

Die Uhr läuft ab

Supportende für Microsoft Windows Server 2008
und Exchange Server 2010



■ PRAXIS

Microsoft Teams

Wie gelingt der Einstieg?

■ SERVICE

Der sichere zweite Standort

Backup im Rechenzentrum

■ PRODUKTE

Kontrolle im Netzwerk

Aruba ClearPass

Die HP JetIntelligence Technologie sorgt dafür, dass mit einer Tonerkartusche mehr Seiten bedruckt werden können, damit Sie noch erfolgreicher sind.



Reinvent Impact.
Original HP Toner



**Einlegen, losdrucken,
beeindrucken.**

Original HP Tonerkartuschen liefern
konstant hohe Druckqualität.¹



Ausdrucke, die stolz machen.

Mit Original HP Tonerkartuschen
profitieren Sie von herausragender
Druckqualität.



**Entscheidung für den
Umweltschutz.²**

Umweltfreundliches Design von
Original HP Tonerkartuschen für
einfaches Recycling und weniger Abfall.²



keep reinventing



Liebe Leserinnen und Leser,

„Aufgabe von Kunst heute ist es, Chaos in die Ordnung zu bringen.“ – Dieser Satz von Adorno muss in der jetzigen IT-Welt lauten: „Aufgabe eines Netzwerk-Administrators heute ist es, Ordnung ins Chaos zu bringen.“ Und das ist tatsächlich in der Welt von IoT und BYOD eine Kunst: Unser Netzwerk-Profi Kai Lauterbach zeigt Ihnen, wie Sie mit der Zugangssteuerung von Aruba ClearPass auch ganz ohne künstlerisches Talent Herr Ihres Netzwerks werden.

Und wenn wir schon beim Thema Chaos sind: Das Supportende von wichtigen Microsoft-Produkten wie Windows 7 stiftet zurzeit eine Menge Unruhe. Als wäre die technische und organisatorische Herausforderung der Umstellung auf Windows 10 noch nicht groß genug, warten außerdem lizenzrechtliche Fußangeln auf Nutzer von downgegradeten OEM-Versionen. Unser Microsoft-Lizenz-Experte Klaus Stein bringt für Sie Licht ins Dunkel.

Viel Spaß beim Lesen wünscht Ihnen
Ihr

Holger Hansen

■ EDITORIAL/INHALT 3

■ PRAXIS

End of Support bei Microsoft-Produkten:
Alles hat ein Ende ... 4

Windows 10 Pro (OEM) verliert das
Recht zum Downgrade auf Windows 7 Pro 6

■ SERVICE

Sicherheitslücke Drucker: Auch
Großformatdrucker werden zur Zielscheibe 8

Ist Ihre Druckumgebung sicher? 10

■ PRODUKTE UND ANWENDUNGEN

Veeam Cloud Connect Backup im H&G
Rechenzentrum:
Der sichere zweite Standort 11

NetApp HCI: NetApp macht Hyper-
Converged zu Hybrid Cloud Infrastructure 14

Netzwerkzugangssteuerung:
Kein Fischen im Trüben 17

HPE Synergy: Der Einstieg in die
Composable Infrastructure 20

Zusammenarbeiten im Projekt:
Microsoft Teams – was es ist und
was es kann 23

■ KONTAKT 27

IMPRESSUM

Herausgeber:

H&G Hansen & Gieraths
EDV Vertriebs GmbH
Bornheimer Straße 42–52
53111 Bonn

V. i. S. d. P.:

Holger Hansen

Redaktion/Organisation:

Svenja Hansen
svenja.hansen@hug.de

Gina Gimnig

gina.gimnig@hug.de

Anzeigendisposition:

Marianne Orthen-Schneider
marianne.orthen-schneider@hug.de

Erscheinungsweise:

zwei Ausgaben pro Jahr

Satz und Gestaltung:

aligator kommunikation GmbH
Kreuzweidenstraße 17
53604 Bad Honnef

PICOS Grafik GmbH
Hauptstraße 101
53619 Rheinbreitbach

Haftung:

Für den Fall, dass Beiträge oder
Informationen unzutreffend oder
fehlerhaft sind, haftet H&G nur
bei Nachweis grober Fahrläs-
sigkeit.

Nachdruck und elektronische Nutzung:

Beiträge aus diesem Magazin
dürfen nur unter Quellenangabe
veröffentlicht werden.

Bildnachweis:

Vorliegende Bilder und Grafiken
wurden uns vom Hersteller zur
Verfügung gestellt, durch die
Agentur aligator produziert und
bei Anbietern lizenzfreier Bilder
eingekauft.
Adpic/Ingram:
Titel, S. 4, S. 6, S. 14, S. 17,
S. 20, S. 23, Hewlett-Packard
Development Company:
S. 8, S. 9, S. 10, TIM AG: S. 16,
Microsoft: S. 24, S. 26,
macrovector/ Freepik: S. 11

End of Support bei Microsoft-Produkten Alles hat ein Ende ...



„Denke immer an das Ende, da die verlorene Zeit nicht zurückkehrt!“ – dieses Zitat des Augustiner-Chorherren Thomas von Kempen stammt aus dem 15. Jahrhundert und könnte doch kaum aktueller sein, wenn es um das Support-Ende vieler Microsoft-Produkte geht. Viel Zeit, seine Systeme umzustellen, bleibt bei Windows 7, Windows Server 2008/R2 und Microsoft Exchange Server 2010 SP3 nicht mehr. Wer clever ist, macht aus der Not eine Tugend und nutzt den Zwang zu handeln dazu, seine Systeme fit für die Zukunft zu machen.

Den 14.01.2020 sollte mittlerweile jeder Systemintegrator so gut kennen wie seinen Geburtstag. In der letzten Ausgabe der READ:IT haben wir uns bereits dem Ende des Supports für Windows 7 gewidmet und einen Ausblick auf Windows 10 gegeben. Diese Umstellung bringt die meisten Reibungen mit sich, da die Anwender direkt von einer großen und sichtbaren Änderung betroffen sind. Nicht so bei den anderen beiden Kandidaten, die zur gleichen Zeit aus dem Rennen gehen: Windows Server 2008 / R2 sowie Microsoft Exchange Server 2010 SP3. Davon betroffen ist ebenfalls der Small Business Server 2011, der auf diesen Versionen basiert.

Aber wie bei einem Geburtstag gibt es auch bei diesem Abschied etwas zu feiern. IT-Abteilungen auf der ganzen Welt können sich über neues Spielzeug freuen, und wir reden nicht von smarten China-Gadgets, sondern von Technologien der aktuellsten Generation, sei es im Server-, Storage-, Betriebssystem- oder Cloud-Umfeld. Denn oft ist die Hardware, auf der aktuell noch eine Server-2008-/R2-Infrastruktur aufgebaut, nicht viel jünger. Man darf dieses Supportende also als Chance sehen, in eine moderne IT-Landschaft zu investieren und, Achtung Buzzword!, einen „Ritt auf der Welle der Digitalisierung“ zu wagen.

Welche Folgen hat das End of Life (EoL) für Ihr Unternehmen?

Was beide Produkte gemeinsam haben, neben dem End-of-Life (EoL)-Datum: Man wird keinerlei kostenfreie Sicherheitsupdates und keinerlei Support mehr durch Microsoft erhalten und die Compliance ist in

Bezug auf die DSGVO nicht mehr gegeben. Dies macht Ihre IT nicht nur anfälliger für Cyberangriffe, sondern es drohen im Zusammenhang mit der DSGVO auch hohe Strafen bei Verstößen. Microsoft bietet nach wie vor die sogenannten „Extended Security Updates“ für abgekündigte Produkte an. Hier kommen jährliche Kosten in Höhe von 75 % der vollen Lizenzgebühren der neuesten Version auf Sie zu. Auf eine geeignete Alternative kommen wir später nochmal zu sprechen.

Nachfolger von Microsoft Exchange Server 2010

Es besteht die Möglichkeit, auf Exchange 2013, Exchange 2016 sowie, über einen Zwischenschritt, auf Exchange Server 2019 zu migrieren. Exchange 2016 ist bereits einige Jahre auf dem Markt und alle Kinderkrankheiten sind beseitigt. Außerdem begnügt sich Exchange 2016 mit deutlich weniger Ressourcen. Das erweiterte Supportende von Exchange 2016 und Exchange 2019 liegt bei beiden Versionen im Jahr 2025. Im Gegensatz hierzu ist Exchange 2019 ein echter Ressourcenfresser. Bereits in den Mindestanforderungen werden 128 GB RAM verlangt. Hinzu kommt, dass man einen Volume-Licensing-Vertrag benötigt, andernfalls kann Exchange 2019 nicht lizenziert werden.

Exchange 2019 wird also als Enterprise-Produkt in Stellung gebracht. Der Exchange Server 2016 ist weiterhin eine gute Investition für KMU, die keine überdimensionierte Hardware anschaffen wollen. Alternativ steht für KMU die Migration nach Exchange online zur Verfügung. Wagen Sie den Schritt in Richtung Cloud noch nicht oder haben Sie grundsätzliche Bedenken? In dem Fall ist unsere Hosted-Exchange-Lösung aus unserem in Deutschland betriebenen Rechenzentrum eine Option für Sie. Sprechen Sie uns an und wir finden eine passende Lösung für Ihre Anforderungen.

Nachfolger zu Microsoft Server 2008 /R2

Hier bieten sich weitaus mehr Möglichkeiten. Entweder ganz klassisch eine Migration auf den aktuellsten Nachfolger, Server 2019, auf Ihrer eigenen Hardware mit all seinen Vor- und Nachteilen. Bei einer Gegenüberstellung von On-Premise- und

Cloud-Lösungen werden im ersten Augenblick oft die Betriebskosten für einen Serverraum oder ein RZ übersehen und nicht eingerechnet. Alternativ kann man sich dazu entschließen, seine Workloads auszulagern. Hierfür bietet H&G Kapazitäten in seinem Rechenzentrum in verschiedensten Ausbaustufen, angefangen bei einzelnen VMs bis zu kompletten Umgebungen mit Domain Controller, File Server, Exchange und allem, was dazugehört. Zusätzlich stehen Ihnen umfangreiche Leistungen aus unserem Managed-Service-Portfolio (u. a. Patchmanagement, Monitoring und Backup) zur Verfügung.

Letzte Rettung: Azure-Cloud

Welchen Vorteil bietet die Cloud von Microsoft? Für alle, die aufgrund von Abhängigkeiten noch Zeit benötigen, bietet es sich an, ihre Server in die Azure-Cloud zu migrieren. Hier offenbart sich die eingangs erwähnte Alternative zu den kostspieligen „Extended Security Updates“: Microsoft gewährt allen VMs, die in der Azure-Cloud betrieben werden, drei weitere Jahre kostenfreien Support auf ihre Server-2008-/R2-Systeme. Sollten Sie also noch Workloads oder Applikationen im Einsatz haben, die sich nicht vor dem EoL migrieren lassen, ist dies vielleicht die beste Alternative.

