AUSGABE 01.2017

Inside ACP

Der Newsletter der ACP IT Solutions

Deutschland ist sich der Gefahr bewusst

Der Industrieversicherer Allianz veröffentlicht jedes Jahr einen „Risk Barometer“ mit den 10 wichtigsten globalen Geschäftsrisiken. Neben den klassischen Risiken wie Betriebsunterbrechung aufgrund von Naturkatastrophen, Bränden oder menschlichem Versagen ist für Unternehmen mittlerweile die Cyberkriminalität eines der größten Geschäftsrisiken, so die Studie.

Für deutsche Unternehmen sind die digitalen Angriffe sogar Problem Nummer eins. 72% der Firmen nannten dabei die Sorge vor Hackerangriffen an erster Stelle, gefolgt von Daten- oder Sicherheitsverletzungen (63%), Malware und anderen Viren (54%) sowie Fehlern oder Täuschungen durch Mitarbeiter (32%). Die fortschreitende Digitalisierung und die damit verbundenen Möglichkeiten in der Vernetzung bedürfen deshalb einer Neubewertung des Sicherheitsrisikos. Viele Unternehmenslenker beschäftigen sich jedoch erst nach einem Angriff mit dem Thema Sicherheit. Erst wenn Daten geklaut oder ganze Netze lahmgelegt werden, bekommt der Risikoschutz den notwendigen Stellenwert, d.h. es wird eilig die Unternehmens-IT aufgerüstet und im besten Fall eine firmenweite Cyber Policy eingeführt – meist jedoch zu spät.

Die neue Allianz-Studie gibt jedoch Hoffnung, dass das Bewusstsein für digitale Bedrohungslagen in den Chefetagen steigt und präventiv gehandelt wird. Aus technischer Sicht hat sich am Security-Markt auch etliches getan und es existieren mittlerweile einige vielversprechende Lösungen zum Schutz vor Angriffen. ACP stellt einige Lösungen seiner Top-Partner vor, die im Kampf gegen Cyberkriminalität helfen.

Cisco
Schutz vor Malware

Watchguard
Ende der klassischen TK-Anlagen

HPE
Erkennen von Anomalien

NEWS

Hewlett Packard Enterprise übernimmt Nimble Storage

HPE übernimmt den Speicherspezialisten Nimble Storage. Das auf Flash-Speicher fokussierte Unternehmen soll zukünftig das Storage-Portfolio von HPE nach unten abrunden. HPE verfügt mit der 3PAR bereits heute über eines der leistungsfähigsten und universellsten Storage-Systeme. Die Analytics-Plattform von Nimble soll auf das gesamte Portfolio ausgedehnt werden. Derzeit sind beide Unternehmen als Leader im Gartner Magic Quadrant vertreten.

VMware beschleunigt die Transformation des digitalen Arbeitsplatzes

VMware stellt neue Lösungen, Services und Features innerhalb des Horizon-Produktportfolios vor. Die Innovationen wurden entwickelt, um Kosten und Komplexität bei der Bereitstellung und Verwaltung von virtuellen Anwendungen und Desktops zu senken, die eine kostengünstige Möglichkeit für die nutzerfreundliche Bereitstellung von Windows-basierten Anwendungen als Teil eines modernen digitalen Arbeitsplatzes darstellen.

Citrix: Deutsche Unternehmen nicht ausreichend geschützt

Fast drei Viertel der deutschen IT-Verantwortlichen sind sich einig: ihre Sicherheitsarchitektur muss dringend erneuert werden. 63 Prozent bescheinigen ihrem Unternehmen veraltete Sicherheitslösungen, mit denen weder Angreifer abgewehrt noch Compliance-Vorgaben eingehalten werden können. Das ergab die aktuelle Studie des Ponemon Institutes in Zusammenarbeit mit Citrix.

