plusserver

Lösungsansätze für Cloud Security

Sichere Digitalisierung mit einer ganzheitlichen Strategie. Erkenntnisse und Maßnahmen aus dem IDC-Whitepaper zur Studie „Datenhoheit in der Cloud”

Management Summary

Die Sicherheit und Integrität von IT-Systemen in Unternehmen wird zunehmend geschäftskritisch. Mit steigendem Digitalisierungsgrad und immer neuen digitalen Geschäftsmodellen wurde Cybersicherheit direkt umsatzrelevant.

„Cybercrime ist längst Teil der weltweiten organisierten Kriminalität und häufig eng mit staatlichen Akteuren uns wenig freundlich gesonnener Länder verknüpft. Eine erfolgreiche Cyberattacke kann die IT eines Unternehmens lahmlegen und damit die gesamte Produktion – und das über Stunden, Tage oder Wochen“, schrieb der Digitalverband Bitkom im August 2023 in einer Pressemeldung zum Cyberlagebild*. Dies unterstreicht die Bedeutung wirksamer Cybersicherheitsmaßnahmen als wesentliche Grundlage der Digitalisierung und verdeutlicht, dass IT-Security Teil jeder Modernisierungsstrategie sein sollte.

Sind aber moderne Cloud-Infrastrukturen automatisch sicherer als die Legacy-IT oder erfordert die Cloud sogar erweiterte Security-Maßnahmen? Das Whitepaper zur IDC-Studie „Datenhoheit in der Cloud - Voraussetzungen, Potenziale und Herausforderungen“ im Auftrag von plusserver zeigt ein ambivalentes Verhältnis der Befragten zur Cloud: Sie sehen diese sowohl als Mittel zur Verbesserung der Cybersicherheit als auch als Herausforderung für die IT-Sicherheit.

Im Folgenden werden daher Lösungsansätze aufgezeigt, wie die IT-Modernisierung in Richtung Cloud sicher gelingt, wenn sie mit den passenden Security-Lösungen Hand in Hand geht. So können Herausforderungen geschickt umschifft und Cloud Security effektiv genutzt werden, um Digitalisierungsziele zu erreichen.

*https://www.bitkom.org/Presse/Presseinformation/Bitkom-und-BKA-zum-Cyberlagebild-2022

plusserver

IT-Sicherheit als Top-Herausforderung

Unternehmen fürchten fehlende Kontrolle in der Cloud

Durch Legacy-IT, heterogen gewachsene IT-Landschaften mit einer Vielzahl an Anwendungen und ggf. verschiedenen Hosting-Varianten herrscht in vielen Unternehmen und öffentlichen Einrichtungen ein wahrer Wildwuchs in der Systemlandschaft. Fachabteilungen nutzen spezielle Anwendungen, die ein im Dunkeln existierendes System von Schatten-IT bilden.

Eine hohe Komplexität, fehlende Übersicht und ein hoher Wartungsaufwand stellen somit für IT-Abteilungen eine große Herausforderung hinsichtlich der IT-Sicherheit dar. Unbekannte Programme, nicht gepatchte Schwachstellen und fehlende Awareness bei den Mitarbeitenden können leicht zum Einfallstor für Angreifer werden.

Gleichzeitig sind sich die von IDC befragten Unternehmen dessen bewusst, dass ein Wechsel in die Cloud nicht all diese Probleme beseitigt. Im Gegenteil: Sie nennen „IT-Sicherheit und Compliance“ als Top-Herausforderung bei der Cloud-Nutzung.

Top-5-Herausforderungen bei der Cloud-Nutzung*

Welche Challenges sehen IT-Verantwortliche in der Cloud?

+ Transparenzverlust
+ Konfigurationsmanagement (Posture Management)
+ Identitätsverlust (Credential-Diebstahl)
+ Complianceverstöße
+ Kompetenzen der Mitarbeitenden
+ Sicherheitsmaßnamen auf dem Stand der Technik

*N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt;
Quelle: IDC-Whitepaper „Datenhoheit in der Cloud”, gesponsert von plusserver, Januar 2023;
F.: Welche Aspekte sind eine Herausforderung bei der Cloud-Nutzung?

Cloud als Stütze der IT-Sicherheit

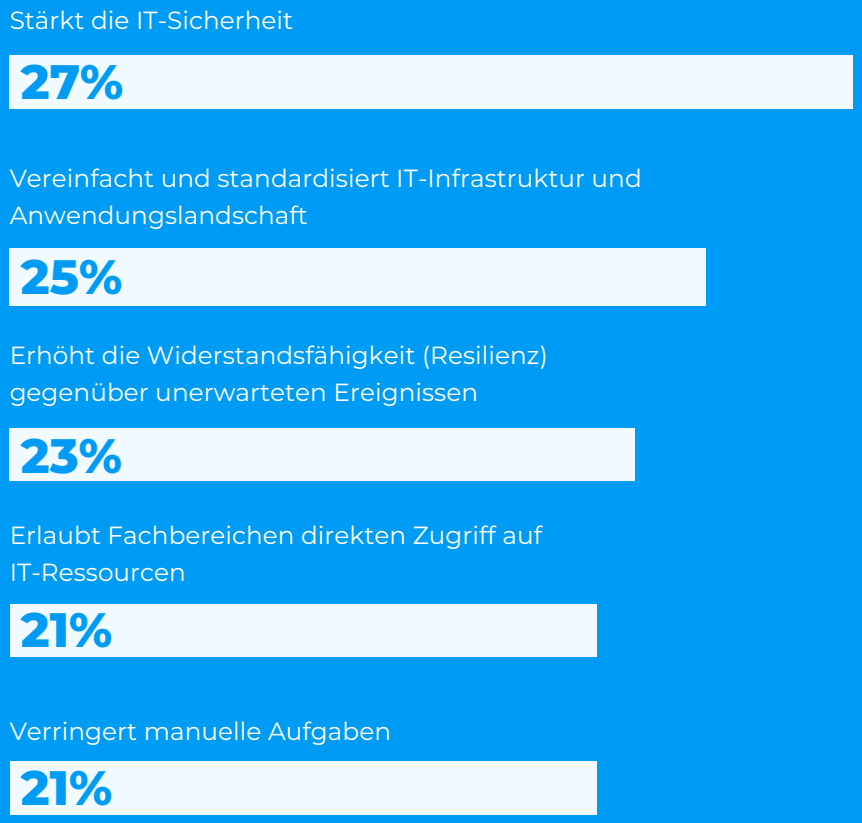
Chancen nutzen statt Herausforderungen scheuen