Server, die in der Cloud betrieben werden, lassen sich ebenfalls durch einen Managed Service von H&G ergänzen. Weiterhin gilt, sprechen Sie uns an und wir erarbeiten zusammen eine Lösung, die für Sie maßgeschneidert ist. Ob nun konservativ oder zukunftsorientiert, die Entscheidung liegt bei Ihnen.

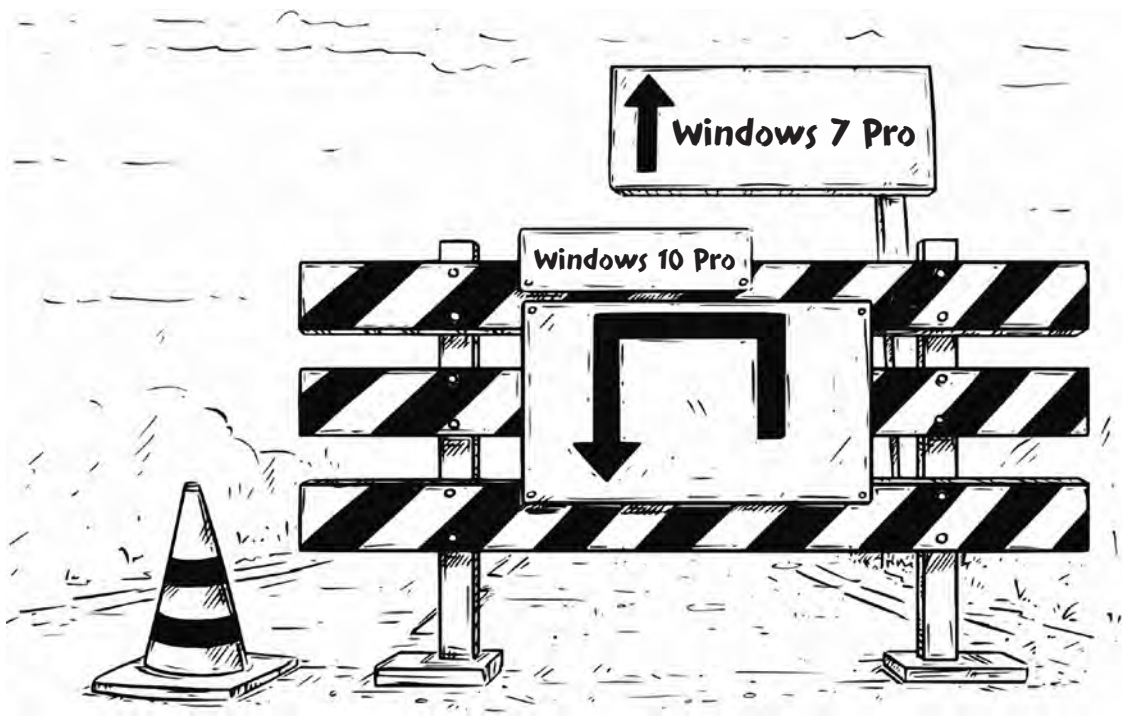


Gold Windows and Devices
Gold Small and Midmarket Cloud Solutions
Silver Cloud Productivity
Gold Datacenter
Silver Collaboration and Content



Ihr Ansprechpartner

Paul Seifert
IT Consulting & Services
Fachbereich IT-Infrastruktur
T +49 228 9080-690
paul.seifert@hug.de



Windows 10 Pro (OEM) verliert das Recht zum Downgrade auf Windows 7 Pro

Mit dem Supportende von Windows 7 Pro am 14.01.2020 ist in vielen Fällen auch das Nutzen des Downgrades von Windows 10 Pro auf Windows 7 Pro nicht mehr zulässig. Entscheidend ist, woher die jeweilige Lizenz stammt.

Keine Zeit, keine Freigabe, Kompatibilitätsprobleme – es gibt viele Gründe, warum Unternehmen noch nicht auf Windows 10 umgestellt haben. Beim Neukauf von Geräten nutzen deshalb viele die Möglichkeit, statt des mitgelieferten Windows 10 Pro auf Windows 7 Pro downzugraden. Das könnte sich jetzt rächen. Wer seine Lizenz über einen OEM-Systembuilder-Kanal bezogen hat, verliert zum 14.01.2020 nicht nur den Support für Windows 7 Pro, sondern gleich auch das Recht, es zu benutzen. Das bedeutet im Klartext: Wer dem nächsten Lizenzaudit standhalten will, muss Windows 7 Pro bis zum 14.01.2020 deinstallieren. Lizenzen, die über einen Volumenlizenzvertrag erworben wurden, sind davon nicht betroffen. Für alle anderen Lizenzen wird es

jetzt höchste Zeit, sich um das Upgrade auf Windows 10 zu kümmern.

Bei Microsoft heißt es konkret in den OEM-Systembuilder-Lizenzbestimmungen unter Punkt 7 (Herabstufungsrechte):

„Wenn Sie ein Gerät von einem Hersteller oder Installer mit einer vorinstallierten Windows Professional-Version erworben haben und diese im Vollfunktionsmodus konfiguriert ist, sind Sie berechtigt, entweder eine Windows 8.1 Pro- oder eine Windows 7 Professional-Version zu nutzen, aber nur solange, wie Microsoft Kundendienst für diese frühere Version erbringt, wie in (aka.ms/windowslifecycle) dargelegt. Dieser Vertrag gilt für Ihre Nutzung der früheren Versionen. Wenn die frühere Version verschiedene Komponenten enthält, gelten Bestimmungen für solche Komponenten im Vertrag der früheren Version für Ihre Nutzung dieser Komponenten. Weder der Hersteller oder Installer noch Microsoft sind verpflichtet, Ihnen frühere Versionen zu liefern. Sie müssen die frühere Version separat erlangen, für die Sie eventuell eine Gebühr entrichten.“

Welche Windows-7-Pro-Lizenzen dürfen weiterbenutzt werden?

- Windows-7-/8.1-/10-Pro-Lizenzen, die über einen Volumenlizenzvertrag erworben wurden
- Windows-7-Pro-OEM-/Systembuilder-Lizenzen, die nicht als Downgrade über Windows 10 Pro bezogen wurden
- Lizenzen, für die Windows-7-ESU-Lizenzen (Extended Security Updates) gekauft werden (grüner Kasten unten)

Wichtig: Mit Ausnahme der ESU-Lizenzen (grüner Kasten unten) gilt auch für die oben genannten Lizenzen, dass Microsoft ab dem 14.01.2020 keinen Support mehr anbietet. Es ist lediglich lizenzrechtlich zulässig, diese Versionen weiter zu nutzen.

Vom Downgrade zurück zu Windows 10 Pro – wie geht das?

Unangetastet vom Erlöschen des Downgrade-Rechts bleibt die Lizenz für die ursprünglich erworbene Version. Das heißt, betroffene Windows-7-Pro-Nutzer besitzen nach wie vor eine gültige Windows-10-Pro-Lizenz, die sie jetzt wieder aktivieren müssen. Dazu lässt sich mit dem Media-Creation-Tool (MCT) eine Neuinstallation oder ein Inplace-Upgrade durchführen. Beim Inplace-Upgrade wird automatisch der im BIOS vorhandene Key für die Aktivierung von Windows 10 Pro genutzt. Das Media-Creation-Tool kann kostenlos bei Microsoft heruntergeladen werden (QR-Codes unten rechts). Diese Methode muss für jeden Rechner einzeln ausgeführt werden.



Soll das Deployment zentral erfolgen, zum Beispiel mit SCCM oder WDS, wird ein Volumenlizenzmedium benötigt. Das MCT-Image funktioniert in diesem Fall nicht. Das heißt, wenigstens eine Lizenz muss über einen Open-Vertrag erworben werden und dieser so lange bestehen, wie diese Deployment-Methode genutzt wird.

Zu allen Fragen rund um die Lizenzierung von Microsoft ist Klaus Stein Ihr Ansprechpartner. Gern hilft Ihnen Jörg Laufer weiter, wenn es darum geht, erfolgreich zu Windows 10 zu migrieren, und bei allen Fragen rund um Hard- und Software-Lösungen von Microsoft.



Ihr Ansprechpartner

Klaus Stein
Teamleiter Einkauf

T +49 228 9080-447
klaus.stein@hug.de



Ihr Ansprechpartner

Jörg Laufer
BDM-Consulting

T +49 228 9080-530
joerg.laufer@hug.de

Mehr zum Umstieg auf Windows 10 auf unserer Homepage:

www.hug.de/windows-10-migration/



Download Media-Creation-Tool von Microsoft:

www.microsoft.com/en-gb/software-download/windows10



Windows 7 Extended Security Updates

Extended Security Updates (ESU) sind ein Volumenlizenzangebot und ersetzen das Customer Services Agreement über Premier Services. Software Assurance (SA) oder E3 sind keine Voraussetzung, um Windows 7 ESU kaufen zu können. Die Lizenzen sind erhältlich für Geräte, die Windows 7 Professional oder Enterprise nutzen. Windows 7 ESU ist erhältlich in EA/EAS, MPSA und CSP. Es enthält Sicherheitsupdates für Vorgänge, die MSRC als kritisch oder wichtig einstuft.



Sicherheitslücke Drucker

Auch Großformatdrucker werden zur Zielscheibe

Da stehen Sie nun also vor dem Großformatdrucker und wollen Ihre Pläne abholen. Stattdessen steht auf der Anzeige eine kryptische Fehlermeldung und, zum Glück, gleich auch die Telefonnummer der Hotline. Der hilfsbereite Mitarbeiter dort kümmert sich um Ihr Problem.

Er fragt, um den Fehler nachvollziehen zu können, nach Ihrem Login und Ihrem Passwort, und ja, er sieht schon, wo das Problem liegt: „Einen Augen-

blick bitte, so, fertig!“ Und jetzt brauchen Sie nur noch den Drucker neu zu starten, und alles läuft wieder, Ihre Deadlines sind gesichert.

Der freundliche Service-Mitarbeiter kann sich jetzt auch über Ihre Anmeldedaten in das Firmennetzwerk einwählen.

Sicherheit beim Drucken? Ist doch kein Thema. Da waren sich jedenfalls rund vier Fünftel der befragten IT-Manager sicher. Dieselben IT-Manager, von denen 90 % überzeugt sind, dass PCs ein Si-

cherheitsrisiko darstellen. Und drei Viertel sehen für Mobilgeräte und Server die Gefahr eines nicht autorisierten Zugriffs.* Es ist dringend Zeit, das Risiko bei den Druckern zu überdenken.

