. In einer solchen digitalen Konstruktion sind Verbindungen strukturell und nicht optional. Es gibt weniger Verbindungs- und Schwachstellen, was die verfügbare Angriffsfläche deutlich verkleinert.



Der Erfolg von LinuxONE Sicherheit basiert auf der Implementierung eines integrierten Stacks. Dieses Schutzkonzept eliminiert Lücken und erschwert Hackern erfolgreiche Angriffe. Es ist zwar nicht unfehlbar, sorgt jedoch für eine signifikant kleinere Angriffsfläche.

Der Erfolg dieser Sicherheitsarchitektur zeigt sich an der Tatsache, dass GSW von SIL bei LinuxONE Implementierungen pro 1.000 bereitgestellten Anwendungen *weniger als 0,01 %* erfolgreiche Sicherheitsverletzungen registrierte als bei den anderen Architekturen.

Im Rahmen der Studie wurden die wichtigsten Verhaltensmerkmale von Software und Hardware für zahlreiche reale Kundensysteme (mehr als 13 Millionen) untersucht. Alle diese Kunden haben in ihren Produktionsumgebungen eine Sicherheitslösung bereitgestellt, wobei sich jedoch Sicherheitsmethoden und -verfahren unterscheiden. Darunter sind auch Unternehmen, die behördliche Normen und Industriestandards für Informationssicherheit wie HIPAA, PCI, SOX usw. unterstützen müssen. Informationen aus diesen Kundenberichten und die begleitenden Daten bieten ein realistisches (nicht nur theoretisches) Verständnis darüber, wie sich die verschiedenen Sicherheitsarten auf Kunden auswirken.

Über 164 Millionen Datenpunkte mit detaillierten Einbruchsaktivitäten und -folgen aus GSW dienen als Fundament für erwartbare Kosten und Risiken, was essentiell ist, um den aktuellen Markt für Sicherheit und Asset-Schutz angemessen beurteilen zu können.

Bei der Zusammenstellung und Analyse der Studiendaten wurden verschiedene Merkmale abgeleitet. Diese Merkmale betreffen die offenkundige Kapazität, Effizienz und Zuverlässigkeit der geschützten Umgebung. Außerdem wurde die Synergie zwischen Sicherheits- und Betriebsprozessen untersucht. Das repräsentierte Verhalten wurde in möglichen Bereitstellungsoptionen projiziert und modelliert. Zum Verständnis wird mehr als nur die Serverleistung benötigt, da Sicherheit den Geschäftsbetrieb letztendlich nicht behindern, sondern schützen soll. Kapazitätsbedarf und Durchsatzeffekte der Sicherheitssysteme spielen zwar eine wichtige Rolle, ihre geschäftliche Umsetzung hängt jedoch mehr vom aktuellen Markt ab. Die geschäftliche Perspektive beinhaltet eine Vielzahl von Faktoren wie Zuverlässigkeit, Sicherheitsniveau, Personalzahl, Gesamtsicherheitskosten (inkl. Wiederherstellung) und andere Aspekte. Das hängt direkt mit den Entscheidungen zusammen, die IT-Manager, CTOs und geschäftliche Führungskräfte täglich treffen.

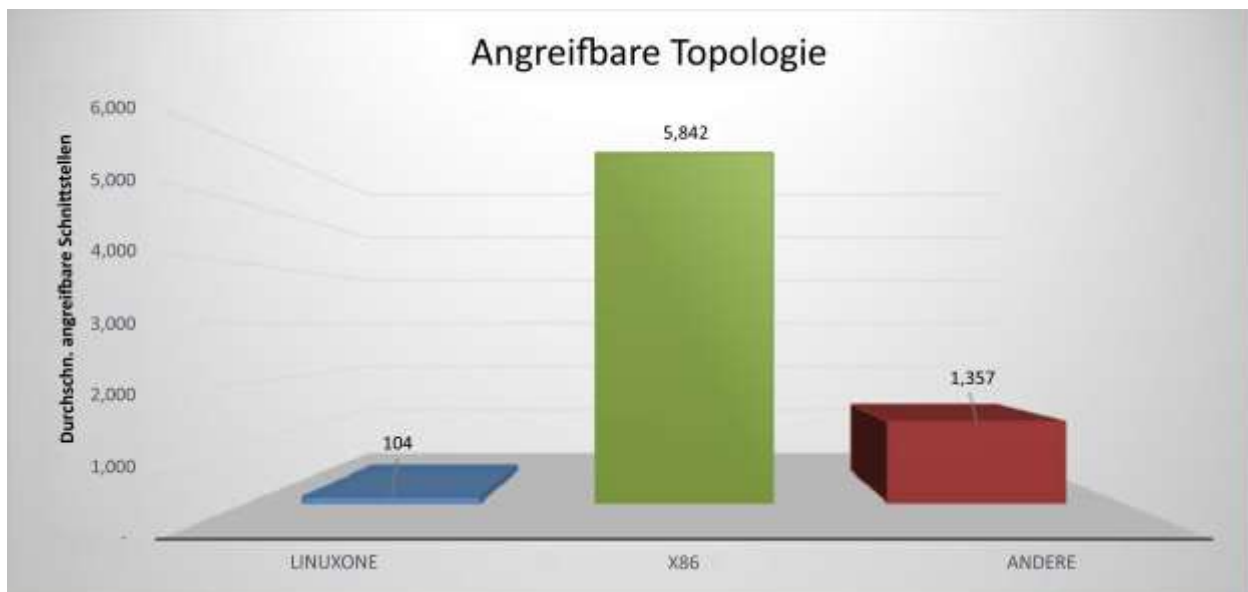
---

## ANGREIFBARE TOPOLOGIE

---

Ein kritischer Faktor für Risiken und Schwachstellen im Sicherheitsbereich ist die angreifbare Topologie. Damit werden die relativen Schwächen verschiedener Architekturen quantifiziert.

Die angreifbare Topologie variiert je nach grundlegender Architektur deutlich. Die allgemeine Analyse einer Gruppe, die über 131.000 Unternehmen umfasst, macht den Unterschied wie dargestellt deutlich.



Die wichtigste Differenz hängt mit der grundlegenden Struktur und verwendeten Strategie hinter der Plattformarchitektur, dem Chipdesign, dem Betriebssystem und der Methode zur Stack-Integration zusammen.

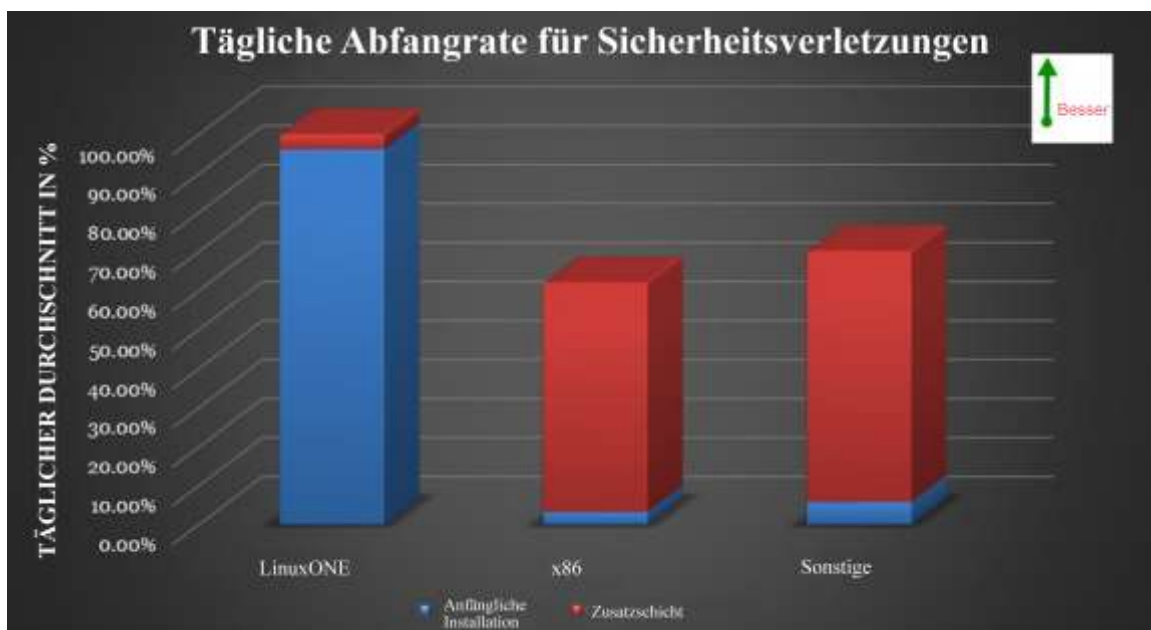
Die Art der integrierten Sicherheit von LinuxONE unterscheidet sich deutlich von dem, was durch zusätzliche Schutzlösungen erzeugt wird. Angesichts einer höheren Zahl zu sichernder Schnittstellen ist der Schutz der Daten und Prozesse von Unternehmen auf der Geräteebene am schwierigsten. Bei einer effizienteren Strategie werden die Kontrolle und Definition von Richtlinien

zentral zusammengefasst. Hier bietet der vollständig integrierte Sicherheits-Stack von LinuxONE enorme Vorteile. Durch Kombination dieser stabilen Grundlage mit der Flexibilität von LinuxONE lassen sich die zentralen Plattformstärken mit der ausgewählten Architektur verbinden.