Zwar betrachten die befragten Unternehmen IT-Sicherheit und Compliance als Herausforderungen, jedoch sehen sie zugleich das hohe Potenzial der Cloud. Auch wenn es darum geht, Sicherheitsthemen zu unterstützen:

+ Externe Rechenzentren sind sehr gut aufgestellt: Sie verwenden moderne Cybersecurity-Tools und bieten eine physische Sicherheit von Hardware und von Daten auf Basis von IT-Industrie-Best-Practices, die die meisten Unternehmen selbst schlichtweg nicht realisieren könnten.
+ Standardisierte Ressourcen in der Cloud erleichtern den IT-Betrieb. Sie vereinfachen die Integration von Lösungen, die Beseitigung von Silos oder die Automatisierung und schaffen Transparenz.
+ Entscheidende sehen Cloud Computing als geeignetes Tool zur Steigerung ihrer Widerstandsfähigkeit (Resilienz).

Top-5-Gründe

für die Nutzung von Cloud Services und Cloud-Technologie*



*N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt; Quelle: IDC, 2023; F.: Welche sind die wichtigsten Gründe für die Nutzung von Cloud Services und Cloud-Technologie?

Cloud als Stütze der IT-Sicherheit

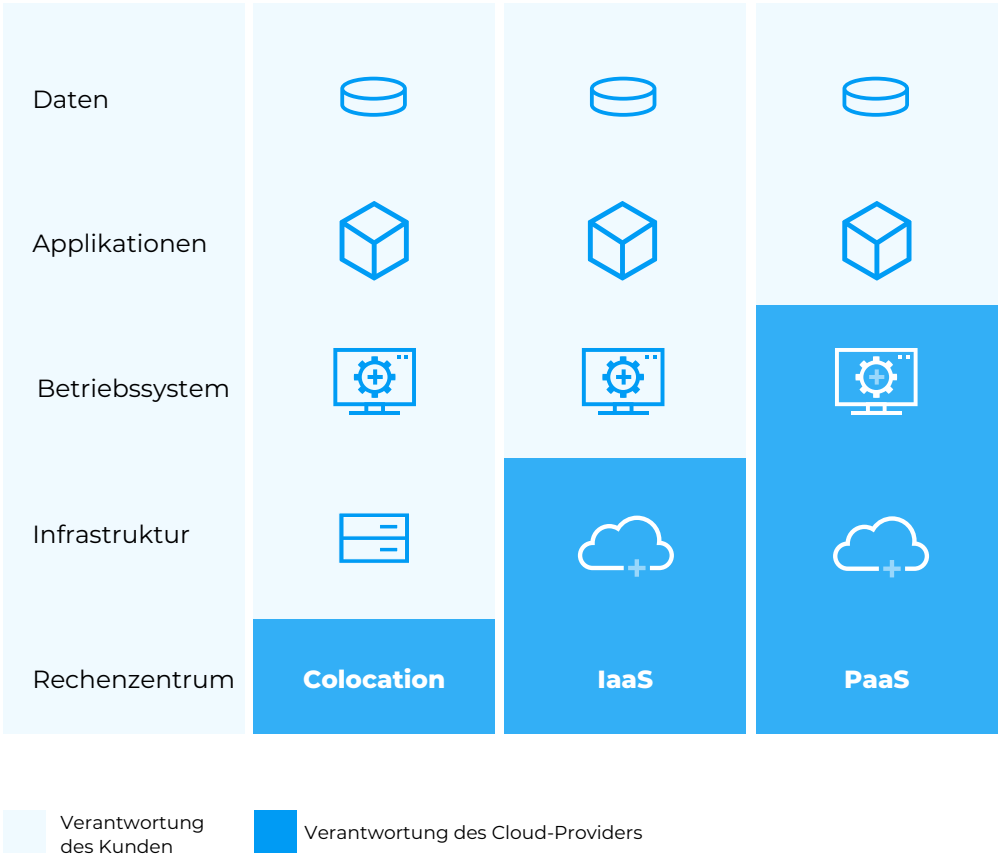
Die Rolle des Cloud Providers

Ein Cloud Provider ist für die Sicherheit und Verfügbarkeit der Cloud-Ressourcen verantwortlich. Somit können Unternehmen im Rahmen einer Cloud-Migration einen Teil der Verantwortlichkeit abtreten. Der Provider kümmert sich bei einem IaaS-Angebot (Infrastructure as a Service) um die zugrunde liegende Infrastruktur inklusive der Anbindung und sorgt für die permanente Verfügbarkeit und Sicherheit. Bei einer sogenannten Platform as a Service (PaaS) übernimmt der Provider zusätzlich das Patching und Updates des Services (z. B. einer Datenbank) und des entsprechenden Betriebssystems.