Drucker sind heutzutage leistungsfähige Computer, deren Zweck es eben ist, zu drucken. Sie haben Prozessoren, sie haben eine Firmware, sie haben ein BIOS und sie haben eine Festplatte, auf der die Druckdaten gespeichert werden. All dies sind potenzielle Einfallstore für Hacker. Und damit nicht genug, denn wenn man sich der Sicherheit beim Drucken einigermaßen ernsthaft nähert, wird klar: Wir sprechen eigentlich über drei Themenbereiche: den Drucker, die Daten und die gedruckten Dokumente.

1. Sicherer Drucker

Um den Drucker zu schützen, hat HP zahlreiche Technologien entwickelt, unter anderem HP SureStart und HP Whitelisting. Beide überwachen das „zentrale Nervensystem“ des Gerätes, die Firm-ware und das BIOS. Sollte die Software des Druckers feststellen, dass BIOS oder Firmware nicht vom Hersteller kommen, greifen sie entweder auf eine ältere Firmware zurück oder auf ein BIOS, das auf einem zweiten Chip im Drucker installiert ist. So ist sichergestellt, dass von außen die beiden Systeme nicht manipuliert werden können.

2. Sichere Daten

Daten werden unter anderem durch die sich selbst verschlüsselnde Festplatte geschützt. Selbst wenn die Festplatte aus einem Drucker entwendet wird, hilft das einem „Hacker“ nicht viel, denn durch die Verschlüsselung ist sichergestellt, dass nur der zur Festplatte gehörige Drucker die Daten auslesen kann.

3. Sichere Dokumente

Und auch die Dokumente verdienen Beachtung, schließlich ist es angebracht, dass nur der „rechtmäßige Besitzer“ der gedruckten Seiten diese auch

bekommt. So kann – im einfachsten Fall – eine PIN mit dem Druckauftrag mitgeschickt werden; der Drucker verlangt nach deren Eingabe am Bedienfeld und fängt erst dann mit dem Druck an. Eine höhere Sicherheit versprechen Lösungen, die Druckaufträge freigeben, wenn der Mitarbeiter beispielsweise seinen Firmenausweis an ein Lesegerät hält, das am Drucker angebracht ist.

Selbstverständlich beschränkt sich das Risiko nicht auf die Bürodruker; auch Großformatdrucker sind ein potenzielles Einfallstor für Böswillige. HP DesignJets sind die sichersten Großformatdrucker auf dem Markt.



Ihr Ansprechpartner

Hermann Hinsin
Vertrieb
T +49 228 9080-519
F +49 228 9080-710
hermann.hinsin@hug.de



* Quelle: Umfrage unter 107 IT-Verantwortlichen in Firmen mit mehr als 250 Mitarbeitern in Nordamerika, Europa, dem Mittleren Osten, Afrika, der Asien-Pazifik-Region und China, im Auftrag von HP durchgeführt von Spiceworks, Januar 2015.

**Analysieren Sie in
nur zwei Minuten
kostenfrei Ihre
Druckumgebung**



www.hug.de/managed-print-services/secure-print-analyse/



Ist Ihre Druckumgebung sicher?

Nur wer mögliche Schwachpunkte kennt, kann sich zuverlässig vor Angriffen schützen. Aber worauf kommt es beim Schutz von Druckumgebungen wirklich an? Unsere kostenfreie Schnellanalyse zeigt Ihnen, wo Risiken lauern und wie Sie sich dagegen absichern.

Gehen Sie den Schutz Ihrer Druckumgebung systematisch an, indem Sie sich einen Überblick verschaffen: In welchen Bereichen drohen Risiken? Dabei geht es nicht nur um Attacken auf das Netzwerk von außen, sondern auch um Themen wie Datenschutz bei Geräten, die abteilungsübergreifend genutzt werden oder in öffentlich zugänglichen Bereichen aufgestellt sind. Mit unserer Secure-Print-Analyse finden Sie unter anderem Antworten auf folgende Fragen:

- Wie schützen Sie Ihre Geräte vor unberechtigtem Zugriff?
- Wie schützen Sie Ihre Dokumente?
- Wie stellen Sie sicher, dass Daten, die im Netzwerk übertragen werden, geschützt sind?
- Wie sichern Sie das Drucken in Ihrem Unternehmen?
- Wie verwalten und überwachen Sie Ihre Druckflotte?

Sie wollen mehr wissen? In unserem Whitepaper „Unter dem Radar – Sicherheitsrisiko Drucken“ informieren wir ausführlich über Gefahren und Lösungen rund ums Thema Sicherheit beim Drucken.

Gern beraten wir Sie persönlich, wie Sie Ihre Druckumgebung sicherer machen.



www.hug.de/uploads/files/whitepaper_hug_online_02.pdf



**Partner First
Platinum**



Veeam Cloud Connect Backup im H&G Rechenzentrum

Der sichere zweite Standort

Zu jeder Backup-Strategie gehören mindestens zwei Standorte für die gesicherten Daten. Der erste liegt im Unternehmen. Aber wohin mit dem zweiten? Als Serviceprovider bietet H&G Unternehmen mit Veeam Cloud Connect Backup die Auslagerung in ein professionelles Rechenzentrum an.

Jeden Freitagnachmittag spielt sich in deutschen Unternehmen ein uraltes Ritual ab: Kurz vor Feierabend übergibt der IT-Administrator der Geschäftsführung das frisch gezogene Backup auf einem Magnetband und verabschiedet sich ins Wochenende. Der Geschäftsführer seinerseits schließt das Speichermedium jetzt wahlweise im Firmtresor oder dem heimischen Büroschrank ein. Ein gutes Gefühl haben weder Admin noch Chef, denn sie wissen, dass wenigstens eine Datensicherung immer außer Haus gelagert und zuverlässig gegen unerlaubten Zugriff und Verlust geschützt sein muss. Das Backup – im Alltag lästige Pflicht und meist stiefmütterlich behandelt – sichert im Ernstfall das Überleben des Unternehmens. Eine zeitgemäße Datensicherung ist nicht nur

eine unternehmerische, sondern auch eine rechtliche Notwendigkeit, denn Geschäftsführer, die an dieser Stelle nachlässig sind, können für die Folgen haftbar gemacht werden. Mindestens eine Sicherungskopie geschützt an einem zweiten Standort aufzubewahren, gilt beim Backup-Management als selbstverständlich. Gerade kleine und mittlere Unternehmen tun sich damit aber schwer, denn ohne externes Rechenzentrum bedeutet das viel Aufwand. Mit dem H&G Veeam Cloud Connect Backup können auch KMU ihre Daten in einem externen Rechenzentrum nach höchsten Standards sichern.

Der Mindeststandard für das Backup: die 3-2-1-Regel

Abhängig vom Umfang und der Bedeutung der einzelnen Unternehmensdaten muss jedes Unternehmen ein individuelles Datensicherungskonzept entwickeln. Kern jeder Backup-Strategie bleibt aber die 3-2-1-Regel. Sie besagt, dass es mindestens drei Kopien der Daten geben sollte. Diese sollen auf mindestens zwei verschiedenen Medien gespeichert sein, wovon mindestens ein Exemplar an einem anderen Standort aufbewahrt wird. Spätestens bei

der Aufbewahrung an einem anderen Standort wird es für kleine und mittelständische Unternehmen oft schwierig.

Kleinen und mittleren Unternehmen fehlt ein externes Rechenzentrum

Während Großunternehmen mehrere eigene Rechenzentren an verschiedenen Standorten betreiben, fehlt kleinen und mittelständischen Unternehmen diese Möglichkeit, Unternehmensdaten an verschiedenen Orten vorzuhalten. Sie behelfen sich daher meist mit Sicherungskopien auf Magnetbändern oder externen Festplatten, die außerhalb des Unternehmens gelagert werden. Dieses Vorgehen ist besser, als ganz auf eine externe Sicherung zu verzichten, bringt aber mehrere Probleme mit sich: Das Erstellen der Kopie selbst ist zeitaufwändig und fehleranfällig. Der Transport zum externen Aufbewahrungsort muss zuverlässig erfolgen. Und die zentrale Frage ist: Wo findet man einen geeigneten Aufbewahrungsort außerhalb des Unternehmens, der den hohen Sicherheitsanforderungen gerecht wird und außerdem ein schnelles Zurückspielen der Daten im Notfall ermöglicht?

Einfach und zuverlässig: Backup in externem Rechenzentrum

Mit der H&G Veeam Cloud Connect Backup-Lösung können physische und virtuelle Backups über eine gesicherte SSL-Verbindung in ein externes Rechenzentrum übertragen werden. Sie bilden damit ein externes Backup-Repository, also den sicheren zweiten Aufbewahrungsort für das Backup. So entfällt das aufwändi-

ge Erstellen und Auslagern von Sicherheitskopien auf Magnetbändern und externen Festplatten.

Wie funktioniert H&G Veeam Cloud Connect Backup?

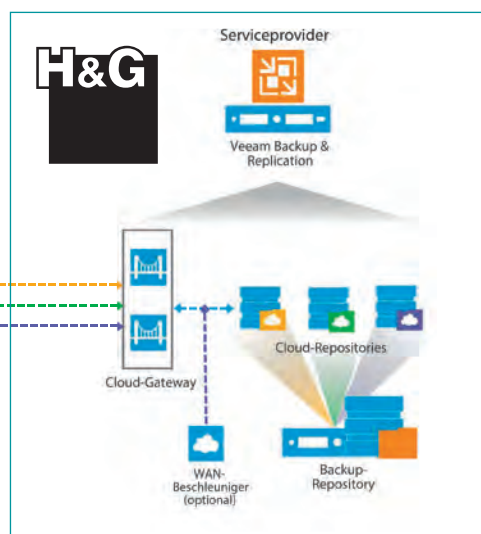
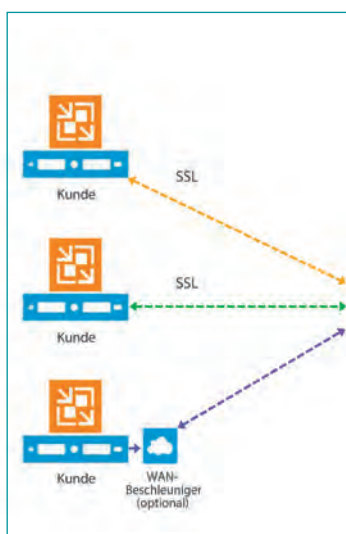
Veeam stellt Ihnen mit Cloud Connect die Software und H&G Kapazitäten in einem Rechenzentrum bereit. Nachdem Sie sich für ein Backup-Repository entschieden haben, nennen Sie uns Ihre IP-Adressen. Sie erhalten von uns einen Benutzernamen und definieren ein Kennwort für das sogenannte Cloud Connect Repository.

Der Cloud Connect Service verschlüsselt Ihre Daten und überträgt sie über eine gesicherte SSL-Verbindung und ein Cloud Gateway. Die Daten werden von Veeam Cloud Connect in unserem Rechenzentrum abgespeichert (siehe Grafik unten).

