

Physische Sicherheit in der Cloud-Ära

Datengestützte Einblicke in die Cloud-Strategie,
-Governance und -Bereitstellung

Erkenntnisse aus der Umfrage zur Lage der physischen Sicherheit 2026





Inhaltsverzeichnis

Kapitel 1	
Mehrere Wege führen zur Enterprise-Cloud	4
Kapitel 2	
Der Cloud-Einsatz ist keine Präferenz, sondern eine Strategie	5
Kapitel 3	
Auf Enterprise-Niveau ist Vertrauen wichtiger als Komfort	6
Kapitel 4	
Langlebigkeit ist für Großunternehmen wichtiger als Disruption	8

„Die Entscheidung zugunsten der Cloud-Nutzung für physische Sicherheitsanwendungen wurde durch die Skalierbarkeits- und Flexibilitätsanforderungen bestimmt. So können wir unsere Ressourcen erweitern, ohne in hohem Maße in die lokale Infrastruktur investieren zu müssen.“

– Befragter aus dem Bereich IT bei einem Einzelhandelsunternehmen, Brasilien (insgesamt 1.001 bis 10.000 Mitarbeiter), Bestandskunde von Genetec



Mehrere Wege führen zur Enterprise-Cloud

Größe verändert alles. Große Unternehmen und Organisationen müssen Hunderte von Standorten, lange Technologie-Lebenszyklen, strenge Vorschriften und eine langfristige Rechenschaftspflicht ständig im Blick behalten. Dies geht weit über die Einführungsphase hinaus. Was bei einem Unternehmen mit 50 Mitarbeitern funktioniert, eignet sich nicht unbedingt auch für ein Unternehmen mit 10.000 Beschäftigten. Die Realität zeigt, dass die Optimierung der physischen Sicherheit in der Cloud für Enterprise-Umgebungen kein einfacher Schritt ist.

Das Fazit? Die Einführung der Cloud ist kein Wettlauf, an dessen Ende ein einziges Ziel steht. Großunternehmen müssen individuelle Komplexität bewältigen, entwickeln sich in unterschiedlichem Tempo weiter und müssen laufend ihrer Rechenschaftspflicht nachkommen.

Daten aus der Genetec Umfrage zur Lage der physischen Sicherheit bestätigen diesen Eindruck. Große Unternehmen möchten sich nicht auf ein bestimmtes Bereitstellungsmodell festlegen. Sie wollen Systeme, die Überwachung, Resilienz und langfristige Kontrolle unterstützen und dabei so flexibel sind, dass sie den dynamischen Anforderungen gerecht zu werden.

Für diese Unternehmen ist die Cloud ein Betriebsmodell zur Koordinierung und Weiterentwicklung komplexer Umgebungen in großem Maßstab. Sie dient nicht als Ersatz für lokale Systeme.



WICHTIGE ERKENNTNISSE

Große Unternehmen setzen mehrere physische Sicherheitsmodelle parallel ein.

Bei Entscheidungen zum Cloud-Einsatz legen Unternehmen mehr Wert auf Kontrolle, Cybersicherheit und langfristiges Vertrauen als auf Geschwindigkeit oder Einfachheit.

Hybrid- und On-Prem-Bereitstellungen bestehen auf Enterprise-Niveau fort und stellen keine Übergangsphase dar.

Der Cloud-Einsatz ist keine Präferenz, sondern eine Strategie

Es gibt kein einheitliches Konzept für die physische Sicherheit in großen Unternehmen. Befragungen in Unternehmen mit mehr als 1.000 Mitarbeitern haben ergeben, dass unterschiedliche Bereitstellungsmodelle weiterhin benötigt werden. Mit der Cloud vernetzte und hybride Konfigurationen werden immer mehr zur Normalität. Doch On-Prem-Systeme haben nach wie vor Bestand – selbst in Unternehmen mit eindeutigen, langfristigen Cloud-Plänen.