Für alle anderen Layer, also die eigenen Daten und Applikationen in der Cloud, ist der Kunde selbst verantwortlich. Durch die Zubuchung von Managed Services lässt sich diese Verantwortung allerdings im gewünschten Maß an den Cloud Provider abtreten. Wer dies beachtet und eine entsprechende Strategie erarbeitet, vermeidet Überraschungen und kann sich beruhigt auf die Transformation seines Geschäfts konzentrieren.

Geteilte Verantwortung – wofür sind Cloud-Kunden zuständig?

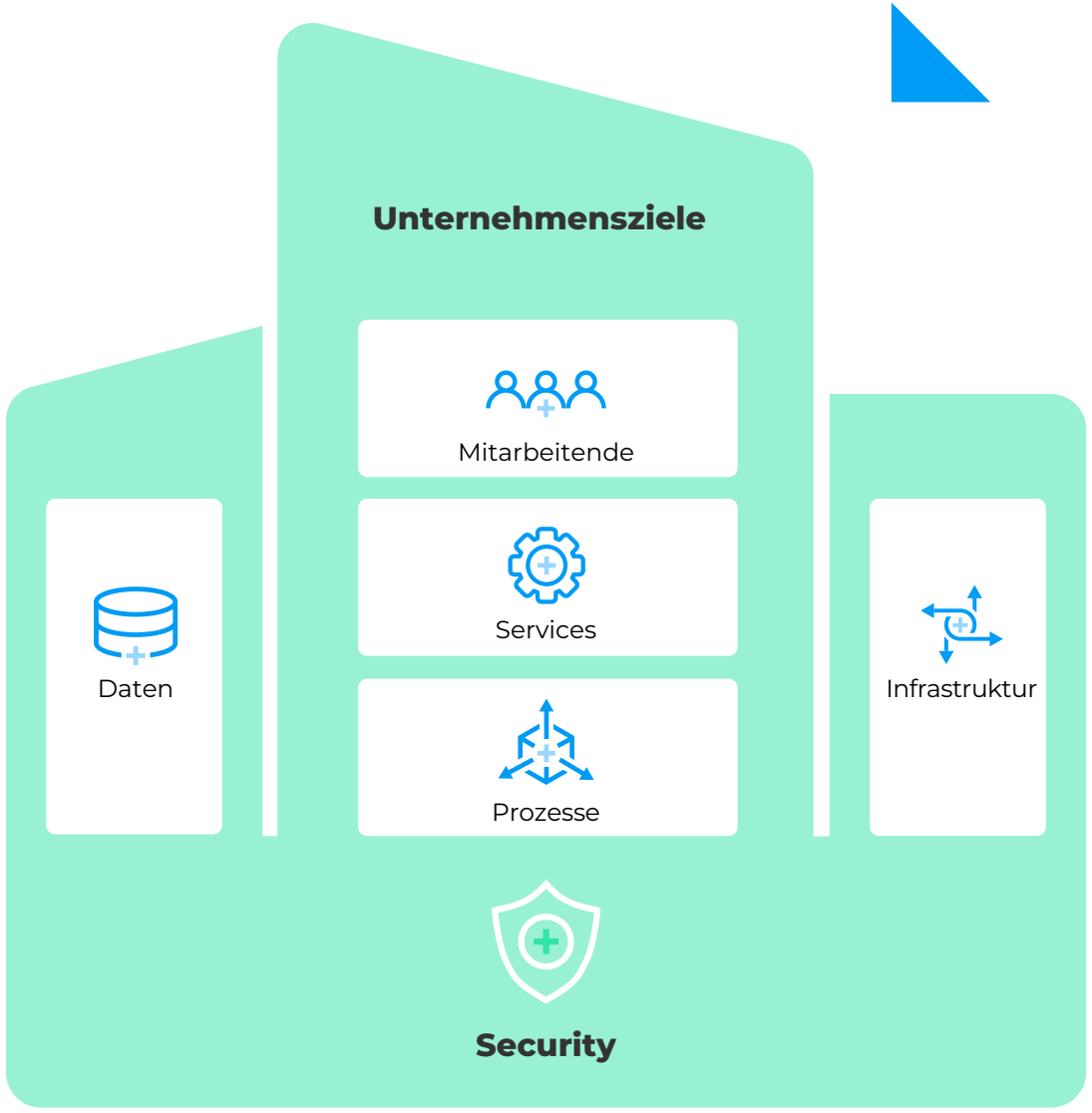
+ Sicherheit und Compliance der Daten in der Cloud
+ Management der Kunden-Anwendungen, Identitäten und Berechtigungen (IAM)
+ Verwaltung von Betriebssystemen und Sicherheitssystemen wie Firewalls
+ Netzwerkmanagement und -sicherheit
+ Verschlüsselung auf Kundenseite
+ Sicherheit, Identitäten und Berechtigungen auf Kundenseite



plusserver

IT-Strategie ist ein Haus, IT-Sicherheit der Mörtel

IT-Sicherheit betrifft das gesamte „Haus der IT“ – jede Etage, jeder Pfeiler muss geschützt sein. Bei Veränderungen innerhalb des Hauses müssen Security-Maßnahmen neu bewertet und angepasst werden.



