Hybrid Everything®

Welcome to Digital Transformation

stemmer

Ein Unternehmen der Bechtle Gruppe

1/2018

Bechtle übernimmt Stemmer

Seit dem 1.12.2018 gehört Stemmer zur Bechtle Unternehmensgruppe. Henning Heimann und Oliver Herrmann wurden als Geschäftsführer der weiterhin eigenständigen Gesellschaft bestätigt.

Innerhalb der Bechtle-Gruppe fokussiert sich Stemmer vor allem auf die Bereiche Automatisierung, Public Cloud Integration und Managed Services. Unter dem Motto „Hybrid Everything“ kombiniert Stemmer Private Cloud, Public Cloud und On Premise Bausteine zu flexiblen, effizienten und sicheren Infrastruktur-Lösungen.

Bechtle ist mit rund 70 IT-Systemhäusern in Deutschland, Österreich und der Schweiz vertreten und zählt europaweit zu den führenden IT-E-Commerce-Anbietern.Die Bechtle Unternehmensgruppe setzt damit auf ein in dieser Größenordnung einzigartiges Geschäftsmodell, das Systemhaus-Dienstleistungen mit dem Direktvertrieb von IT-Handelsprodukten verbindet.

Seit der Gründung 1983 ist Bechtle beständig auf Wachstumskurs. Mehr als 70.000 Kunden aus den verschiedensten Industrie- und Dienstleistungsbranchen sowie dem öffentlichen Sektor vertrauen auf die Kompetenz der Bechtle Mitarbeiter und die Leistungsstärke der gesamten Gruppe.

Über 9.800 Mitarbeiter setzen sich täglich dafür ein, die Bechtle Erfolgsgeschichte fortzuschreiben. Bechtle ist seit 2000 an der Börse notiert und im MDAX sowie im TecDAX gelistet. 2017 lag der Umsatz bei rund 3,6 Milliarden Euro.

NEWS

Stemmer ist Teilnehmer an der Allianz für Cyber-Sicherheit

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Die innerhalb dieses Netzwerks gewonnenen Informationen tragen auch dazu bei, die Sicherheitslage der Stemmer Kunden zu verbessern.
www.allianz-fuer-cybersicherheit.de

Allianz für Cyber-Sicherheit
Teilnehmer

Stemmer UCC Cloud Services

Die Stemmer UCC Cloud Services schaffen Übergänge zwischen den verschiedenen Kommunikations- und Kollaborations-Plattformen. Dabei werden z.B. Nachrichten zwischen Microsoft Teams Channels und Cisco WebEx Spaces synchronisiert, so dass ein systemübergreifender Austausch stattfinden kann. Die Liste der unterstützten Applikationen (REST, MQTT, Cisco WebEx Teams oder Microsoft Teams, …) wird stetig erweitert.

Veeam: Verfügbarkeitslösung mit Cisco HyperFlex

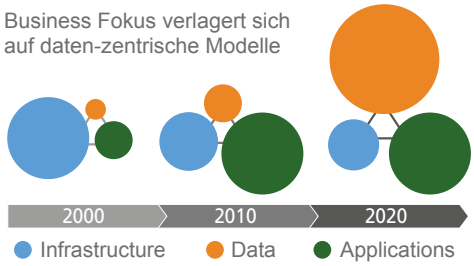
Veeam Software, hat seine Zusammenarbeit mit Cisco deutlich erweitert. Mit Veeam Availability on Cisco HyperFlex liefern die beiden Unternehmen eine neue, zuverlässige Datenmanagementplattform mit hoher Skalierbarkeit und einfacher Bedienung. Die integrierte Lösung für Multi-Cloud- Umgebungen wird ab dem vierten Quartal 2018 angeboten.

Datacenter

NetApp Data Fabric Strategie

Informationen gehören heute zu den wichtigsten Vermögenswerten eines Unternehmens. Mit der Data Fabric Strategie von NetApp behalten Unternehmen die Kontrolle über ihre verteilten Daten.