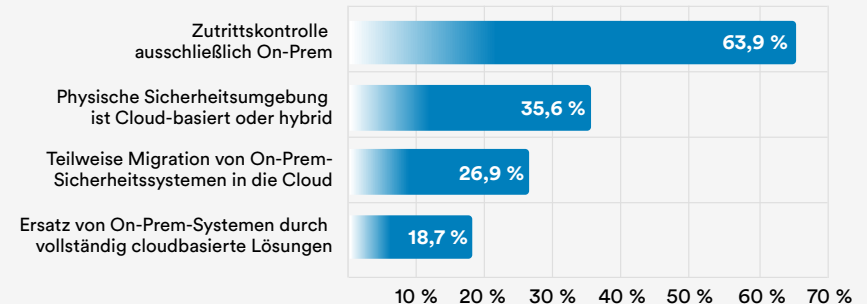
Ein Trend zur Zusammenführung dieser Systeme lässt sich aus den Daten nicht ablesen. Vielmehr deuten sie auf einen Fortbestand der verschiedenen Bereitstellungsmodelle hin. Dies lässt vermuten, dass Enterprise-Umgebungen bewusst modernisiert werden. Dabei wird die Einführung neuer Funktionen und Möglichkeiten auf der einen Seite gegen bestehende Investitionen und Budgets, behördliche Anforderungen sowie die Notwendigkeit langfristiger Betriebskontinuität auf der anderen Seite abgewogen.

Eine wesentliche Erkenntnis daraus ist, dass gemischte Umgebungen nicht etwa mit Unentschlossenheit zu tun haben. Sie spiegeln Unternehmensentscheidungen wider, die von komplexen Anforderungen und Einschränkungen geprägt sind. Diese variieren je nach Unternehmen:

- 26,9 % der befragten Unternehmen verlagern ihre lokalen Systeme teilweise in die Cloud.
- Weitere 18,7 % ersetzen lokale Systeme vollständig durch cloudbasierte.

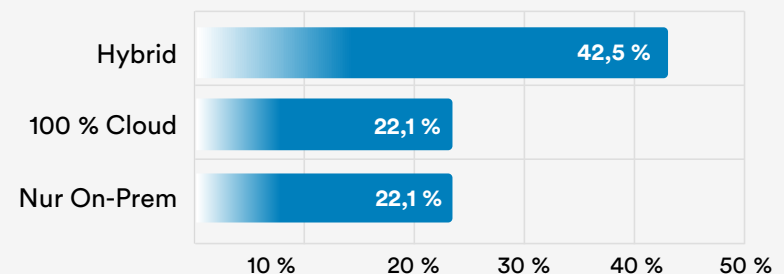
Vielfältige Bereitstellungsmodelle sind kein Kollateralschaden des Wachstums, sondern ein wesentliches Merkmal von Enterprise-Umgebungen. Physische Sicherheitssysteme müssen dem laufenden technologischen Wandel gewachsen sein und gleichzeitig Erweiterungen, Audits und veränderten Vorschriften standhalten. Diese Art von Langlebigkeit erfordert keine Einheitlichkeit, sondern Flexibilität.

Cloud-basierte und hybride Bereitstellungen auf Enterprise-Ebene*: aktuelles Lagebild



DIE CLOUD NIMMT IM BEREICH DER PHYSISCHEN UNTERNEHMENSSECURITY AN BEDEUTUNG ZU, DOCH ON-PREM-SYSTEME, INSBESONDERE BEI DER ZUTRITTSKONTROLLE, SIND WEITERHIN FEST ETABLIERT.

Cloud-Ziele für die nächsten fünf Jahre in Unternehmen*



LANGFRISTIGE CLOUD-STRATEGIEN IN UNTERNEHMEN: FLEXIBILITÄT HAT VORRANG VOR EINER FESTGELEGTEN, INDIVIDUELLEN BEREITSTELLUNG.

*Nur Befragte in großen Unternehmen (mehr als 1.000 Beschäftigte)

Auf Enterprise-Ebene ist Vertrauen wichtiger als Komfort

Auf Enterprise-Niveau spiegeln Cloud-Entscheidungen die unternehmerische Verantwortung wider und nicht etwa individuelle Präferenzen.