Cybersecurity ist geschäftskritisch

Sie sollte als Transformationstreiber gesehen werden, nicht als Costcenter

*„**23 Prozent** der Befragten nutzen ein Security Operations Center (SOC), um Cybersecurity Incidents auf Basis aktueller Informationen zu lösen.“*
IDC

Als Verantwortliche:r im Unternehmen benötigen Sie heutzutage eine übergreifende Security-Architektur. Denn Sicherheit mit der Cloud ist nicht nur „Cloud Security“, sondern funktioniert immer nur „hybrid“ über alle Schichten hinweg. Dieses architekturale Denken hilft Ihnen dabei, Lücken zu finden und zu bewerten: Welche Absicherungslücken sollte ich zuerst schließen? Unternehmen benötigen eine Sicherheitslandschaft, die sowohl Cloud-Lösungen als auch bisherige Datacenter-Lösungen und Endgeräte einheitlich und auf das Unternehmensrisiko angepasst absichert.

Zum Beispiel: Welche bestehenden Sicherheitskonzepte kann ich aus meinem Datacenter in die Cloud erweitern? Dieses Denken zieht sich vom Endgerät über die eigenen Rechenzentren und die Cloud bis hin zu übergeordneten Schichten. Dazu gehören regulatorische Vorgaben und übergreifende Absicherungen wie Access Management und Security Operations Center.

Wer kein SOC nutzt, könnte in den kommenden Jahren Schwierigkeiten bekommen. Denn hinter einem SOC steht nicht nur die Technologie, sondern auch das Personal, Know-how und die Regelwerke, die insbesondere der Mittelstand selbst kaum gleichwertig abbilden kann.

Daniel Graßer
Senior Director of Security Services, plusserver

plusserver

Entwicklung einer Cloud-Security-Strategie

Bestandteile Ihres Security-Lifecycles im Kontext der Digitalisierung

Unabhängig von Ihrem aktuellen Digitalisierungsziel sind bei jedem Projekt eine Reihe grundlegender Sicherheitsaspekte zu berücksichtigen. Die folgenden Schritte sollten daher als Lebenszyklus verstanden und für jede IT-Infrastruktur wiederholt werden, die Sie modernisieren möchten.

Zieldefinition der Digitalisierungs-strategie

+ Was soll digitalisiert werden?
+ Welcher Weg führt dorthin?
+ Erfolgs- und Abnahmekriterien

Identifikation der sicherheitsrelevanten Anforderungen

+ Regulatorische Vorgaben
+ Schutz (geschäfts-) kritischer Daten
+ Organisatorische Veränderungen
+ Absicherung der bestehenden und Ziel-Technologien

Analyse der Bestands-architektur zur Festellung der sicherheitsrelevanten Aspekte

Technologie
+ Anwendungen
+ Infrastruktur

Daten
+ kritisch
+ nicht kritisch

Organisation
+ Personal
+ Prozesse

Umsetzung der Security-Strategie über die Infrastruktur hinweg

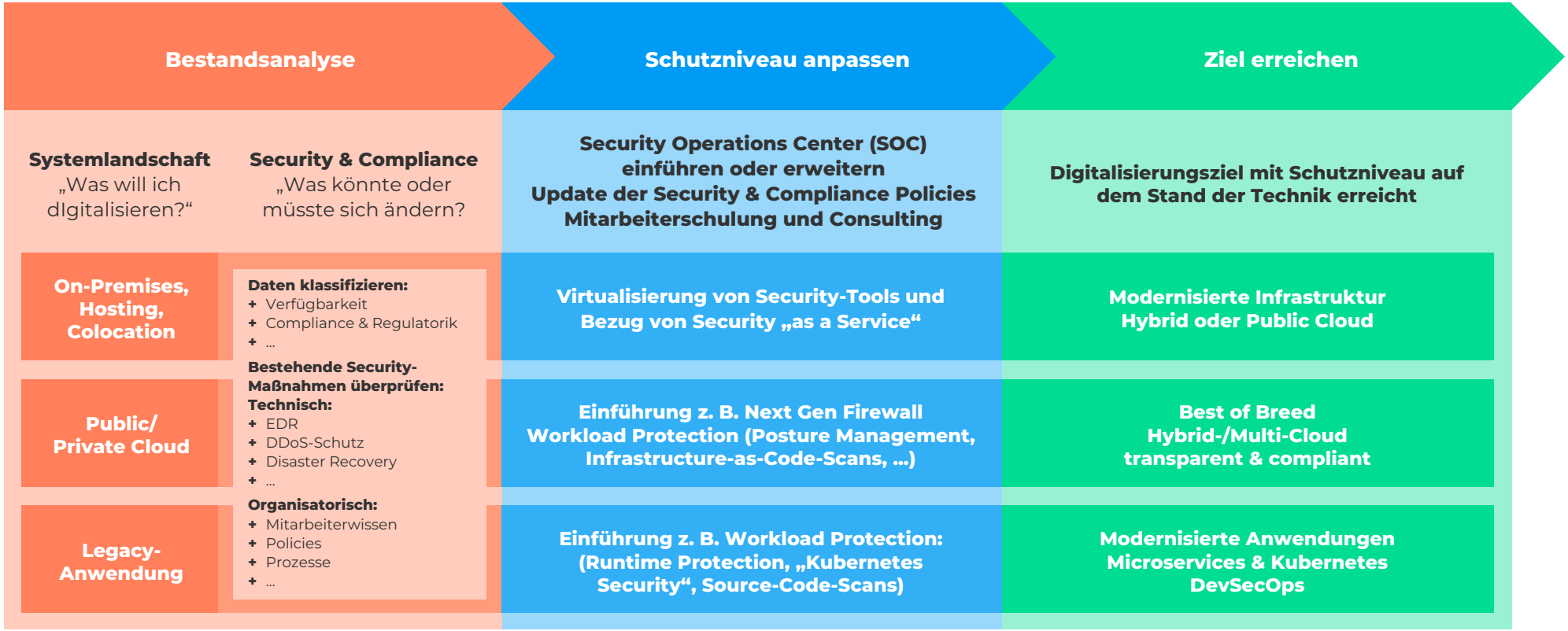
+ Risikomanagement (zur Sicherstellung der Geschäftsziele)
+ Maßnahmen zur Absicherung des Geschäftsbetriebes
  – IT-Governance (Zertifizierung)
  – Technische Lösungen
  – Organisatiorische Maßnahmen