DELL

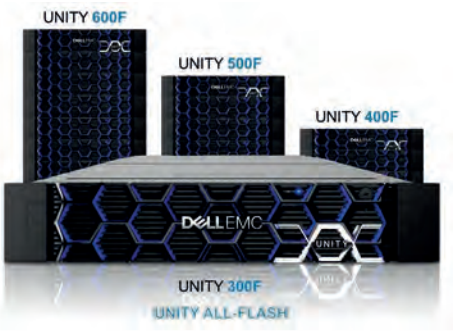
EMC UNITY™ ALL-FLASH

Die Unity All-Flash-Arrays wurden speziell für den Einsatz in Hochgeschwindigkeits-Umgebungen entwickelt. Die auf den Midrange-Markt ausgerichteten Systeme überzeugen vor allem durch ihre hohe Speicher-Dichte, Wirtschaftlichkeit und Anwenderfreundlichkeit.

Unity ist innerhalb von wenigen Minuten aufgebaut und konfiguriert. Unity All-Flash-Konfigurationen enthalten die gesamte Soft - ware, die für eine einfache Konsolidierung und Verwaltung von virtualisierten Anwendungs-Workloads benötigt wird.

Durch ein nahtloses Tiering von inaktiven File- und Block-basierten Daten von Unity in die Cloud kann die IT neue Kapazitäten auf dem primären Speicher schaffen, Investitions- und Betriebskosten senken und somit die Effizienz des Unternehmens verbessern. Die integrierte File Tiering/Archivierungssoftware von Unity ermöglicht Kunden das Tiering inaktiver Dateien in Public Clouds wie Microsoft Azure oder Amazon S3.

Unity All-Flash setzt die Tradition der Dell EMC Midrange-Speicher fort und ermöglicht es, Datei-Workloads und transaktionsbezogene Workloads im Unternehmen kostengünstig über NAS und SAN auf einem einzigen Speichersystem zu konsolidieren und zu managen.



HPE

Sicherheit durch Anomalien-Erkennung

Klassische Security-Systeme schützen meistens nur gegen Bedrohungen von außen – gegenüber fahrlässigen und kriminellen Mitarbeitern sind sie in der Regel wirkungslos. Ist das Unternehmen erst einmal unterwandert oder kontaminiert, helfen nur noch Systeme zur Verhaltensanalyse von Nutzern und Geräten (User and Entity Behavior Analytics, UEBA).

Mit der Übernahme von Niara hat HPE sein Security Portfolio entsprechend erweitert. Niara ist darauf spezialisiert, mittels maschinellem Lernen und Big-Data-Analyse Anomalien innerhalb des Intranets zu erkennen. Auf dieselbe Weise werden auch Aktivitäten von externen Angreifern, die andere präventive Maßnahmen erfolgreich umgangen haben, erkannt.

Entscheidend für eine erfolgreiche Verhaltensanalyse ist die ganzheitliche Überwachung des Network-Traffics. Im Falle von Niara und HPE Aruba dürfte die Integration nahezu reibungslos erfolgen, da beide Unternehmen seit langem eng kooperieren.

Inwieweit die Technologie auch bei den Nicht-Aruba-Produkten zum Einsatz kommt, wird sich zeigen. HPE hat bei seinen Netzwerkprodukten konsequent auf das Thema Software Defined Networking gesetzt. Diese Weitsicht könnte sich nun bezahlt machen.

ACP Network- und Security-Teams arbeiten eng zusammen und sorgen somit für den Aufbau sicherer Infrastrukturen.

FORTINET

FORTIGATE RUGGED für den Schutz kritischer Infrastruktur und Leittechnik

Überwachungs- und Steuerungssysteme (SCADA = Supervisory Control and Data Acquisition) von Industrie-, Versorgungs- und Logistikunternehmen stehen zunehmend im Fokus maßgeschneiderter Angriffe.

Ungeachtet ihrer Bedeutung, werden diese Systeme aus sicherheitstechnischen Gesichtspunkten oftmals vernachlässigt.

Getreu dem Motto „never touch a running system" werden sicherheitsrelevante Updates nicht eingespielt und veraltete Komponenten nur selten ausgetauscht.