Wenn in Großunternehmen über die Cloud nachgedacht wird, geht es am Anfang um das Thema Governance. Die Entscheidungsträger verknüpfen Cloud-Entscheidungen eher mit Cybersicherheit, Compliance und IT-Anforderungen. In kleineren Umgebungen spielen Komfort und Outsourcing eine größere Rolle.

Cloud-Entscheidungen in großen Unternehmen fallen selten im Alleingang. Diese Entscheidungen werden von IT-, Sicherheits- und Führungsteams geprägt, deren Mitglieder auch noch weit nach der Bereitstellung in Verantwortung sind. Diese Denkweise, bei der die Governance im Vordergrund steht, zeigt sich deutlich in den vorliegenden Daten. Auf die Frage, welche Faktoren ihre Cloud-Einführung vorantreiben, nennen kleinere Unternehmen das Outsourcing-Potenzial an zweiter Stelle. Bei Großunternehmen steht dieser Faktor an sechster Stelle – ein Beleg dafür, dass ihnen Kontrolle und Aufsicht wichtiger ist als Komfort.



Das sagen die Zahlen aus

26,7 %

der Befragten in Großunternehmen gaben an, dass sich die Cloud-Einführung aufgrund der behördlichen Aufsicht verlangsamt hat

42,4 %

wiesen auf die IT-Beteiligung an Kaufentscheidungen in Bezug auf physische Sicherheit hin

41,7 %

gaben an, dass die Zahl der physischen oder cyberspezifischen Vorfälle im vergangenen Jahr zugenommen hat

58,7 %

waren häufiger als zuvor von Phishing- oder Smishing-Angriffen betroffen

Auch die Art der Bedrohungen unterscheidet sich. Social-Engineering-Angriffe sind der zweithäufigste Vorfall in großen Unternehmen (43,5 %). Kleinere Unternehmen gaben häufiger an, dass Geräte für den Netzwerkzugriff gehackt werden (43,8 %).

Bei der Entscheidung im Hinblick auf Hybrid-Cloud-Bereitstellungen legen große Unternehmen mehr Wert auf langfristige Resilienz als auf kurzfristigen Komfort:

✓ Skalierbarkeit

39,3 % der Befragten in
Großunternehmen gegenüber
25,7 % in kleineren Unternehmen

✓ Redundanz

38,1 % der Befragten in
Großunternehmen gegenüber
22,1 % in kleineren Unternehmen

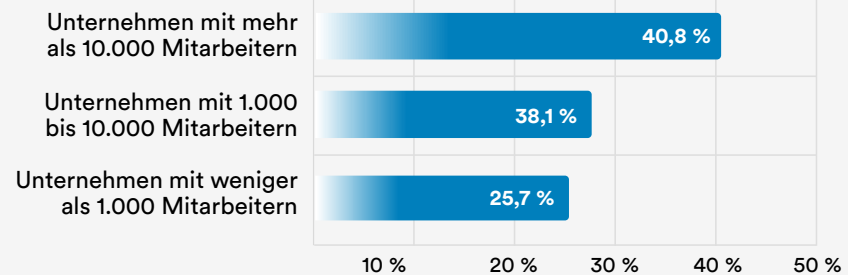
Mit zunehmender Unternehmensgröße dominieren Skalierbarkeit und Redundanz die Entscheidungsfindung. Unternehmen mit mehr als 10.000 Beschäftigten neigen eher zu Hybrid-Cloud-Modellen mit dem Ziel, nachhaltiges Wachstum und Betriebskontinuität in großem Maßstab zu fördern.

WICHTIGE ERKENNTNIS

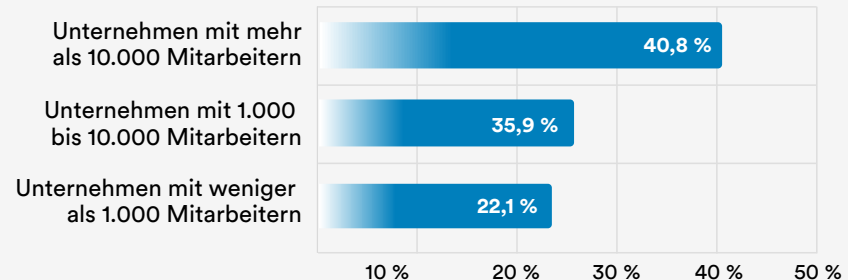
In Großunternehmen geht es bei der Cloud-Einführung weniger darum, wo Systeme ausgeführt werden, als vielmehr um die Sicherstellung von Vertrauen, Resilienz und Kontrolle. Den größten Nutzen bietet die Cloud, wenn sie große Unternehmen dabei unterstützt, über gemischte Umgebungen hinweg zu koordinieren und dabei die Governance sicherzustellen.