plusserver

Digitalisierungsziele sicher erreichen

IT-Transformation und Security-Strategie gehen Hand in Hand

Die Modernisierung und Transformation der IT erfolgt idealerweise in Teilschritten. Viele Organisationen starten mit einer klassischen IT-Infrastruktur im Eigenbetrieb und gehen zunächst den Schritt in die Public Cloud oder in ein hybrides Szenario. Andere sind auf ihrer Cloud Journey schon weiter fortgeschritten. Hier finden Sie die wichtigsten Sicherheitsmaßnahmen, die – ausgehend vom jeweiligen Ist-Zustand – begleitend zu den einzelnen Transformationsschritten umgesetzt werden sollten.



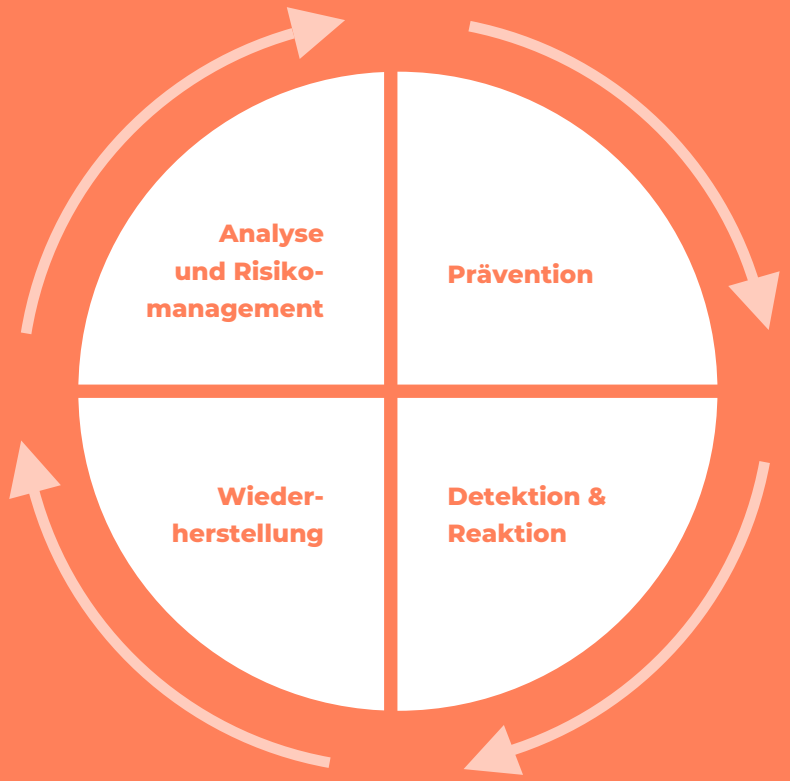
plusserver

Cloud Security als Prozess etablieren

Ein umfassender Security-Ansatz deckt immer den gesamten Security Lifecycle von Prevention bis Disaster Recovery ab. Er muss als Prozess und nicht als Technologie betrachtet und risikobasiert etabliert werden, denn es geht um die Absicherung der verschiedenen Workloads. Datenschutz, Datensicherheit und Datenhoheit sind hier wichtige Elemente, grundsätzlich müssen aber auch weitere Security-Aspekte betrachtet werden.“
IDC

+ Risikomanagement
+ Cloud- und Security-Reifegrad-Assessments

+ Risikobasierte Cloud-Security-Maßnahmen



+ Disaster Recovery ermöglicht Business Continuity

+ 24/7 Monitoring der Infrastruktur auf sicherheitsrelevante Ereignisse

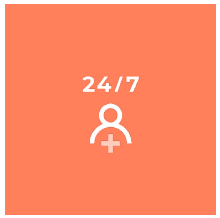
plusserver

Cloud Security mit plusserver

360° Security, die mit Ihrer IT-Modernisierung Schritt hält

plusserver begleitet Sie ganzheitlich bei Ihrer IT-Modernisierung und Security-Strategie in der Cloud und greift dabei auf ein breites Partner-Ökosystem zurück. Einen Überblick über das Leistungsangebot erhalten Sie auf der folgenden Seite.