## RESISTENZ GEGEN SICHERHEITSVERLETZUNGEN

Die primäre Kennzahl für erfolgreiche Sicherheit ist die Zahl der Einbruchsversuche, die erkannt, neutralisiert oder daran gehindert wurden, in irgendeiner Weise Schaden zu verursachen. Die in der Kennzahl zusammengefassten Angriffe beinhalten keine Versuche, die von Add-on-Firewalls und Sicherheitsgeräten blockiert wurden. Stattdessen wurden nur jene Versuche gezählt, die von der vorhandenen Sicherheitslösung blockiert wurden. Die Zahlen wurden anhand der tatsächlichen VM-Zahl auf einer Plattform normalisiert, da jede VM eine separate logische Einheit darstellt. Dabei handelt es sich um eine indikative Kennzahl, da keine Anpassung an die Zahl der Benutzer auf einzelnen virtuellen Maschinen vorgenommen wurde.

Das Maß der Blockierung von Sicherheitsverletzungen durch die anfängliche Installation der jeweiligen Plattform dient als Grundlage für alle anderen erforderlichen oder installierten Add-on-Sicherheitsprodukte. Dieses Diagramm veranschaulicht die Sicherheit, die von der anfänglichen Installation und der Zusatzschicht gewährleistet wird, ausgedrückt als Prozentanteil der blockierten Einbruchsversuche.



Bei Betrachtung der anfänglichen Installationen zeigt sich, dass die grundlegenden LinuxONE Sicherheitslösungen eine bis zu *15,74-mal* höhere Abfangquote aufweisen als alternative Plattformlösungen. Außerdem bietet die LinuxONE Lösung einen Basisschutz, der 96 % übersteigt – und das ohne Zusatzprodukte, die bei anderen Architekturen erforderlich sind.

Zusätzliche Sicherheitsschichten umfassen Add-on-Anwendungen, -Taktiken, -Verfahren usw. Diese unterscheiden sich von Unternehmen zu Unternehmen je nach Sicherheitskontrolle, Status und Governance. Ein höheres Niveau an zusätzlichen Sicherheitsanforderungen deutet auf mehr Engagement seitens der Sicherheitssoftware und des Personals hin.

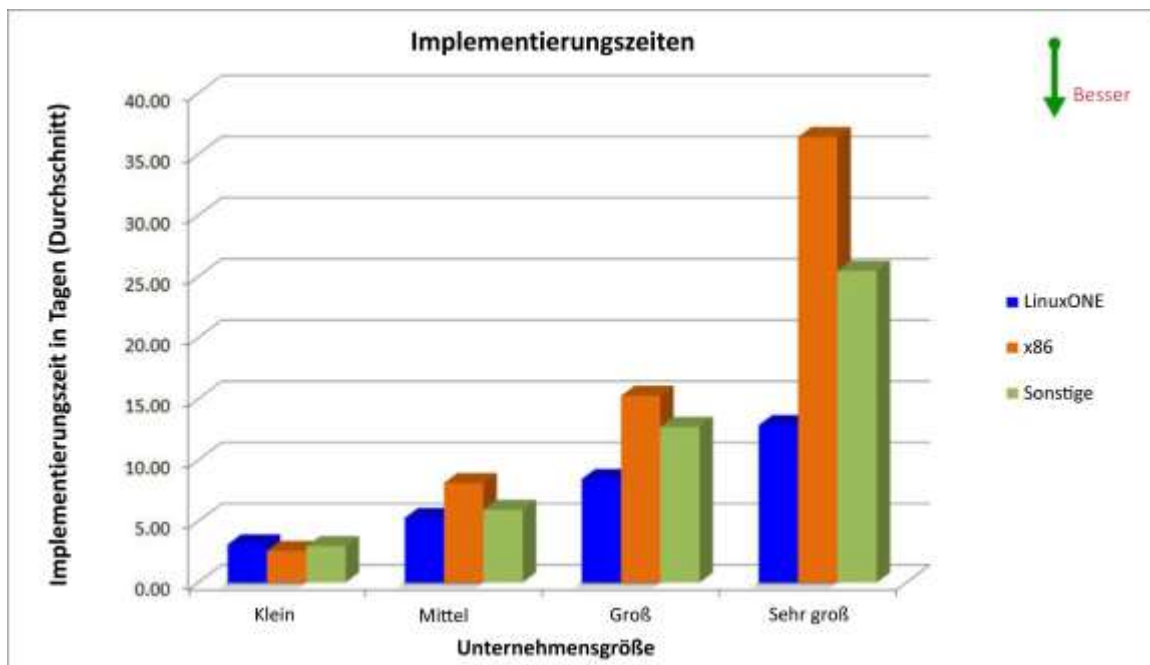
Die Kombination aus geistigem Eigentum und automatisierten Services sorgen gemeinsam mit dem architektonischen Design der LinuxONE Cybersicherheitslösungen für eine deutlich höhere Abfangquote bei Sicherheitsverletzungen. So bietet die LinuxONE Plattform eine grundlegende Abfangrate, die um bis zu 61,4 % besser ist als die kombinierte Sicherheit von Fundamenten, die um umfangreiche, kompetente und effektive Maßnahmen für ergänzende Sicherheitstaktiken, -techniken und -verfahren, die von anderen Plattformlösungen bereitgestellt werden, ergänzt wurden.

Weitere Erkenntnisse zur Effektivität einer Sicherheitslösung setzen eine genauere Analyse voraus. Sicherheitsservices setzen bei der Architektur an, inklusive sämtlicher Hardware-, Software- und Middlewarekomponenten. In Schichten darüber befinden sich die Richtlinien, Verfahren, Status und Governance eines Unternehmens. Diese lassen sich zwar mithilfe aktueller Best Practices messen und als wichtige Unterschiede betrachten, der Schwerpunkt dieser Studie liegt jedoch auf der Untersuchung von Anbieterlösungen, die plattformspezifische Hardware, Software und Middleware inkl. Betriebssystemen zusammenfassen.

## AGILITÄT UND FLEXIBILITÄT

Kunden im Cyberspace erwarten angemessene Reaktionen. Egal ob diese Reaktionen auf Anforderungen oder Probleme auf Innovationen oder Marktänderungen basieren: Wer in diesem Bereich nicht liefern kann, setzt sein Unternehmen beträchtlichen Nachteilen aus.

Um den Unterschied zu verstehen, die eine spezifische Plattform in diesem Bereich macht, wurden Millionen von an SIL gemeldeten Erfahrungspunkten analysiert und im folgenden Diagramm zusammengefasst. Diese Grafik macht die durchschnittliche Bereitstellungszeit basierend auf einer normalisierten Anwendung von 200 Funktionspunkten deutlich. Um Verwirrung zu vermeiden, die durch die kontinuierliche Aktualisierung von Tools entsteht, wurden die analysierten Bereitstellungen auf jene beschränkt, die im letzten Kalenderjahr vorgenommen wurden.



Je nach zugrunde liegender Architektur gibt es deutliche Unterschiede bei der Frage, wie lang ein Unternehmen für die Bereitstellung neuer Versionen oder Anwendungen benötigt. In die LinuxONE Plattform integrierte Optimierungen verbessern

Bereitstellung, Tests und andere Faktoren und sorgen für eine Agilität, die im Durchschnitt nur 35,3 % der anderen Plattformen erfordert.

Diese zusätzliche Agilität ist signifikant, da die meisten Unternehmen in einem Kalenderjahr Dutzende oder gar Hunderte von Updates und Releases bereitstellen. Alle Einsparungen – von der Initiierung bis hin zur Bereitstellung – sorgen direkt für geringere Kosten und eine bessere Reaktionsfähigkeit auf Kundenanforderungen. Da diese Kennzahl zu den wichtigsten im Cyberspace gehört, ist dieser Faktor bemerkenswert.