Warum sich Großunternehmen für die Hybrid-Cloud entscheiden

Skalierbarkeit



Redundanz



SOWOHL SKALIERBARKEIT ALS AUCH REDUNDANZ STEIGEN MIT DER GRÖSSE DES UNTERNEHMENS STETIG AN. DAS BEDEUTET, DASS GRÖßERE UNTERNEHMEN BEI DER ENTSCHEIDUNG FÜR EINE HYBRID-CLOUD-LÖSUNG MEHR WERT AUF LANGFRISTIGE RESILIENZ LEGEN.

Je größer das Unternehmen, desto stärker geben Skalierbarkeit und Redundanz den Ausschlag zugunsten einer Hybrid-Cloud-Lösung.

Langlebigkeit ist für Großunternehmen wichtiger als Disruption

Umfrageergebnisse zeigen, dass sich große Unternehmen nicht auf ein einziges Cloud-Modell festlegen. Stattdessen konzipieren sie physische Sicherheitsumgebungen, die auf Langlebigkeit angelegt sind sowie regulatorische Änderungen, Wachstum, Cybersicherheitsrisiken und lange Technologie-Lebenszyklen berücksichtigen.

Aus den Daten kristallisieren sich vier Themen heraus:



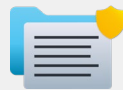
Langlebigkeit ist wichtiger als Einheitlichkeit

Unternehmen entscheiden sich für weiterentwicklungsfähige Architekturen und vermeiden so einschneidende Austauschvorgänge oder eine fragmentierte Kontrolle.



Die Cloud als Betriebsmodell

Der Nutzen entsteht nicht durch die Stilllegung von On-Prem-Systemen, sondern durch Koordination, Transparenz und Kontrolle über Hybrid-Umgebungen hinweg.



Governance und Vertrauen sind wichtiger als Tempo

Cybersicherheit, Compliance und Auditfähigkeit haben Vorrang vor bequemer Bereitstellung oder kurzfristiger Effizienz.



Physische Sicherheitsdaten spielen eine größere Rolle

Aufgrund der immer stärkeren Vernetzung von Systemen erwarten Unternehmen, dass die Sicherheitsplattformen den Kontext, die Integrität und die Rechenschaftspflicht sicherstellen.

Aktuelle Angaben von Befragten in Großunternehmen

37,4 %

nutzen physische Sicherheitsdaten außerhalb des Sicherheitsteams, um die Betriebseffizienz in anderen Unternehmensbereichen zu unterstützen.

26,5 %

betreiben Plattformen für vereinheitlichte Zutrittskontrolle und Videoüberwachung

19,5 %

teilen Metadaten aus Videoanalysen mit anderen Enterprise-Systemen

Diese Muster verstärken sich mit zunehmender Größe des Unternehmens. Da die Anzahl der Standorte, Nutzer und regulatorischen Verpflichtungen wächst, müssen Cloud-Strategien dem betrieblichen Dauerdruck standhalten. Letztlich entscheidet die Governance – und nicht das Bereitstellungsmodell – darüber, ob physische Sicherheitssysteme in Unternehmen dauerhaft zuverlässig funktionieren.

Sind Sie an weiteren Erkenntnissen zu physischer Sicherheit interessiert?

Laden Sie den vollständigen Bericht zur Lage der physischen Sicherheit 2026 herunter.

Den Bericht herunterladen





Genetec Deutschland GmbH
genetec.com/de
salesdach@genetec.com
[@genetec](https://www.genetec.com)