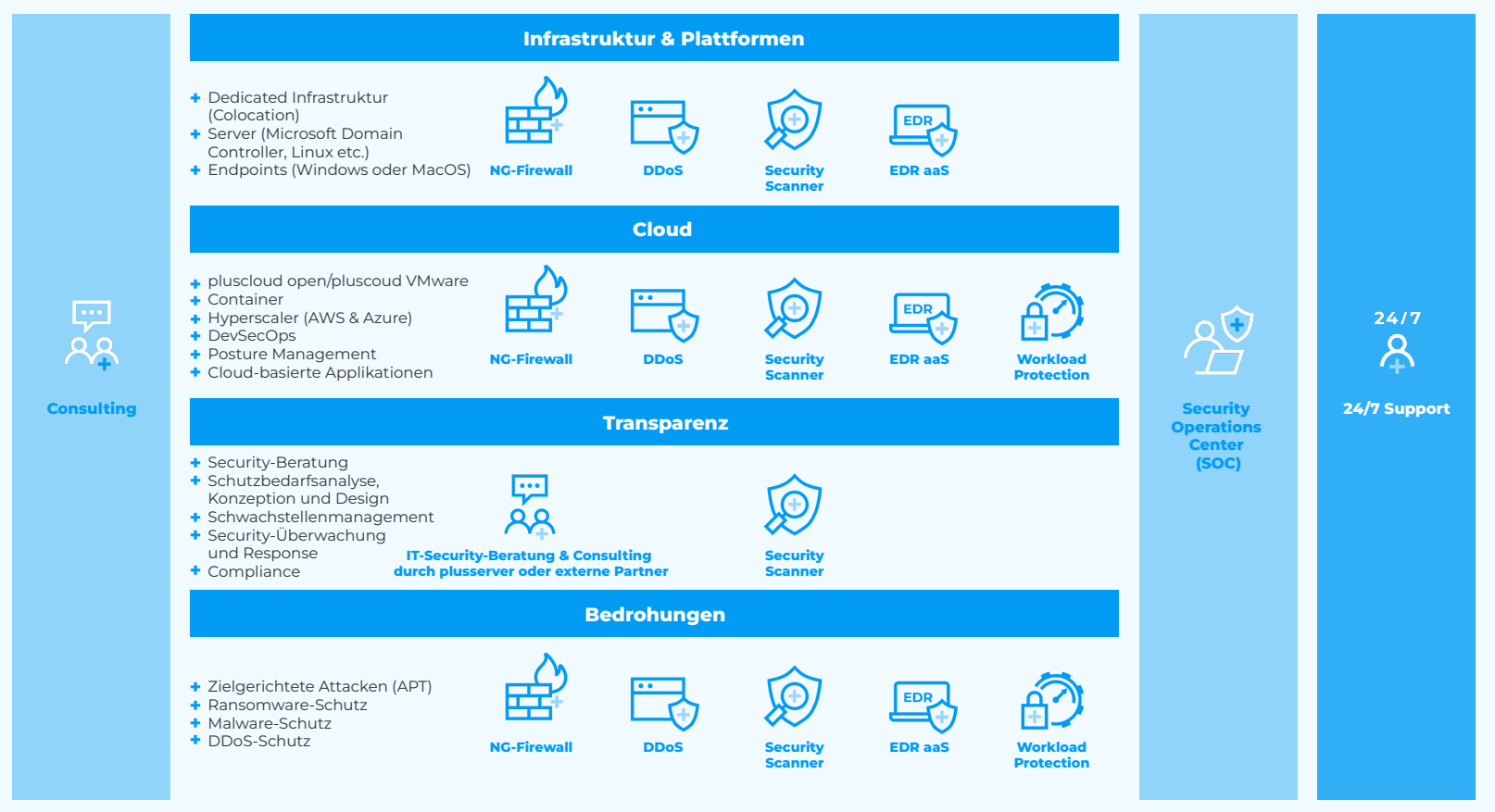
- Auf Wunsch kann plusserver die Security-Strategie der Kunden durch ein umfassendes Consulting begleiten.
- Das Angebot an Security-Lösungen wird kontinuierlich erweitert und deckt bereits die wichtigsten Anforderungen an Cloud Security auf dem Stand der Technik ab.
- Besonders hervorzuheben ist die Möglichkeit, eingehende Meldungen der eingesetzten Sicherheitslösungen rund um die Uhr durch das Security Operations Center auswerten zu lassen und so frühzeitig und adäquat zu reagieren.
- Auch der plusserver-Support ist 24/7 erreichbar, um die Verfügbarkeit der Sicherheitslösungen zu gewährleisten und bei technischen Fragen zu unterstützen.



plusserver

Cloud Security mit plusserver

360° Security, die mit Ihrer IT-Modernisierung Schritt hält



> *Die Beherrschung der Security-Komplexität ist die größte Herausforderung und der Fachkräftemangel ist eine akute Bedrohung für den Betrieb der Security-Lösungen sowie für präventive Maßnahmen.“*
> **IDC**

Gleichen Sie fehlende Security-Fachkräfte aus

Managed Services aus der Cloud

Viele Unternehmen versprechen sich von Cloud Services eine Entlastung im täglichen Betrieb, wie auch die IDC-Umfrage zeigt. Die Cloud ermöglicht einerseits die Reduzierung manueller Aufgaben, indem Vorgänge automatisiert werden. Zusätzlich kann der Cloud Provider durch Managed Cloud Services genau dort unterstützen, wo die interne IT Verantwortung abgeben kann und muss.

Dies lässt sich auch auf das Thema Security übertragen. Denn bei „As a Service“-Lösungen aus der Cloud muss sich das eigene IT-Team weder um die Installation noch um den Betrieb kümmern.