Transparenz und Kontrolle

Die Backup-Konsole ermöglicht Ihnen, jederzeit auf die Daten zuzugreifen und diese bei Bedarf ins eigene System zurückzuspielen. Außerdem gibt die Konsole mit Hilfe der Tracking-Funktion Auskunft über die Auslastung der Speicherkapazität im Rechenzentrum und benachrichtigt Sie über die gehosteten Storage-Updates.

Ist Ihre Internetverbindung kurzzeitig gestört, setzt die Übermittlung der Backups kurzzeitig aus. Sobald die Verbindung wieder steht, werden die Daten ohne Verluste automatisch weiter übertragen.



Ihre Daten werden mit Veeam Cloud Connect in ein H&G Rechenzentrum übertragen.

Wer hat Zugriff auf meine Datensicherungen, die per Veeam Cloud Connect Backup hochgeladen wurden?

Die optionale End-to-End-Verschlüsselung sorgt dafür, dass die Daten auf Wunsch auf dem Quellsystem verschlüsselt werden, bevor sie das Netzwerk des Unternehmens verlassen, und ausschließlich verschlüsselt übertragen und gespeichert werden. Wie im eigenen Rechenzentrum hat dann nur das Unternehmen selbst Zugriff auf die Backup-Daten. Über eine Backup-Konsole kann der IT-Verantwortliche jederzeit die gespeicherten Daten abrufen und bei Bedarf im eigenen System wiederherstellen.

Wer unterstützt mich, wenn es Probleme mit der Cloud-Connect-Verbindung oder dem Übertragen von Sicherungen gibt?

Unser Servicedesk ist von Montag bis Freitag zwischen 08:00 und 17:00 Uhr per E-Mail und telefonisch erreichbar und beantwortet Ihnen gern Fragen zur Einrichtung oder Fehlersuche zu Veeam Cloud Connect.

Wo werden die in Cloud-Connect hochgeladenen Datensicherungen gespeichert?

H&G betreibt eigene Hosting Infrastrukturen ausschließlich in deutschen Rechenzentren. Im Gegensatz zu einem Firmentresor, Bankschließfach o. Ä. sind professionelle Rechenzentren so konzipiert, dass sie die Sicherheit

und Verfügbarkeit digitaler Daten gewährleisten. Von H&G genutzte Rechenzentren sind entsprechend ISO 27001 zertifiziert. Das heißt, neben der üblichen Sicherung gegen den physischen Zugriff durch Unbefugte, verfügt es über spezielle Sicherungen gegen Stromausfall, eine Temperatur- und Klimasteuerung sowie besonderen Brandschutz.

Sind die in das Cloud Connect ausgelagerten Datensicherungen auch für eine Disaster Recovery geeignet?

Grundsätzlich ja. Allerdings müssen Sie im Fall einer Komplett-Wiederherstellung immer die zur Verfügung stehende Bandbreite im Auge behalten. Auch dies ist eine Frage, die im Rahmen eines Datensicherungskonzepts geklärt werden sollte. Wir beraten Sie gern beim Berechnen der Übertragungsdauer einer Disaster Recovery und bei der Entwicklung eines eigenen Datensicherungskonzepts für Ihr Unternehmen.

Was passiert mit den hochgeladenen Datensicherungen, wenn der Cloud-Connect-Speicher gekündigt wird?

Nach Vertragsende werden die gespeicherten Daten umgehend und unwiederbringlich aus unseren Systemen gelöscht. Daher ist es wichtig, dass Sie die benötigten Daten vorher abrufen und an anderer Stelle speichern. Wir garantieren ein sicheres Löschen und bestätigen Ihnen die Löschung gern schriftlich.

VEEAM

**PROPARTNER
Gold Reseller**



Ihr Ansprechpartner

Robert Schneider
IT Consulting & Services
Fachbereich IT-Infrastruktur
T +49 228 9080-671
robert.schneider@hug.de



HYBRID CLOUD INFRASTRUCTURE

NetApp HCI

NetApp macht Hyper-Converged zu Hybrid Cloud Infrastructure

Hyper-converged oder nicht? Bei NetApp HCI gehen die Meinungen auseinander. Auf jeden Fall hat NetApp mit seinem neuen Ansatz die gleichen Kunden im Blick wie die etablierten HCI-Anbieter und verschafft insbesondere den Betreibern großer Rechenzentren erhebliche Vorteile.

„HCI bedeutet etwas anderes für uns“, vermeldete Brett Roscoe, Vice President of Product Management bei NetApp. Während die erste Generation HCI darauf abzielte, traditionelle 3-Tier-Architekturen – Compute, Storage und Netzwerk – zu konsolidieren und in eine Infrastruktur zu bringen, die einfachen Zugriff ermöglicht, gehe es heute nicht mehr um traditionelle Architekturen. Im Mittelpunkt stehe jetzt vielmehr, Public und Private Clouds, VMs sowie Microservices zu verbinden und alle über ein einziges Portal zu verwalten. Dieser Sichtweise nach steht HCI nicht mehr für Hyper-Converged, sondern für Hybrid Cloud Infrastructure.

Erst Ende 2017 – und damit vergleichsweise spät – stieg NetApp ins HCI-Segment ein. Das aber mit vollem Elan und einer Reihe neuer Ideen. Im Gegensatz zu anderen HCI-Anbietern lassen sich bei NetApp Storage und Compute getrennt voneinander aufrüsten. Außerdem ermöglicht die NetApp Data Fabric Unternehmen, Workloads zwischen HCI, einer eher traditionellen 3-Tier-IT-Architektur und einer Multi-Cloud zu verteilen.

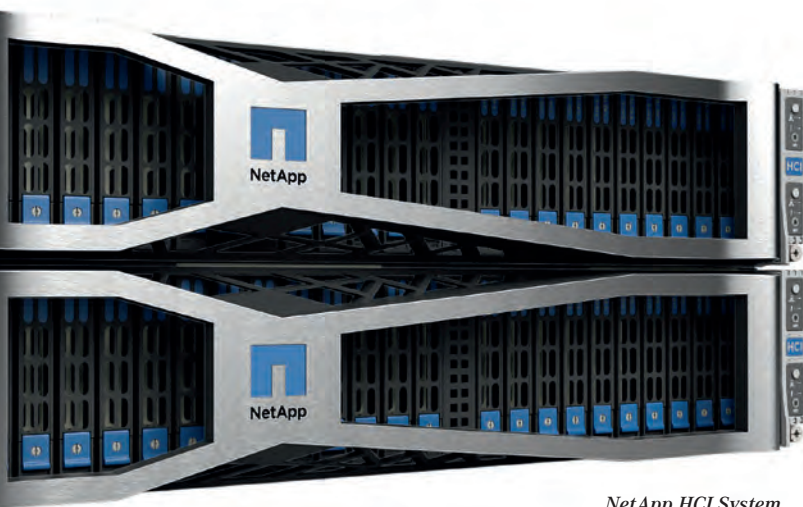
Neuer Ansatz beim Speicher-management

NetApp HCI betreibt das Storage-Management nicht über den Hypervisor in einer VM. Es erfolgt getrennt über SolidFire Element OS, dem im Chassis bestimmte Knoten vorbehalten sind, während die Übrigen dazu dienen, VMs unter unterschiedlichen Hypervisoren zu betreiben, beispielsweise vSphere von vmWare. Element OS basiert auf der Technologie des All-Flash-Speicherherstellers SolidFire, den NetApp 2016 übernahm. Entsprechend sind Kunden auf ein All-Flash-System festgelegt. Dem gegenüber steht eine Reihe von Vorteilen und Einsparpotenzialen, die die „nicht wirklich hyper-converged“ Infrastruktur vor allem für große Rechenzentren attraktiv macht.

Technisch gesehen ist die NetApp-HCI-Lösung eine getrennte, software-definierte Architektur mit ausgewiesenen Speicher- und Compute-Knoten in einem einzigen Gerät. Streng genommen entspricht das nicht der üblichen Definition von hyper-converged, aber das ist wohl für die wenigsten Kunden von Bedeutung, wenn die Lösung den gleichen Zweck erfüllt und sie dafür von anderen Vorteilen profitieren.

Unabhängiges Speicherwachstum spart Server-Lizenzen

DeepStorage.net-Autor Howard Marks erklärt den Aufbau und die Vorteile der NetApp-Lösung folgendermaßen: NetApp HCI entkoppelt Compute und Storage als Cluster-Scale. Die meisten HCI-Anbieter verkaufen die Knoten zwar mit verschiedenen



NetApp HCI System

Anteilen an Storage und Compute. In jedem Fall aber muss der Kunde immer eine vollständige neue Maschine kaufen, wenn er aufrüstet. Das heißt, auch wer nur mehr Storage braucht, muss immer zusätzliche Compute-Ressourcen erwerben und umgekehrt. Läuft der Storage als VM unter vSphere, erwachsen aus dem zusätzlichen Compute nicht nur Kosten für überflüssige Serverressourcen, sondern auch für die damit verbundenen Softwarelizenzen.

Nutanix und wenige andere HCI-Hersteller bieten reine Storage-Knoten für Kunden an, die sich die vSphere-Lizenzkosten sparen wollen. In den meisten Fällen unterstützen Anbieter aber nicht die Möglichkeit, externe Server an den Storage der HCI-Maschine anzuschließen, um mehr VMs zu hosten. Die Kunden müssen daher teure HCI-Knoten kaufen oder, im Falle von VMware, eine vSAN-Lizenz für jeden Server. NetApps HCI-Lösung soll dagegen externe Server unterstützen.

Storage-Management außerhalb einer VM sichert kurze Latenzzeiten und vereinfacht Updates

Werden VM-Hosts als Storage-Knoten verwendet, erhöht das grundsätzlich die Komplexität, denn in einem traditionellen Server-Storage-Modell sind VM-Hosts zustandslos. Wenn bei einem Host die Hardware-Wartung oder der Hypervisor ein Upgrade braucht, migriert der Administrator also einfach die VM und führt das Upgrade der Firmware des Motherboards aus. Wird der Knoten zusätzlich für Storage benutzt, muss er auch bei diesen Arbeiten wie ein Speicherelement behandelt werden.

Einen weiteren Vorteil der NetApp-HCI-Lösung sieht Experte Howard Marks in der Quality of Service (QoS) von Element OS. Mit der Entscheidung, Element OS separat und nicht in einer VM zu betreiben, sorgt NetApp dafür, dass die Latenzzeiten von Element OS nicht durch den Zugang über den Hypervisor nachteilig beeinflusst werden.