Der Bedarf von Kunden nach Flexibilität in der digitalen Welt hat Auswirkungen für IT und Geschäfte. Auf der geschäftlichen Seite gilt dies vor allem für Strategie und Ansatz. Die Bereitschaft von Unternehmen, ihre Richtung zu ändern und Markt- oder Kundenanforderungen zu folgen, ist eine Frage der Philosophie.

Zusätzlich zu den Betriebsprinzipien, die über die Richtung eines Unternehmens bestimmen, bedeutet geschäftliche Flexibilität, Sortimente und Produkte so zu verändern, dass sie für den Kundenstamm stets relevant sind. Keiner dieser Aspekte ist direkt mit der IT-Plattform verbunden, auf der sie beruhen.

Der Beitrag von Flexibilität, den physische und virtuelle Plattformen leisten, besteht aus umfassender Anpassbarkeit. Wenn Anforderungen für lokalisierten Support definiert werden, muss sich die Plattform effizient neu konfigurieren lassen. Wenn Nachfrage entweder saisonal oder aufgrund einer positiven Marktreaktion nach oben schnellst, muss die Plattform diesem Bedarf gerecht werden können.

Die Zuverlässigkeit der Implementierung lässt als die Fähigkeit betrachten, unerwartete Nachfrage nach Ressourcen ohne Ausfall der Gesamtplattform zu meistern. Extreme Fälle lassen sich in Umgebungen beobachten, die durch konzentrierte Denial-of-Service-Angriffe zum Absturz gebracht werden. Zuverlässigere Implementierungen beruhen auf der Kapazität und Elastizität von Betriebssystem und Hardware. Zuverlässigkeit ist eine typische Kennzahl, wenn es um die Evaluierung von zu kaufender Hardware und bereitzustellenden Betriebssystemen geht.

Die kombinierte Zuverlässigkeitsbewertung der Plattformgruppen können Sie der Grafik entnehmen. Die Bewertung selbst ist das Ergebnis erfasster und gemeldeter Skalierungs-Breakpoints jener Produktionsimplementierungen, die Teil der Studie waren. Die Bewertung wird als Workload-Prozentwert ausgedrückt und stellt die Menge der Warteschlangenbildung und Überlastung dar, die Verarbeitungsalgorithmen, Pufferverfahren und andere Komponenten tolerieren können, ohne dass der Gesamtbetrieb beeinträchtigt wird.



Es gibt einen klaren Unterschied zwischen der Zuverlässigkeit der LinuxONE Umgebungen und dem Rest der Lösungen. Die gemeldete durchschnittliche Zuverlässigkeit von LinuxONE Implementierungen war bis zu *7,41-mal* höher als bei den anderen Optionen. Das bedeutet, dass die vorhandene IT-Lösung seltener überarbeitet werden muss. Die Folgen: geringere Total Cost of Ownership (TCO) sowie niedrigere Total Cost of Information (TCI), eine weitere wichtige geschäftliche Kennzahl.

Ein zusätzlicher Aspekt von Flexibilität ist die Fähigkeit zur Sicherstellung einer konsistenten Kundenerfahrung. Es hat sich gezeigt, dass vorhersagbares und konsistentes Verhalten ein Pfeiler für hohe Kundenzufriedenheit ist. Unberechenbares oder stark schwankendes Verhalten irritiert Käufer und führt zu mehr Supportanrufen und Beschwerden.

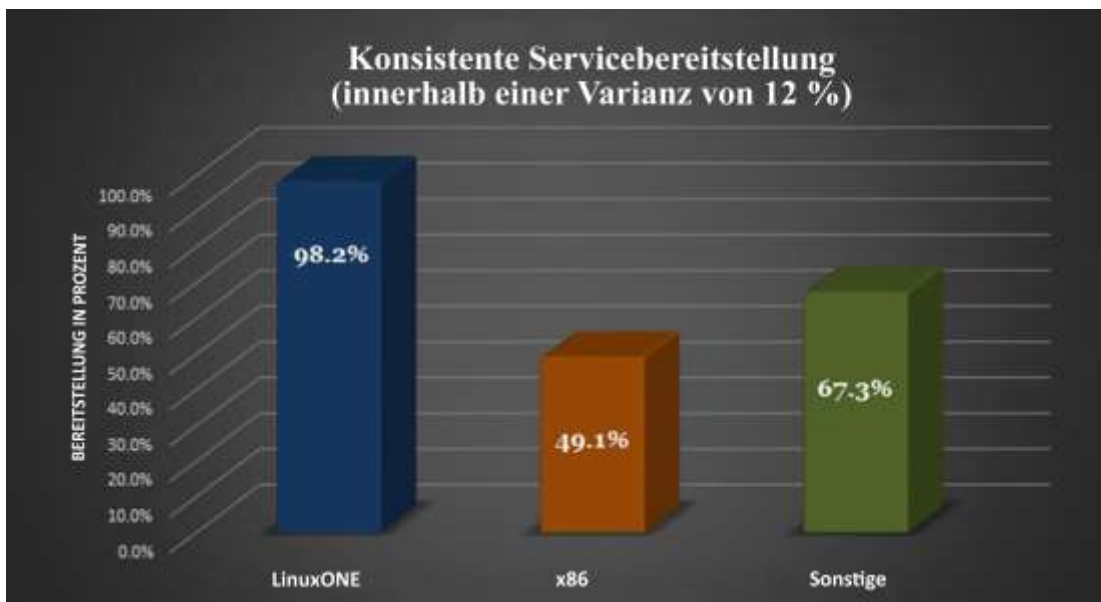
Die Möglichkeit der Bereitstellung konsistenter Antwortzeiten ist vor allem von der Plattform abhängig. Zwar bietet das Anwendungsdesign ein Framework für den Gesamtdatenverkehr vom und zum Kunden, die Konsistenz hängt jedoch vor allem von internen Merkmalen der Infrastruktur ab.

Eine Analyse von über 17 Millionen Beschwerden über schlechte Antwortzeiten hat ergeben, dass die Schwelle für das Erkennen schwankender Antwortzeiten bei ca. 12 % liegt. Auf dieser Grundlage wurde in der Studie die Performance der Plattformen untersucht, um zu sehen, welcher Anteil der Antwortzeiten bei Transaktionen mit diesen Parametern zusammenhing.

Es sollte beachtet werden, dass die geprüften Anwendungen ein breites Spektrum an Kunden-, Anbieter- und internen Anwendungen abdeckten. Es wurde kein Versuch gemacht, das Verhalten zu normalisieren, da es in der Analyse um die Abweichungen der einzelnen Anwendungen für die gleiche Aktivität ging.

Zusätzlich zu den prozentualen Unterschieden, die in den Erkennungsbereich für Konsistenz fielen, wies die Höhe der Varianz, die beim Schutzverhalten beobachtet wurde, zwischen den verschiedenen Architekturgruppen klare Unterschiede auf. Der Effekt der gleichen Mechanismen, mit denen IBM LinuxONE für eine konsistente Bereitstellung sorgt, verringert auch das Ausmaß der Abweichungen.





Die LinuxONE Lösung weist einen bis zu *2-mal* höheren Prozentwert bei der konsistenten Bereitstellung von Transaktionen auf als die anderen architektonischen Gruppen. Während es bei den anderen Lösungen zu Variationen kam, die sich bis *17-mal* von den durchschnittlichen Antwortzeiten unterschieden, betrug die größte Abweichung bei LinuxONE gerade einmal *36,2 %*.

Der Vergleich hinsichtlich der unberechenbaren und inkonsistenten Bereitstellung digitaler Services zeigt, dass die IBM Lösung deutlich seltener zu unzufriedenen Kunden führt.

---

## KOSTEN UND AUSGABEN

---

Die Kosten sind eine zentrale Kennzahl für Unternehmen. Die Steigerung der Umsätze und Minimierung der Kosten stellen in der Geschäftswelt eine kontinuierliche Aufgabe dar. Zwar gibt es verschiedene Methoden zur Analyse von Kosten und Ausgaben, die am besten vergleichbaren Kennzahlen für einen Vergleich des finanziellen Profils zwischen Unternehmen sind jedoch die TCO und TCI. Da sich beide mit einer standardisierten Workload-Einheit (z. B. Funktionspunkten) normalisieren lassen, ist die Vergleichsmethode sowohl für sehr kleine als auch sehr große Unternehmen geeignet.