Entscheidend für die Modernisierung der SCADA-Infrastruktur ist die Verwendung der geeigneten Komponenten. Spezielle Protokolle wie DNP3, ICCP und Modbus kommen hier ebenso zum Tragen wie bestimmte Anforderungen an die Client-Server-Kommunikation, das Timing und die Encodierung der Daten. Zusätzlich zu den Security-Systemen für die „Bürokommunikation" unterhält Fortinet mit FortiGate Rugged eine eigene Produktlinie zur Sicherung industrieller Steuerungssysteme.

Eigenschaften von FortiGate Rugged:

Segmentierung: Eine hohe Portdichte und virtuelle Domänen ermöglichen physische oder logische Trennung.

Strenge Authentifizierung: Zwei-Faktor-Verfahren verstärken Identität und Zugriff.

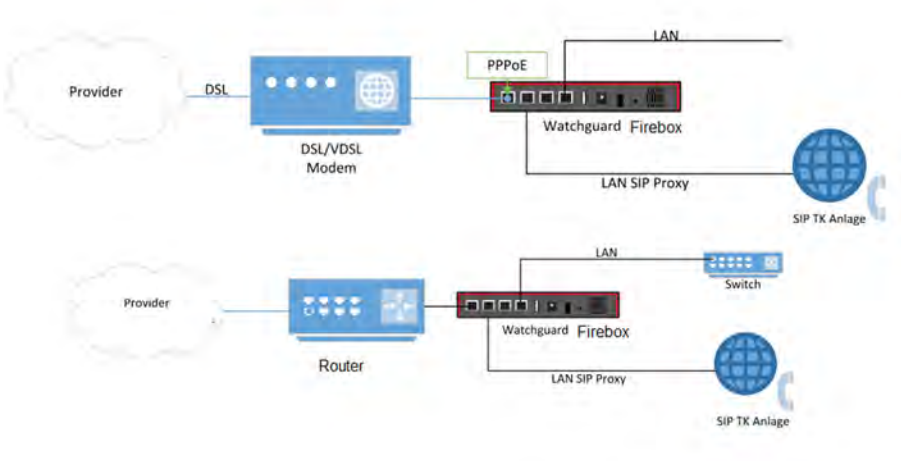
Bedrohungsabwehr: Erstklassige industrielle steuerungsspezifische IPS, App-Steuerung und mehr, um Angriffe abzuwehren.

Erweiterte Bedrohungserkennung: Client-Zuverlässigkeit, Sandboxing und andere Verfahrensweisen, um fortgeschrittene Angriffe zu identifizieren.

WATCHGUARD

Gut gewappnet in die Post-ISDN-Ära

Unternehmen, die noch immer auf ISDN oder analoge Anschlüsse angewiesen sind, sollten nun schleunigst handeln. Bis Ende 2018 wird die Deutsche Telekom ihr gesamtes kabelbasiertes Geschäftsmodell auf All-IP umstellen.



Eile ist vor allem dann geboten, wenn das alte TK-System neben der Telefonie zusätzlich für die Datenübertragung und/oder Sonderanwendungen (z.B. SMS, Datex-P und Dreierkonferenzen) benötigt wird.

Auch die Tage der klassischen TK-Anlage sind gezählt. Es ist zwar möglich, die Einsatzdauer mittels Gateways zu verlängern, langfristig ist ein Umstieg auf neuere Technologien jedoch kaum vermeidbar. Vor der Beschaffung eines neuen Kommunikationssystems sollte jedoch überprüft werden, ob vorhandene Infrastrukturbausteine (Switches, Security-Systeme, usw.) überhaupt dafür geeignet sind.

Watchguard hat diese Entwicklung frühzeitig erkannt und seine Produkte entsprechend ausgestattet. Die Next-Generation-Firewall und alle Unified Threat Management (UTM) Systeme unterstützen die Einbindung moderner SIP TK-Anlagen. Bei der Verwendung von DSL-Modems können die PPPoE-Einwahldaten zudem auf der Watchguard hinterlegt werden.

J. u. A. Frischeis – neue IT-Strukturen für mehr Effizienz und Sicherheit

ACP erneuerte die IT-Strukturen beim führenden Großhändler für Holz und Holzwerkstoffe in Zentraleuropa, der J.u.A. Frischeis Ges.m.b.H. Das Unternehmen wurde mit modernsten Technologien zur Steigerung von Effizienz und Datenschutz ausgestattet. Darüber hinaus gewährleisten Managed Services von ACP zusätzliche Sicherheit und laufende Betreuung durch Experten.