Schnelleres Setup durch automatisierte Installation und cleveres Datenmanagement mit der NetApp Data Fabric

Das Implementieren findet via NetApp Deployment Engine (NDE) statt. Hierbei werden viele Schritte der Installation vereinfacht und automatisiert. Das sorgt neben deutlich kürzerer Installationszeit auch für die Einhaltung der Best Practices. Das Verwalten der Speicher-Ressourcen wird komplett im vCenter vorgenommen. Über APIs kann das System von anderen Applikationen für Orchestrierung, Backup oder Disaster Recovery angesteuert werden.

Bekannt ist NetApp vor allem als Spezialist für Datenmanagement. Von diesen Kompetenzen profitieren die Kunden auch bei NetApp HCI. Das Unternehmen bringt seine Ontap-Data-Management- und Storage-Software in die HCI-Lösung ein. So können Daten automatisch an dem jeweils günstigsten Speicherort, lokal, in einer Public Cloud oder einer Hybrid Cloud, abgelegt werden. Als Public-Cloud-Anbieter bindet NetApp Storage bereits Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform ein.



Ihr Ansprechpartner

Manfred Wollweber
Vertrieb Server, Storage, Network

T +49 228 9080-510
manfred.wollweber@hug.de



Netzwerkzugangssteuerung

Kein Fischen im Trüben

Mobiles Arbeiten, BYOD, IoT, sichere Gastzugänge – der Aufwand, Geräte sicher ins Unternehmensnetzwerk einzubinden, wird für IT-Abteilungen immer größer. Wer und was im eigenen Netz unterwegs ist, lässt sich kaum noch zuverlässig kontrollieren. Mit Aruba ClearPass ist eine herstellerunabhängige Netzwerkzugangssteuerung auf dem Markt, die mit automatisierter Geräte- und Benutzererkennung Licht ins Dunkel

bringt. Individuelle Richtlinien sorgen dafür, dass sich alle und alles im Netz an die Regeln hält.

„Was ist das? Loch an Loch und es hält doch – ein Netz. Dieses Kinderrätsel beschreibt erschreckend präzise das Netzwerk vieler Unternehmen. Ob und wie lange es Angriffen und Bedrohungen standhält, ist dabei meist fraglich. Bring your own device (BYOD), der Siegeszug der IoT-Geräte und die Anforderungen des mobilen Arbeitens machen die Netzwerkzugangskontrolle für IT-Verantwortliche zu

einer Sisyphus-Aufgabe. Den Überblick zu behalten, wer und was sich im Netz tummelt, ist kaum möglich. Jedoch ist dieses Wissen die Voraussetzung, um Sicherheitsrisiken zu erkennen und das Unternehmen vor ihnen zu schützen.

Aruba ClearPass löst die drei dringendsten Probleme, die IT-Verantwortliche im Hinblick auf ihr Netzwerk haben: Transparenz, Zugangssteuerung und Schutz vor Cyberangriffen. Im Gegensatz zu anderen Lösungen identifiziert Aruba ClearPass in Echtzeit und ohne den Einsatz von Agents Endpunkte und Netzwerkgeräte in kabelgebundenen und kabellosen Netzwerken. ClearPass ist dabei nicht an die Netzwerkkomponenten eines bestimmten Herstellers gebunden, sondern funktioniert in jedem Netzwerk. Es lässt sich außerdem in über 120 Sicherheits- und allgemeine IT-Lösungen integrieren – z. B. um in Kombination mit Firewalls, SIEM oder Sandboxes auf Cyberangriffe zu reagieren.

Sicherheit und Compliance: Transparenz ist die Voraussetzung

Nur wer weiß, wer und was in seinem Netz unterwegs ist, kann mögliche Risiken erkennen. BYOD, eine Flut von IoT-Geräten und die Forderung von Anwendern, möglichst von überall Zugang zum Netz zu haben, machen es Netzwerkadministratoren schwer, den Überblick zu behalten. Hinzu kommen die Bereitstellung von Gastzugriffen und die Kontrolle von nicht autorisierten kabelgebundenen und kabellosen Endpunkten. Bisherige Verfahren zur Identifizierung der verbundenen Endpunkte erweisen sich in der Praxis oft als wenig hilfreich, da sie mit Agents arbeiten und regelmäßige Updates der Endpunktdatenbanken erfordern. Letztlich bleibt es bei vielen IT-Abteilungen Handarbeit, den Netzwerkzugang freizugeben und zu kontrollieren.

Mit Aruba ClearPass behalten Administratoren jetzt die Übersicht in ihren Netzwerken. Da ClearPass nicht mit Agents arbeitet, erkennt es auch BYOD-Smartphones und IoT-Geräte. Endpunkte in kabelgebunden und kabellosen Netzwerken werden automatisch identifiziert und kategorisiert. Dies geschieht anhand von Attributen wie Gerätekategorie, Herstel-

ler, Betriebssystem, IP-Adresse, Hostname, Besitzer und anderen. Neue und unbekannte Geräte lassen sich so unmittelbar klassifizieren und der entsprechenden Zugriffsrichtlinie unterwerfen.

Zugangssteuerung: Wer darf was im Netz?

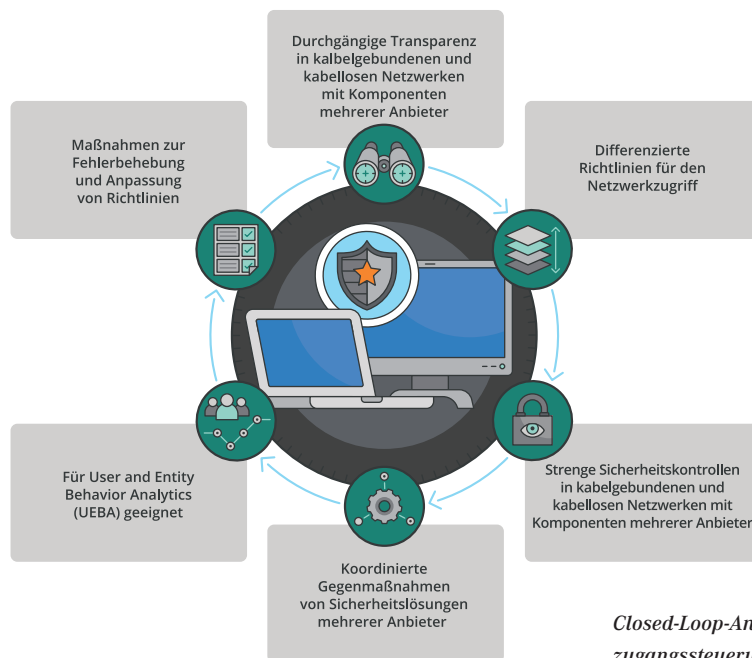
Vom IT-Mitarbeiter bis zum Besucher, vom Server bis zum Drucker: Viele Personen und Geräte brauchen Zugang zum Netzwerk, aber nicht jeder und jedes sollte gleich Zugriff auf alle Ressourcen haben. Über Richtlinien, die unter anderem Faktoren wie Gerät, Tageszeit und Benutzertyp berücksichtigen, vergibt ClearPass Zugriffsrechte, die jedem Benutzer, jedem System und jedem Gerät nur den Zugriff erlauben, der für die jeweilige Rolle notwendig ist. Diese richtlinienbasierte Segmentierung ermöglicht es, Besuchern ein Netzwerk zur Verfügung zu stellen, das vom eigenen Firmennetzwerk getrennt bleibt. Ergänzt durch ein Selbstregistrierungsportal bleibt der IT-Abteilung obendrein viel administrativer Aufwand erspart.

Unabhängig von der jeweiligen Rolle und dem jeweiligen Segment, erlaubt ClearPass im Gegensatz zu einigen anderen Lösungen grundsätzlich nur solchen Geräten und Benutzern den Zugang mit positiver Authentifizierung und der entsprechenden richtlinienbasierten Berechtigung.

„Farblose Ports“: Das Endgerät bestimmt die Zugriffsrechte

Die sichere Konfiguration von Ports bereitet IT-Abteilungen oftmals Kopfzerbrechen. Besonders in öffentlich zugänglichen Bereichen stellen sie ein Sicherheitsrisiko dar. Die generelle Einschränkung der Zugriffsrechte oder die Konfiguration für bestimmte Anwendungsfälle wie z. B. Drucker macht die Nutzung der Ports unflexibel. Eine Änderung der Nutzung ist immer mit zusätzlichem Aufwand verbunden.

ClearPass ermöglicht die Strategie der „farblosen Ports“. Da ClearPass jedes Gerät erkennt und hinsichtlich seiner Zugriffsrechte prüft, bevor es ins



Closed-Loop-Ansatz für Netzwerkzugangssteuerung und Reaktion.

Netz aufgenommen wird, kann jeder Port mit jedem Gerät verbunden werden, ohne die Portnutzung generell einschränken zu müssen. IT-Verantwortliche sparen somit viel Zeit bei der Einrichtung und Konfiguration von Switchen und können gleichzeitig die Portnutzung optimieren.

Offene und nahtlose Integration: ClearPass in Kombination mit Firewall und Co.

ClearPass bietet einen Closed-Loop-Ansatz zum Schutz von Netzwerken. Das heißt, ein geschlossener Regelkreis sorgt dafür, dass die Sicherheit stets gewährleistet ist, obwohl ständig neue und unbekannte Elemente Teil des Netzwerks werden oder es Cyberattacken ausgesetzt sein könnte.

Den ersten Schritt dazu bildet die umfassende Transparenz, die ClearPass in jedem Netzwerk ermöglicht – unabhängig vom Hersteller der Netzwerkkomponenten oder der Geräte, die auf dieses Netzwerk zugreifen. Differenzierte Richtlinien für den Netzwerkzugriff, die beliebig auf Gerätemerkmale und Rollen der Nutzer angepasst werden können, bilden die Basis für eine sichere Zugangssteuerung in kabelgebundenen und kabellosen Netzwerken. Wird ClearPass in Kombination mit Firewalls, SIEM, Sandboxes und Ähnlichem eingesetzt, können auch Richtlinien als Reaktion auf Cyberangriffe definiert