Teil der Rechtfertigung für eine Ausführung von Geschäften im Cyberspace ist die Kontrolle und Reduzierung der Ausgaben. Ohne Kosten für Ladengeschäfte ist der digitale Markt deutlich freundlicher, wenn es um die geschäftlichen Ergebnisse geht.

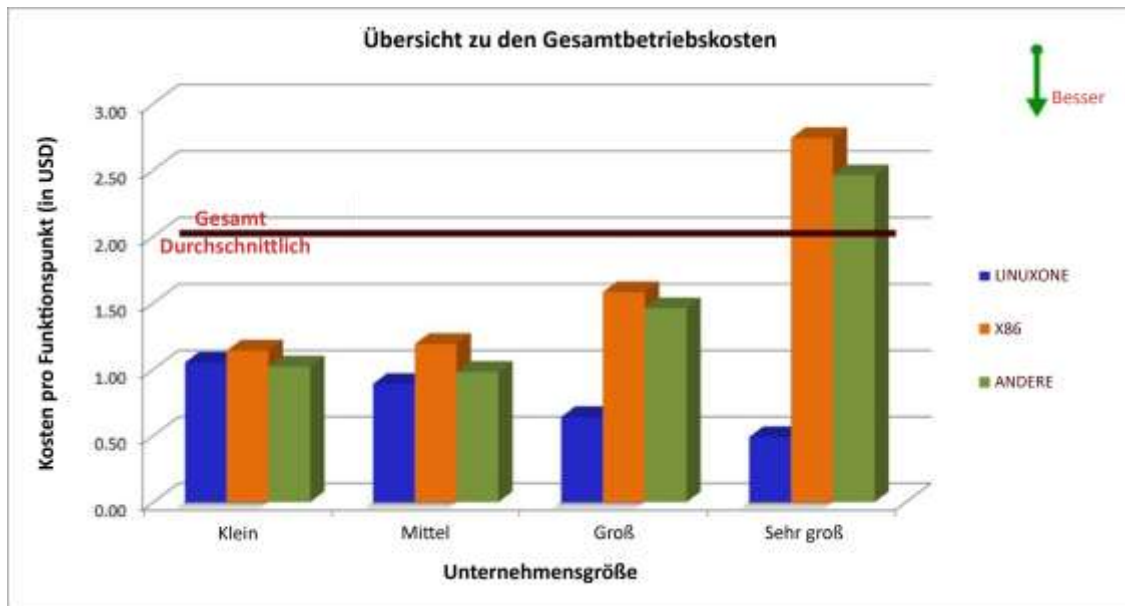
---

## TOTAL COST OF OWNERSHIP

---

Die TCO stellen eine zentrale geschäftliche Kennzahl für die Wirtschaftlichkeit dar. Diese übergeordnete Zahl fasst alle Ausgaben im Unternehmen zusammen, die einen Beitrag zu einem beliebigen Aspekt des Betriebs leisten. Auch hier wurden die Projekte und ihre Ausgaben auf Grundlage der Standardbasis normalisiert. So lassen sich große und kleine Unternehmen besser vergleichen.

Durch eine Normalisierung der TCO auf Grundlage einer Standarddefinition für Arbeitseinheiten (z. B. Funktionspunkte) lässt sich ein präziser Vergleich erstellen und können Trends erkannt werden. Die Ausgabenmuster zeigen bei einigen Plattfortmtypen eine steigende Tendenz, wenn die Komplexität der Umgebung wächst.



LinuxONE fällt durch einen gegenläufigen Trend auf. Ein abnehmendes Ausgabenmuster pro Einheit sorgt für Skaleneffekte, sodass die Nutzung von Framework und Fundament ein kosteneffizientes Modell für finanzielle Investitionen ermöglicht. Wie dem begleitenden Diagramm zu entnehmen ist, fallen die Ausgaben für LinuxONE Sicherheitsimplementierungen um bis zu 82,12 % niedriger aus als bei anderen Plattformen.

Dies hängt zum Teil mit der Kombination aus architektonischen Komponenten und hochskalierbarer Plattform zusammen. Effizienzsteigerungen durch diese Synergie werden sichtbar, wenn die Architektur stärker ausgelastet wird, da die Kosten pro Arbeitseinheit deutlich sinken. Diese Bilanz zeigt sich in allen Fällen, in denen die Struktur für hochskalierbare Umgebungen entwickelt wurde – normalerweise jedoch nur im Hardwarebereich. Im Sicherheitsbereich ist ein einheitliches Design für Skalierbarkeit sowohl in der physischen Hardware als auch im Betriebssystem gegeben.

*„Unsere LinuxONE VMs bieten eine überzeugende Investitionsrendite. Sie weisen geringere inkrementelle Kosten pro VM auf und lassen sich deutlich leichter bereitstellen und ändern. Das sorgt für geringere Personalkosten, die in unserem Unternehmen eine große Herausforderung darstellen. Wenn es ein System gibt, das wir rasch bereitstellen möchten, fällt die Wahl definitiv auf LinuxONE. Damit lassen sich Kosten leichter rechtfertigen, während Bereitstellungen schneller und einfacher verlaufen.“*

CTO – Mittelständisches Fertigungsunternehmen

Architekturinhärente Skalierbarkeit wird mit steigender Komplexität von Systemen immer wichtiger – zum Beispiel dann, wenn die Benutzerzahl nach oben skaliert wird, die Zahl der persönlichen BYOD-Geräte wächst bzw. Cloud-Anwendungen bereitgestellt werden. Die explosionsartig zunehmende Cloud-Nutzung und die wachsende Bereitstellung von Anwendungen in der Cloud haben die Probleme beim Erzielen reaktiver Sicherheit sowie bezüglich konsistenter Antwortzeiten und flexibler Anwendungen weiter verschärft. Auch die Art der Cloud-Bereitstellung wirkt sich auf die Herausforderungen aus. Egal ob private, öffentliche, Community-basierte oder hybride Cloud: Betriebs- und Sicherheitspraktiken bei der Bereitstellung müssen kontinuierlich angepasst werden.

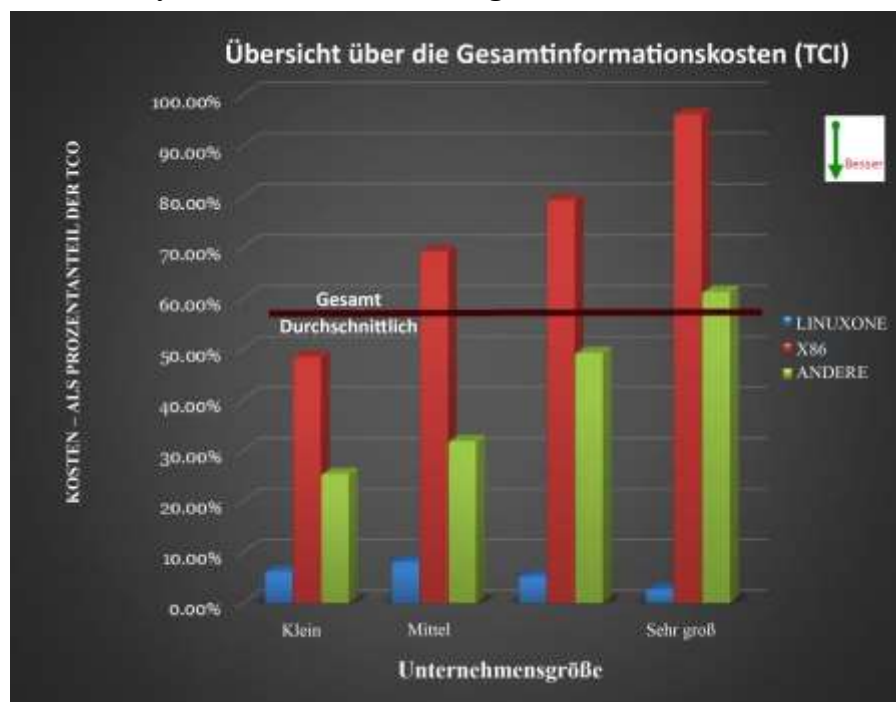
## TOTAL COST OF INFORMATION

Die mit digitalen Geschäften verbundenen Kosten beinhalten sowohl die traditionelle Kennzahl der TCO (Total Cost of Ownership) als auch die neuere Kennzahl der TCI (Total Cost of Information), welche einen genaueren Überblick über die Kostenverteilung in Unternehmen liefert.