Gegründet im Jahr 1948 als kleiner Familienbetrieb im niederösterreichischen Stockerau, hat sich die J. u. A. FRISCHEIS Ges.m.b.H. kontinuierlich zum führenden Großhändler für Holz und Holzwerkstoffe in Zentraleuropa entwickelt. Heute betreibt das Unternehmen 49 Niederlassungen in 14 Ländern und beschäftigt mehr als 2.400 Mitarbeiter. FRISCHEIS garantiert die zuverlässige Versorgung gewerblicher und industrieller Abnehmer mit qualitativ hochwertigen Rohstoffen und Halbfertigprodukten. Neben einer umfangreichen Produktauswahl verfügt das Unternehmen über eine leistungsstarke Logistik und moderne Bearbeitungszentren.

Strukturerneuerung

ACP zeichnet seit 1998 für die Hardwareausstattung der FRISCHEIS Ges.m.b.H. verantwortlich. Später etablierte sich der IT Provider auch als Dienstleister für die Server- und Storage-Infrastruktur im FRISCHEIS Datacenter. Storage-Systeme von NetApp, Server von HP sowie Software-Verteilung mittels Microsoft SCCM waren die gemeinsam umgesetzten Projekte. Eine von ACP implementierte Citrix-Lösung ermöglicht zudem den ortsunabhängigen Zugriff aller Frischeis-Mitarbeiter auf virtuelle Desktops. Als langjähriger Partner wurde ACP auch mit der Umsetzung eines neuen WAN-Konzeptes für alle FRISCHEIS-Niederlassungen betraut. Die gewachsenen Strukturen sowie Datenleitungen mit niedriger Bandbreite konnten die gestiegenen Anforderungen moderner betrieblicher Kommunikations- und Sicherheitsstandards nicht mehr erfüllen und sollten nun erneuert werden.

Firewall-Technologie von FORTINET

Nach ausführlichen Teststellungen und Vorarbeiten durch das ACP Team entschied sich die J.u.A. Frischeis für ein umfangreiches Konzept unter Verwendung von FortiGate Firewalls von FORTINET sowie lokaler Internetleitungen unterschiedlichster Technologien (xDSL, Glasfaseranbindungen) und VPN-Tunnels in die Unternehmenszentrale. „Das Sicherheitskonzept basiert auf dem Einsatz von FortiGate Firewalls. Abhängig von Größe und Anforderung des jeweiligen Standorts, kommen unterschiedliche Modelle (FortiGate 60C, FortiGate 111C, FortiGate 300C) als Cluster oder Einzelsystem zum Einsatz. Der Internetzugriff wurde für alle Filialen mit einem lokalen Outbreak realisiert“, erklärt Ing. Wolfgang Ailec, FortiGate-Spezialist bei ACP, die neue Lösung.

Managed Services von ACP

Alle zentralen Dienste, wie beispielsweise Exchange Service oder ERP-Systeme, sind über die redundanten VPN-Verbindungen von jeder Filiale aus erreichbar. Die Redundanz wird mit Hilfe einer zweiten Internetanbindung erzeugt, die nur im Fehlerfall zum Einsatz kommt. Als Backup-Systeme sind UMTS Router, ADSL-Leitungen und Funknetze in Verwendung. Die Umschaltung erfolgt volltransparent durch die FortiGate Firewalls. Für zusätzlichen Schutz werden an sämtlichen Standorten außerdem die UTM Features IPS (Intrusion Protection System), AV (Anti Virus) und WF (Webfilter) sowie ein Proxyserver verwendet. Der Proxyserver ist mit unterschiedlichen Berechtigungsprofilen versehen, die je nach Gruppenzugehörigkeit des Benutzers im Active Directory zur Anwendung kommen. Die Verbindung zum Active Directory erfolgt mit Hilfe des FSSO Agents (Fortigate Single Sign On). Dies ermöglicht eine Authentifizierung am Proxyserver mit den Active Directory Credentials, ohne erneut Benutzer und Passwort eingeben zu müssen.