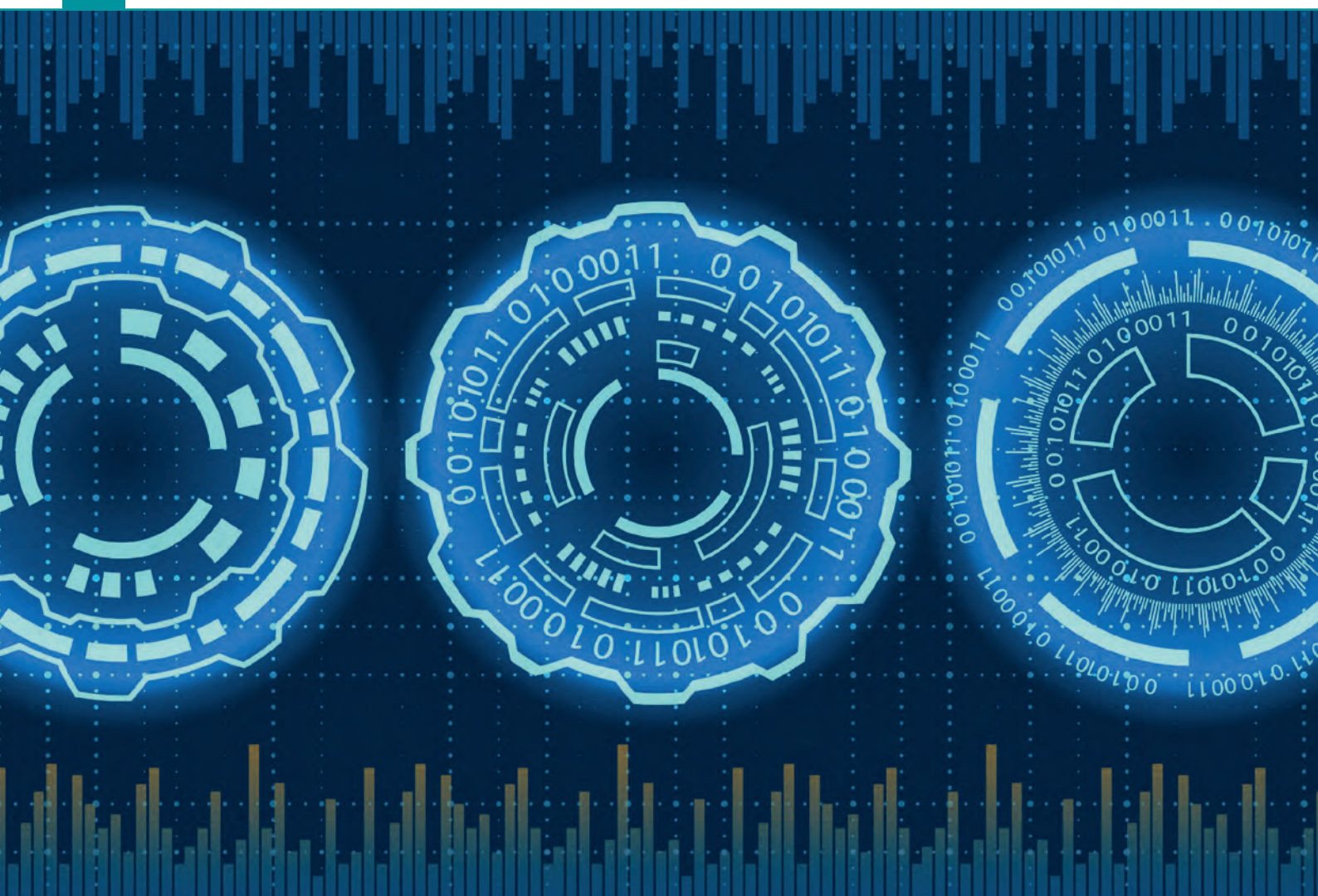
werden. Sobald die Sicherheitslösungen Hinweise auf einen solchen Vorfall melden, löst ClearPass festgelegte Aktionen aus, wie z. B. erneute Authentifizierung, Bandbreitenbegrenzung, Quarantäne oder Blockierung. ClearPass ermöglicht die Erfassung und Analyse des Verhaltens von Nutzern und Geräten im Netz. Diese Daten bilden die Grundlage zur kontinuierlichen Anpassung der Richtlinien und zur Optimierung des Netzwerks.

ClearPass kann noch mehr! Lassen Sie sich beraten, wie ClearPass Ihr Netzwerk sicherer macht, Ihnen hilft, Compliance-Anforderungen zu erfüllen, und dabei Ihre IT-Abteilung entlastet.



Ihr Ansprechpartner

Kai Lauterbach
IT Consulting & Services
Fachbereichsleiter
Netzwerk & Security
T +49 228 9080-675
kai.lauterbach@hug.de



HPE Synergy

Der Einstieg in die Composable Infrastructure

Traditionelle IT-Strukturen stoßen in Zeiten von Cloud Computing, sozialen Netzwerken, Big Data und Mobilität an ihre Grenzen. Composable Infrastructure trägt der neuen Generation von Geschäftsmodellen mit agilen und flexiblen Systemen

Rechnung. Bei HPE Synergy treten an die Stelle fester Silo-Strukturen fließende Ressourcenpools, aus denen über eine zentrale Schnittstelle in kurzer Zeit beliebige Strukturen nach Bedarf bereitgestellt werden können.

Traditionelle IT-Infrastrukturen sind auf Stabilität und Kostenkontrolle ausgerichtet. Heutige Geschäftsmodelle verlangen allerdings neue Anwendungen und Services, für deren Bereitstellung vor allem Agilität und Schnelligkeit gefordert sind. Die Ansprüche in diesen Bereichen ändern sich so schnell, dass die kontinuierliche, zeitnahe Anpassung der IT in einer klassischen Architektur aufgrund der Kosten und des zeitlichen Aufwands nicht möglich ist. Die Folge: Traditionelle Infrastrukturen sind häufig überdimensioniert oder können die neuen Anforderungen der Geschäftsprozesse nur unzureichend abbilden. Sie werden so zu Bremsklötzen im Wettbewerb.

Mit der Plattform Synergy bietet HPE eine Infrastruktur, die vollständig auf dem Prinzip der Zusammensetzbarkeit basiert. Die Composable Infrastructure soll Unternehmen in die Lage versetzen, den Spagat zwischen den Anforderungen klassischer IT-Systeme und neuer, applikationsgetriebener Technologien zu meistern. Auf der einen Seite stehen dabei Forderungen nach Stabilität und Effizienz, auf der anderen nach Geschwindigkeit und Agilität.

Diesen gegensätzlichen Ansprüchen begegnet die HPE-Synergy-Plattform mit fließenden Ressourcenpools von Rechen-, Speicher- und Fabric-Komponenten. Sie ermöglichen ein Nutzungsmodell, bei dem Hard- und Software in einem System verbunden sind. Über eine zentrale Schnittstelle können die Ressourcen ganz nach Bedarf zu individuellen IT-Strukturen zusammengesetzt werden. Ändern sich die Anforderungen, lässt sich mit Hilfe einer softwaredefinierten Management-Oberfläche in kurzer Zeit eine entsprechende Anpassung der Komponenten vornehmen. Workload-Vorlagen erleichtern und beschleunigen dabei die Konfiguration. Nicht benötigte Ressourcen stehen im Pool für andere Anwendungen zur Verfügung.

Aus einer hardware-definierten, starren IT-Umgebung soll so eine Plattform zur kontinuierlichen

Service- und Anwendungsbereitstellung werden. Die Composable Infrastructure der HPE Synergy stellt den derzeitigen Endpunkt einer konsequent weitergedachten Converged bzw. Hyper-Converged Infrastructure dar. Diese Zwischenschritte bilden gleichsam die Trittleiter für Kunden in die Composable Infrastructure, denn Produkte wie das IT-Infrastrukturmanagement-Tool HPE OneView, das HPE BladeSystem/ConvergedSystem mit HPE 3PAR und HPE ProLiant mit HPE StoreVirtual VSA sind Bausteine einer Converged Infrastructure, die auch mit HPE Synergy weiterverwendet werden können. Wem der Umstieg auf HPE Synergy noch zu radikal ist, kann so beim jetzigen Ausbau seiner Infrastruktur die Weichen für die Zukunft stellen und seine Investitionen schützen.

So funktioniert HPE Synergy

Architektur ohne TOR-Switches (Top of Rack)
Das verteilte, rack-basierte Design von HPE Synergy Composable Fabric nutzt eine intelligente Master/Satelliten-Architektur, um Netzwerkverbindungen im Rechenzentrum zu konsolidieren, die Hardware- und Managementkomplexität zu verringern und die Netzwerkbandbreite über mehrere Gehäuse (sogenannte „Frames“) hinweg zu skalieren. Das Master-Modul umfasst intelligente Netzwerkfunktionen, die Konnektivität für Satelliten-Frames zur Verfügung stellen. Dadurch ist kein TOR-Switch erforderlich, was Kosten spart. Die Reduzierung der Komponenten vereinfacht nicht nur das Fabric-Management, sondern optimiert auch knappe Netzwerkressourcen und belegt weniger Anschlüsse auf der Aggregations-schicht des Rechenzentrums.

Alle Daten speichern

Der HPE Synergy Composable Storage ist vollständig in den Frame integriert. Jedes Speichermodul ist mit 40 Laufwerken ausgestattet und HPE Synergy Composer kann bis zu 200 Speicherlaufwerke in einer Zone für ein Rechenmodul bereitstellen. Für DAS-zentrierte Workloads ermöglicht das blockierungsfreie SAS-Fabric die vollständige Nutzung der

Flash-Speicherleistung für lokale Anwendungen. Die physisch eingebetteten Managementfunktionen erstellen eine vollständig verbundene softwaredefinierte Infrastruktur, in der über eine einzige programmierbare Schnittstelle Speicher-, Rechen- und Fabric-Ressourcen zusammengesetzt werden können.

Für größere Unternehmensanwendungen, die für Tier-1-Service-Levels erforderlich sind, stellt die FlatSAN-Technologie von HPE eine direkte Verbindung von HPE Synergy zu HPE 3PAR StoreServ Flash-Arrays zur Verfügung. Diese Verbindung unterstützt sowohl Block- als auch Dateianwendungen mit einer Verfügbarkeit von 99,9999 % und bietet bis zu 60 PB sowie 10 Mio. IOPs in einem einzigen Verbundspeicherpool.

Dank dieser Flexibilität können alle Daten – unabhängig davon, ob sie aus traditionellen Anwendungen oder aus Anwendungen für den New Style of Business stammen – in Repositories für Datei-, Block- oder Objektdaten gespeichert werden, die direkt mit Workloads und Anwendungen verbunden sind.

Composer

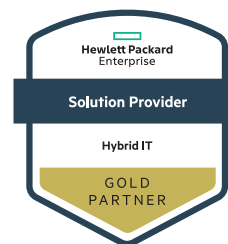
HPE Synergy Composer ist eine einzige Schnittstelle, die logische Infrastrukturen präzise und extrem schnell in beliebigen Kombinationen zusammensetzt. Durch Erhöhung der Ressourcenauslastung kann die IT die Bereitstellung von Überkapazitäten oder isolierten, nicht nutzbaren Ressourcen vermeiden und sicherstellen, dass den Anwendungen die jeweils erforderlichen Ressourcen zur Verfügung stehen. Mit HPE Synergy Composer können IT-Abteilungen zudem – in nur einem Schritt und mit einer einzigen Schnittstelle – Infrastrukturen für traditionelle, virtualisierte und Cloud-Umgebungen in wenigen Minuten implementieren, überwachen und aktualisieren. Ressourcen lassen sich ohne Serviceunterbrechungen aktualisieren, anpassen und erneut bereitstellen. Auf Workloads basierende Vorlagen definieren, wie die Infrastruktur funktionieren muss, und die interne softwaredefinierte Intelligenz implementiert Änderungen programmgesteuert.