TCO umfassen die Ausgaben, die zur Sicherstellung eines kontinuierlichen Betriebs erforderlich sind. Die Kostenkategorien dieser Kennzahl beinhalten das IT-Betriebspersonal, Support bei der Behebung von Anwendungsproblemen, externe Dienstleistungen zur Unterstützung des Betriebspersonals oder der Problembeseitigung, Strom- und Kühlausgaben, Wartung und Lizenzen für Hardware und Software sowie Stellplatzkosten.

TCI sind eine Kennzahl, die Betriebsausgaben in Beziehung zum Unterhalten und Schützen von IT-Ressourcen und geistigem Eigentum (IP) des Unternehmens setzt. Dazu gehören Daten, Geschäftsprozesse, Forschungsergebnisse, Anwendungsstrukturen und anderes geistiges Eigentum. Die in dieser Kennzahl enthaltenen Ausgaben beinhalten die Infrastruktur, die Ressourcen enthält und bereitstellt, sowie Personal, Strom, Kühlung, Sicherheitsmaßnahmen usw., die für die Sicherheit der Ressourcen sorgen. Bei dieser Kennzahl werden die negativen Folgen von Verlusten oder Beschädigungen geistigen Eigentums berücksichtigt (z. B. Denial-of-Service und Ausfallzeiten). Die Kennzahl, die den Effekt von IT-Sicherheit in Unternehmen am besten abbildet, sind die TCI, da diese ein Verständnis der reflektiven Sicherheit ermöglichen.

Bei Betrachtung der TCI für verschiedene Architekturen gibt es unterschiedliche Methoden zur Zusammenfassung der jeweiligen Probleme. Da es bei der Größe der Infrastrukturbereitstellungen starke Unterschiede gibt, ist eine Zusammenfassung auf Grundlage des Gesamtwerts der IT- und IP-Ressourcen statistisch vage. Eine normalisierte Vergleichsbasis drückt die TCI als Prozentanteil der TCO aus. Die Ergebnisse dieser Analyse lassen sich dem Diagramm entnehmen.



In Unternehmen unterschiedlicher Größen überzeugen die IBM LinuxONE Implementierungen durch um bis zu 92,04% niedrigere TCI. Da diese Kennzahl ein wichtiger Faktor für neue Implementierungsausgaben ist, unterstreicht der geringe

Wert die effiziente Skalierung von LinuxONE Umgebungen. Der TCI-Vergleich beinhaltet die Ausgaben für Verfügbarkeit, Folgen von Sicherheitsverletzungen und Kennzahlen zu Ausfallzeiten, sodass keine zusätzlichen Aspekte berücksichtigt werden müssen. Der Unterschied zwischen den Lösungen basiert vor allem auf drei Bereichen:

- Personalkosten
- Folgekosten von Sicherheitsverletzungen
- Architektonische Add-ons in der Infrastruktur

Die Kosten für Personal und Infrastruktur lassen sich prüfen, während die Ausgaben für Folgen von Sicherheitsverletzungen eine Kombination aus objektiven und projizierten subjektiven Beträgen beinhalten. In allen Fällen stammen die Kosten direkt aus Kundenberichten und wurden nicht verändert, sondern einfach aggregiert und für die Studienbasis gemittelt.

Die mit den LinuxONE Sicherheitskonfigurationen verbundenen Kosten sind geringer als bei x86- und anderen Sicherheitsoptionen – und zwar sowohl bei der herkömmlichen Kostenbasis als auch bei den reflektiven Kosten, die durch Sicherheitsverletzungen entstehen. Daran zeigt sich der Unterschied zwischen einem umfassend integrierten Sicherheits-Stack gegenüber aufgepfropften Lösungen, welche die Anfälligkeiten sowie Zahl der Schwachstellen erhöhen.

---

## PERSONALAUFWAND

---

Ein bedeutender Faktor, der sich auch in vielen anderen Bereichen bemerkbar macht, ist die Effizienz der Schnittstelle zwischen Systemadministrator und Infrastruktur. Dazu gehören Software-, Hardware- und Betriebssystemkomponenten sowie der entsprechende Effekt auf den Personalbedarf. Wenn die Effizienz des Personals zunimmt, steigt die Produktivität. Der Aufwand für die Erledigung der gleichen Aufgaben verringert sich, wodurch jedes Mitglied im Team produktiver wird.

---

*„Wir sind mit den LinuxONE Umgebungen mehr als zufrieden! Sie sind deutlich stabiler und problemfreier als unsere anderen Linux-Umgebungen. Bei ähnlich großen Workloads benötigen wir für LinuxONE vier Vollzeitmitarbeiter, während es bei den x86-Systemen 13 Vollzeit- und zwei Teilzeitmitarbeiter sind. Aufgrund der schnelleren und leichteren Einrichtung und Konfiguration stellen wir nun immer mehr VMs in LinuxONE bereit.“*

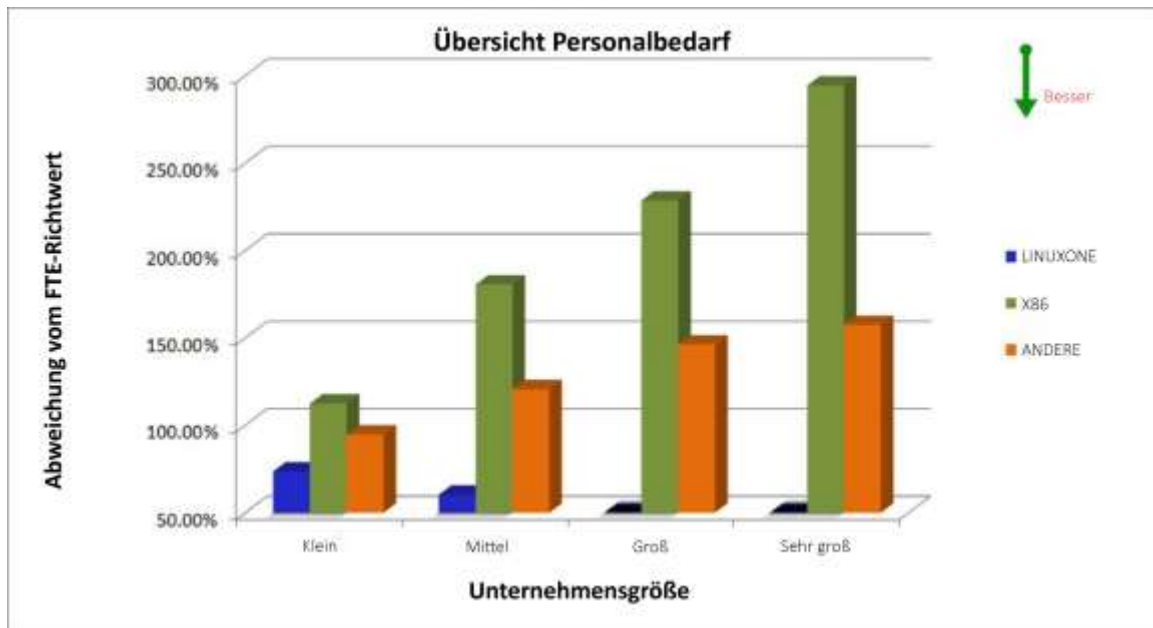
---

### CIO – Mittelständisches Fertigungsunternehmen

Die Effizienz der spezifischen Komponenten, die sich auf die Benutzererfahrung auswirken, lässt sich schwer in Kennzahlen ausdrücken; möglich sind nur übermäßig detaillierte Vergleiche, die durch die Menge der Details an Erkenntnisgewinn einbüßen. Eine allgemeine Übersicht über die Personalaufwandsgruppen in Vollzeitstellen (FTEs) soll als allgemeine Kennzahl für den Plattformvergleich dienen. Der Gesamtdurchschnitt für den Aufwand von Sicherheitspersonal wurde als weiterer Vergleichsmesswert in die Grafik aufgenommen. Dieser Durchschnitt fasst alle Berichte unabhängig von der Unternehmensgröße zusammen.

Die verglichenen Aufwandswerte stehen für den Aufwand, der in jeder Betriebssystemgruppe für das Pflegen einer „Goldstandard“-Umgebung betrieben werden muss. Der Arbeitsaufwand für die Systeme wurde auf identische Ebenen normalisiert, um das Vergleichsfeld beizubehalten, das in früheren Vergleichen etabliert wurde. Der Richtwert für den Vergleich ist der Median des gesamten Antwortfelds, da es bei Sicherheitskomponenten viele unterschiedliche Optionen gibt.