Data Fabric ist die NetApp Strategie für Datenmanagement, bei der verschiedene Clouds – Private, Public oder Hybrid – nahtlos vernetzt werden. Die Data-Fabric-Strategie vereinheitlicht das Datenmanagement über verteilte Ressourcen hinweg und ermöglicht dadurch Konsistenz und Kontrolle der Datenmobilität, Sicherheit, Sichtbarkeit, Sicherung und Zugriff auf die Daten.



Kunden, die von der Data-Fabric-Strategie von NetApp profitieren, nutzen damit jede Cloud einfach als weitere Storage-Tier innerhalb ihres Unternehmens. So können sie ein besseres Verständnis für ihre Business-Workloads entwickeln, neue Applikationen schneller bereitstellen, den Betrieb automatisieren und ihre IT-Servicebereitstellung besser kontrollieren.

Aus technischer Sicht werden die lokalen physikalischen Storage-Systeme und die virtuellen Public Cloud Speicher via SnapMirror miteinander verbunden. Dank Managementtools, APIs und breit angelegter Integration von Storage-Systemen können sie ganz einfach gemeinsam genutzt werden. Services auf verschiedenen Schichten ermöglichen einen allgemeinen Überblick über die Geschäftsabläufe sowie ihre Kontrolle. Da die Data-Fabric-Infrastruktur mehrere Clouds unterstützt, können Unternehmen aus einer Vielzahl von Umgebungen auswählen.

Datacenter

NetApp HCI

NetApp HCI ist eine hyperkonvergente Cloud-Infrastruktur für verschiedenste Unternehmensanwendungen. Die Systeme verbinden Solidfire Storage-Arrays und VMware vSphere zu hochautomatisierten Private-Cloud-Datacentern.

Alle IT-Abteilungen verfolgen das Ziel, Routineaufgaben zu automatisieren und dabei das Risiko von Anwenderfehlern bei manuellen Vorgängen zu beseitigen. NetApp HCI optimiert die Installation mithilfe einer intuitiven Implementierungs-Engine und hat über 400 Inputs auf weniger als 30 reduziert. Dadurch steht die Plattform in rund 45 Minuten bereit.

Die Administration der NetApp HCI Systeme erfolgt über das zentralisierte Management von VMware. Außerdem ermöglicht eine stabile API-Suite eine nahtlose Integration in übergeordnete Tools für Management, Orchestrierung, Backup und Disaster Recovery.

NetApp HCI Vorteile auf einen Blick:

- Ausführung mehrerer Applikationen mit garantierter Performance
- Problemlose Implementierung von HCI im gesamten Datacenter
- Senkung der Betriebskosten um bis zu 67 % durch Vereinfachung und Automatisierung des Managements
- Integration in die NetApp Data-Fabric-Infrastruktur, um jederzeit Zugriff auf Daten in jeder Cloud zu haben

NetApp HCI

Cisco DNA - Schlüsselfaktor gegen Cyber-Kriminalität

Unzureichend geschützte Systeme bieten Cyber-Kriminellen viele Möglichkeiten, sensible Daten auszuspähen, Geräte zu manipulieren und Prozesse zu sabotieren. Ein einziges Datenleck reicht aus, um die komplette Organisation zu infiltrieren. Hybride Infrastrukturen und eine steigende Anzahl an Endgeräten machen herkömmliche Sicherheitsmaßnahmen zunehmend wirkungslos.

Die wichtigste Verteidigungslinie gegen Cyber-Kriminelle ist zukünftig das Netz. Cisco ist mit seiner Digital Network Architecture (DNA) Vorreiter im Bereich intelligenter, selbstverteidigender Netzwerke.