Image Streamer

Zur Beschleunigung der Workload-Implementierung nutzt HPE Synergy einen Image Streamer, das heißt ein Repository mit bootbaren Images, die innerhalb von Sekunden an zahlreiche Rechenmodule gestreamt werden können. Dank dieser Funktion kann HPE Synergy die Infrastruktur deutlich schneller einrichten und aktualisieren als der traditionelle sequenzielle Prozess der Einrichtung von Rechenmodulen (physische Bereitstellung, gefolgt von der Installation des Betriebssystems oder Hypervisors). Das ist besonders für Web-Scale-Implementierungen ideal, bei denen die IT eine Betriebsumgebung für eine große Anzahl an Infrastrukturblöcken bereitstellen muss.

Reibungslose Änderungen

Heute ist das Change-Management ein „Ereignis“, für dessen Erfolg die IT planen, Vorbereitungen treffen und beten muss. Die IT muss den gesamten Stack (Firmware, Treiber etc.) durch manuelle Prozesse schützen und aktualisieren. Für einen vollständigen HPE Synergy Frame und jede darin enthaltene Komponente kann die Aktualisierung der Firmware von einem einzigen Administrator ohne Betriebsunterbrechung ausgeführt werden. Die Firmware und die Treiber des Rechenmoduls werden zwischengespeichert und können in einem späteren Wartungsfenster für die Anwendung aktiviert werden. Damit sind keine zusätzlichen Ausfallzeiten mehr notwendig.



Ihr Ansprechpartner

Holger Seelig
Vertrieb

T +49 228 9080-515
holger.seelig@hug.de



Zusammenarbeiten im Projekt

Microsoft Teams – was es ist und was es kann

Verwirrung war die wesentliche Reaktion des Publikums, als Microsoft vor etwa zwei Jahren Teams öffentlich vorstellte. Nach Office 365, Sharepoint und Skype for Business sollte mit Teams die eierlegende Wollmilchsau für die Projektarbeit geschaffen werden. Der Ansatz hinter Teams ist simpel und heißt Integration. Die Folgen sind enorm, denn der Einsatz von Teams kann Projektarbeit um vieles effizienter

machen, bringt aber auch eine Reihe organisatorischer Fragen mit sich. Wir erklären, was Teams ist, wie Sie es nutzen und worauf Sie achten müssen.

Was ist Microsoft Teams?

Die Antwort des Herstellers auf diese Frage lautet: „Microsoft Teams – der zentrale Ort für Teamarbeit in Office 365 – verbindet Nutzer, Inhalte und Werkzeuge, um die Motivation und Effizienz zu steigern.“

Nüchtern betrachtet handelt es sich bei Microsoft Teams um eine Plattform, die diverse Anwendungen gebündelt zur Verfügung stellt, damit eine Gruppe von Anwendern (ein Team) sie gemeinsam nutzen kann. Teams soll Personen, die eng zusammenarbeiten, unter anderem ermöglichen,

- Informationen und Updates offen auszutauschen, um stets auf dem Laufenden zu sein,
- an zentraler Stelle in der Gruppe Diskussionen zu führen, um zu Entscheidungen zu kommen,
- gemeinsam Inhalte zu erstellen.

Von der Dateiablage über die Anwendungen von Office 365 bis zu Kommunikationstools wie Chat oder Spezialanwendungen von Drittanbietern lässt sich dazu alles an einem Ort bereitstellen. „An einem Ort bereitstellen“ bedeutet, dass Microsoft Teams den Nutzern eine Oberfläche bietet, von der aus sie nicht eine bestimmte Anwendung öffnen, sondern ein Projekt – in Microsoft Teams „Kanal“ genannt. Von dort können alle Projektbeteiligten auf sämtliche Daten

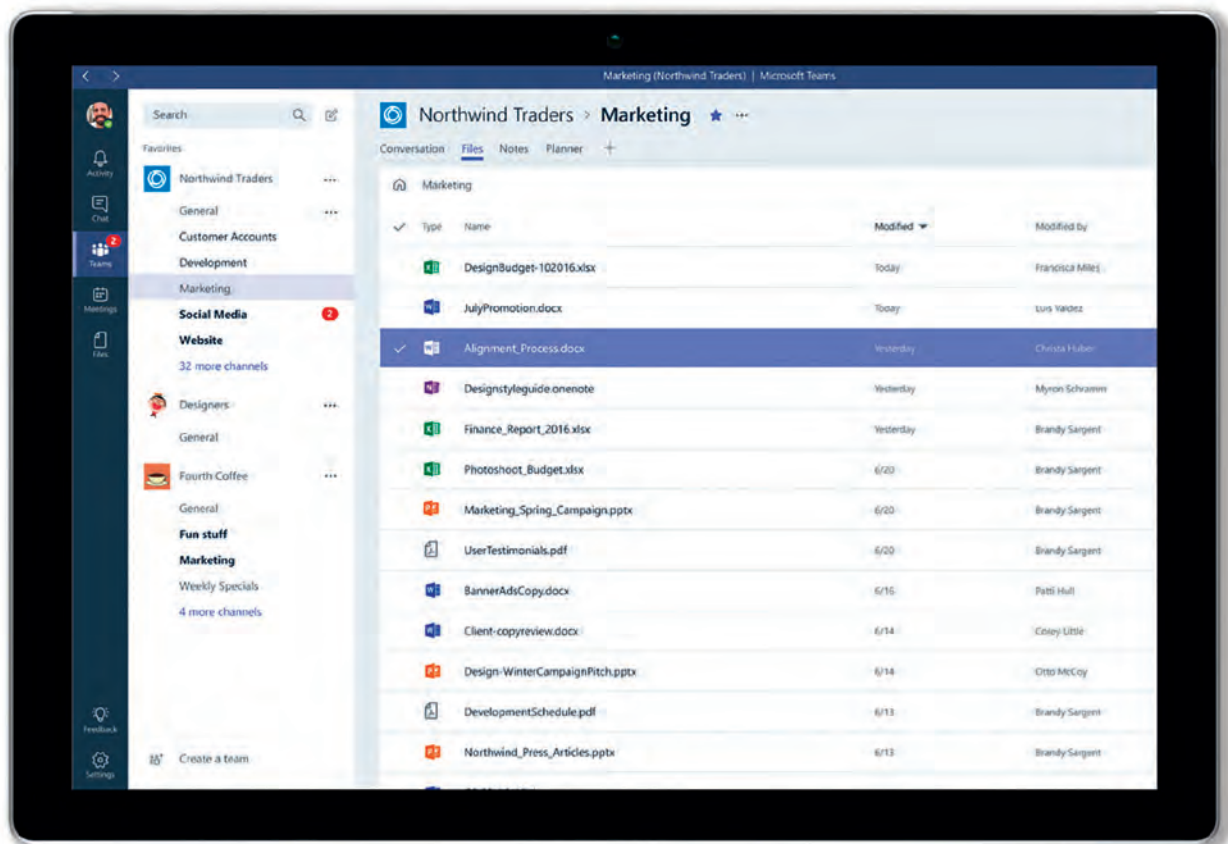
und Anwendungen, die für das Projekt benötigt werden, zugreifen. Der Arbeitseinstieg erfolgt also nicht mehr über eine bestimmte Anwendung, sondern über das Projekt.

Lizenzen: Wie beziehe ich Teams?

Teams ist kostenloser Bestandteil in diversen Office-365- und Microsoft-365-Lizenzverträgen. Dazu gehören Lizenzprodukte der Office-365-Variante E1, E3 und E5 sowie Business Premium und Essentials und der Microsoft-365-Variante Business und E3, E5.

Was ist der Mehrwert von Microsoft Teams gegenüber anderen Kommunikations- und Kollaborationstools?

Die zentrale Idee von Microsoft Teams ist Integration: Projektteams sollen ihre Zusammenarbeit nicht über diverse Einzelanwendungen organisieren müssen, sondern an einer zentralen Stelle alle Informationen und Werkzeuge für ihr Projekt zur Verfügung haben.



Benutzeroberfläche von Microsoft Teams.

Das ist ein zentraler Wandel in der Zusammenarbeit: Arbeiten Nutzer zusammen an einem Projekt, so werden meist Dokumente, Daten und Dateien lokal erstellt, dann versendet oder über eine Filesharing-Lösung bereitgestellt. Mit Hilfe diverser Kommunikationstools von E-Mail, Audio- und Videokonferenzen, Chat etc. erfolgen dann der Austausch und die Abstimmung innerhalb der Arbeitsgruppe.

Besonders schwierig wird es regelmäßig, wenn Personen aus anderen Unternehmen und Organisationen mitarbeiten. Mit Microsoft Teams lassen sich externe Nutzer einladen und damit unternehmensübergreifende Arbeitsgruppen bilden, bei denen allen Beteiligten die gleichen Ressourcen zur Verfügung stehen.

Ein Team – viele Kanäle: Wie organisiert man sich mit Teams?

Die Struktur Team – Kanal ist die einzige Hierarchie, die Teams vorgibt. Entsprechend viele Möglichkeiten gibt es, wie ein Unternehmen oder eine Abteilung sich mit Hilfe von Teams organisiert. So kann eine Fachabteilung ein Team bilden und für jedes zu bearbeitende Projekt oder bestimmte Arbeitsbereiche einen Kanal anlegen. Bei abteilungsübergreifenden Projekten können alle Projektbeteiligten ein Team bilden und die Teilaspekte des Projekts in Kanälen abbilden. Diese Organisationsform ist besonders für die Zusammenarbeit mit Personen außerhalb des eigenen Unternehmens interessant – seien es Kunden oder Partnerunternehmen.

Microsoft Teams ist darauf ausgelegt, Hindernisse für eine Zusammenarbeit aus dem Weg zu räumen, und unterstellt, dass alle Beteiligten gleichberechtigt sind – das heißt, dass jeder im Team alles wissen darf und tun kann. Wer Mitglied eines Teams ist, hat grundsätzlich Zugriff auf alle Kanäle und damit auf sämtliche abgelegten Daten.

Konfiguration und Datenschutz: Wo liegen die Daten und wie sind sie gesichert?