Da verschiedene Architekturen unterschiedliche Implementierungsstandards haben, ist es wichtig, beim Prüfen des Personalbedarfs die genaue Einhaltung dieser Standards vor Augen zu haben. Der deutlich geringere Personalaufwand für Sicherheit bei der Bereitstellung und Verwendung der IBM LinuxONE Plattform ist direkt auf das integrierte Konzept des Betriebs-Stacks zurückzuführen. Dies ist besonders wichtig für Unternehmen, die sich vergrößern oder ein Cloud-Servicebereitstellungsmodell implementieren möchten.



Detaillierte Kundenberichte haben gezeigt, dass der Personalaufwand bei der Bereitstellung mit LinuxONE um 61,07 bis 88,05 Prozent niedriger ist als bei den Alternativen.

Die Effizienz im ermittelten Produktionsverhalten des Betriebspersonals macht deutlich, dass die Arbeitsbelastung für einzelne Mitarbeiter deutlich niedriger ist. Aus einer arbeitspsychologischen Perspektive ist es entscheidend, dass Mitarbeiter Aufgaben mit einem Minimum an Kontextwechseln erledigen können. So lässt sich die Zahl der durch Konfusion entstehenden Fehler reduzieren und die Expertise des Personals zur Anwendung von Best Practices nutzen.

Da Best Practices in den Bereichen Systemverwaltung, Sicherheit und Betrieb eine wichtige Rolle bei der Begrenzung von Risiken spielen, ist die Zeit, die zur Ausführung proaktiver Evaluierungen und vollständigen Implementierung von Best Practices benötigt wird, ein entscheidender Sicherheitsfaktor für Unternehmen. Die Unterschiede an professionellem Verhalten oder Fähigkeiten zwischen den Mitarbeitern verschiedener Unternehmen lassen sich nur schwer ermitteln. Ineffiziente Tools, die für eine Aufgabe bereitgestellt werden, lassen sich jedoch an einer geringeren Implementierung von Best Practices erkennen. Mitarbeitern fehlt oft schon die Zeit, um ihre täglichen Aufgaben zu erledigen – ganz zu schweigen von proaktiven und strategischen Aktivitäten, die der Verhinderung von Problemen dienen, bevor diese auftreten.

Eine Analyse der Anwendung von Best Practices unter den teilnehmenden Unternehmen und Websites ergab ein auffälliges Muster, das anhand architektonischer Grenzen verlief. Die Effizienz der Toolsets, der Integration in die Architektur und des Software-Stacks sowie anderer Komponenten ergab ein aussagekräftiges Bild.



Die Haupteckdaten bestehen darin, dass die Wahrscheinlichkeit einer vollständigen Befolgung von Best Practices in LinuxONE Umgebungen mehr als *3,1-mal* höher ist als bei anderen Architekturen. Das stellt einen bedeutenden Faktor für die Risikoreduzierung dar und hat Folgeeffekte für alle anderen Betriebsaktivitäten.

### **KOSTEN VON SICHERHEITSVERLETZUNGEN**

Ein weiterer Faktor, der in Form von Kosten ausgedrückt wird, ist ein Beitrag, den viele ausschließlich im Sicherheitsbereich berücksichtigen. Diese Kosten sind jedoch ein geschäftliches Anliegen und sollten von jenen Mitarbeitern evaluiert werden, die Geschäftsszenarien untersuchen. Dabei geht es um die Ausgaben für Sicherheitsverletzungen.

Eine Sicherheitsverletzung lässt sich als erfolgreicher Einbruch in die Landschaft eines Unternehmens definieren. Dies kann in Form von Diebstahl, Zerstörung oder Blockade geschehen. Der aktuelle Schutz muss eine größere Vielfalt von Zugangspunkten unterstützen, um auf der Plattformebene für Sicherheit sorgen zu können. In diesem Fall müssen alle Aspekte der Datenverarbeitung kontrolliert werden. Viele behördliche und geschützte Installationen setzen einen Schutz der Zuweisung und Verwaltung der zentralen IT-Sphären voraus: I/O, Netzwerkzugriff, Arbeitsspeichermanagement und normaler allgemeiner Ausführungszugriff.

Bei manchen Sicherheitsverletzungen dauert es lange, bis sich die Kosten für ein Unternehmen beziffern lassen. Dies kann zum Beispiel bei Diebstahl geistigen Eigentums der Fall sein. Ein solcher Verlust kann auf dem Markt beträchtliche Folgen haben.

Die durchschnittlichen mit einer Sicherheitsverletzung verbundenen Kosten geben Auskunft über das relative Risiko der einzelnen Technologien. Leider hat sich auf dem Markt ein Klima für „akzeptable Verluste“ gebildet. Das hängt mit den gemittelten Kosten zusammen, die auch die vielen kleinen Sicherheitsverletzungen umfassen. Dies hat zu einer gewissen Lässigkeit bei der Sicherheitsdefinition und -kontrolle geführt. Die sehr reale Exposition gegenüber größeren und heftigeren Folgen durch Sicherheitsverletzungen wird dabei jedoch ignoriert. Wenn ein Unternehmen so geführt wird, dass wiederholte „überschaubare“ Verluste hingenommen werden können, belässt es seine Informationen und Operationen in einem gefährdeten Zustand und anfällig für größere Schäden.

Eine Analyse der durchschnittlichen Kosten pro erfolgreicher Sicherheitsverletzung zeigt, dass sich die finanziellen Folgen je nach Architektur stark unterscheiden. Im folgenden Diagramm sind lediglich jene Sicherheitsverletzungen ausgeschlossen, die aus der Verwendung gestohlener Kennwörter resultierten.



Die durchschnittlichen Kosten einer Sicherheitsverletzung steigen – und die Steigerungsrate beschleunigt sich. Die Ausgaben im Zusammenhang mit Sicherheitsverletzungen liegen heute um 650 % höher als vor zehn Jahren. Zum Teil hängt dies mit der zunehmenden Verwendung von Cloud-Anwendungen zusammen, da hier mehr Personen und Daten von Sicherheitsverletzungen betroffen sein können. Der andere wichtige Faktor besteht darin, dass Angreifer bei ihren Angriffen immer besser und aggressiver werden. Das weist auf ein Bedrohungsrisiko hin, das bei der Auswahl von IT-Komponenten berücksichtigt werden sollte.

Die durchschnittlichen Kosten einer Sicherheitsverletzung werden von zahlreichen Faktoren beeinflusst. Die Geschwindigkeit und Effektivität der Erkennung, die Fähigkeit zur Isolierung der Sicherheitsverletzung, sodass kein weiterer Schaden entstehen kann, die Gründlichkeit der Behebung usw. haben allesamt Folgen für die allgemeinen finanziellen Auswirkungen. An den deutlich geringeren Kosten pro Sicherheitsverletzung der LinuxONE Plattform zeigt sich das Zusammenspiel dieser Faktoren.

---

## KOSTEN VON RISIKEN

---

Der wachsende geschäftliche Schaden durch Cyberkriminelle hat zur Einführung spezieller Cyberversicherungspolicen geführt. Dieser stark wachsende Markt umfasst eine konstante Erfassung ausreichender Daten, mit denen sich das Risiko der geschäftlichen Aktivitäten von Klienten akkurat einschätzen lässt.

Zusätzlich zu einer komplexen Mischung aus benötigten Protokollen und Komponenten verlangen Versicherungsunternehmen, die solche Policen anbieten, von ihren Kunden beträchtliche Rückstellungen (also inaktive Finanzmittel), damit sich diese bei erfolgreichen Sicherheitsverletzungen eine angemessene Reaktion leisten können.

Es ist bemerkenswert, dass die finanziellen Rücklagen bei LinuxONE Systemen aufgrund der geringen Wahrscheinlichkeit von Sicherheitsverletzungen zum Teil nur 3,2 % dessen betragen, was Kunden für die Verwendung anderer Plattformen und Lösungen ausgeben müssen. Im Vergleich zu einem Branchendurchschnitt von 14,7 % stellt dies einen deutlichen geschäftlichen Vorteil dar.

Dies zeigt eine klare, präzise und branchenübergreifende Perspektive hinsichtlich finanzieller Risiken und projizierter Kosten, wenn es um geschäftliche Aktivitäten im Cyberspace geht – erarbeitet von einer Gruppe, deren Geschäftsfeld es ist, Risiken zu kalkulieren. Der Effekt der Rückstellungen ist nur ein Indiz für das Gesamtbild.