Vorteile und Nutzen

DI Robert Klausner, IT-Leiter von Frischeis, erklärt: „Durch die lokale Internet-Anbindung ist die nutzbare Bandbreite in unseren Filialen nun um ein Vielfaches größer als vorher und damit eine merkliche Produktivitätssteigerung erreicht worden. Gleichzeitig konnten wir mit dem neuen Konzept unsere Kosten maßgeblich optimieren. Die neuen Datenleitungen sind im laufenden Betrieb günstiger als die ursprüngliche Verbindung. Darüber hinaus entfallen durch die zentrale Firewall-Lösung bisher notwendige, laufende Sicherheitsüberprüfungen an jedem einzelnen Standort.“ „Die Sicherheit der Datenverbindungen wird durch das Full Managed Service von ACP gewährleistet. Etwaige Probleme können somit durch unsere Experten im Voraus verhindert, respektive im Störungsfall zeitnah behoben werden. Mit der neuen Gesamtlösung bieten wir außerdem höchstmögliche Verfügbarkeit für einen reibungslosen Ablauf aller IT- Prozesse der J.u.A. Frischeis“, ergänzt Alexander Neubauer, Leiter des ACP Security Competence Centers.

NEWS

ACP setzt auf HPE Service Provider-Kompetenz

Nicht alle Service Provider nehmen die Sicherung und den Schutz der ihnen anvertrauten Daten ernst genug. Umgerüstete PCs und Bastellösungen prägen noch immer das Bild vermeintlich billiger Cloud-Anbieter. Dass es hierzu auch professionelle und dennoch preisgünstige Alternativen gibt, zeigen die Rechenzentren der ACP-Gruppe. Auf Basis von Hewlett Packard Enterprise (HPE)-Systemen und -Technologien betreibt ACP mehrere eigene Datacenter in Deutschland und Österreich. Dass dies nicht zu Lasten der Preisgestaltung geht, liegt an zwei Faktoren. Über das HPE Service Provider-Programm hat ACP die Möglichkeit, spezielle Produkte und Lösungen deutlich günstiger zu erwerben. Gleichzeitig ergeben sich hieraus Einsparungen der Betriebskosten, von denen die Kunden profitieren.

Microsoft: Rechenzentren in Deutschland stärken Vertrauen in Cloud-Dienste

Die Speicherung von Daten ausschließlich in Deutschland spielt für Entscheider in der digitalen Transformation eine wesentliche Rolle. Dies zeigt eine aktuelle Studie der techconsult GmbH im Auftrag der Microsoft Deutschland GmbH, die vor allem Unternehmen aus dem Mittelstand und den Branchen Finanzwesen, Bildung, Gesundheitswesen und öffentliche Verwaltung untersucht. Mehr dazu unter: www.techconsult.de

CISCO AMP

Schutz gegen Malware

Cisco verfügt derzeit über ein sehr breites Portfolio an integrierten AMP-Lösungen (Advanced Malware Protection), die sowohl im Netzwerk als auch in Endgeräten und Applikationen nach Verhaltensauffälligkeiten suchen.

Cisco AMP bedient sich dabei verschiedenster Technologien, wie weltweit erfasster Threat-Intelligence, fortschrittlichem Sandboxing und Echtzeit-Blockierung von Malware. Allein vorbeugende Maßnahmen reichen jedoch nicht mehr aus. Cisco AMP analysiert daher zusätzlich sämtliche Dateiaktivitäten im gesamten Netzwerk. Komplexe Malware kann so schneller aufgespürt, eingegrenzt und beseitigt werden. Cisco AMP bietet damit einen sehr leistungsfähigen Schutz vor bekannten und unbekannten Bedrohungen.

Die abonnementbasierte Lösung steht für zahlreiche Plattformen zur Verfügung. Die Administration erfolgt über eine webbasierte Management-Konsole. ACP und SWS (Cisco Goldpartner) unterstützen ihre Kunden bei der Einführung dieser und weiterer Cisco-Security-Lösungen.