Um mit den Daten zu einem Projekt arbeiten zu können, müssen Sie sich Gedanken zur Arbeit mit

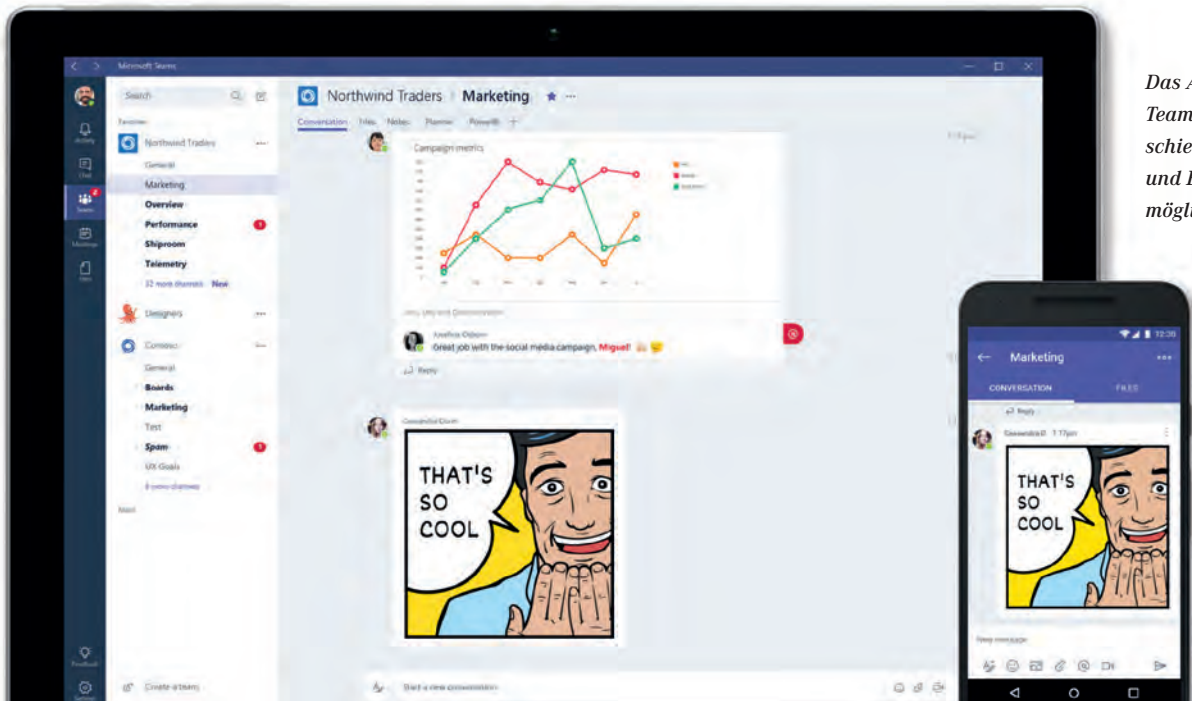
Daten in der europäischen DSGVO-konformen Cloud machen. Welche Daten wollen Sie wem zur Verfügung stellen? Teams arbeitet als Datenablage mit Sharepoint Online und stellt Ihnen pro Team eine Dateiablage bzw. eine Team-Site zur Verfügung. Je nach Einstellung Ihres Teams wird auch die Berechtigung für die Team-Site auf Sharepoint und damit die Dateiablage gesetzt: Die Einstellung „privat“ erlaubt nur eingeladenen Mitgliedern die Teilnahme, „offen“ bedeutet, dass jeder im Unternehmen Teil des Teams werden kann.

Wichtig zu wissen: Neben dem Sharepoint für die Daten wird auch ein Exchange online konfiguriert. Jeder Kanal hat eine eigene E-Mail-Adresse, so dass Teammitglieder News oder E-Mails von Outlook aus direkt in die einzelnen Kanäle posten können. Vorher muss deshalb geplant werden, wie die Cloud-Benutzer mit dem Unternehmensnetzwerk, also dem AD, verknüpft werden. Zudem sollte eine geeignete Backup-Lösung für die Cloud-Datenspeicher eingerichtet werden, wie z. B. Veeam Office 365.

Sollen Mitarbeiter auf die wesentlichen Daten von Teams offline zugreifen können, empfiehlt sich der Einsatz von OneNote für Protokolle, Recherche und Ideensammlung und OneDrive for Business als Sharepoint Client. Beide Produkte sind nicht neu, jedoch vom Funktionsumfang und der Nutzbarkeit erheblich erweitert worden. So lassen sich offline alle Mitschriften und Unterlagen aus Teams bearbeiten. Bei der nächsten Onlineverbindung synchronisieren sich die Dateien dann mit dem Teams Projektraum – inklusive Versionsverfolgung.

Kommunikation: Wie sind Video-Konferenzen und Telefonie eingebunden?

Sie haben nun ein Team, Mitglieder, Projektkanäle, Chat, Daten und einen Exchange für E-Mails. Es fehlt noch die Meetingplattform für interne und externe Konferenzen und ggf. Telefonie. Hier bietet Teams eine mit Skype for Business vergleichbare Lösung, die ihre Stärke im Bereich Audio- und Videokonferenzen hat. Nicht nur die Qualität, auch der Funktionsumfang ist überzeugend. Da wären z. B. das Ausblenden oder die Wahl des Hintergrunds



Das Anzeigen von Teams ist auf verschiedenen Geräten und Betriebssystemen möglich.

in Videosessions oder auch die Aufzeichnungsfunktion, die Videos in STREAM speichert und Ihnen für Schulungszwecke zur Verfügung stellen kann. Selbstverständlich können Sie Ihren Desktop und Anwendungen sowie Daten zur Verfügung stellen. Ein neues Whiteboard, das erstmals mit allen Beteiligten im Meeting verwendet werden kann (gegenüber Skype for Business nur vom Präsentator), rundet die bessere Funktionalität ab.

Mobile Zusammenarbeit: Mit welchen Geräten lässt sich Teams nutzen?

Teams steht auf den Betriebssystemen Windows 10, Android oder iOS zur Verfügung. Dies gilt für Desktop, Laptop und Smartphones. Der Funktionsumfang ist auf den Plattformen nahezu identisch – Details sind online zu recherchieren.

Von ganz klein zu groß: Auch für Konferenzräume existieren bereits Lösungen, basierend auf Teams, wie die Teams Room System Lösung von Polycom und Logitech, bei denen Kamera, Soundsystem und Steuerungspult verwendet werden. Oder auch das Microsoft Surface Hub, das ca. im August 2019 in der Variante 2S und im Sommer 2020 in der Variante 2X erscheinen wird. Über das Touchsystem kann der Anwender direkt in Teams mit Whiteboard und

Planner (Projektplanungssoftware aus Office 365) arbeiten.

Wie finden Sie den Einstieg für Ihr Unternehmen?

Gern unterstützen wir Sie bei Ihrem Einstieg in die Nutzung von Teams. Über Demolizenzen können Sie unverbindlich einen Blick auf Teams werfen und sich einen eigenen Eindruck verschaffen. Auf Wunsch präsentieren wir Ihnen Teams persönlich vor Ort oder per Webcast. Für alle, die tiefer einsteigen möchten, bieten wir Inhouse-Workshops an – von ein bis zu zwei Tagen – bei Bedarf zusätzlich mit Microsoft-Consultants.



Gold Windows and Devices
Gold Small and Midmarket Cloud Solutions
Silver Cloud Productivity
Gold Datacenter
Silver Collaboration and Content



Ihr Ansprechpartner

Jörg Laufer
BDM-Consulting

T +49 228 9080-530
joerg.laufer@hug.de

Der direkte Draht

H&G Hansen & Gieraths EDV Vertriebs GmbH

Bornheimer Straße 42-52
53111 Bonn
T +49 228 9080-0
F +49 228 9080-405
info@hug.de

Durchwahlen und E-Mail-Adressen

Vertrieb

T +49 228 9080-700
F +49 228 9080-405
verkauf@hug.de

IT Consulting & Services (ITCS)

T +49 228 9080-680
F +49 228 9080-607
info@hug.de

Servicecenter

T +49 228 9080-630
F +49 228 9080-605
service@hug.de

Vertriebsbüro Düsseldorf

T +49 228 9080-433
F +49 228 9080-405
info@hug.de

Vertriebsbüro Oldenburg

T +49 441 885-3659
F +49 228 9080-405
info@hug.de

Vertriebsbüro Münster

T +49 228 9080-533
F +49 228 9080-405
info@hug.de

Weitere Informationen und Anfahrtsbeschreibungen
erhalten Sie unter www.hug.de.



Vertrieb

Manfred Wollweber

Vertrieb Server, Storage, Network

T +49 228 9080-510
manfred.wollweber@hug.de



Vertrieb

Jan Gieraths

MPS Sales Manager

T +49 228 9080-781
jan.gieraths@hug.de



Organisation

Birgit Strahl

Qualitäts- u. Umweltmanagement,
Datenschutzbeauftragte

T +49 228 9080-449
birgit.strahl@hug.de



Vertrieb

Jörg Laufer

BDM-Consulting

T +49 228 9080-530
joerg.laufer@hug.de



Servicecenter

Steffen Kleinloth

Teamleiter Servicecenter

T +49 228 9080-650
steffen.kleinloth@hug.de



Einkauf

Klaus Stein

Teamleiter Einkauf

T +49 228 9080-447
klaus.stein@hug.de

HP empfiehlt Windows 10 Pro.



keep reinventing

EliteBook x360 1040 G5

Maximale Flexibilität trifft
auf leistungsstarke Funktionalität.



**Eine Größe.
Passend für jede Situation.**

Arbeiten Sie wie und wo immer Sie möchten mit einem optionalen entspiegelten Touch-Display für den Einsatz im Freien, 360-Grad-Flexibilität und dem wiederaufladbaren HP Active Pen¹.



**Mit integrierter Sicherheit.
Zu Ihrer Sicherheit.**

Schützen Sie Ihren PC vor Bedrohungen mit der exklusiv bei HP verfügbaren Hardware-sicherheit und dem optional integrierten² HP Sure View Gen2 Blickschutz-Bildschirm.



**Vom Café aus zusammen-
arbeiten. Oder von einem
anderen Kontinent.**

Ob Arbeit oder Entertainment: Mit HP profitieren Sie dank optimierter Geräuschunterdrückung und optionalem 4G LTE-Ethernet³ von der Freiheit, sich praktisch überall zu verbinden, wo Sie möchten.



**Partner First
Platinum**

© Copyright 2018 HP Development Company, L.P. Die enthaltenen Informationen können sich ohne Vorankündigung ändern.¹ Der Stift ist optional und muss separat erworben werden.

² Der integrierte HP Sure View-Blickschutz ist ein optionales Feature, das beim Kauf konfiguriert werden muss. HP Sure View wurde für eine horizontale Bildschirmdarstellung optimiert.

³ Das WWAN-Modul ist optional erhältlich und erfordert eine werkseitige Konfiguration sowie einen separat erworbenen Servicevertrag. Wenden Sie sich an Ihren Service-Provider, um mehr über die Netzabdeckung und Verfügbarkeit in Ihrer Region zu erfahren. Verbindungsgeschwindigkeiten variieren je nach Standort, Umgebung, Netzwerkbedingungen und weiteren Faktoren. 4G LTE ist nicht für alle Produkte in allen Regionen verfügbar.