Führungskräfte, die solche Anforderungen bewältigen müssen, sehen sich zunehmend die TCO an und blicken nicht mehr nur auf die Anschaffungskosten. Wie ein CEO kürzlich in einer E-Mail sagte: „Die Anschaffungskosten sind einmalig, Rückstellungen können für immer sein. Und wir wollen nicht, dass 7,5 Millionen Dollar für ein System dauerhaft aus dem Betriebsbudget verschwinden.“

Das sollte Führungskräfte definitiv nachdenklich stimmen und bei jeder geschäftlichen Evaluierung für die Auswahl oder Bereitstellung einer Plattform berücksichtigt werden.

## FAZIT

*Ein Bundesberufungsgericht in Washington D.C. hat entschieden, dass Kunden Unternehmen verklagen können, die ihre personenbezogenen Daten nicht richtig schützen. EPIC reichte diesbezüglich einen Amicus-Schriftsatz zur Unterstützung von Kunden ein und argumentierte, dass wenn „Unternehmen nicht in Sicherheitsmaßnahmen investieren, Kunden weiter durch Sicherheitsverletzungen geschädigt werden können“. Das Berufungsgericht stimmte EPIC zu, dass das untere Gericht die Klage fälschlicherweise abgelehnt hatte.*

[Electronic Privacy Information Center, „DC Circuit Upholds Right of Data Breach Victims to Seek Legal Relief“, 1. August 2017](#)

Der aktuelle Release der LinuxONE Plattform weist im Vergleich zu anderen Plattformoptionen auf dem Markt deutliche Vorteile in den Bereichen TCO, Performance und Risiko auf. Das aktuell verfügbare Niveau an selektiver Verschlüsselung und die Resistenz der nativen Plattform gegenüber häufigen Bedrohungsvektoren bietet Unternehmen einen wichtigen Grundlagenschutz.

Unternehmen, die Geschäfte im Cyberspace betreiben und/oder auf ein Cloud-Modell umgestiegen sind, sind extrem empfindlich, was Cybersicherheit angeht. Die Sicherheit von Daten und anderem geistigen Eigentum eines Unternehmens gerät zunehmend in den Fokus, da sich unsere Welt Tag für Tag mehr vernetzt. Verbunden mit dieser wachsenden Integration sind größere Herausforderungen. So kämpfen Unternehmen darum, ihre Marktanteile und finanziellen Ergebnisse zu schützen. IBM hat eine lange Geschichte des Asset-Schutzes und optimal gesicherter Umgebungen. Mit dieser Reife verbunden sind Funktionen, die in die LinuxONE Lösung integriert sind und bei anderen Lösungen fehlen.

Im Folgenden finden Sie einige der Highlights aus den Studienergebnissen.

### Kurzübersicht

Kategorie	Kommentar	Zusammenfassung
Implementierungszeit	Die Einrichtung und Inbetriebnahme eines Systems mit LinuxONE dauert zum Teil nur <i>35,3 % der Zeit</i> , die bei anderen Plattformen benötigt wird.	Sorgen Sie dafür, dass Ihre Systeme schneller einsatzbereit sind.
Flexibilität	Die gemeldete durchschnittliche Zuverlässigkeit von LinuxONE Implementierungen ist bis zu <i>7,41-mal</i> höher als bei den Alternativen.	Bewältigen Sie unerwartete Spitzen deutlich leichter.
Flexibilität	Kunden, die LinuxONE verwenden, profitieren von bis zu <i>2-mal</i> mehr Konsistenz bei der Bereitstellung von Endbenutzeranfragen als bei anderen Plattformen.	Verbessern Sie die Kundenerfahrung mittels einer konsistenten Bereitstellung.
Gesamtbetriebskosten	Die Gesamtbetriebskosten (TCO) für LinuxONE Implementierungen fallen bis zu <i>82,12 %</i> niedriger aus als bei anderen Plattformen.	Sorgen Sie im Vergleich zur Konkurrenz für deutlich geringere TCO.



Kategorie	Kommentar	Zusammenfassung
Gesamtinformationskosten (TCI)	In Unternehmen unterschiedlicher Größen überzeugen die IBM LinuxONE Implementierungen durch um bis zu 92,04% niedrigere TCI.	Profitieren Sie bei der Arbeit mit Daten von geringeren Kosten.
Mitarbeiter	Die FTE-Ausgaben zur Ausführung von LinuxONE Systemen sind um 61,07 bis 88,05 % niedriger als bei anderen Architekturen.	Erreichen Sie mehr mit weniger Personal.
Risiko und Kosten	Finanzielle Rücklagen, die Versicherungsunternehmen im Cyberbereich verlangen, betragen bei LinuxONE Implementierungen im Vergleich zu anderen Architekturen zum Teil nur 3,2 %.	Reduzieren Sie die erforderlichen Rücklagen.
Risiko	Die von SIL erstellten Risikoprofile zeigen eine Risikobewertung der LinuxONE Plattform, die weniger als 1/20 der Bewertung der anderen Lösungen ausmacht.	Sorgen Sie für deutlich weniger Sicherheitsrisiken.
Sicherheitseffektivität	Bei Betrachtung der anfänglichen Installationen zeigt sich, dass die grundlegende LinuxONE Sicherheitslösung eine bis zu 15,74-mal bessere Abfangquote aufweist als andere Plattformlösungen.	Profitieren Sie mit einem integrierten Ansatz von besonders sicheren Anwendungsumgebungen.
Sicherheitseffektivität	LinuxONE Kunden berichten von Raten schädlicher Angriffe, die im Vergleich zu anderen Architekturen bei unter 0,01 % pro 1.000 bereitgestellten Anwendungen liegen.	Stellen Sie eine grundlegende Sicherheitsplattform bereit, die deutlich effektiver ist als bei der Konkurrenz.
Mitarbeiter	Bei LinuxONE Implementierungen ist die Wahrscheinlichkeit, dass Best Practices umfassend befolgt werden, 3,1-mal höher als bei anderen Architekturen.	Setzen Sie Zeit und Ressourcen frei, um Innovationen voranzutreiben.

Die Geschäfte im Cyberspace verändern sich immer schneller. Rapider Wandel, mehr aktive Angriffe und das schwierige Risikomanagement führen dazu, dass es neben Chancen auch immense Risiken gibt.

Eigentliches Ziel der Untersuchung in der von SIL durchgeführten Analyse waren die realen Folgen für geschäftliche Sicherheit unter Berücksichtigung der jeweiligen Plattformarchitektur. Zu diesem Zweck wurden verbreitete Architekturen wie x86, die LinuxONE Plattform von IBM und andere Produkte miteinander verglichen.

Hauptergebnis der Analyse war, dass sich in der Branche jene Faktoren, die Unternehmen bei der Wahl ihrer Rechenarchitektur berücksichtigen müssen, dramatisch verändern.

---

## **SOLITAIRE INTERGLOBAL LTD.**

---

Solitaire Interglobal Ltd. (SIL) hat sich als Beratungsunternehmen auf die angewandte Performancevorhersage-Modellierung spezialisiert. Das 1978 gegründete Unternehmen SIL nutzt leistungsstarke AI-Technologie und selbst entwickelte chaostheoretische Rechenmodelle zur Analyse zukunftsgerichteter und forensischer Szenarien. Über 7.600 Kunden weltweit vertrauen auf SIL-Analysen, wenn es um regelmäßige Risikoprofilerstellung, Performance-Ursachenanalyse, die Bewertung von Umweltauswirkungen, Kapazitätsmanagement, Markttrendberechnung, Fehleranalyse, angewandte Fordham-Effizienzanalyse, die Ermittlung dynamischer Hebel auf Organisationsebene sowie die Aufschlüsselung von Kosten und Aufwendungen geht. SIL bietet auch RFP-Zertifizierungen für Anbieterantworten an staatliche Einrichtungen weltweit und viele gewerbliche Unternehmen an.

Zahlreiche gewerbliche und staatliche Hardware- und Softwareanbieter wenden sich an SIL zur Zertifizierung der Leistungsdaten und Beschränkungen ihrer Angebote. SIL unterstützt diese Anbieter auch bei der Verbesserung von Durchsatz und Skalierbarkeit von Kundenbereitstellungen und erstellt Risikoprofile und Strategien zur Risikominderung. SIL war in den letzten Jahrzehnten maßgeblich an der Einführung von Branchenstandards und Leistungsnachweismodellen beteiligt und sammelte zum Beispiel aktiv Daten für die Operational Characterization Master Study (OPMS), die ein besseres Verständnis der IT-abhängigen Organisationskosten und Verhaltenscharakteristiken ermöglichen sollte. OPMS hat in großem Umfang zum Aufbau der heuristischen Datenbank von SIL beigetragen, die derzeit mehr als 538 PB Daten umfasst. Diese große statistische Basis sorgt dafür, dass SIL hinsichtlich der Genauigkeit seiner Aussagen und der Geschwindigkeit der Analyseerstellung zu den Besten der Branche zählt. Insgesamt stellt SIL jedes Jahr Berechnungen zu über 16 Millionen Modellen an, sowohl auf Kundenabonnementbasis als auch auf Anfrage.