Security Intelligence

Ein modernes „digitalisiertes“ Netzwerk verwendet maschinelles Lernen und künstliche Intelligenz um Angriffe sowie Bedrohungen schnellstmöglich aufzuspüren. Hinzu kommt die Fähigkeit, Gegenmaßnahmen automatisiert und ohne Zeitverzug (time to detect) einzuleiten. Denn umso schneller ein Angriff bekämpft wird, desto geringer sind die Wiederherstellungskosten.

Segmentierung

Traditionelle Segmentierungen sind bis dato sehr komplex in der Pflege und im Betrieb. Um möglichst wenig Aufwand zu betreiben und vorrangig die Komponente „Automatisierung“ im Bereich der Segmentierung einzusetzen, baut Cisco auf eine „sofware-defined“ Segmentierung. Dieser Ansatz gruppiert Geräte vollautomatisch in Sicherheitsgruppen, dies OHNE die bisherige Netzwerkstruktur großartig zu verändern.

Unterstützung für SaaS

Der Datenverkehr verschiebt sich zunehmend hin zu einem Software-as-a-Service (SaaS) Modell, bei dem sich Unternehmens- und öffentliche Ressourcen jenseits der Mauern eines Unternehmens befinden – und zwar in einem der vielen tausend Rechenzentren auf der ganzen Welt. Ein digitalisierungsbereites Netzwerk sollte den Datenverkehr durchgängig sichern, unabhängig davon, ob es sich dabei um SaaS-basierten oder herkömmlichen Datenverkehr handelt.

Datacenter

Cisco stellt Server für KI und Machine Learning vor

Laut dem Gartner Hype Cycle für Künstliche Intelligenz geben bislang nur 4 Prozent der CIOs weltweit an, dass sie an KI-Projekten arbeiten. Diese Zahl wird in den nächsten Jahren jedoch deutlich ansteigen. IT-Abteilungen werden vor dem Problem stehen, zusätzliche Workloads, neue Trafficmuster und neue Querverbindungen innerhalb ihres Unternehmens zu bewältigen. Um sie hier zu unterstützen, stellt Cisco seinen ersten Server vor, der speziell für KI- und ML-Workloads entwickelt wurde.

Der neue Cisco UCS-Server beschleunigt Deep Learning. Das ist eine rechenintensive Form des maschinellen Lernens, die neuronale Netze und große Datensätze nutzt, um Computer für komplexe Aufgaben zu trainieren. Der Server ist mit leistungsstarken NVIDIA-GPUs ausgestattet und wurde entwickelt, um viele der bekanntesten ML-Software-Stacks zu beschleunigen.

Datenwissenschaftler und Entwickler können zwar mit maschinellem Lernen am Laptop experimentieren, aber Deep Learning in großem Maßstab erfordert viel mehr Rechenleistung. Außerdem bedarf es einer IT-Architektur, die große Datensets verarbeiten kann. Darüber hinaus benötigt Deep Learning Werkzeuge, die diese Daten in sinnvollen Zusammenhang bringen und daraus lernen können. Aus diesem Grund arbeitet Cisco mit seinen Technologiepartnern daran, viele der heute wichtigsten Werkzeuge für maschinelles Lernen zu validieren. Dieser Prozess soll deren Bereitstellung vereinfachen und schneller Ergebnisse liefern.

Stemmer Phone BLF

Die von Stemmer neu entwickelte Software „Stemmer Phone BLF“ konfiguriert die Tasten und Belegtlampen eines Cisco Telefons komfortabel über ein Windows Programm. Mit „Stemmer Phone BLF“ ist es nicht mehr notwendig einen Callmanager Administrator mit dieser Aufgabe zu betrauen. Der Anwender konfiguriert hier selbst.

Der Mitarbeiter sieht in der Software sein Telefon und kann die für die Konfiguration hinterlegten Schaltflächen bequem anklicken und anschließend die Zielnummer und den Namen der Zielperson eintragen. Die Administratoren werden durch Stemmer Phone BLF erheblich entlastet, da die Änderungen der Belegt-Lampen-Felder auf den Endgeräten der Nutzer für sie entfällt. Benutzer sind flexibler in der Verwendung der Belegt-Lampen-Felder, da sie diese jederzeit rekonfigurieren und für ihren persönlichen Nutzen anpassen können.