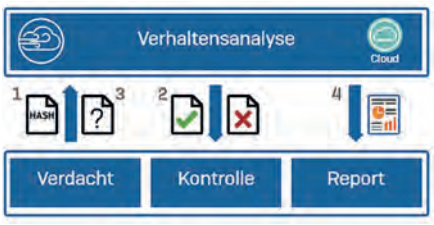
Vorteile der Cisco-AMP-Lösung:

- Abdeckung des gesamten Angriffskontinuums – vor, während und nach einem Angriff
- Flexibilität und Auswahl – bedarfsgerechte Bereitstellung von AMP
- Hervorragende Transparenz und Kontrolle dank detaillierter Informationen und präzise festlegbaren Richtlinien
- Managed-Services – Cisco-Experten und prädiktive Analysen unterstützen das Sicherheitsteam
- Cisco AMP bietet Schutz für ein umfangreiches Spektrum an Angriffsvektoren

SOPHOS SANDSTORM

Next-Generation-Sandboxing für mehr Sicherheit

Sandboxing ist eine Möglichkeit, unbekannte Malware innerhalb von Dateien aufzuspüren. Beim Sandboxing werden zu überprüfende Dateien in einer isolierten Umgebung ausgeführt und überwacht. Dabei gibt es ein stetiges Kopf-an-Kopf-Rennen zwischen Malware- und Sandbox-Entwicklern.



Den derzeit vielversprechendsten Ansatz zur Abwehr dieser Gefahren liefert das cloudbasierte Sandboxing. Und genau hier spielt Sophos Sandstorm seine Stärken aus. In Verbindung mit den klassischen Sophos-Security-Produkten wehrt Sophos Sandstorm sowohl Ransomware als auch Advanced Persistent Threats (APTs) zuverlässig ab. Durch Einsatz leistungsstarker cloudbasierter Next-Generation-Sandbox-Technologie ermöglicht Sophos Sandstorm eine schnelle und zuverlässige Erkennung, Blockierung und Reaktion auf evasive Malware, die andere Lösungen übersehen.

ÜBER ACP

Ihre IT ist unser Business

ACP gehört zu den wachstumsstärksten IT-Providern in Deutschland und ist Nummer 1 in Österreich. Top-Zertifizierungen der wichtigsten Technologieunternehmen zeichnen uns aus. Wir betreuen mit über 1.200 Mitarbeitern an 36 Standorten Unternehmen, Behörden und Organisationen jeder Größe in den Bereichen Hybrid Datacenter, Security, Network, Communications & Collaboration sowie Applications & Workplace. Die ACP Gruppe steht zu 100% im Eigentum der Mitarbeiterinnen und Mitarbeiter. Sie sind auch der Garant für diesen Erfolg.

ACP Partner (ein Auszug)

Cisco, Citrix, DataCore Software, NVIDIA, DELL EMC, nimblestorage, Fortinet, Fujitsu, intel, hp, Kaspersky lab, KEMP Technologies, lenovo, Microsoft, NetApp, Hewlett Packard Enterprise, SOPHOS, TREND MICRO, VEEAM, vmware