---

## **HINWEISE ZUR METHODOLOGIE**

---

Um den Effekt von LinuxONE Plattformen als essentieller Komponente der IT-Infrastruktur von Unternehmen sowie die Auswirkungen auf die Kundenerfahrung zu verstehen, wurde eine große Zahl von Implementierungen untersucht. Der relative Grad der Abweichung im Betriebsverhalten für jeden Faktor, z. B. die Gesamtzahl an Ausfällen usw., wurde dann verglichen, um den Nettoeffekt der jeweiligen Kombinationen zu verstehen. Die Effekte wurden durch die allgemeine Leistung und Kapazitätsnutzung sowie andere Geschäftskennzahlen beobachtet.

Der Ansatz von SIL umfasst eine Kompilierung und Korrelation des operativen Produktionsverhaltens anhand realer Systeme und Geschäftsaktivitäten. Für die Zwecke dieser Untersuchung wurden 13.041.692 Umgebungen beobachtet, erfasst und analysiert, um die Ergebnisse zu untermauern. Die Kundenerfahrung wurde erfasst und mit den Bereitstellungsdaten abgeglichen. Mehr als 8,1 Millionen Feedbackprofile von Kunden wurden hinsichtlich ihrer Erfahrung analysiert, mit den IT-Umgebungen korreliert und in die Studie aufgenommen. Durch die Nutzung einer großen Menge von Kunden- und empirischen Branchendaten lässt sich ein genaueres Verständnis des realen Verhaltens gewinnen. Die Daten aus diesen Systemen wurden verwendet, um eine aussagekräftige Sicht auf aktuelle operative Herausforderungen und Vorteile zu gewinnen. Das gemeldete Verhalten der Systeme wurde analysiert, um Merkmale der Architektur sowohl aus einer reinen Leistungs- als auch einer Nettogeschäftseffektsperspektive zu isolieren.

Da in einem Teil der Studie die Auswirkungen neuer Technologie auf Gesamtperformance, -kosten und -risiken einer großen Zahl von Unternehmen untersucht werden, wurden mit von Kunden bereitgestellten Daten detaillierte Betriebsemlationen ausgeführt. Im Rahmen dieser Emulationen wurde die virtuelle Umgebung für diese Unternehmen in einem Zeitraum von 14 Monaten täglich trainiert. Die Ergebnisse dieser Übung sind in die in diesem Dokument vorgestellten Ergebnisse eingeflossen.

In Situationen, wie sie in dieser Studie dargestellt werden, nutzt SIL eine Methode, die die Erfassung von Betriebsdaten umfasst, einschließlich Systemaktivitätsdaten in einem sehr detaillierten Rahmen. Wir weisen darauf hin, dass alle Daten der Produktionsplattformen von den Kunden bereitgestellt wurden. Es ist wichtig festzuhalten, dass keine Daten mithilfe künstlicher Benchmarks oder konstruierter Tests erfasst wurden. Der Nutzen dieser Studie ergibt sich aus einem Verständnis des tatsächlichen operativen Prozesses in einem Unternehmen anstatt der aktuellen Wahrnehmung der durchgeführten Aufgaben. Deshalb sind die Anpassungen an diesen Standorten repräsentativ für reale Situationen und keine künstlichen Benchmark-Konfigurationen. Der Fokus dieser Analyse lag darauf, die Unterschiede kleinerer Betriebssystem- oder Hardwarevarianten nicht zu sehr zu betonen. Deshalb wurden die verschiedenen Releases und Versionen kombiniert, um die Unterschiede der Architekturen insgesamt zu zeigen. Dadurch ergibt sich ein allgemeineres Bild der Architekturstrategie.

Zur Unterstützung der umfassenden Natur dieser Analyse wurden Daten aus verschiedenen Implementierungen, Branchen, Regionen und von verschiedenen Anbietern erfasst. Bei jeder Erfassung dieser Art gibt es unweigerlich ein paar Überschneidungen, z. B., wenn bei einem Unternehmen mehrere Anbieter vorhanden sind. In solchen Fällen kann die Summe der einzelnen Prozentsätze 100 % übersteigen. Unternehmen mit einer mehrschichtigen Implementierung, wie z. B. mehreren geografischen Standorten oder Branchenklassifizierungen, wurden mit eigenen Untergliederungen ihres Feedbacks für alle Kennzahlen analysiert. Es wurden zusätzliche Filter eingesetzt, um Implementierungen zu eliminieren, die Best Practices deutlich verfehlten. Da die Ausfallraten, die niedrige Leistung und die hohen Kosten, die bei solchen Implementierungen in großem Umfang auftreten, wenig mit der tatsächlich eingesetzten Hardware und Software zu tun haben, wurden diese Projekte aus der Analysebasis der Studie entfernt.

Folgende Branchen waren vertreten: Fertigung (24,17 %), Vertrieb (11,38 %), Gesundheitswesen (7,56 %), Einzelhandel (14,00 %), Finanzwesen (21,91 %), öffentlicher Sektor (7,61 %), Kommunikation (11,47 %) sowie Sonstige (1,89 %).

Auch die geografischen Regionen sind breit gefächert: 41,38 % der Unternehmen, die eine Rückmeldung gaben, stammten aus Nordamerika, 10,61 % aus Süd- und Mittelamerika, 23,68 % aus Europa, 21,23 % aus Asien und dem Pazifischen Raum, 3,04 % aus Afrika und 0,07 % aus anderen Regionen.

Da Strategien und Vorteile oft je nach Unternehmensgröße variieren, hat SIL die Unternehmen weiter unterteilt: in kleine, mittelgroße, große und sehr große Unternehmen. In diese Kategorien fließen sowohl die Zahl der Mitarbeiter als auch der Bruttojahresumsatz der Unternehmen ein. Der Personalbestand multipliziert mit dem Bruttoumsatz bildet eine Kennzahl zur Definition, die in der gesamten Analyse verwendet wird. Nach dieser Definition ist anzunehmen, dass ein kleines Unternehmen weniger als 100 Mitarbeiter und einen Bruttoumsatz unter 20 Millionen \$ hat. Das entspricht einem Wert von 2.000 – 100 (Mitarbeiter) mal 20 (Millionen Dollar Bruttoumsatz). Ein Unternehmen mit 50 Mitarbeitern und einem Bruttoumsatz von 40 Millionen \$ würde die gleiche Größenbewertung erhalten und in der Analyse mit dem ersten Unternehmen gruppiert werden. Die Klassifikationen von SIL haben Schwellenwerte von 2.000 (klein), 10.000 (mittel), 100.000 (groß) und 1.000.000 (sehr groß).

Die Informationen in dieser Studie wurden im Rahmen der fortlaufenden Datenerfassung und Systemunterstützung gesammelt, an der SIL seit 1978 beteiligt ist. Alle Tests an SIL-Kundenstandorten wurden von Kundenmitarbeitern durchgeführt.

Die Ergebnisse der Tests wurden über die normalen, sicheren Datenerfassungspunkte an SIL gesendet, die von diesen Kunden seit der Initiierung ihrer SIL-Geschäftsbeziehung verwendet werden. Nach dem Empfang der Informationen am sicheren Datenpunkt wurden die Daten mit der standardmäßigen SIL AI-Verarbeitung in ein Standardformat umgewandelt und alle detaillierten Kundenreferenzen entfernt. Diese bereinigten Daten dienen dann als Input für die Analyse und Ergebnisse.

---

## **MARKENHINWEISE UND HAFTUNGSAUSSCHLÜSSE**

---

IBM, IBM LinuxONE, LinuxONE, IBM Z und z Systems sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und anderen Ländern.

Weitere Unternehmens-, Produkt- und Servicenamen können Marken anderer Hersteller/Anbieter sein.

Die Erstellung dieses Dokuments wurde von IBM finanziert. Wenn in diesem Dokument öffentlich verfügbares Material anderer Hersteller (inklusive IBM) verwendet wird, bedeutet dies nicht, dass das Material die Positionen dieser Hersteller hinsichtlich der in diesem Dokument genannten Probleme widerspiegelt.