Funktionsweise

Anhand des Windows Benutzernamens ermittelt die Software über die Cisco AXL Dienste im Call-Manager die dem Mitarbeiter zugeordneten Telefone und Beistellmodule. Für jedes Telefon und Beistellmodul wird die im Call-Manager hinterlegte Schaltflächenkonfiguration ausgelesen und die für den Mitarbeiter konfigurierbaren Belegt-Lampen-Felder werden auf dem Geräte-Bild in der Software entsprechend hervorgehoben.

Der Mitarbeiter kann nun die hervorgehobenen Schaltflächen anwählen, eine entsprechende Zielnummer eintragen oder aus dem Firmen-Telefonverzeichnis auswählen und der Taste eine Bezeichnung geben. Die vergebene Bezeichnung wird auf dem Telefon im Display neben der Taste angezeigt. Die geänderte Telefonkonfiguration wird per REST über die Cisco AXL Schnittstelle im Call-Manager gespeichert und im Anschluss automatisch an das Endgerät übertragen.

Vorteile auf einem Blick:

- Komfortable Bedienung durch den Endanwender, da die im Call-Manager hinterlegte Vorlage der konfigurierbaren Schaltflächen in der Software automatisch berücksichtigt wird
- Unterstützt Telefone mit Beistellmodulen
- Konfiguration im Cisco Call-Manager erfolgt über die AXL Dienste
- Hinterlegung von neuen Telefonmodellen durch einen Administrator möglich

Broadsoft: Telefonie und Collaboration aus der Cloud

Stemmer erweitert das Collaboration Portfolio durch die Bereitstellung einer zukunftssicheren und flexiblen Cloud PBX Lösung. Die auf Broadsoft basierende Public Cloud Plattform bietet eine natürliche Evolution zu klassischen On Premise Lösungen. Im Bereich Communication und Collaboration verfügt Stemmer über zwei Jahrzehnte Erfahrung in Beratung, Implementierung und Betrieb.

Seit diesem Jahr ist Broadsoft ein Teil von Cisco. Mit der Übernahme des Marktführers für cloudbasierende TK- und Collaboration Lösungen erweitert Cisco sein bestehendes Webex Portfolio.

- Flexibilität durch On Demand Bereitstellung von Collaboration Tools und Lösungen die den Modern Workplace Anforderungen gerecht werden. Hierzu zählen Lösungen für Home-Office, Mobile-Office und agiles Arbeiten in dynamischen Teams.
- Optimale Voraussetzungen für das Planen und Durchführen von Meetings durch die Verfügbarkeit von marktführenden Real-Time Konferenzdiensten
- Integrierte Anbindung an das Telefonnetz mit flexibler und schneller Bereitstellung der Rufnummern für Unternehmensstandorte
- Schnelleres und kosteneffizienteres Deployment durch einen geringeren Anteil an erforderlicher Infrastruktur und geringere Komplexität.

Maßgebliche Erfolgsfaktoren für eine Implementierung sind sowohl in der technischen Netzwerkplanung, die Qualität des Betriebs aus der Managed Service Perspektive, wie auch beim Adoption Consulting und Success Management zu finden. Hierdurch wird eine optimale Anpassung an die Business Anforderungen des Kunden, wie auch eine stabile und hochverfügbare Umgebung geschaffen die gleichzeitig ein hohes Maß an Flexibilität bietet.

Mobile Device Management mit Microsoft Intune

Mittels Microsoft Intune können Mitarbeiter über nahezu jedes Endgerät (Z.B. Notebooks, Tablets und Smartphones) und Betriebssystem (Windows, Android und Apple IOS) auf ihre gewohnten Office Applikationen (Z. B. Word, Excel und Outlook) einschließlich Daten zugreifen. Die in der Cloud verwalteten Apps und Daten sind dabei vom Wirtssystem entkoppelt.