TERMINE 3

03. Mai 2017
Köln: CAD-Arbeitsplätze revolutionieren

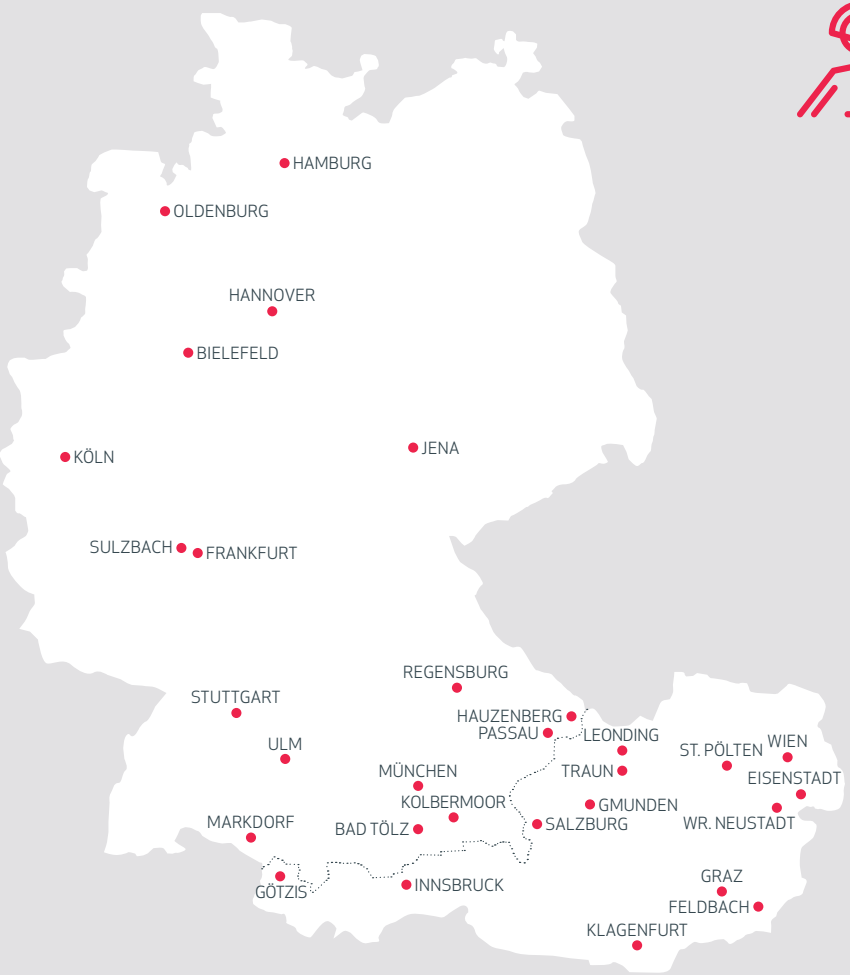
04. Mai 2017
Hamburg: Hybride IT-Betriebsmodelle

11. Mai 2017
Hannover: Hybride IT-Betriebsmodelle

18. Mai 2017
München: Forum 2017

06. Juli 2017
Regensburg: Brainshare 2017

Mehr Informationen unter
➜ www.acp.de/events



IHR ACP-KONTAKT IN DEUTSCHLAND

Bad Tölz
Tel.: 08041-799988-0
E-Mail: bad-toelz@acp.de

Bielefeld
Tel.: 0521-945662-00
E-Mail: bielefeld@acp.de

Frankfurt
Tel.: 06109-69691-0
E-Mail: frankfurt@acp.de

Hamburg
Tel.: 040-822168-600
E-Mail: acp.nord@acp.de

Hannover
Tel.: 0511-35777-0
E-Mail: acp.nord@acp.de

Hauzenberg (SWS Computersysteme AG)
Tel.: 08586-9604-0
E-Mail: info@swsnet.de

Jena (GODYO Gruppe)
Tel.: 03641-287-0
E-Mail: marketing@godyo.com

Kolbermoor
Tel.: 08031-2902-0
E-Mail: kolbermoor@acp.de

Köln
Tel.: 0221-66992-0
E-Mail: koeln@acp.de

Markdorf
Tel.: 07544-50399-0
E-Mail: markdorf@acp.de

München
Tel.: 089-358980-0
E-Mail: muenchen@acp.de

Oldenburg
Tel.: 0441-779221-0
E-Mail: acp.nord@acp.de

Passau
Tel.: 0851-987797-50
E-Mail: kolbermoor@acp.de

Regensburg (SWS Computersysteme AG)
Tel.: 0941-20605-0
E-Mail: info@swsnet.de

Stuttgart
Tel.: 0711-23917-0
E-Mail: stuttgart@acp.de

Sulzbach/Taunus
Tel.: 06196-56142-0
E-Mail: sulzbach@acp.de

Ulm
Tel.: 0731-141151-0
E-Mail: info.ulm@acp.de

HERAUSGEBER
ACP Holding Deutschland GmbH
Stuttgarter Straße 3-5
80807 München
E-Mail: inside_acp@acp.de