So sind beispielsweise beim EDR-Angebot (Endpoint Detection & Response) von plusserver zahlreiche Erleichterungen inklusive. Im Rahmen eines Full-Managed Services kümmert sich der Provider neben dem Regelwerks- und Changemanagement auch um das Patchmanagement, Wartung, Alarmierung, Reporting etc.

Das Angebot SOC as a Service ermöglicht es Organisationen, ein Höchstmaß an Transparenz und Reaktionsfähigkeit zu erzielen, ohne eigene Spezialist:innen zu beschäftigen. Das Analysten-Team sowie das SIEM (Security Information & Event Management) stellt plusserver zentral für seine Kunden bereit. So wird State-of-the-Art Security für eine Vielzahl an Firmen und öffentlichen Einrichtungen zugänglich.

Zudem sorgen Onboardings bei den plusserver-Produkten dafür, dass Unternehmen auch ohne eigene Security-Expert:innen schnell und erfolgreich mit den Lösungen arbeiten können.

Service-Level für Managed Cloud bei plusserver

Self-Service

+ Sie behalten die Administrationsrechte – wir sorgen für einen zuverlässigen Betrieb Ihrer Hardware und beheben Störungen an Ihrer Netzinfrastruktur.

Operational Service

+ Wir teilen die Administrationsrechte mit Ihnen und unterstützen Sie bei der Serveradministration, beim Patching sowie der Störungsbearbeitung.

Full Management

+ Sie erhalten den jeweiligen Dienst komplett als Service und wir kümmern uns professionell um alle untergeordneten Ebenen.

21%

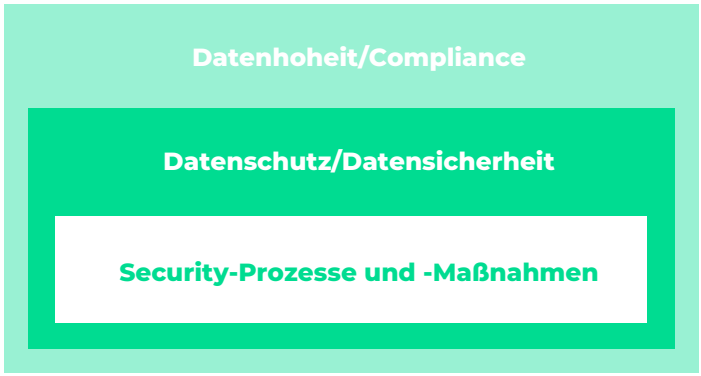
der Befragten sehen die Sicherstellung von Datenhoheit in der Cloud als Top-Herausforderung der Cloud-Nutzung.

Sichern Sie Ihre Datenhoheit

Warum digitale Souveränität und IT-Security zusammen gehören

Während Compliance und Datenhoheit die Grundlage für nachhaltige digitale Geschäftsmodelle sind, erfordern sie ihrerseits eine effektive Cloud-Sicherheitsarchitektur.

Zusätzlich müssen sich Unternehmen beim Wechsel in die Cloud mit Fragen des Datenschutzes (DSGVO) und der Datensicherheit befassen.



Worauf Entscheider:innen hier achten sollten: Einschlägige Zertifizierungen und Testate, wie zum Beispiel nach dem Cloud Computing Compliance Criteria Catalogue (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI), geben Auskunft über das Sicherheitsniveau eines Cloud-Anbieters.

Der Datenstandort und vor allem der Unternehmenssitz geben Auskunft über Fragen des Datenschutzes und der Rechtsraumsouveränität.

plusserver ist ein Anbieter mit Firmensitz in Deutschland und die Kundendaten werden ausschließlich in mehrfach zertifizierten Rechenzentren in Deutschland ge- speichert. Darüber hinaus unterstützen wir die Datenhoheit unserer Kunden, indem wir sie mit ihren digitalen Applikationen nicht an uns binden. Wo immer möglich setzen wir auf Open-Source-Technologien und berechnen keine Traffic-Gebühren – auch nicht bei einer Migration weg von uns.

Einige der Zertifizierungen und Testate von plusserver

TÜV SÜD ISO 9001 · TÜV SÜD ISO 27001 · JAN-2023 PCI DSS compliant · C5 Typ II BSI C5 CLOUD SECURITY · DATENSCHUTZ IDW PH 9.860.1 · Typ II ISAE 3402

plusserver

Erreichen Sie Modernisierungsziele

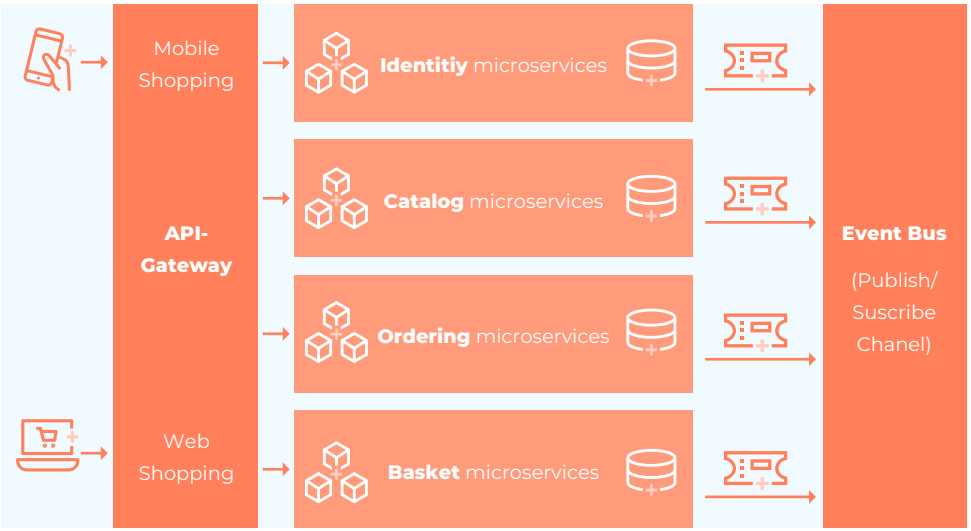
Sicher in Richtung Cloud-native Applikationen