Um bestmöglich den individuellen Anforderungen von Unternehmen und Mitarbeiter gerecht zu werden, bietet Microsoft Intune verschiedene Sicherheits- und Management-Level. Beginnend mit der Verwaltung und Absicherung einzelner Anwendungen im Rahmen eines sogenannten Mobile Applikation Managements (MAM) steigert sich der Leistungsumfang von Microsoft Intune bis hin zu einem vollumfänglichen Mobile Device Management (MDM), mit welchem die ganzheitliche Verwaltung von Endgeräten sowie der darauf befindlichen Applikationen und Daten gewährleistet werden kann.

Schutz von Daten und Zugriffen

Im Zusammenspiel mit Produkten wie Microsoft Azure Active Directory und Microsoft Azure Information Protection stellt Microsoft Intune sicher, dass berechtigte Personen nur dann Zugriff auf ihre Daten und Applikationen erhalten, wenn der Zugriff über genehmigte und geprüfte Endgeräte erfolgt. Ebenso kann damit sichergestellt werden, dass schützenswerte Inhalte nicht an öffentlichen oder potentiell unsicheren Speicherorten gespeichert werden können.

Einsatz in vielfältigen IT-Szenarien

Kunden haben die Möglichkeit Microsoft Intune sowohl als Public-Cloud-Dienst, als auch als Hybrid-Lösung im Zusammenspiel mit Microsoft System Center Configuration Manger (SCCM) oder als reinen On-Premise-Services (Bereitstellung von SCCM im eigenen Rechenzentrum) zu beziehen.

Vorteile:

- Unkomplizierte Einrichtung der Umgebung
- Einfache Administration der Umgebung
- Umfassende Verwaltung von Endgeräten

Datacenter | Security

ProLion: Dedizierter SnapShot-Restore auf Datei-Ebene

CryptoSpike wurde entwickelt, um NetApp ONTAP-Systeme vor Malware-Angriffen zu schützen. Viele Unternehmen investieren noch immer einen Großteil ihrer Security-Budgets in aktive Verteidigungssysteme wie Firewalls und Virenscanner. Eine ganze Reihe von Cyberattacken unterwandern jedoch diese Schutzmechanismen und werden erst im Nachhinein anhand ihrer Auswirkungen, bzw. durch Anomalien-Scanner, sichtbar.

Nach ihrer Entdeckung ist das Problem jedoch meistens nicht gelöst! Einige aggressive Malware-Varianten lassen sich erst durch das Einspielen von Backups vollständig beseitigen. Je nachdem wie weit zurückgesichert werden muss, kann dies, für die betroffenen Unternehmen, existenzbedrohend sein.

Neben verschiedenen Erkennungsmethoden fokussiert sich die Software vor allem auf die Minimierung des Datenverlustes. Dafür protokolliert CryptoSpike sämtliche Datenaufrufe und -bewegungen innerhalb der NetApp-Systeme. In einer Datenbank wird hinterlegt, welche Endgeräte, wann und mit welchen Dateien in Berührung gekommen sind. Anhand dieser Verbindungsdaten ist CryptoSpike in der Lage, via SnapShot-Technologie, befallene und gefährdete Dateien dediziert durch Vorgängerversionen zu ersetzen.

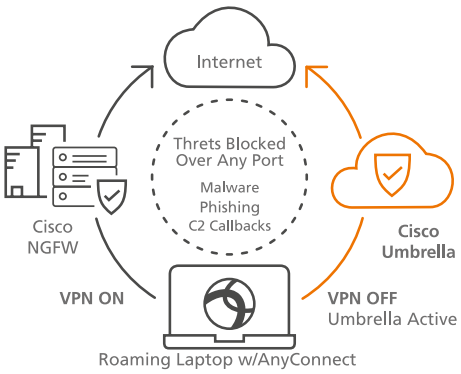
Cisco Umbrella - Mobile All-Client Security

Zur Abwehr von Cyber-Attacken und internen Bedrohungen verfügen die meisten Unternehmen über eine Vielzahl verzahnter Schutzsysteme. Hiervon profitieren nicht nur Mitarbeiter im Office, sondern auch mobile User, die sich via VPN mit dem Unternehmensnetzwerk verbinden. Dieser Umweg wird jedoch meistens - und speziell beim Surfen oder der Verwendung von Clouddiensten - als Behinderung wahrgenommen und wenn möglich umgangen.