Die Cloud bildet die Basis, um digitale Services schnell und sicher zu entwickeln und stetig an die Bedürfnisse der Kunden anzupassen. Sogenannte Microservices ersetzen dabei die monolithische Bauweise von Applikationen. Jeder Microservice kann für sich weiterentwickelt werden oder auch ausfallen, ohne dass die komplette Anwendung davon betroffen ist. Microservices werden in Containern betrieben und diese mit Kubernetes verwaltet.

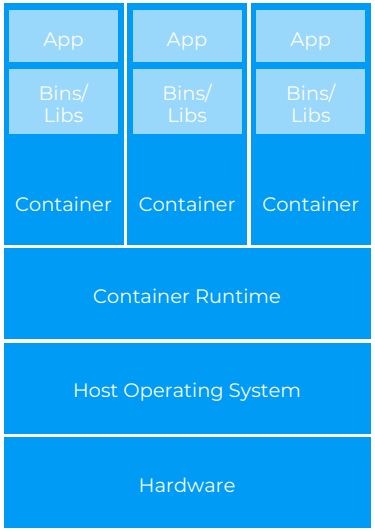
Die Vielzahl an Containern und die schnellen Enwicklungszyklen erfordern eine entsprechende Sicherheitslösung, um Fehler bereits im Code auszuschließen, Konfigurationsprobleme aufzudecken, Verbindungen transparent zu machen und zu überwachen, auffälliges Verhalten frühzeitig zu entdecken und rechtzeitig zu reagieren.

Hier eignet sich eine einfach zu implementierende Workload-Protection-Lösung, wie sie plusserver „as a Service“ anbietet.

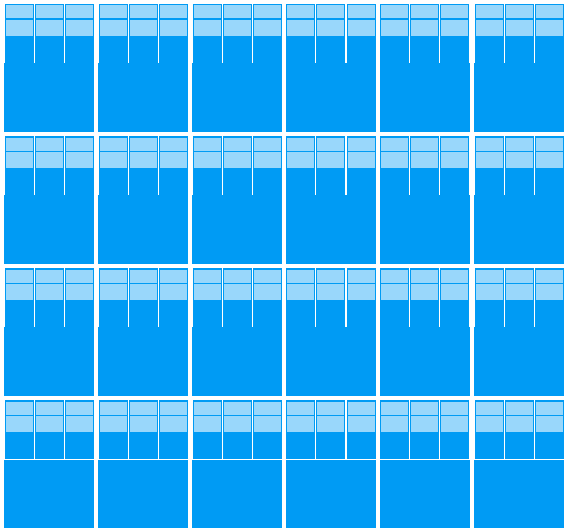
Microservices – am Beispiel eines Webshops



Ein Host mit mehreren Containern



Dutzende Hosts mit hunderten von Containern



plusserver

Lesen Sie das gesamte IDC Whitepaper

„Datenhoheit in der Cloud – Voraussetzungen, Potenzial und Herausforderungen" IDC, Januar 2023

+ Zum IDC Whitepaper

Weitere Executive Insights:

+ IT-Modernisierung

+ Datenhoheit in der Cloud

+ IT-Fachkräftemangel

Über plusserver

Eine zukunftsfähige, sichere und vielseitige Cloud

Wir bieten deutschen Unternehmen eine datensouveräne und anbieterunabhängige Basis für ihre digitalen Geschäftsprozesse. Auf unseren sicheren, skalierbaren Cloud-Plattformen realisieren Kunden zukunftsfähige und kosteneffiziente digitale Anwendungen. Wir beraten unsere Kunden zu Cloud-Architekturen sowie zur Integration bestehender IT-Umgebungen. Dabei agieren wir schnell, dynamisch und stets persönlich.

+ Mehr über plusserver

+ Mehr über Cloud Security

+ Mehr über SOC as a Service

Cloud Security mit plusserver

Profitieren Sie von einer ganzheitlichen Sicht auf IT-Sicherheit, die wir gemeinsam mit unserem Partnernetzwerk ermöglichen. Von Consulting-Leistungen bis hin zur Einbindung Ihrer Tools und Analyse eingehender Meldungen im Security Operations Center. Unser Portfolio erweitern wir kontinuierlich für Sie. Sprechen Sie uns an, um eine Lösung für Ihre individuellen Anforderungen aus einer Hand zu erhalten.

Security Operations Center as a Service

Unser Security Operations Center analysiert Ihre IT-Umgebung gemäß Ihrem Schutzbedarf mit State-of-the-Art-Technologie, schafft Transparenz und erkennt Abhängigkeiten, die auf zielgerichtete Angriffe wie Ransomware oder Malware hinweisen können. So lässt sich die Bedrohungslage in Ihrer Infrastruktur sowie der Cloud gezielter bewerten und passende Gegenmaßnahmen einleiten.