Unternehmen, die gleichzeitig auf Sicherheit und Mitarbeiterzufriedenheit setzen, finden in Cisco Umbrella eine optimale Alternative. Dieses cloudbasierte Secure Internet Gateway (SIG) ermöglicht es mobilen Mitarbeitern, sich auch ohne VPN-Verbindung sicher im Internet zu bewegen.

Um unbekannte und neue Bedrohungen zu erkennen und Verbindungen zu schädlichen Zielen bereits auf der DNS- und IP-Ebene zu blockieren, setzt Cisco auf intelligente Proxys und maschinelles Lernen. Hierdurch lassen sich sogar SSL-Verschlüsselte Webseiten auf Schadsoftware untersuchen.

Für die Anwender ist die Umbrella-Technologie nahezu unsichtbar. Das liegt daran, dass beim Design des Dienstes (neben den Sicherheitsaspekten) vor allem die User Experience im Vordergrund steht.



Cisco Master Security Specialization

Stemmer ist eines von zwei Unternehmen in Deutschland, das von Cisco mit der Master Security Spezialisation ausgezeichnet wurde.

Um das von Cisco verliehene Zertifikat zu erhalten, müssen Partner ein dreistufiges Audit erfolgreich bestehen und dabei nachweisen, dass sie über die entsprechende Expertise unter anderem in den Bereichen Technologie, Kundenberatung und Sales verfügen.

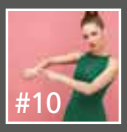
Den Kern des Stemmer Security Teams bilden dabei hochqualifizierte Consultants und Engineers. Auch auf diesem Gebiet belegt Stemmer eine Spitzenposition unter den Cisco Partnern. Stemmer verfügt über einen der beiden deutschen „Fire Jumper Elite“ Consultants, einem Spezialisten mit der höchsten Zertifizierungsstufe im Cisco Umfeld.

Hybrid Everything erscheint 4x pro Jahr. Alle Inhalte sind sorgfältig recherchiert. Alle Angaben erfolgen ohne Gewähr. Alle Rechte vorbehalten.

Bildnachweis: stock.adobe.com

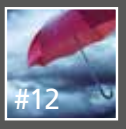
stemmer
Ein Unternehmen der Bechtle Gruppe

Webinare



TTD (time to detect)
Im Kampf gegen Malware spielt der Faktor Zeit die entscheidende Rolle.
30 Min. | Security

Cisco Stealthwatch Cloud
Anomalieerkennung in der Hybrid Cloud. Bestimmte Malware-Varianten sind an den Unternehmensgrenzen nicht aufzuhalten.
30 Min. | Security



Mobile All-Client Security
Cisco Umbrella ermöglicht mobilen Mitarbeitern, sich auch ohne VPN-Verbindung sicher im Internet zu bewegen.
30 Min. | Security

Notfallplan für Emotet Trojaner
Achtung: Extrem gefährlicher Trojaner im Umlauf.
30 Min. | Security

Anmeldung unter:
www.stemmer.de/webinare.html

Herausgeber

Stemmer GmbH
Peter-Henlein-Straße 2
82140 Olching (Germany)

Stemmer Standorte

München, Köln, Siegen, Stuttgart, Karlsruhe, Duisburg

Partner in dieser Ausgabe:

Allianz für Cyber-Sicherheit, Broadsoft, Cisco Systems, Microsoft, NetApp, ProLion, Veeam